Оставьте отзыв о скачивании PDF-файла.

Документация по развертыванию Windows

Сведения о развертывании и обновлении устройств с Windows в организации.

Планирование

КОНЦЕПЦИЯ

Планирование Windows 11

Создание плана развертывания

Планирование активации корпоративных лицензий

Поваренная книга по совместимости Windows

Windows с собственной облачной средой

Подготовка

НАЧАЛО РАБОТЫ

Подготовка к Windows 11

Подготовка к развертыванию обновлений Windows

Подготовка к клиентский компонент Центра обновления Windows клиентским политикам

Оценка и обновление инфраструктуры

Развертывание

РАЗВЕРТЫВАНИЕ

Сравнение решений Windows Autopilot

Развертывание обновлений с помощью Intune

Развертывание обновлений Windows с помощью Configuration Manager

Оптимизация и кэширование содержимого

Использование Windows Autopilot

ОБЗОР

Общие сведения о подготовке устройств Windows Autopilot

Обзор Windows Autopilot

УЧЕБНИК

Сценарии Windows Autopilot

Сценарии подготовки устройств Windows Autopilot

Использование автозаполнения Windows

ОБЗОР

Что такое автоматическое исправление Windows?

Предварительные условия

Руководство по развертыванию

Дополнительные >

Использование политик клиента клиентский компонент Центра обновления Windows

ПРАКТИЧЕСКОЕ РУКОВОДСТВО

Что такое политики клиента клиентский компонент Центра обновления Windows?

Настройка политик клиента клиентский компонент Центра обновления Windows

Обзор отчетов Центра обновления Windows для бизнеса

Использование средств для обновления и создания образов

ССЫЛКА

Настройка загрузочных образов Среды предустановки Windows

Преобразование диска из MBR в GPT

Настройка PXE-сервера для загрузки Windows PE

Устранение ошибок обновления Windows

Дополнительные ресурсы

СКАЧАТЬ

Скачивание и установка Windows ADK

Средства развертывания

НОВОЕ

Блог ит-специалистов для Windows

Рабочие часы Windows

Windows сценарии развертывания

Статья • 27.02.2025 • Применяется к: ✅ Windows 11, ✅ Windows 10

Чтобы успешно развернуть операционную систему Windows в организации, важно понимать различные способы ее развертывания. Ключевые задачи включают выбор из этих сценариев и понимание возможностей и ограничений каждого из них.

Категории развертывания

В следующих таблицах приведены различные сценарии развертывания Windows. Каждый сценарий отнесен к одной из трех категорий.

- Рекомендуется использовать современные методы развертывания, если для конкретной необходимости не требуется использовать другую процедуру. Эти методы поддерживаются существующими средствами, такими как Microsoft Configuration Manager.

  > **Примечание**
  >
  > После развертывания Windows в организации важно поддерживать актуальность, создавая план развертывания обновлений компонентов Windows.

- Методы динамического развертывания позволяют настраивать приложения и параметры для конкретных вариантов использования.

- Традиционные методы развертывания используют существующие средства для развертывания образов операционной системы.

Современный

Развернуть таблицу

Сценарий	Описание	Дополнительные сведения
Windows Autopilot	Настройка готового интерфейса (OOBE) для организации и развертывание новой системы с уже настроенными приложениями и параметрами	Общие сведения о Windows Autopilot

Сценарий	Описание	Дополнительные сведения
Обновление на месте	Используйте программу установки Windows, чтобы обновить версию Windows и перенести приложения и параметры. Данные отката сохраняются в каталог Windows.old.	Выполните обновление на месте до Windows с помощью Configuration Manager

Динамический

Развернуть таблицу

Сценарий	Описание	Дополнительные сведения
Активация подписки	Переключение с Windows Pro на Корпоративную при входе пользователя с подпиской.	Активация подписки Windows
Microsoft Entra ID / MDM	Устройство автоматически присоединяется к Microsoft Entra ID и настраивается MDM.	интеграция Microsoft Entra с MDM
Пакеты подготовки	Использования конструктора образов и конфигураций Windows для создания пакетов подготовки, которые можно применить к устройствам.	Настройка устройств без MDM

Традиционный

Развернуть таблицу

Сценарий	Описание	Дополнительные сведения
Устройство без операционной системы	Развертывание нового устройства или очистка существующего устройства и развертывание свежего образа.	Развертывание Windows с помощью PXE и Configuration Manager
Обновление	Также называется очисткой и загрузкой. Повторное развертывание устройства путем сохранения состояния пользователя, очистки диска и последующего восстановления состояния пользователя.	Обновите клиент Windows с поддерживаемой версией Windows с помощью Configuration Manager

Сценарий	Описание	Дополнительные сведения
Замена	Замена существующего устройства новым путем сохранения состояния пользователя на старом устройстве и его последующего восстановления на новом.	Замените клиент Windows поддерживаемой версией Windows с помощью Configuration Manager

> **ⓘ Важно!**
>
> В сценариях активации Windows Autopilot и подписки требуется, чтобы начальная ОС была поддерживаемой в настоящее время версией Windows.
>
> За исключением сценариев чистой установки, таких как традиционная осная система и Windows Autopilot, все описанные методы могут при необходимости переносить приложения и параметры в новую ОС.

Современные методы развертывания

Современные методы развертывания охватывают как традиционные локальные, так и облачные службы, чтобы обеспечить упрощенное и экономичное развертывание.

Windows Autopilot

Windows Autopilot — это новый набор возможностей, предназначенных для упрощения и модернизации развертывания новых компьютеров с Windows и управления ими. Windows Autopilot позволяет ИТ-специалистам настраивать готовую версию (OOBE) для компьютеров с Windows и предоставлять пользователям полностью настроенное новое устройство с Windows. Вам не придется развертывать образы, добавлять драйверы или управлять инфраструктурой. Пользователи могут независимо пройти процедуру развертывания без помощи ИТ-администратора.

Дополнительные сведения о Windows Autopilot см. в разделах Обзор Windows Autopilot и Модернизация развертывания Windows с помощью Windows Autopilot.

Обновление на месте

Для существующих компьютеров с поддержкой версий Windows рекомендуемым способом для организаций, развертывающих Windows, является обновление на месте. При обновлении на месте используется программа установки Windows (`Setup.exe`) для:

- Автоматически сохраняет все данные, параметры, приложения и драйверы из существующей версии операционной системы.
- Требует наименьших усилий ит-специалистов, так как нет необходимости в сложной инфраструктуре развертывания.

Хотя потребительские компьютеры обновляются с помощью клиентский компонент Центра обновления Windows, организациям требуется больший контроль над процессом. Управление осуществляется с помощью таких средств, как Microsoft Configuration Manager для полной автоматизации процесса обновления с помощью простых последовательностей задач.

Процесс обновления на месте предназначен для обеспечения надежности. При обновлении на месте можно автоматически выполнить откат к предыдущей операционной системе при возникновении каких-либо проблем в процессе развертывания без участия ИТ-специалистов. Откат вручную также можно выполнить с помощью автоматически созданных сведений о восстановлении (хранящихся в папке Windows.old) в случае возникновения каких-либо проблем после завершения обновления. Процесс обновления также обычно выполняется быстрее, чем при традиционных развертываниях, так как приложения не нужно переустанавливать в рамках процесса.

Существующие приложения сохраняются в процессе. В процессе обновления используется стандартный образ установочного носителя Windows (Install.wim). Пользовательские образы не только не требуются, но и не могут использоваться. Пользовательские образы нельзя использовать, так как процесс обновления не может справиться с конфликтами между приложениями в старой и новой операционной системе. Например, timecard Contoso 1.0 в Windows 10 и Contoso Timecard 3.0 в образе Windows 11.

Сценарии, поддерживающие обновление на месте с помощью некоторых других процедур, включают переход с BIOS на режим загрузки UEFI и обновление устройств, использующих программное обеспечение шифрования дисков сторонних разработчиков.

- **Переход с традиционной загрузки BIOS на UEFI**. Для обновления на месте системы с поддержкой UEFI, которая на данный момент загружается с использованием традиционного BIOS, необходимо выполнить обновление на месте Windows 10 с сохранением режима традиционной загрузки BIOS.

Windows 10 не требуется UEFI, поэтому он подходит для обновления системы с помощью эмуляции BIOS прежних версий. После обновления системный диск можно преобразовать в формат, поддерживающий загрузку UEFI, с помощью средства MBR2GPT . Для спецификации UEFI требуется макет диска GPT. После преобразования диска встроенное ПО устройства также должно быть настроено для загрузки в режиме UEFI. Включение UEFI также функций UEFI, таких как безопасная загрузка.

> **ⓘ Важно!**
>
> Обновление на месте в системе с поддержкой UEFI, которая в настоящее время загружается с использованием устаревших BIOS, возможно только с Windows 10. Версии Windows, более новые, чем Windows 10 поддерживают только системы с поддержкой UEFI и не поддерживают устаревшие BIOS или MBR.

- **Стороннее ПО для шифрования дисков**. Устройства, зашифрованные с помощью BitLocker обновить легко, а вот для средств шифрования дисков от сторонних производителей потребуется выполнить больше работы. Некоторые поставщики программного обеспечения могут предоставлять инструкции по интеграции своего программного обеспечения в процесс обновления на месте. Обратитесь к isv, чтобы узнать, есть ли у него инструкции. В следующих статьях представлены подробные инструкции по подготовке драйверов шифрования к работе во время установки Windows с помощью параметра ReflectDrivers:
  - Обзор автоматизации установки Windows
  - Параметры командной строки программы установки Windows

В некоторых ситуациях невозможно использовать обновление на месте. В таких ситуациях используйте вместо этого традиционные методы развертывания. Примеры таких ситуаций:

- Переход с версии x86 Windows 10 на версию Windows x64. Версии Windows, более новые, чем Windows 10, являются только x64 и не имеют версию x86. Процесс обновления не может перейти с 32-разрядной операционной системы на 64-разрядную из-за возможных осложнений с установленными приложениями и драйверами.

- Загрузка из установок VHD. Процесс обновления не может обновить эти установки. Вместо этого потребуется выполнить новые установки.

- Обновление существующих образов. Может возникнуть соблазн попытаться обновить существующие образы Windows до более новой версии Windows, установив старый образ, обновив его, а затем повторно создав новый образ Windows. Однако этот сценарий не поддерживается. Подготовка обновленной ОС с помощью `Sysprep.exe` перед записью образа не поддерживается и не работает. При `Sysprep.exe` обнаружении обновленной ОС происходит сбой.

- Двухвариантная загрузка и многозагрузочные конфигурации. Процесс обновления предназначен для устройств с одной ОС. При использовании систем с двумя или несколькими операционными системами следует проявлять особую осторожность. Двухзагрузочные и многозагрузочные системы не включают использование виртуальных машин для второй и последующих операционных систем.

Динамическая подготовка

Для новых компьютеров организации исторически заменяли версию Windows, включенную на устройстве, собственным пользовательским образом Windows. Пользовательский образ использовался, так как пользовательский образ часто был быстрее и проще, чем использовать предустановленную версию. Однако повторное создание образа с помощью пользовательского образа — это дополнительные затраты из-за необходимого времени и усилий. Благодаря новым возможностям и средствам динамической подготовки, предоставляемым в Windows, теперь можно избежать использования пользовательских образов.

Цель динамической подготовки — взять новый ПК, включить его и преобразовать в устройство для продуктивной работы с минимальными затратами времени и усилий. Типы доступных преобразований:

Активация подписки Windows

Активация подписки Windows — это динамический метод развертывания, позволяющий изменить выпуск Windows с Pro на Корпоративный. Активация подписки Windows не требует ключей и перезагрузки. Дополнительные сведения об активации подписки см. в разделе Активация подписки Windows.

Microsoft Entra присоединение с помощью автоматического управления мобильными устройствами (MDM)

В этом сценарии участнику организации нужно просто указать свой рабочий или учебный идентификатор пользователя и пароль. Затем устройство может быть автоматически присоединено к Microsoft Entra ID и зарегистрировано в решении для управления мобильными устройствами (MDM) без взаимодействия с пользователем. После регистрации решение MDM может завершить конфигурацию устройства по мере необходимости. Дополнительные сведения см. в разделе Microsoft Entra интеграции с MDM.

Конфигурация пакета подготовки

С помощью Designer образов и конфигурации Windows (ICD) ИТ-администраторы могут создать автономный пакет, содержащий все конфигурации, параметры и приложения, которые необходимо применить к устройству. Затем эти пакеты можно развернуть на новых компьютерах различными способами, как правило, ИТ-специалистами. Дополнительные сведения см. в разделе Пакеты подготовки для Windows.

Эти сценарии можно использовать для включения программ "Принеси свое устройство" (BYOD) или "Выберите свое устройство" (CYOD). С помощью этих программ пользователи организации могут выбрать собственный компьютер. Они не ограничены небольшим списком утвержденных или сертифицированных моделей. Эти программы трудно реализовать с помощью традиционных сценариев развертывания.

Хотя Windows включает различные параметры подготовки и механизмы развертывания, параметры подготовки и механизмы развертывания по-прежнему совершенствуются и расширяются на основе отзывов организаций. Как и в случае со всеми функциями Windows, организации могут отправлять предложения по дополнительным функциям через приложение "Отзывы о Windows" или через свои служба поддержки Майкрософт контакты.

Обычное развертывание

В прошлом организации обычно развертывали Windows с помощью процесса на основе образа, основанного на средствах, предоставляемых в:

- Комплект средств для оценки и развертывания Windows.
- Microsoft Configuration Manager.
- Службы развертывания Windows (WDS).
- Microsoft Deployment Toolkit.

Такие сценарии, как обновление на месте и динамическая подготовка, могут уменьшить потребность в традиционных возможностях развертывания в некоторых организациях. Однако традиционные методы могут по-прежнему применяться при определенных обстоятельствах.

Обычный сценарий развертывания можно разбить на вспомогательные сценарии. Эти под-сценарии подробно описаны в следующих разделах, но в следующем списке содержится краткая сводка:

- **Новый компьютер**. Развертывание нового устройства без операционной системы.
- **Обновление компьютера**: переустановка того же устройства (с миграцией пользовательского состояния и необязательным полным резервным копированием образа Windows (WIM).
- **Замена компьютера**. Замена старого устройства новым устройством (с миграцией пользовательского состояния и необязательной полной резервной копией образа WIM).

Новый компьютер

Также называется развертыванием на чистой новой машине. Этот сценарий возникает при наличии устройства без установленной ОС, которое необходимо развернуть. Этот сценарий также может быть существующим устройством, которое необходимо очистить и повторно развернуть без необходимости сохранения существующих данных. Программа установки запускается с загрузочного носителя, с компакт-диска, USB, ISO-файла или предзагрузочной среды выполнения (PXE). Также можно создать полный автономный носитель, включающий все файлы, необходимые для развертывания клиента, что позволяет выполнить развертывание без подключения к общей папке центрального развертывания. Целью может быть физический компьютер, виртуальная машина или виртуальный жесткий диск (VHD), запущенный на физическом компьютере (загружающийся с VHD).

Процесс развертывания для нового сценария устройства выглядит следующим образом:

1. Запустите программу установки с загрузочного носителя (USB, компакт-диска, ISO-файла или PXE-среды).

2. Полностью очистите жесткий диск и создайте новые тома.

3. Установите образ операционной системы.

4. Установите другие приложения (в качестве части последовательности задач).

После выполнения этих действий компьютер готов к использованию.

Обновление компьютера

Процесс обновления иногда также называется очисткой и загрузкой. Процесс обычно запускается в работающей операционной системе. В ходе выполнения процесса развертывания пользовательские данные и параметры архивируются и позже восстанавливаются. Цель может быть такая же, как в сценарии с новым компьютером.

Процесс развертывания для сценария «очистки и загрузки» выполняется следующим образом:

1. Запустите программу установки в работающей операционной системе.
2. Локально сохраните пользовательскую среду.
3. Полностью очистите жесткий диск (за исключением папки с резервной копией).
4. Установите образ операционной системы.
5. Установить другие приложения.
6. Восстановите пользовательскую среду.

После выполнения этих действий устройство готово к использованию.

Замена компьютера

Замена компьютера сходна со сценарием обновления компьютера. Однако, поскольку мы заменяем устройство, мы разделим этот сценарий на две main задачи: резервное копирование старого клиента и развертывание нового клиента без операционной системы. Как и в случае со сценарием обновления, пользовательские данные и параметры архивируются и восстанавливаются.

Процесс развертывания для сценария замены компьютера выполняется следующим образом:

1. Сохраните пользовательскую среду (данные и параметры) на сервере, запустив задание резервного копирования в работающей операционной системе.
2. Выполните чистое развертывание на новый компьютер.

> **Примечание**
>
> В некоторых ситуациях сценарий замены можно использовать, даже если целевой объект является тем же устройством. Например, заменить можно, если необходимо изменить макет диска с master загрузочной записи (MBR) на таблицу разделов GUID (GPT). Это преобразование позволяет воспользоваться функциональностью UEFI.

Связанные статьи

- Обновление до Windows с помощью Microsoft Configuration Manager.
- Развертывание Windows с помощью PXE и Configuration Manager.
- Технический справочник по настройке Windows.
- Designer образов и конфигурации Windows.
- Встроенное ПО UEFI.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Краткое руководство по Windows как услуге

Применяется к: ✅ Windows 11, ✅ Windows 10

Вот краткое руководство по наиболее важным понятиям в Windows как услуга.

Определения

В рамках Windows как услуги появились некоторые новые термины, поэтому вам следует знать их значение.

- **Обновления компонентов** выпускаются ежегодно. Как следует из названия, эти обновления добавляют новые компоненты и выходят поэтапно, в отличие от прежней практики Windows, когда обновления выходили каждые 3–5 лет.
- **Исправления** обеспечивают исправления безопасности и исправления, не связанные с безопасностью. Они обычно выпускаются во второй вторник каждого месяца, хотя они могут быть выпущены в любое время. В исправления включаются обновления системы безопасности, критически важные обновления, обновления служебного стека и обновления драйверов. Исправления имеют характер накопительных обновлений, поэтому достаточно установить последнее исправление, чтобы получить все доступные исправления для определенного обновления компонентов Windows 10. "Стек обслуживания" — это код, который устанавливает другие обновления, поэтому они важны для поддержания актуальности. Дополнительные сведения см. в статье Обновления служебного стека.
- Сборки **предварительных версий для участников программы предварительной оценки** выпускаются во время разработки компонентов, которые выйдут в составе следующего обновления компонентов. Они позволяют организациям проверять новые компоненты и подтверждать их совместимость с существующими приложениями и инфраструктурой, сообщая Майкрософт о любых возникших проблемах.
- **Каналы обслуживания** позволяют организациям выбирать время развертывания новых компонентов.
  - **Канал общей доступности** ежегодно получает обновления компонентов.
  - **Long Term Servicing Channel**, который предназначен только для специализированных устройств (на которых обычно не устанавливается Office), например устройств для управления медицинским оборудованием или банкоматами, получает новые выпуски обновлений компонентов примерно раз в два-три года.

- **Круги развертывания** — это группы устройств, сначала используемые для пилотного, а затем и для широкого развертывания каждого обновления компонентов в организации.

Дополнительные сведения см. в разделе Обзор модели "Windows как услуга".

Интересные подробные сведения о работе накопительных обновлений содержатся в статье Обновления Windows на основе прямых и обратных различий.

Основные понятия

Каждый выпуск на Канале общей доступности мы сопровождаем рекомендацией сразу приступить к развертыванию на устройствах, отобранных для раннего внедрения (целевой проверки), и по своему усмотрению перейти к полному развертыванию.

Версии Windows Enterprise LTSC — это отдельные версии **канала долгосрочного обслуживания** . Каждый выпуск поддерживается в общей сложности 10 лет (пять лет стандартной поддержки и пять лет расширенной). Ожидается, что новые выпуски будут выходить каждые три года.

Дополнительную информацию см. в разделе Назначение устройств каналам обслуживания для обновления клиентов Windows.

Поддержание в актуальном состоянии

Для поддержания систем в актуальном состоянии следует выполнять развертывание обновлений компонентов в предусмотренные для этого сроки. Вы можете использовать различные средства управления и обновления, такие как клиентский компонент Центра обновления Windows, политики клиентский компонент Центра обновления Windows клиентов, Windows Server Update Services, Microsoft Configuration Manager и продукты сторонних продуктов, которые помогут в этом процессе.

Расширенное расширенное тестирование не требуется. Потребуется протестировать только критически важные для бизнеса приложения, тогда как остальные приложения проверяются в ряде кругов пилотного развертывания. После проверки большинства приложений в этих пилотных развертываниях можно начать широкое развертывание.

Этот процесс повторяется с каждым новым обновлением компонентов. Это небольшие проекты развертывания по сравнению с крупными проектами, которые были необходимы при старых циклах выпуска Windows от трех до пяти лет.

Другие технологии, такие как BranchCache и оптимизация доставки, оба средства одноранговой распространения, могут помочь с распространением файлов установки обновлений компонентов.

Last updated on 01.04.2025

Обзор модели "Windows как услуга"

Применяется к: ✅ Windows 11, ✅ Windows 10

> **Ищете информацию для потребителей?** См. раздел клиентский компонент Центра обновления Windows: вопросы и ответы.

Windows как услуга — это способ упростить жизнь ИТ-специалистов и обеспечить согласованное взаимодействие с Windows для своих клиентов. Эти улучшения связаны с активным включением пользователей в разработку Windows, упрощением развертывания и обслуживания клиентских компьютеров Windows и равномерным планированием ресурсов, необходимых для развертывания и обслуживания Windows в долгосрочной перспективе.

Создание

До выхода Windows 10 корпорация Майкрософт выпускала новые версии Windows раз в несколько лет. Традиционный график развертывания оказывал серьезную нагрузку на пользователей, которые были вынуждены регулярно изучать новые функции и компоненты, а различия между версиями были достаточно серьезными. Это расписание также означало длительный период ожидания без новых функций. Этот сценарий не всегда работает в современном быстро меняющемся мире, в котором для решения проблем необходимы новые возможности безопасности, управления и развертывания.

В прошлом, когда корпорация Майкрософт разрабатывала новые версии Windows, она, как правило, выпускала технические предварительные версии, когда разработка была почти завершена и Windows была готова к выпуску. Теперь новые функции предоставляются в программу предварительной оценки Windows как можно скорее во время цикла разработки с помощью процесса, называемого *тестированием*. Организации могут видеть, что именно разрабатывает Корпорация Майкрософт, и начать тестирование как можно скорее.

Корпорация Майкрософт также ориентируется на получаемые от организаций в процессе разработки отзывы, поскольку они позволяют ей быстро вносить коррективы, а не дожидаться времени после выпуска. Дополнительные сведения о Программе предварительной оценки Windows и регистрация доступны в разделе Программа предварительной оценки Windows.

Корпорация Майкрософт также проводит обширное внутреннее тестирование: команды инженеров ежедневно устанавливают новые сборки, а более крупные группы

сотрудников часто устанавливают сборки, все это до того, как эти сборки будут выпущены в программу предварительной оценки Windows.

Развертывание

Развертывание современной версии Windows проще, чем в предыдущих версиях Windows. При переходе с более ранних версий Windows вы можете воспользоваться удобной процедурой обновления "на месте", позволяющей автоматически сохранить все приложения, параметры и данные. После этого развертывание обновлений компонентов выполняется так же просто.

Совместимость приложений

Тестирование совместимости приложений традиционно являлось одной из самых сложных задач при развертывании или обновлении Windows. По сравнению с более ранними версиями Windows значительно улучшились совместимость приложений с точки зрения классических приложений, веб-сайтов и приложений универсальной платформы Windows (UWP). Для наиболее важных критически важных бизнес-приложений организации по-прежнему должны регулярно выполнять тестирование для проверки совместимости с новыми сборками.

Обслуживание

Традиционное обслуживание Windows включало несколько типов выпусков: основные версии (например, операционные системы Windows 8.1, Windows 8 и Windows 7), пакеты обновления и ежемесячные обновления. В Windows 10 и Windows 11 существует два типа выпусков:

- **Обновления качества**: Обновления, которые обеспечивают исправления безопасности и надежности, а также могут периодически добавлять новые функции или функции.
- **Обновления компонентов**: Обновления, которые выпускаются раз в год, на которых основана временная шкала обслуживания для операционной системы. Эти обновления могут содержать новые функции и функции, а также ранее выпущенные обновления качества.

Ветви обслуживания — это первый способ разделить пользователей по группам развертывания для обновлений компонентов и исправлений. Дополнительные сведения о разработке стратегии развертывания, которая использует каналы обслуживания, см. в статье Планирование стратегии обслуживания для обновлений клиента Windows.

Сведения о каждом средстве обслуживания см. в разделе Средства обслуживания.

Предусмотрено три канала обслуживания, каждый из которых позволяет с разной степенью гибкости выбирать время доставки обновлений на клиентские компьютеры. Дополнительные сведения см. в статье Каналы обслуживания.

В настоящее время существует три канала выпуска для клиентов с Windows:

- **Канал общедоступной доступности** получает обновления компонентов, как только они будут доступны.
- **Канал долгосрочного обслуживания** (LTSC) предназначен для использования только для специализированных устройств, таких как те, которые управляют медицинским оборудованием или банкоматами. LTSC получает новые выпуски функций каждые два-три года.
- **Программа предварительной оценки Windows** предоставляет организациям возможность протестировать функции, которые будут поставляться в следующих обновлениях, и предоставлять отзывы о ней.

С каждым выпуском общей доступности вы обычно начинаете развертывание сразу на устройствах, выбранных для раннего внедрения (целевая проверка), а затем наращиваете развертывание до полного развертывания по своему усмотрению. Это позволяет получить доступ к новым функциям, возможностям и интегрированной безопасности как можно скорее.

> ⓘ **Внимание**
>
> Для устройств в Канале общей доступности диагностическим данным должно быть присвоено значение **1 (основные)** или выше, чтобы обеспечить работу службы с должным качеством. Инструкции по настройке уровня диагностических данных см. в разделе Настройка диагностических данных Windows в организации.

Обновления компонентов

Вы можете развернуть обновления компонентов с помощью существующих средств управления. Эти изменения происходят в небольших размерах, а не все сразу, как в предыдущих версиях Windows, что сокращает время готовности пользователей.

Исправления

Ежемесячные обновления в предыдущих версиях Windows часто были слишком объемными, потому что число доступных каждый месяц обновлений было огромным.

Многие организации выборочно выбирали, какие обновления они хотели установить, а какие нет, и это создало бесчисленные сценарии, в которых организации развертывали важные обновления безопасности, но выбрали только подмножество исправлений, не относящихся к безопасности.

Вместо того чтобы получать несколько обновлений каждый месяц и пытаться выяснить, что нужно организации, что в конечном итоге приводит к фрагментации платформы, администраторы видят одно накопительное ежемесячное обновление, заменяющее обновление за предыдущий месяц, содержащее полезные данные безопасности и небезопасности. Этот подход упрощает обновление и гарантирует некое единообразие устройств с системами, которые тестирует Майкрософт. В результате вероятность возникновения неожиданных проблем из-за обновлений снижается.

Каналы обслуживания

Существует три канала обслуживания. Программа предварительной оценки Windows предоставляет организациям возможность протестировать и предоставить отзывы о компонентах, которые войдут в состав следующего обновления компонентов. Канал общей доступности предоставляет новые возможности посредством выпуска обновлений компонентов. Организации могут выбирать время развертывания обновлений посредством Канала общей доступности. Long-Term Servicing Channel, который предназначен только для специализированных устройств (на которых обычно не устанавливается Office), например компьютеров для управления медицинским оборудованием или банкоматами, получает новые выпуски обновлений компонентов примерно раз в два-три года. Дополнительные сведения о версиях в каждом канале обслуживания см. в разделе Сведения о выпуске Windows.

Каналы обслуживания — это не единственный способ разделения групп устройств при использовании обновлений. Каждый канал может содержать подмножества устройств, что еще больше осложняет обслуживание. Сведения о стратегии обслуживания и процессе непрерывного развертывания для Windows 10, включая роль каналов обслуживания, см. в разделе Планирование стратегии обслуживания для обновлений клиентов с Windows.

Канал общей доступности

В Канале общей доступности обновления компонентов доступны ежегодно. Эта модель обслуживания идеально подходит для пилотных развертываний и тестирования обновлений компонентов, а также для пользователей (например, разработчиков), которым нужен доступ к новейшим компонентам. После того как последний выпуск

пройдет пилотное развертывание и тестирование, вы сможете выбрать время, в течение которого он перейдет в широкое развертывание.

Когда корпорация Майкрософт официально выпускает обновление компонентов, оно становится доступным для любого устройства, не настроенного на отсрочку обновлений компонентов, и может быть установлено на нем. Однако организации, использующие Windows Server Update Services (WSUS), Microsoft Configuration Manager или клиентский компонент Центра обновления Windows клиентские политики, могут отложить обновления компонентов на выборочные устройства, удерживая их. их утверждение и развертывание. В этом сценарии содержимое канала общедоступной доступности доступно, но не обязательно сразу, в зависимости от политики системы управления. Организации могут выборно откладывать обновления компонентов на любое количество этапов с помощью средств обслуживания. Дополнительные сведения о средствах обслуживания см. в разделе Средства обслуживания.

Long-term Servicing Channel

Специализированные системы, например устройства, управляющие медицинским оборудованием, POS-системы и банкоматы, часто требуют более длительного цикла обслуживания в силу своего назначения. Эти устройства обычно выполняют одну важную задачу и не нуждаются в обновлении компонентов так часто, как другие устройства в организации. Важнее, чтобы эти устройства были как стабильными и безопасными, чем при изменении пользовательского интерфейса. Модель обслуживания LTSC блокирует получение устройствами с выпуском "Корпоративная LTSC" стандартных обновлений компонентов и отправляет на них только исправления, чтобы поддерживать систему безопасности в актуальном состоянии. Исправления по-прежнему сразу доступны клиентам Windows 10 Корпоративная LTSC, однако клиенты могут отложить их с помощью одного из средств обслуживания, упомянутых в разделе "Средства обслуживания".

Канал долгосрочного обслуживания не предназначен для развертывания на большинстве или всех устройствах в организации. Он должен использоваться только для устройств специального назначения. В качестве общего руководства устройство с установленным Microsoft Office является устройством общего назначения, которое обычно используется информационным работником, поэтому оно лучше подходит для канала общей доступности.

Корпорация Майкрософт никогда не публикует обновления компонентов через Центр обновления Windows на устройствах под управлением Windows 10 Корпоративная LTSC. Вместо этого он обычно предлагает новые выпуски LTSC каждые 2–3 года, и организации могут установить их в качестве обновлений на месте или даже пропустить выпуски в течение жизненного цикла продукта. Всегда проверяйте ваш выпуск LTSC, чтобы

определить его жизненный цикл обслуживания. Дополнительные сведения см. в сведениях о выпуске. Также можно выполнить поиск на странице сведений о жизненном цикле продуктов.

> ⓘ **Примечание.**
>
> Выпуски LTSC будут поддерживать актуальные на момент выпуска LTSC процессоры и наборы микросхем. По мере выпуска дальнейших поколений ЦП поддержка будет добавляться в последующих выпусках LTSC, которые клиенты смогут развертывать для этих систем. Дополнительные сведения см. в разделе **Поддержка новейших процессоров и наборов микросхем в Windows** в статье **Вопросы и ответы о политике поддержки жизненного цикла — продукты Windows**.

Канал долгосрочного обслуживания доступен только в выпусках Windows Enterprise LTSC. Этот выпуск Windows не включает некоторые приложения, такие как Microsoft Edge, Microsoft Store, Microsoft Mail, Календарь, OneNote, Погода, Новости, Спорт, Деньги, Фотографии, Камера, Музыка и Часы. Эти приложения не поддерживаются в выпусках Enterprise LTSC, даже если вы устанавливаете с помощью загрузки неопубликованных приложений.

Программа предварительной оценки Windows

Для многих ИТ-специалистов раннее получение сведений об обновлениях компонентов может быть интригующим и полезным для будущих взаимодействий с конечными пользователями, а также предоставить средства для тестирования на наличие проблем в следующем выпуске общей доступности. Участники программы предварительной оценки Windows могут использовать и развертывать предварительную версию кода на своих тестовых компьютерах и первыми получать представление о том, какой будет новая сборка. Тестирование ранних сборок помогает Майкрософт и ее клиентам, так как они имеют возможность обнаружить потенциальные проблемы до того, как выпуск станет общедоступным, и сообщить о них Майкрософт.

Майкрософт рекомендует всем организациям иметь хотя бы несколько устройств, зарегистрированных в Программе предварительной оценки Windows, и предоставлять отзывы о любых возникающих проблемах. Сведения об этой программе см. в статье Программа предварительной оценки Windows для бизнеса.

Средства обслуживания

Существует множество средств, с помощью которых вы можете обслуживать модель "Windows как услуга". Каждый вариант имеет свои преимущества и недостатки с точки зрения возможностей, контроля, простоты и низких административных требований. Ниже приведены примеры средств обслуживания, доступных для управления обновлениями Windows.

- **Центр обновления Windows (автономный)** предоставляет ограниченное управление обновлениями компонентов, в то время как ИТ-специалисты вручную настраивают устройство для Канала общей доступности. Организации могут контролировать, для каких устройств откладываются обновления, посредством установки флажка **Отложить обновления** в меню **Пуск\Параметры\Обновления и безопасность\Дополнительные параметры** на клиентском устройстве с Windows.
- **клиентский компонент Центра обновления Windows клиентские политики** включают контроль над отсрочкой обновления и обеспечивают централизованное управление с помощью групповая политика или MDM. клиентский компонент Центра обновления Windows политики клиента можно использовать для отсрочки обновлений до 365 дней в зависимости от версии. Эти варианты развертывания доступны клиентам в Канале общей доступности. Помимо возможности использовать групповая политика для управления клиентский компонент Центра обновления Windows клиентскими политиками, любой из этих вариантов можно настроить без необходимости использовать локальную инфраструктуру с помощью Microsoft Intune.
- **Windows Server Update Services (WSUS)** обеспечивают расширенное управление обновлениями и доступны в операционной системе Windows Server на уровне кода. Помимо возможности откладывать обновления организации могут также добавить уровень утверждения обновлений и развертывать их на конкретных компьютерах или в группах компьютеров по мере готовности.
- **Microsoft Configuration Manager** обеспечивает максимальный контроль над обслуживанием Windows как услуга. ИТ-специалисты могут откладывать обновления, утверждать их и использовать различные возможности для целевых развертываний и контроля над использованием пропускной способности и временем развертывания.

Сравнение средств обслуживания

Развернуть таблицу

Средство обслуживания	Возможность отложить обновления?	Возможность утверждать обновления	Поддержка одноранговых элементов	Дополнительные возможности
Центр обновления Windows	Да (вручную)	Нет	Оптимизация доставки	Нет
политики клиента клиентский компонент Центра обновления Windows	Да	Нет	Оптимизация доставки	Другие объекты групповой политики
WSUS	Да	Да	BranchCache или оптимизации доставки	Масштабируемость серверов в любом направлении
Configuration Manager	Да	Да	BranchCache, кэш одноранговой клиента или оптимизация доставки. Для последнего см. раздел Одноранговая рассылка контента и Оптимизация доставки обновлений Windows	Точки распространения, несколько вариантов развертывания

Last updated on 17.06.2025

Цикл выпуска обновлений для клиентов Windows

Применяется к: ✅ Windows 11, ✅ Windows 10

Обновления Windows помогают оставаться продуктивными и защищенными. Они предоставляют пользователям и ИТ-администраторам необходимые исправления безопасности, а также защищают устройства, чтобы не удалось использовать уязвимости без исправления. Обновления для клиентской ОС Windows обычно являются накопительными. Они включают все ранее выпущенные исправления для защиты от фрагментации операционной системы. Проблемы с надежностью и уязвимостью могут возникать при установке только подмножества исправлений.

В этой статье содержатся сведения о типах обновлений, которые предоставляет корпорация Майкрософт, а также о том, как они помогают упростить и согласованное взаимодействие с пользователем.

> **Совет**
>
> Если вы хотите узнать, что происходит с Windows, проверка **стратегию развития Windows**. Дорожная карта представляет собой общий обзор функций и функций, запланированных для будущих выпусков Windows.

Типы выпусков обновлений

Развернуть таблицу

Тип выпуска	Описание	Цикл выпуска
Ежемесячный выпуск обновления для системы безопасности	Накопительный выпуск обновления, включающий как содержимое для безопасности, так и содержимое, не относящееся к безопасности	Второй вторник каждого месяца, обычно публикуется в 10:00 по тихоокеанскому времени (PST/PDT)
Необязательный предварительный выпуск без безопасности	Необязательный накопительный выпуск обновления, который обычно используется для ранней проверки ежемесячного выпуска обновления для системы безопасности.	Четвертый вторник каждого месяца, как правило, публикуется в 10:00 по тихоокеанскому времени (PST/PDT)

Тип выпуска	Описание	Цикл выпуска
Выпуск вне диапазона (OOB)	Устранена недавно обнаруженная проблема или уязвимость.	По мере необходимости
Ежегодное обновление компонентов	Обновление с новыми функциями и улучшениями, которые также изменяют версию Windows	Один раз в год во второй половине календарного года
Непрерывные инновации для Windows 11	В этой статье представлены новые функции и улучшения для Windows 11	Периодически включается в необязательный предварительный выпуск, отличный от безопасности, а затем в ежемесячных выпусках обновлений для системы безопасности

Ежемесячный выпуск обновления для системы безопасности

Большинство пользователей знакомы с **ежемесячным выпуском обновлений для системы безопасности**. **Ежемесячный выпуск обновления для системы безопасности** публикуется во второй вторник каждого месяца, как правило, в 10:00 по тихоокеанскому времени (PST/PDT). Этот выпуск обычно называется:

- Вторник исправлений
- Обновление вторника
- B-недельные выпуски (то есть вторая неделя месяца)
- Исправления
- Обновления системы безопасности
- Последнее накопительное обновление (LCU)

Ежемесячные выпуски обновлений для системы безопасности являются накопительными. Этот выпуск включает как новые, так и ранее выпущенные исправления безопасности, а также содержимое, отличное от безопасности, представленное в **предварительной версии Optional nonsecurity за** предыдущий месяц. Эти обновления помогают обеспечить безопасность и соответствие устройств Windows путем развертывания исправлений стабильности и устранения уязвимостей системы безопасности. Большинство организаций считают ежемесячные выпуски обновлений для системы безопасности обязательными.

Ежемесячные выпуски обновлений для системы безопасности доступны по следующим каналам:

- Центр обновления Windows

- Службы Windows Server Update Services (WSUS)
- Каталог Центра обновления Майкрософт

Многие средства управления обновлениями, такие как Microsoft Configuration Manager и Microsoft Intune, используют эти каналы для развертывания обновлений.

Начиная с Windows 11 версии 24H2 корпорация Майкрософт может периодически выпускать накопительные обновления в качестве контрольных точек. Последующие обновления будут состоять из следующих:

- Файлы пакета обновления, связанные с контрольными точками, и
- Новые файлы пакетов обновления, содержащие добавочные двоичные различия по отношению к версии двоичных файлов в последней контрольной точке.

В течение жизненного цикла конкретного выпуска Windows может быть отправлено несколько контрольных точек. Устройства, обновляемые с клиентский компонент Центра обновления Windows и WSUS, могут без проблем устанавливать последнее ежемесячное обновление для системы безопасности независимо от наличия каких-либо предыдущих накопительных обновлений контрольных точек. В **процессе обновления не требуется никаких изменений**. Пользователи каталога могут просматривать накопительные обновления контрольных точек и использование каталога Центра обновления Майкрософт для справки.

Необязательный предварительный выпуск без безопасности

Необязательные предварительные версии, не связанные с безопасностью , предоставляют ИТ-администраторам возможность ранней проверки этого содержимого до **ежемесячного выпуска обновлений для системы безопасности**. Администраторы могут тестировать и проверять выпуски в рабочей среде перед запланированным ежемесячным выпуском обновлений для системы безопасности на следующий месяц. Эти обновления являются необязательными накопительными, предварительными версиями, не относящихся к безопасности. Новые функции могут быть изначально развернуты в **предварительной** версии предварительной версии за предыдущий месяц, а затем поставляются в следующем **ежемесячном выпуске обновления для системы безопасности**. **Необязательные предварительные выпуски, не связанные с безопасностью** , обычно выпускаются в четвертый вторник месяца в 10:00 по тихоокеанскому времени (PST/PDT). Эти выпуски доступны только для самых последних поддерживаемых версий Windows.

Необязательные предварительные выпуски, не связанные с безопасностью , обычно называются следующими:

- Выпуски недели D (означает четвертую неделю месяца)
- Предварительный просмотр обновлений
- Предварительная версия CU
- Предварительная версия LCU

Чтобы получить доступ к необязательным предварительным версиям, не связанные с безопасностью, выполните следующие действия.

- Перейдите в **раздел Параметры**>**Обновление & Безопасность**>**клиентский компонент Центра обновления Windows** а затем выберите **Проверить наличие обновлений**.
- Использование программы предварительной оценки Windows для бизнеса
- Используйте каталог Центра обновления Майкрософт .

Начиная с Windows 11 версии 24H2 корпорация Майкрософт может периодически выпускать накопительные обновления в качестве контрольных точек. Последующие обновления будут состоять из следующих:

- Файлы пакета обновления, связанные с контрольными точками, и
- Новые файлы пакетов обновления, содержащие добавочные двоичные различия по отношению к версии двоичных файлов в последней контрольной точке.

В течение жизненного цикла конкретного выпуска Windows может быть отправлено несколько контрольных точек. Устройства, обновляемые с клиентский компонент Центра обновления Windows и WSUS, могут без проблем устанавливать последнее ежемесячное обновление для системы безопасности независимо от наличия каких-либо предыдущих накопительных обновлений контрольных точек. В **процессе обновления не требуется никаких изменений**. Пользователи каталога могут просматривать накопительные обновления контрольных точек и использование каталога Центра обновления Майкрософт для справки.

Выпуски OOB

Для устранения недавно обнаруженной проблемы или уязвимости можно предоставить **выпуски OOB**. Они используются в нетипичных случаях, когда обнаружена проблема и не может дождаться следующего ежемесячного выпуска, так как устройства должны быть немедленно обновлены для устранения уязвимостей системы безопасности или устранения проблем с качеством, влияющих на многие устройства. **Внеплановые выпуски (OOB)** предоставляются за пределами ежемесячного расписания при исключительной необходимости.

Ниже приведены некоторые ключевые рекомендации по выпуску OOB.

- Выпуски OOB всегда являются накопительными.
  - Выпуски OOB заменяют все предыдущие ежемесячные обновления для системы безопасности и необязательный предварительный выпуск, отличный от безопасности.
- Выпуски OOB обычно требуют, чтобы ИТ-администраторы развертывали вне цикла.
- Некоторые выпуски OOB классифицируются как критически важные.
  - Критически важные выпуски OOB автоматически доступны для WSUS и клиентский компонент Центра обновления Windows клиентских политик, как и ежемесячные выпуски обновлений для системы безопасности.
- Некоторые выпуски OOB классифицируются как некритические.
  - Некритические выпуски отправляются только в каталог Центра обновления Майкрософт, чтобы пользователи или организации добровольно получили обновление.

Начиная с Windows 11 версии 24H2 корпорация Майкрософт может периодически выпускать накопительные обновления в качестве контрольных точек. Последующие обновления будут состоять из следующих:

- Файлы пакета обновления, связанные с контрольными точками, и
- Новые файлы пакетов обновления, содержащие добавочные двоичные различия по отношению к версии двоичных файлов в последней контрольной точке.

В течение жизненного цикла конкретного выпуска Windows может быть отправлено несколько контрольных точек. Устройства, обновляемые с клиентский компонент Центра обновления Windows и WSUS, могут без проблем устанавливать последнее ежемесячное обновление для системы безопасности независимо от наличия каких-либо предыдущих накопительных обновлений контрольных точек. В **процессе обновления не требуется никаких изменений**. Пользователи каталога могут просматривать накопительные обновления контрольных точек и использование каталога Центра обновления Майкрософт для справки.

Непрерывные инновации для Windows 11

Начиная с Windows 11 версии 22H2, периодически вводятся новые функции и улучшения для непрерывного внедрения инноваций для Windows 11. Эти функции и улучшения используют обычные каналы обслуживания обновлений, с которыми вы уже знакомы. Сначала новые функции появляются с **дополнительным предварительным выпуском, не защищенным безопасностью** , и постепенно развертываются на неуправляемых клиентах. Эти новые функции будут выпущены позже в рамках **ежемесячного выпуска обновлений для системы безопасности**.

Некоторые из новых функций могут нарушить работу организаций. По умолчанию эти компоненты временно отключены для всех управляемых устройств до установки следующего ежегодного обновления компонентов. В этом сценарии устройство считается управляемым, если оно использует одно из следующих компонентов для определения устанавливаемых обновлений:

- политики клиента клиентский компонент Центра обновления Windows
  - Устройства с обновлениями, управляемыми Microsoft Intune используют политики клиента клиентский компонент Центра обновления Windows
- WSUS
  - Устройства с обновлениями, управляемыми Configuration Manager, используют СЛУЖБЫ WSUS

Функции, отключенные по умолчанию, перечислены в статье базы знаний ежемесячного накопительного пакета обновления. Если вы хотите включить эти функции, существует политика клиента, которая позволяет администраторам включать функции, стоящие за временным корпоративным управлением. Дополнительные сведения об этой политике см. в разделе Включение функций, стоящих за временным корпоративным управлением функциями.

Ежегодные обновления компонентов

Ежегодные обновления компонентов выпускаются во второй половине календарного года. Эти обновления обычно являются накопительными и включают все ранее выпущенные исправления. Они также включают новые функции и улучшения. Ежегодное обновление компонентов знаменует собой начало жизненного цикла поддержки:

- 24 месяца поддержки выпусков Windows Для дома и Pro
- Поддержка выпусков Enterprise и Education за 36 месяцев

Дополнительные сведения см. в статье Вопросы и ответы о жизненном цикле Windows.

Сведения о выпуске

Дополнительные сведения о конкретных выпусках см. в следующих разделах:

- Windows 11, журнал обновлений версии 22H2
- Windows 11, журнал обновлений версии 21H2
- Журнал обновлений Windows 10
- Состояние выпуска Windows
- Что нового в Windows

Last updated on 27.03.2025

Обновления клиента Windows, каналы и средства

Статья • 18.03.2023

Область применения

- Windows 10
- Windows 11

Принцип работы обновлений Windows

Процесс обновления Windows имеет четыре этапа:

- **Сканирования:** Устройство проверяет сервер Центра обновления Майкрософт, службу клиентский компонент Центра обновления Windows или конечную точку Windows Server Update Services (WSUS) через случайные интервалы, чтобы узнать, были ли добавлены какие-либо обновления с момента последнего поиска обновлений, а затем оценивает, является ли обновление подходящим, проверяя политики, которые были настроены администратором. Этот процесс невидим для пользователя.
- **Скачать:** Когда устройство определит, что обновление доступно, оно начинает скачивание обновления. Процесс скачивания также невидим для пользователя. При обновлении компонентов скачивание происходит в несколько последовательных этапов.
- **Установить:** После загрузки обновления в зависимости от параметров клиентский компонент Центра обновления Windows устройства обновление устанавливается в системе.
- **Фиксация и перезапуск:** После установки устройство обычно (но не всегда) необходимо перезапустить, чтобы завершить установку и начать использовать обновление. Прежде чем это произойдет, устройство по-прежнему работает под управлением предыдущей версии программного обеспечения.

Типы обновлений

Мы включаем здесь сведения о различных типах обновлений, о которых вы услышите, но два основных типа, которые вы имеете самый непосредственный контроль, — это *обновления компонентов* и *обновления качества*.

- **Обновления компонентов:** Выпускается ежегодно. Обновления компонентов добавляют новые функции и функции в Windows 10. Так как они поставляются часто (а не каждые 3–5 лет), ими проще управлять.
- **Обновления качества:** Исправления предоставляют исправления безопасности и исправления, не относящиеся к системе безопасности. В исправления включаются обновления системы безопасности, критически важные обновления, обновления служебного стека и обновления драйверов. Как правило, они выпускаются во второй вторник каждого месяца, но могут выпускаться и в любое другое время. Выпуски второго вторника посвящены обновлениям для системы безопасности. Обновления качества *являются накопительными*, поэтому установки последнего обновления качества достаточно, чтобы получить все доступные исправления для конкретного обновления компонентов, включая любые исправления безопасности вне диапазона и все *обновления стека обслуживания* , которые могли быть выпущены ранее.
- **Обновления стека обслуживания:** Стек обслуживания — это компонент кода, который фактически устанавливает обновления Windows. Время от времени необходимо обновлять сам стек обслуживания, чтобы обеспечить бесперебойную работу. Если не установить последнее обновление стека обслуживания, существует риск того, что ваше устройство не сможет обновиться с помощью последних исправлений системы безопасности Майкрософт. Обновления стека обслуживания не обязательно включаются в *каждое* ежемесячное обновление качества, и иногда выпускаются вне диапазона для решения проблемы с задержкой. Всегда устанавливайте последнее доступное обновление качества, чтобы перехватывать все обновления стека обслуживания, которые могли быть выпущены. Стек обслуживания также содержит "стек обслуживания на основе компонентов" (CBS), который является ключевым базовым компонентом для нескольких элементов развертывания Windows, таких как DISM, SFC, изменение функций или ролей Windows и восстановление компонентов. CBS — это небольшой компонент, который обычно не имеет обновлений, выпущенных каждый месяц. Список обновлений стека обслуживания см. в разделе Последние обновления стека обслуживания. Дополнительные сведения об обслуживании обновлений стека см. в разделе Обновления стека обслуживания.
- **Обновления драйверов**. Эти драйверы обновлений применимы к вашим устройствам. Обновления драйверов отключены по умолчанию в Windows Server Update Services (WSUS), но для облачных методов обновления можно управлять установкой или нет.

- **Обновления продуктов Майкрософт:** Они обновляют другие продукты Майкрософт, например Office. Вы можете включить или отключить обновления Майкрософт с помощью политик, управляемых различными средствами обслуживания.

Каналы обслуживания

Существует три канала обслуживания, каждый из которых обеспечивает разный уровень гибкости с тем, как и когда обновления доставляются на устройства. Использование различных каналов обслуживания позволяет развертывать Windows "как услугу", которая предполагает развертывание как непрерывный процесс обновления, который развертывается по всей организации волнами. При таком подходе обновление подключается к этому процессу, и во время его выполнения вы отслеживаете аномалии, ошибки или влияние на пользователей и реагируете по мере возникновения проблем, не прерывая весь процесс.

Первым шагом управления тем, когда и как устройства устанавливают обновления, является назначение их соответствующему каналу обслуживания. Вы можете назначить устройства определенному каналу с помощью любого из нескольких средств, включая Microsoft Configuration Manager, Windows Server Update Services (WSUS) и групповая политика параметры, применяемые любым из нескольких способов. Разделив устройства на разные группы ("группы развертывания" или "круги"), можно использовать назначение канала обслуживания, а затем другие функции управления, такие как политики отсрочки обновлений, для создания поэтапного развертывания любого обновления, которое позволяет начать с ограниченного пилотного развертывания для тестирования перед переходом к широкому развертыванию в организации.

Канал общей доступности

В канале общедоступной доступности обновления компонентов выпускаются ежегодно. До тех пор, пока устройство не настроено на отсрочку обновлений компонентов, любое устройство в этом канале установит обновление компонентов сразу после выпуска. Если вы используете клиентский компонент Центра обновления Windows для бизнеса, канал предоставляет три месяца дополнительного общего времени развертывания, прежде чем потребуется выполнить обновление до следующего выпуска.

Программа предварительной оценки Windows для бизнеса

Предварительные выпуски предварительной оценки становятся доступными во время разработки функций, которые будут отправлены в следующем обновлении компонентов, что позволяет организациям проверять новые функции и совместимость с существующими приложениями и инфраструктурой, предоставляя корпорации Майкрософт отзывы о любых возникших проблемах. В канале Программы предварительной оценки Windows для бизнеса есть три варианта:

- Разработка для программы предварительной оценки Windows
- Бета-версия программы предварительной оценки Windows
- Программа Windows Insider Release Preview

Для действий по проверке рекомендуется использовать канал предварительной версии предварительной оценки Windows.

Long-term Servicing Channel

Канал долгосрочного обслуживания предназначен для использования только для специализированных устройств (которые обычно не работают под управлением Office), таких как устройства, управляющие медицинским оборудованием или банкоматами. Устройства в этом канале получают новые выпуски функций каждые два-три года. LTSC выпускает специальный выпуск LTSC Windows 10 и доступен только в Центре корпоративного лицензирования Майкрософт.

Канал общедоступной доступности — это канал обслуживания по умолчанию для всех устройств Windows, за исключением устройств с установленным выпуском LTSC. В следующей таблице показаны каналы обслуживания, доступные для каждого выпуска.

Выпуск	**Канал общей доступности**	**Программа предварительной оценки**	**Long-Term Servicing Channel**
Домашняя	✓	✗	✗
Pro	✓	✓	✗
Корпоративная	✓	✓	✗
Корпоративная LTSC	✗	✗	✓
Pro для образовательных учреждений	✓	✓	✗

Выпуск	Канал общей доступности	Программа предварительной оценки	Long-Term Servicing Channel
Education	✔	✔	✘

Средства обслуживания

Средства для локальной доставки обновлений

Windows Server Update Services (WSUS): вы настраиваете сервер WSUS, который массово загружает обновления из корпорации Майкрософт. Затем отдельные устройства подключаются к серверу для установки обновлений оттуда.

Вы можете настроить сервер и процесс обновления, управлять им и управлять им с помощью нескольких средств:

- Автономный сервер Windows Server Update Services работает напрямую
- Configuration Manager
- Средства сторонних корпораций

Дополнительные сведения см. в разделе Windows Server Update Services (WSUS).

Средства для облачной доставки обновлений

Ваши отдельные устройства подключаются к конечным точкам Майкрософт напрямую для получения обновлений. Сведения об этом процессе (как часто устройства загружают обновления различных типов, из каких каналов, отложений и сведения об опыте установки пользователей) задаются на устройствах с помощью политик групповая политика или MDM, которыми можно управлять с помощью любого из нескольких средств:

- консоль управления групповая политика (Gpmc.msc)
- Microsoft Intune
- Инструменты MDM сторонних корпораций

Гибридные сценарии

Кроме того, можно объединить локальное распределение обновлений на основе WSUS с облачной доставкой обновлений.

Определение устройств, управляемых обновлениями Windows

Статья • 26.06.2024 • Применяется к: ✅ Windows 11, ✅ Windows 10

Как ИТ-администратор, понимание различий между управляемыми и неуправляемым устройствами имеет решающее значение для эффективного управления обновлениями Windows. Эта статья содержит ясность в терминологии и методах управления обновлениями Windows для обоих типов устройств.

Что такое управляемые обновлениями устройства Windows?

Управляемые обновлениями устройства — это устройства, на которых ИТ-администратор или организация управляют обновлениями Windows с помощью средства управления, например Microsoft Intune, или путем прямого задания политик. Политики можно задать напрямую с помощью объектов групповой политики (GPO), политик поставщика служб конфигурации (CSP) или Microsoft Graph.

> ⓘ **Примечание**
>
> Это определение верно, даже если вы устанавливаете разделы реестра напрямую. Однако мы не рекомендуем выполнять это действие, так как разделы реестра можно легко перезаписать.

Управляемые устройства могут включать настольные компьютеры, ноутбуки, планшеты, серверы и производственное оборудование. Эти устройства защищены и настроены в соответствии со стандартами и политиками вашей организации.

Управляемое ИТ-решение: предложение центра обновления Windows

Устройства считаются управляемыми обновлениями Windows, если вы управляете предложением обновлений следующими способами:

- Политики настраиваются для управления обновлениями, предлагаемыми для конкретного устройства.

- Вы устанавливаете, когда ваша организация должна получать обновления функций, качества и драйверов, среди прочего.
- Для настройки этих предложений используются объекты групповой политики,поставщик служб конфигурации (CSP) или Microsoft Graph .

Управляемое ИТ-решение: возможности обновления Windows

Устройства считаются управляемыми обновлениями Windows, если вы используете политики (GPO, CSP или Microsoft Graph) для управления поведением устройств при установке обновлений Windows.

Примеры управляемого поведения устройства включают часы активности, льготные периоды и крайние сроки обновления, уведомления об обновлениях, планирование обновлений и многое другое. Полный список см. в разделе CSP политики обновления.

Примеры устройств Windows, управляемых обновлениями

Ниже приведено несколько примеров устройств, управляемых обновлениями:

- **Устройства, принадлежащие компании:** Устройства, подготовленные ИТ-отделом с корпоративными учетными данными, конфигурациями и политиками.
- **Устройства, принадлежащие сотрудникам в программах BYOD:** Личные устройства, зарегистрированные в системе управления устройствами компании для безопасного доступа к корпоративным ресурсам.
- **Устройства, подготовленные с помощью Windows Autopilot:** Устройства, которые настроены и предварительно настроены, чтобы быть готовыми к бизнесу, прямо из коробки.
- **Обязательные параметры безопасности:** Устройства с требованиями к работоспособности, такими как шифрование устройств, ПИН-код или надежный пароль, определенные периоды времени ожидания бездействия и актуальные операционные системы.
- **Устройства, зарегистрированные в Intune:** Устройства, зарегистрированные в Microsoft Intune для доступа к сети и принудительных политик безопасности.
- **Сторонние управляемые устройства:** Устройства, зарегистрированные в средствах управления сторонних поставщиков с настроенными политиками

обновления Windows через объект групповой политики, CSP или раздел реестра.

Что такое неуправляемые устройства Windows с обновлением?

В отличие от устройств, управляемых обновлениями, неуправляемые устройства не управляются с помощью политик, средств управления или программного обеспечения. Эти устройства не регистрируются в таких средствах, как Microsoft Intune или Configuration Manager. Если вы настраиваете страницу Параметры только для управления общим поведением устройства при принятии обновлений, это считается неуправляемым устройством.

> ⓘ **Примечание**
>
> Термин "устройства, управляемые Корпорацией Майкрософт", используется для обозначения того, что мы теперь называем "обновление неуправляемых устройств Windows". На основе отзывов мы обновили нашу терминологию для ясности.

Примеры неуправляемых устройств Windows с обновлением

Примеры неуправляемых устройств с обновлением:

- **Личные устройства:** Устройства, принадлежащие отдельным лицам в вашей организации, которые не зарегистрированы ни в одной корпоративной системе управления.
- **Устройства BYOD, не зарегистрированные в программах управления:** Устройства, используемые для работы, но не в составе организации, используют собственную программу для устройств (BYOD).
- **Периферийные устройства:** Такие устройства, как принтеры, IP-телефоны и источники бесперебойного питания (UPS), которые не могут принимать централизованно управляемые административные учетные данные.

Дополнительные сведения об управляемых и неуправляемых устройствах см. в статье Защита управляемых и неуправляемых устройств.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Подготовка стратегии обслуживания для обновлений клиента Windows

Статья • 18.03.2023

Область применения

- Windows 10
- Windows 11

> **Ищете информацию для потребителей?** См. раздел Центр обновления Windows: вопросы и ответы

Вот пример того, как может выглядеть этот процесс:

- **Настройка тестовых устройств.** Настройте тестовые устройства в программе предварительной оценки Windows, чтобы участники программы предварительной оценки могли тестировать обновления компонентов, прежде чем они будут доступны в канале общедоступной доступности. Как правило, это будет несколько тестовых устройств, которые ИТ-сотрудники используют для оценки предварительных сборок Windows. Корпорация Майкрософт предоставляет текущие сборки от разработчиков участникам программы предварительной оценки Windows примерно раз в неделю, чтобы заинтересованные пользователи могли ознакомиться с добавляемой функциональностью. Дополнительные сведения о регистрации в программе предварительной оценки Windows для бизнеса см. в разделе Программа предварительной оценки Windows.
- **Определение исключенных устройств.** В некоторых организациях устройствам специального назначения, например устройствам, которые управляют заводским или медицинским оборудованием или работают с банкоматами, требуется более строгий и менее частый цикл обновления компонентов, чем может предложить канал общей доступности. Для этих устройств установите выпуск Enterprise LTSC, чтобы избежать обновлений компонентов на срок до 10 лет. Определите эти устройства и отделите их от циклов поэтапного развертывания и обслуживания, чтобы устранить путаницу для администраторов и обеспечить правильную обработку устройств.
- **Набор добровольцев.** Цель тестирования развертывания — получение отзывов. Одним из эффективных способов набора пилотных пользователей является привлечение добровольцев. При этом необходимо четко обозначить, что вас интересуют отзывы, а не люди, которые просто «хотят попробовать», и что с освоением обновлений компонентов иногда могут

возникать проблемы. Ожидается, что при использовании Windows как услуги проблем будет немного, однако в случае их возникновения необходимо, чтобы тестировщики сообщали вам о них как можно скорее. Выбирая участников для пилотных групп, обязательно включайте тех, кто работает с самым широким набором приложений и устройств, чтобы проверить как можно больше приложений и устройств.

- **Обновление групповая политика.** Каждое обновление компонентов включает новые групповые политики для управления новыми функциями. Если вы используете групповая политика для управления устройствами, групповая политика Администратор для домена Active Directory потребуется скачать ADMX-пакет и скопировать его в центральное хранилище (или в каталог PolicyDefinitions в папке SYSVOL контроллера домена, если не используется центральное хранилище). Вы можете управлять новыми групповыми политиками из последней версии Windows с помощью средств удаленного администрирования сервера. Пакет загрузки ADMX создается в конце каждого цикла разработки, а затем публикуется для скачивания. Чтобы найти пакет загрузки ADMX для конкретной сборки Windows, найдите "ADMX download for Windows build xxxx". Дополнительные сведения об управлении групповая политика см. в статье Создание центрального хранилища для групповая политика административных шаблонов в Windows и управление им.
- **Выбор средства обслуживания.** Решите, какой продукт вы будете использовать для управления обновлениями Windows в своей среде. Если вы в настоящее время используете Windows Server Update Services (WSUS) или Microsoft Configuration Manager для управления обновлениями Windows, вы можете продолжать использовать эти продукты для управления обновлениями Windows 10 или Windows 11. Кроме того, можно использовать Центр обновления Windows для бизнеса. В дополнение к тому, какой вы будете использовать продукт, подумайте, как вы будете доставлять обновления. Для ускорения распространения обновлений доступно несколько одноранговых параметров. Сравнение этих средств см. в разделе Средства обслуживания.
- **Ранжирование приложений по приоритету.** Сначала создайте портфель приложений. Этот список должен включать в себя все приложения, установленные в вашей организации, и все размещенные в ней веб-страницы. Затем определите приоритет в этом списке, чтобы определить приложения, которые являются наиболее важными для бизнеса. Так как ожидается, что совместимость приложений с новыми версиями Windows будет высокой, перед пилотным этапом необходимо протестировать только самые критически важные для бизнеса приложения. все остальное можно

протестировать после этого. Подробнее о выявлении проблем совместимости с приложениями см. в статье Manage Windows upgrades with Upgrade Analytics (Управление обновлениями Windows с помощью Upgrade Analytics).

Каждый раз, когда корпорация Майкрософт выпускает обновление компонентов, ИТ-отдел должен использовать следующий высокоуровневый процесс, чтобы обеспечить успешное широкое развертывание:

1. **Проверка совместимости критических бизнес-приложений.** Протестируйте наиболее важные бизнес-приложения на совместимость с новым обновлением функций Windows 10, запущенным на компьютерах предварительной оценки Windows, описанных в предыдущем шаге "Настройка тестовых устройств" предыдущего раздела. Список приложений, охватываемых этой проверкой, должен быть небольшим, потому что большинство приложений можно протестировать на стадии пилотного развертывания.
2. **Проведение пилотного развертывания и реагирование на отзывы.** Корпорация Майкрософт ожидает, что совместимость приложений и устройств будет высокой, но по-прежнему важно иметь целевые группы в ИТ-отделе и бизнес-подразделениях для проверки совместимости приложений для остальных приложений в портфеле приложений. Так как только самые критически важные для бизнеса приложения тестируются заранее, это действие будет представлять большую часть тестирования совместимости приложений в вашей среде. Это не обязательно формальный процесс, а проверка пользователя с помощью определенного приложения. Таким образом, следующим шагом является развертывание обновления компонентов для ит-пользователей с ранним внедрением и целевых групп, работающих в канале общедоступной доступности, который вы определили на шаге "Набор добровольцев" предыдущего раздела. Не забудьте четко объяснить, что вы хотели бы как можно скорее получить отзывы, а также как именно пользователи могут передать вами эти отзывы. Если возникла проблема, используйте план ее устранения.
3. **Широкомасштабное развертывание.** Наконец, сосредоточьтесь на крупномасштабном развертывании с помощью кругов развертывания. Постройте круги развертывания, нацеленные на группы компьютеров в выбранном вами продукте для управления обновлениями. Чтобы максимально снизить риск, стройте круги развертывания так, чтобы каждый отдел был разбит на несколько кругов. Таким образом, если вы столкнетесь с проблемой, это не приведет к прерыванию каких-либо критических бизнес-процессов. С помощью этого метода каждый круг развертывания снижает риск, так как в любом конкретном отделе обновляется больше людей.

Планирование Windows 11

Применяется к: ✅ Windows 11

В этой статье содержатся рекомендации по планированию Windows 11 в организации.

Планирование развертывания

Так как Windows 11 построена на той же основе, что и Windows 10, можно использовать те же возможности развертывания, сценарии и средства. Вы также можете использовать ту же базовую стратегию развертывания, которая используется сегодня для Windows 10. Проверьте и обновите стратегию обслуживания, чтобы скорректировать изменения в обслуживании и поддержке Windows 11.

На высоком уровне эта стратегия должна включать следующие действия:

- Создание плана развертывания
- Определение условий готовности
- Оценка инфраструктуры и средств
- Тестирование приложений
- Определение стратегии обслуживания

Если вы ищете способы оптимизации подхода к развертыванию Windows 11 или развертывание новой версии Windows не является привычным процессом, рассмотрите факторы, приведенные в следующих разделах.

Определение приемлемости

Сначала определите, какие из ваших текущих устройств соответствуют требованиям к оборудованию Windows 11. Чтобы обеспечить совместимость, убедитесь, что ваше устройство соответствует требованиям Windows 11 или превышает его.

Корпорация Майкрософт имеет средства анализа, которые помогут вам оценить устройства в соответствии с требованиями к оборудованию Windows 11. Если вы используете выпуски Windows 10 Домашняя, Pro или Pro для рабочих станций, вы можете использовать приложение "Проверка работоспособности компьютера", чтобы определить, Windows 11 право на соответствие требованиям. Пользователи выпусков Windows 10 Корпоративная и для образовательных учреждений, должны обратиться к своим ИТ-администраторам: администраторы скажут пользователям, имеют ли они право на обновление.

Корпоративные организации, желающие оценить готовность устройств в своих средах, могут ожидать, что эта возможность будет интегрирована в существующие средства Майкрософт, такие как аналитика конечных точек.

Доступность Windows 11

Доступность Windows 11 зависит от оборудования устройства и от того, получает ли устройство обновления непосредственно от корпорации Майкрософт или от решения управления, поддерживаемого ИТ-администратором.

Дополнительные сведения см. в разделе Определение устройств, управляемых обновлениями Windows.

Управляемые устройства

Управляемые устройства — это устройства, которые находятся под контролем организации. К управляемым устройствам относятся устройства, управляемые Microsoft Intune, Microsoft Configuration Manager или другими решениями по управлению конечными точками.

Если вы управляете устройствами от имени своей организации, вы можете обновить соответствующие устройства до Windows 11 с помощью существующих средств развертывания и управления.

Организации, использующие клиентский компонент Центра обновления Windows клиентские политики, также имеют следующие преимущества:

- Убедитесь, что автоматическое обновление до Windows 11 не предлагается для устройств, не соответствующих минимальным требованиям к оборудованию.
- Дополнительные сведения о мерах защиты. Хотя функции удержания защиты для Windows 11 устройств так же, как и для Windows 10 сегодня, администраторы, использующие клиентский компонент Центра обновления Windows клиентские политики, имеют доступ к информации о том, какие средства защиты не позволяют отдельным устройствам выполнять обновление до Windows 11.

> ⓘ **Примечание.**
>
> Кроме того, Windows 11 имеет новые условия лицензионного соглашения на использование программного обеспечения корпорации Майкрософт. При развертывании с клиентский компонент Центра обновления Windows клиентскими

политиками или Windows Server Update Services вы принимаете эти новые условия лицензии от имени пользователей в вашей организации.

Неуправляемые устройства

Неуправляемые устройства — это устройства, которыми ИТ-администратор не управляет от имени организации. При развертывании ОС на эти устройства не распространяются политики организации, которые управляют обновлениями или обновлениями.

Windows 11 в 2021 году было предложено Windows 10 устройств. Обмен сообщениями на новых устройствах зависит от производителя компьютера.

Обновление Windows 11 доступно на подходящих неуправляемых устройствах для пользователей, которые вручную ищут обновление через клиентский компонент Центра обновления Windows. Как и для всех устройств, управляемых клиентский компонент Центра обновления Windows, страница параметров **клиентский компонент Центра обновления Windows** подтверждает, когда устройство подходит.

Как и Windows 10, при развертываниях обновлений используется интеллектуальный процесс развертывания на основе машинного обучения. Машинное обучение использует сочетание тестирования, тесного взаимодействия с партнерами, обратной связи, диагностических данных и реальных аналитических данных для управления качеством. Этот процесс улучшает процесс обновления и гарантирует, что устройства, впервые назначенные для обновления, будут иметь удобный интерфейс. Устройства, у которых могут возникнуть проблемы с совместимостью с обновлением, могут решить эти проблемы до того, как будет предложено обновление.

Рекомендации по готовности к Windows 11

Рекомендуемый метод определения готовности инфраструктуры, процессов развертывания и инструментов управления для Windows 11 — присоединиться к программе предварительной оценки Windows для бизнеса. Как участник канала предварительной версии выпуска вы можете проверить, работают ли ваши устройства и приложения должным образом, и изучить новые возможности.

При планировании стратегии управления конечной точкой для Windows 11 рассмотрите переход к облачному управлению мобильными устройствами (MDM), например Microsoft Intune. Если полностью облачный подход пока не подходит для вашей организации, все равно можно модернизировать и упорядочить основные компоненты стратегии управления конечными точками:

- Чтобы управлять клиентами Configuration Manager через Интернет, создайте шлюз управления облачными клиентами (CMG).
- Подключите существующее свойство Configuration Management к облаку с подключением клиента, чтобы управлять всеми устройствами из центра администрирования Microsoft Intune.
- Используйте совместное управление для одновременного управления устройствами с помощью диспетчера конфигураций и Microsoft Intune. Это параллельное управление позволяет использовать преимущества облачных возможностей, таких как условный доступ.

Дополнительные сведения о преимуществах этих подходов см. в разделе Cloud Attach Your Future: The Big 3.

Внедрение Windows 11 также является хорошим моментом для проверки планов обновления оборудования и определения приоритетов подходящих устройств, чтобы обеспечить оптимальные возможности пользователей.

Обслуживание и поддержка

Наряду с усовершенствованием взаимодействия с пользователем и безопасностью, в Windows 11 внесены усовершенствования в подход к обслуживанию Майкрософт, основанный на ваших предложениях и отзывах.

- **Обновления качества**: Windows 11 и Windows 10 устройства получают регулярные ежемесячные обновления качества для обеспечения обновлений системы безопасности и исправлений ошибок.

- **Обновления компонентов**. Корпорация Майкрософт ежегодно предоставляет одно обновление компонентов Windows 11, предназначенное для выпуска во второй половине каждого календарного года.

- **Жизненный цикл:**
  - Выпуски Home, Pro, Pro для рабочих станций и Pro для образовательных учреждений Windows 11 получать поддержку в течение 24 месяцев с даты общей доступности.
  - Выпуски Windows 11 для предприятий и образовательных учреждений поддерживаются в течение 36 месяцев с даты общедоступной доступности.

Доступен объединенный журнал обновлений Windows 11. Аналогичным образом центр работоспособности выпусков Windows предоставляет быстрый доступ к объявлениям об обслуживании Windows 11, известным проблемам и удержанию средств защиты.

Важно, чтобы у организаций было достаточно времени, чтобы спланировать внедрение Windows 11. Корпорация Майкрософт также признает, что многие организации имеют сочетание Windows 11 и Windows 10 устройств в своей экосистеме. Устройства в служебных версиях Windows 10 по-прежнему получают ежемесячные Windows 10 обновления для системы безопасности, а также добавочные улучшения Windows 10 для поддержки текущих развертываний Microsoft 365. Дополнительные сведения см. на странице сведений о выпуске Windows 10.

> **Совет**
>
> Если вы хотите узнать, что происходит с Windows, проверка **стратегию развития Windows**. Дорожная карта представляет собой общий обзор функций и функций, запланированных для будущих выпусков Windows.

Совместимость приложений

Обещание Майкрософт в области совместимости для Windows 10 поддерживается для Windows 11. Данные из программы App Assure показывают, что уровень совместимости Windows 10 для корпоративных организаций, включая бизнес-приложения, превышает 99,7 %. Корпорация Майкрософт по-прежнему привержена обеспечению того, чтобы приложения, на которые вы рассчитываете, продолжали работать должным образом при обновлении. На Windows 11 распространяются те же требования к проверке совместимости приложений, которые существуют сегодня для Windows 10, как для обновлений функций, так и для исправлений.

Дополнительные сведения см. в разделе Поваренная книга по совместимости Windows.

Assure для приложений

Если у вас возникли проблемы с совместимостью или вы хотите убедиться, что приложения вашей организации совместимы с первого дня, app Assure может помочь. При регистрации в службе App Assure все проблемы совместимости приложений, обнаруженные с Windows 11, можно устранить. Корпорация Майкрософт помогает устранять проблемы с приложениями бесплатно. С 2018 года App Assure оценил почти 800 000 приложений, а подписки бесплатны для соответствующих клиентов с более чем 150 устройствами.

Дальнейшие действия

Подготовка к Windows 11

Планирование развертывания обновлений для Windows 10 и приложений Microsoft 365

Last updated on 27.03.2025

Создание плана развертывания

Статья • 18.03.2023

Область применения

- Windows 10
- Windows 11

Мышление "управление службами" означает, что устройства в вашей организации попадают в континуум, при этом процесс обновления программного обеспечения постоянно планируется, развертывается, отслеживается и оптимизируется. И как только вы используете этот процесс для обновления компонентов, обновление качества становится упрощенной процедурой, которая является простой и быстро выполняемой, что в конечном итоге увеличивает скорость.

При переходе к модели управления службами требуются эффективные способы развертывания обновлений для репрезентативных групп устройств. Мы обнаружили, что кольцевое развертывание хорошо подходит для корпорации Майкрософт и многих других организаций по всему миру. Круги развертывания в клиенте Windows похожи на группы развертывания, созданные большинством организаций для предыдущих основных обновлений редакций. Это просто способ разделения устройств на временная шкала развертывания.

На самом высоком уровне каждое "кольцо" состоит из группы пользователей или устройств, которые получают определенное обновление одновременно. Для каждого круга ИТ-администраторы устанавливают критерии для контроля времени отсрочки или внедрения (завершения), которые должны быть выполнены до развертывания на следующем более широком круге устройств или пользователей.

Общая кольцевая структура использует три группы развертывания:

- Предварительная версия: планирование и разработка
- Ограничено: пилотный проект и проверка
- Широкое: широкое развертывание

> ⓘ **Примечание**
>
> Организации часто используют разные имена для своих "колец", например:
>
> - First > Fast > Broad
> - Canaries > Early Adopters > Users
> - Предварительная версия > "Широкий > критический"

Сколько колец должно быть?

Не существует определенных правил для точного количества кругов для развертываний. Как упоминалось ранее, вы можете обеспечить нулевое время простоя критически важных устройств, поместив их в собственное кольцо. Если у вас крупная организация, может потребоваться назначить устройства кольцам в зависимости от географического расположения. Или назначьте на основе размера кругов, чтобы ресурсы службы технической поддержки были более доступными. Рассмотрите потребности вашего бизнеса и введите круги, которые будут иметь смысл для вашей организации.

Переход между кольцами

В основном существует две стратегии перемещения развертываний с одного круга на другой. Один из них основан на службе, другой — на основе проекта.

- "Красная кнопка" (на основе службы): предполагает, что содержимое хорошо, пока не доказано плохое. Содержимое будет передаваться до тех пор, пока не будет обнаружена проблема, после чего ИТ-администратор нажимает "красную кнопку", чтобы остановить дальнейшее распространение.
- Зеленая кнопка (на основе проекта): предполагает, что содержимое является плохим, пока не будет проверено. После прохождения всех проверок ИТ-администратор нажимает "зеленую кнопку", чтобы отправить содержимое в следующий круг.

Когда дело доходит до развертываний, выполнение ручных действий в процессе обычно препятствует скорости обновления. Стратегия "красная кнопка" лучше, когда это ваша цель.

Кольцо предварительного просмотра

Круг предварительного просмотра предназначен для оценки новых возможностей обновления. Это *не* для широких частей организации, но ограничивается людьми, которые отвечают за то, что будет дальше, как правило, ИТ-администраторов. В конечном счете, на этом этапе выполняется проектирование и планирование, чтобы при отправке общедоступного обновления вы могли иметь большую уверенность в обновлении.

ⓘ Примечание

Участие в **программе предварительной оценки Windows** предоставляет ранний доступ к выпускам Windows, что позволяет использовать сборки Insider Preview в круге предварительной версии для проверки приложений и инфраструктуры, подготавливая вас к общедоступным выпускам Windows.

Кто входит в круг предварительного просмотра?

Пользователи круга предварительной версии являются наиболее технически подкованных и устойчивых людей, которые не потеряют производительность, если что-то пойдет не так. Как правило, эти пользователи являются ИТ-специалистами и, возможно, несколькими людьми в организации.

На этапах планирования и подготовки следует сосредоточиться на следующих действиях:

- Работа со сборками Windows Insider Preview.
- Определите функции и функции, которые может или хочет использовать ваша организация.
- Определите, кто будет использовать эти функции и как они будут полезны.
- Поймите, почему вы откладываете обновление.
- Планируйте обратную связь об использовании.

Помните, что вы работаете с предварительным выпуском программного обеспечения в кольце предварительной версии и будете оценивать функции и тестировать обновление для целевого выпуска.

ⓘ Важно!

Если вы используете выпуски предварительной оценки Windows (предварительная версия) для круга предварительной версии и используете WSUS или клиентский компонент Центра обновления Windows для бизнеса, обязательно задайте следующие политики, чтобы разрешить предварительные сборки:

- **Управление предварительными сборками: 2. Включение предварительных сборок** • В разделе **Уровень готовности ветви** выберите **При получении предварительных сборок и Обновления компонентов: 4- Программа предварительной оценки Windows медленно**

Ограниченное кольцо

Цель ограниченного круга — проверить обновление на репрезентативных устройствах в сети. В течение этого периода создаются данные и отзывы, позволяющие принять решение о переходе к более широкому развертыванию. Аналитика компьютеров может помочь с определением хорошего ограниченного круга репрезентативных устройств и мониторингом развертывания.

Кто идет в ограниченном ринге?

Наиболее важной частью этого этапа является поиск репрезентативной выборки устройств и приложений в сети. По возможности должно быть представлено все оборудование и все приложения. Важно, чтобы люди, выбранные для этого круга, регулярно использовали свои устройства для создания данных, необходимых для принятия решения о более широком развертывании в вашей организации. ИТ-отдел, лабораторные устройства и пользователи с самым передовым оборудованием обычно не имеют приложений или драйверов устройств, которые действительно являются репрезентативной выборкой вашей сети.

На этапах пилотного проекта и проверки следует сосредоточиться на следующих действиях:

- Развертывание новых инноваций.
- Оцените и действовать, если возникли проблемы.
- Перемещение вперед, если не заблокировано.

При развертывании в ограниченном круге вы сможете собирать данные и реагировать на инциденты, происходящие в среде, быстро устраняя любые проблемы, которые могут возникнуть. Убедитесь, что вы отслеживаете достаточное внедрение в этом кольце. Круг с ограниченными возможностями представляет вашу организацию по всем направлениям. Когда вы достигнете достаточного уровня внедрения, вы можете быть уверены, что более широкое развертывание будет работать более гладко.

Широкое развертывание

После того как устройства в ограниченном кольце имеют достаточный период стабилизации, пришло время для широкого развертывания по сети.

Кто входит в круг широкого развертывания?

В большинстве предприятий широкий круг включает в себя остальную часть вашей организации. Из-за работы в предыдущем кольце по проверке стабильности и минимизации сбоев (с диагностическими данными для поддержки вашего решения) широкое развертывание может произойти относительно быстро.

> ⓘ **Примечание**
>
> В некоторых случаях вы можете сдерживаете критически важные устройства (например, медицинские устройства), пока развертывание в широком кольце не завершится. Ознакомьтесь с рекомендациями и рекомендациями по развертыванию обновлений клиентских компонентов Windows на критически важных устройствах.

На широком этапе развертывания следует сосредоточиться на следующих действиях:

- Развертывание на всех устройствах в организации.
- Проработайте все последние необычные проблемы, которые не были обнаружены в круге с ограниченным кругом.

Определение условий готовности

Статья • 18.03.2023

Область применения

- Windows 10
- Windows 11

Определение ролей и персонала

Планирование развертывания и управление ими включает в себя множество различных действий и ролей, наиболее подходящих для каждого из них. По мере планирования стоит выяснить, какие роли вам потребуются для развертывания и кто должен их заполнить. Различные роли активны на разных этапах развертывания. В зависимости от размера и сложности организации некоторые из ролей может заполнить один и тот же человек. Однако лучше всего иметь установленного *менеджера процессов*, который будет контролировать все задачи для развертывания.

Диспетчер процессов

Руководитель процесса руководит процессом развертывания обновлений и имеет право на то, чтобы отправить процесс вперед или остановить его, если это необходимо. Они также отвечают за организацию этих мероприятий:

Рабочий поток совместимости	**Развертывание**	**Возможности и модернизация**
Назначение приоритета приложения	Просмотр требований к инфраструктуре	Определение изменений инфраструктуры
Оценка приложений	Проверка инфраструктуры в соответствии с требованиями	Определение изменений конфигурации
Оценка устройства	Создание плана обновления инфраструктуры	Создание предложения возможностей

Задача руководителя процессов заключается в сборе отчетов об усилиях по исправлению, эскалации сбоев и принятии решения о готовности вашей среды к пилотном развертыванию, а затем широкому развертыванию.

В этой таблице описывается одно представление других ролей с их обязанностями, соответствующими навыками и этапами развертывания, где они необходимы:

Роль	**Обязанности**	**Навыки**	**Активные фазы**
Диспетчер процессов	Управляет процессом до конца; обеспечивает запись входных и выходных данных; обеспечивает выполнение действий	Управление ИТ-службами	Планирование, подготовка, пилотное развертывание, широкое развертывание
Владелец приложения	Определение плана тестирования приложений; назначение тестировщиков приемки пользователей; сертифицировать приложение	Знание критически важных и важных приложений	Планирование, подготовка, пилотное развертывание
Разработчик приложений	Убедитесь, что приложения разработаны для обеспечения совместимости с текущими версиями Windows	Разработка приложений; исправление приложения	Планирование, подготовка
Вычисления конечных пользователей	Как правило, группа, включающая инженеров инфраструктуры или инженеров развертывания, которые обеспечивают совместимость средств обновления с Windows.	Развертывание без операционной системы; управление инфраструктурой; доставка приложений; управление обновлениями	Планирование, подготовка, пилотное развертывание, широкое развертывание
Операции	Убедитесь, что поддержка доступна для текущей версии Windows. Обеспечение поддержки после развертывания, включая взаимодействие с пользователями и откат.	Безопасность платформы	Подготовка, пилотное развертывание, широкое развертывание
Security	Проверка и утверждение базовых показателей безопасности и средств	Безопасность платформы	Подготовка, пилотное развертывание

Роль	Обязанности	Навыки	Активные фазы
Заинтересованных сторон	Представляет группы, затронутые обновлениями, например руководители финансов, службы конечных пользователей или управление изменениями	Ключевые решения для подразделения или отдела	Планирование, пилотное развертывание, широкое развертывание

Установка критериев для приложений для оценки

Некоторые приложения в вашей среде имеют основополагающее значение для основных бизнес-действий. Другие приложения помогают сотрудникам выполнять свои роли, но не являются критически важными для бизнес-операций. Прежде чем приступить к инвентаризации и оценке приложений в вашей среде, следует установить некоторые критерии для классификации приложений, а затем определить приоритет для каждого из них. Этот процесс поможет вам понять, как лучше всего развертывать обновления и как устранять любые проблемы, которые могут возникнуть.

На этапе подготовки вы будете применять критерии, которые вы определили сейчас, к каждому приложению в организации.

Ниже приведена предлагаемая схема классификации.

Категория	Определение
Критический	Наиболее важные приложения, которые обрабатывают основные бизнес-действия и процессы. Если эти приложения были недоступны, бизнес или подразделение вообще не могли работать.
Важно!	Приложения, необходимые отдельным сотрудникам для поддержания их производительности. Простой в этом случае повлияет на отдельных пользователей, но будет иметь лишь минимальное влияние на бизнес.
Не важно	Это не влияет на бизнес, если эти приложения недоступны в течение некоторого времени.

После классификации приложений необходимо определить, что каждая классификация означает для организации с точки зрения приоритета и серьезности. Это действие поможет убедиться, что вы сможете рассмотреть

проблемы с правильным уровнем срочности. Каждому приложению следует назначить приоритет на основе времени.

Ниже приведен пример системы оценки приоритета. специфика может отличаться для вашей организации:

Priority	Определение
1	Все выявленные проблемы или риски должны быть расследованы и устранены как можно скорее.
2	Начните исследовать риски и проблемы в течение двух рабочих дней и исправьте их *в течение* текущего цикла развертывания.
3	Начните изучение рисков и проблем в течение 10 рабочих дней. Вам не нужно исправлять их все в рамках текущего цикла развертывания. Однако все проблемы должны быть устранены к концу следующего цикла развертывания.
4	Начните изучение рисков и проблем в течение 20 рабочих дней. Их можно исправить в текущем или любом будущем цикле разработки.

Связана с приоритетом, но отличается концепция серьезности. Вы также должны определить рейтинг серьезности на основе того, как вы считаете, что проблема с приложением должна повлиять на цикл развертывания.

Вот пример.

Серьезность	Эффект
1	Остановка работы или потеря дохода
2	Снижение производительности для бизнес-подразделения
3	Снижение производительности для отдельных пользователей
4	Минимальное влияние на пользователей

Пример: крупная финансовая корпорация

Используя предлагаемую схему, финансовая корпорация может классифицировать свои приложения следующим образом:

Приложение	Категория
Приложение для обработки кредитов	Критический
Приложение службы поддержки клиентов с интерфейсом	Критический

Приложение	Категория
Средство просмотра PDF-файлов	Важно!
Приложение для обработки изображений	Не важно

Кроме того, они могут сочетать эту классификацию с ранжированием серьезности и приоритета следующим образом:

Категория	Серьезность	Priority	Ответ
Критический	1 или 2	1 или 2	Для параметра 1 остановите развертывание до тех пор, пока не будет разрешено; Для 2 остановите развертывание только для затронутых устройств или пользователей.
Важно!	3 или 4	3 или 4	Для версии 3 продолжайте развертывание даже для затронутых устройств, если существуют рекомендации по обходу.
Не важно	4	4	Продолжайте развертывание для всех устройств.

Оценка инфраструктуры и средств

Статья • 31.10.2023 • Применяется к: ✅ Windows 11, ✅ Windows 10

Перед развертыванием обновления оцените инфраструктуру развертывания. Например, такие системы управления, как Configuration Manager, Microsoft Intune или аналогичные. Также оцените текущие конфигурации, такие как базовые показатели безопасности, административные шаблоны и политики, влияющие на обновления. Затем задайте некоторые критерии для определения готовности к работе.

Инфраструктура

Требуются ли обновления для средств развертывания?

- Если вы используете Configuration Manager, находится ли она в текущей ветви с установленным последним выпуском? Наличие в этой ветви гарантирует, что она поддерживает следующее обновление компонентов клиента Windows. Configuration Manager выпуски поддерживаются в течение 18 месяцев.
- Использование облачного средства управления, например Microsoft Intune сокращает проблемы с поддержкой, так как связанные продукты не требуют обновления.
- Если вы используете средство сторонних разработчиков, проверка с поддержкой продукта, чтобы убедиться, что вы используете текущую версию и поддерживаете следующее обновление клиентских компонентов Windows.

Положитесь на опыт и данные из предыдущих развертываний, чтобы оценить, сколько времени занимают изменения инфраструктуры, и выявить проблемы, с которыми вы столкнулись.

Параметры устройств

Убедитесь, что базовые показатели безопасности, административные шаблоны и политики имеют правильные параметры для поддержки устройств после установки нового клиентского обновления Windows.

Базовые показатели безопасности

Следите за актуальностью базовых показателей безопасности, чтобы обеспечить безопасность вашей среды и правильно настроить новую функцию безопасности в

предстоящем обновлении клиента Windows.

- **Базовые показатели безопасности Майкрософт**. Необходимо реализовать базовые показатели безопасности от корпорации Майкрософт. Они включены в набор средств обеспечения соответствия требованиям безопасности, а также средства для управления ими.
- **Отраслевые или региональные базовые показатели**. В конкретной отрасли или регионе могут быть определенные базовые показатели, которые необходимо соблюдать в соответствии с нормативными требованиями. Убедитесь, что все новые базовые показатели поддерживают версию клиента Windows, которую вы планируете развернуть.

Обновления конфигурации

Существует несколько политик Windows, влияющих на установку обновлений Windows, отсрочку, взаимодействие с конечными пользователями и многие другие аспекты. Например, политики, заданные групповой политикой, Intune или другими методами. Проверьте эти политики, чтобы убедиться, что они настроены правильно.

- **Административные шаблоны Windows**. Каждое обновление компонентов клиента Windows содержит вспомогательный файл административного шаблона (ADMX-файл). групповая политика средства используют файлы административных шаблонов для заполнения параметров политики в пользовательском интерфейсе. Шаблоны доступны в Центре загрузки, например этот для Windows 11 версии 23H2.

- **Политики для соответствия обновлений и взаимодействия с конечными пользователями**. Несколько параметров влияют на установку обновлений устройством, на то, может ли пользователь отложить обновление, перезапустить после установки и многие другие аспекты поведения обновления. Особенно важно искать существующие политики, которые устарели или могут конфликтовать с новыми.

Определение критериев готовности к работе

При развертывании обновления необходимо убедиться, что обновление не содержит новых операционных проблем. Если возникают инциденты, убедитесь в наличии необходимой документации и процессов. Обратитесь в службу поддержки и эксплуатации, чтобы определить приемлемые тенденции и определить, какие документы или процессы требуют обновления:

- **Тенденция вызовов**. Определите, какое процентное увеличение количества вызовов, связанных с обновлениями функций клиента Windows, является приемлемым или может поддерживаться.
- **Тенденция инцидентов**. Определите, какой процент увеличения числа обращений, запрашивающих поддержку, связанных с обновлениями компонентов клиента Windows, является приемлемым или может поддерживаться.
- **Документация по поддержке**. Ознакомьтесь со вспомогательной документацией, которая требует обновления для поддержки новых средств инфраструктуры или конфигурации в рамках обновления компонентов клиента Windows.
- **Обработка изменений:** Определите и обновите все процессы, которые будут изменены в результате обновления компонентов Windows.

Специалисты по работе и поддержке помогут вам определить, отслеживается ли соответствующая информация в данный момент. Если это не так, узнайте, как получить эту информацию, чтобы получить правильную информацию.

Задачи

Наконец, можно приступить к выполнению работы, необходимой для обеспечения поддержки обновления инфраструктурой и конфигурацией. Чтобы помочь вам отслеживать, можно классифицировать работу на следующие общие задачи:

- **Ознакомьтесь с требованиями к инфраструктуре**. Ознакомьтесь с подробными сведениями о требованиях для поддержки обновления и убедитесь, что все они определены.
- **Проверка инфраструктуры на соответствие требованиям**. Сравните инфраструктуру с требованиями, определенными для обновления.
- **Определение плана обновления инфраструктуры**. Подробные сведения о том, как должна измениться инфраструктура для поддержки обновления.
- **Просмотр текущего тома поддержки**. Изучите текущий том поддержки, чтобы понять, сколько влияния оказывает обновление при его развертывании.
- **Выявление пробелов, требующих внимания**. Определите проблемы, которые необходимо устранить для успешного развертывания обновления. Например, придется ли инженеру инфраструктуры исследовать, как новая функция, которая поставляется с обновлением, может повлиять на инфраструктуру?
- **Определение плана операционного обновления**. Подробные сведения о том, как необходимо изменить операционные службы и процессы для

поддержки обновления.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Определение стратегии обновления с помощью календаря

Статья • 29.08.2023 • Применяется к: ✅ Windows 11, ✅ Windows 10

Традиционно в организациях развертывание обновлений операционной системы (особенно обновлений компонентов) рассматривалось как дискретный проект, имеющий начало, середину и конец. Выпуск был "создан" (обычно в виде образа), а затем распространялся среди пользователей и их устройств.

Сегодня все больше организаций рассматривают развертывание как непрерывный процесс обновлений, которые развертываются по всей организации волнами. При таком подходе обновление подключается к этому процессу, и во время его выполнения вы отслеживаете аномалии, ошибки или влияние на пользователей и реагируете на возникающие проблемы, не прерывая весь процесс. Корпорация Майкрософт постоянно расширяет циклы выпуска Windows, механизмы обновления и соответствующие средства для поддержки этой модели. Дополнительные сведения о жизненном цикле Windows см. в статье Вопросы и ответы о жизненном цикле Windows.

Мы рекомендуем развертывать каждый доступный выпуск и поддерживать быструю периодичность для определенной части вашей среды. Мы также понимаем, что у вас может быть большое количество устройств, и вам потребуется мало или вообще не беспокоиться. Периодичность жизненного цикла позволяет некоторым частям вашей среды перемещаться быстрее, в то время как большинство может перемещаться менее быстро.

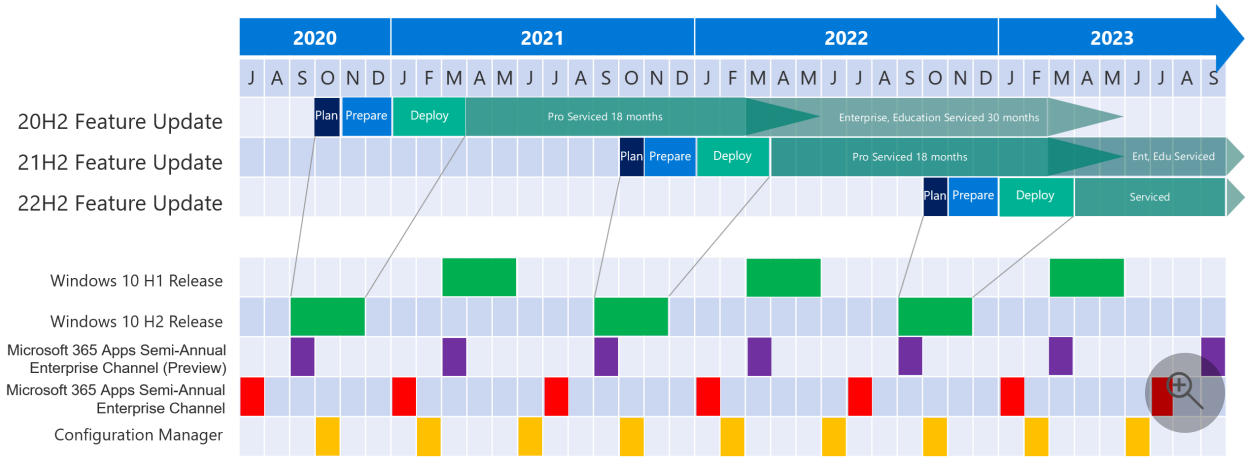
Подходы к календарю

Календарный подход можно использовать для более быстрой частоты в два раза в год или ежегодной. В зависимости от размера компании установка обновлений компонентов реже одного раза в год рискует выйти из эксплуатации устройств и стать уязвимыми к угрозам безопасности, так как они перестают получать ежемесячные обновления для системы безопасности после выхода версии из-под поддержки.

Годовой подход

Ниже приведен календарь с примером расписания, которое применяет одно обновление компонентов Windows за календарный год в соответствии с Microsoft

Configuration Manager и Приложения Microsoft 365 циклами выпуска:



Этот подход обеспечивает приблизительно 12 месяцев использования каждого обновления компонентов до установки следующего обновления путем согласования с обновлением компонентов Windows H2.

Эта периодичность может быть наиболее подходящей для вас, если применяются какие-либо из следующих условий:

- Вы только начинаете свой путь с процесса обслуживания Windows. Если вы не знакомы с новыми процессами, поддерживающими обслуживание Windows, переход от проекта, который выполняется раз в три-пять лет, к процессу обновления компонентов может оказаться сложной задачей. Этот подход дает вам время для изучения новых подходов и инструментов для сокращения усилий и затрат.
- Вы хотите подождать и посмотреть, насколько успешными являются другие компании при внедрении обновления компонентов Windows.
- Вы хотите быстро идти с обновлениями компонентов и иметь возможность пропустить обновление компонентов, сохраняя при этом Обслуживание Windows в случае изменения бизнес-приоритетов.

Безопасность Центра обновления Windows

Статья • 15.08.2024 • Применяется к: ✅ Windows 11, ✅ Windows 10

Система клиентский компонент Центра обновления Windows (WU) обеспечивает безопасное обновление устройств. Его сквозная защита предотвращает манипуляции с обменом протоколами и обеспечивает установку только утвержденного содержимого. Для некоторых защищенных сред может потребоваться обновить правила брандмауэра и прокси-сервера, чтобы обеспечить правильный доступ к обновлениям Windows. В этой статье приводятся общие сведения о функциях безопасности клиентский компонент Центра обновления Windows.

Общие сведения о безопасности клиентский компонент Центра обновления Windows

Система клиентский компонент Центра обновления Windows распространяет множество содержимого. Ниже приведены некоторые примеры этого содержимого:

- Обновления к операционной системе Windows
- обновления Приложения Microsoft 365 (обновления Office)
- Драйверы оборудования
- Определения антивирусной программы
- Приложения Microsoft Store

Эта система инициируется, когда пользователь взаимодействует со страницей параметров клиентский компонент Центра обновления Windows или когда приложение выполняет вызов API службы клиента WU. Эти вызовы могут выполняться в разное время приложениями Майкрософт и различными частями Windows, такими как Приложения Microsoft 365, Microsoft Defender и Plug and Play (PnP).

При таких взаимодействиях служба клиентский компонент Центра обновления Windows, запущенная на устройстве, активирует серию обменов через Интернет с клиентский компонент Центра обновления Windows серверами Майкрософт. Общий рабочий процесс:

1. Устройство Windows устанавливает несколько подключений к службам клиентский компонент Центра обновления Windows по протоколу HTTPS

(HTTP через TLS, TCP-порт 443).
2. Метаданные обновления обмениваются по этим подключениям и приводят к списку обновлений, приложений, драйверов и других обновлений.
3. Устройство решает, следует ли скачивать элементы из результирующего списка и когда.

После того как будет определен список загрузок, фактические двоичные файлы обновления загружаются. Скачивание выполняется через компонент оптимизации доставки через сочетание стандартных HTTP-вызовов (TCP-порт 80) и безопасных одноранговых сетевых вызовов (TCP-порт 7680). Используемый метод основан на конфигурациях или групповых политиках устройства.

При скачивании обновлений с помощью одноранговой сети оптимизации доставки (P2P) содержимое проверяется по получении от каждого однорангового узла. Если запрошенное содержимое недоступно в сети P2P, компонент оптимизации доставки загрузит его по протоколу HTTP.

Независимо от того, какой метод используется для скачивания содержимого, полученные файлы проверяются с помощью цифровых подписей и хэшей файлов перед установкой. Проверка подтверждает, что скачивание предназначено, проверено на подлинность и не было изменено.

Защита подключений к метаданным

Когда клиентский компонент Центра обновления Windows проверяет наличие обновлений, он проходит ряд обменов метаданными между устройством и серверами клиентский компонент Центра обновления Windows. Этот обмен выполняется по протоколу HTTPS (HTTP через TLS). Эти защищенные подключения закреплены сертификатом, что обеспечивает следующее:

- Проверяется сертификат сервера TLS-подключения (доверие к сертификату, срок действия, отзыв, записи SAN и т. д.)
- Издатель сертификата проверяется как подлинный Microsoft клиентский компонент Центра обновления Windows

Подключение завершается ошибкой, если издатель непредвиден или не является допустимым клиентский компонент Центра обновления Windows промежуточным сертификатом. Закрепление сертификатов гарантирует, что устройство подключается к законным серверам Майкрософт и предотвращает атаки типа "злоумышленник в середине".

Так как клиентский компонент Центра обновления Windows подключения TLS закреплены сертификатом, важно, чтобы прокси-серверы TLS передавали эти подключения без перехвата. Полный список DNS-имен, для которых требуются исключения прокси-сервера или брандмауэра, можно найти в статье об устранении неполадок клиентский компонент Центра обновления Windows.

Корпорация Майкрософт не предоставляет IP-адреса или диапазоны IP-адресов для этих исключений, так как они могут отличаться с течением времени по мере внесения изменений, таких как балансировка нагрузки трафика.

Ожидаемое использование сервера клиентский компонент Центра обновления Windows

Серверы службы клиентский компонент Центра обновления Windows используются только компонентами wu. Нет никаких ожиданий, что конечные пользователи будут взаимодействовать с этими удаленными конечными точками. Таким образом, эти конечные точки службы могут не разрешать в веб-браузере должным образом. Пользователь, случайно просматривающий эти конечные точки, может заметить несоблюдение последних ожиданий веб-браузера, таких как общедоступные доверенные PKI, ведение журнала прозрачности сертификатов или требования TLS. Это ожидаемое поведение не ограничивает или иным образом не влияет на безопасность и безопасность клиентский компонент Центра обновления Windows системы.

Пользователи, пытающиеся перейти к конечным точкам службы, могут видеть предупреждения системы безопасности и даже сбои доступа к содержимому. Опять же, это поведение ожидается, так как конечные точки службы не предназначены для доступа к веб-браузеру или случайного использования пользователем.

Защита доставки содержимого

Процесс скачивания двоичных файлов обновления защищен на уровне выше транспорта. Несмотря на то, что содержимое может быть загружено через стандартный http (TCP-порт 80), содержимое проходит тщательный процесс проверки безопасности.

Загрузка распределяется через сети доставки содержимого (CDN), поэтому использование TLS приведет к разрыву цепочки хранения Майкрософт. Так как

TLS-подключение к кэшированию CDN завершается в сети CDN, а не в корпорации Майкрософт, сертификаты TLS не относятся к корпорации Майкрософт. Это означает, что клиент WU не может доказать надежность сети CDN, так как корпорация Майкрософт не контролирует сертификаты CDN TLS. Кроме того, подключение TLS к СЕТИ CDN не подтверждает, что содержимым не было манипулировано в сети кэширования CDN. Таким образом, TLS не предоставляет никаких обещаний безопасности для сквозного рабочего процесса клиентский компонент Центра обновления Windows, которые он предоставляет в противном случае.

Независимо от способа доставки содержимого, после скачивания оно проверяется должным образом. Содержимое проверяется на предмет доверия, целостности и намерения с помощью различных методов, таких как проверка цифровой подписи и проверка хэша файлов. Этот уровень проверки содержимого обеспечивает еще больше уровней безопасности, чем только TLS.

Службы Windows Server Update Services (WSUS)

Предприятия, использующие WSUS, имеют аналогичный рабочий процесс. Однако клиентские устройства подключаются к корпоративному серверу WSUS, а не через Интернет к серверам Майкрософт. Организация решает, следует ли использовать подключения HTTP или TLS (HTTPS) для обмена метаданными. Корпорация Майкрософт настоятельно рекомендует использовать подключения TLS и настраивать клиентские устройства с соответствующими конфигурациями закрепления сертификатов TLS для обмена метаданными с WSUS. Дополнительные сведения о закреплении сертификатов TLS WSUS см. в разделе:

- Блог Windows IT Pro: Изменения для повышения безопасности устройств Windows, сканирующих WSUS
- Блог WINDOWS IT Pro: Проверка изменений и сертификатов добавляет безопасность для устройств Windows с помощью WSUS для обновлений

Когда сервер WSUS обновляет свой собственный каталог обновлений, он подключается к службам синхронизации серверов Майкрософт и проверяет наличие обновлений. Процесс синхронизации сервера WSUS аналогичен процессу обмена метаданными для клиентских устройств, подключающихся к клиентский компонент Центра обновления Windows. Подключение WSUS к Майкрософт осуществляется по протоколу TLS и проверяется с помощью сертификата Майкрософт, аналогично закреплению сертификата TLS клиента WU.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Рекомендации по обновлению и переносу Windows

Применяется к: ✅ Windows 11, ✅ Windows 10

Файлы и параметры приложений можно перенести на новое оборудование под управлением операционной системы Windows или поддерживать их во время обновления операционной системы на том же компьютере. В этой статье перечислены средства Майкрософт, которые можно использовать для перемещения файлов и параметров между установками, а также специальные рекомендации по обновлению или миграции.

Обновление с предыдущей версии Windows

Более ранние версии Windows можно обновить до более поздних версий. В рамках процесса обновления можно установить более новую версию Windows, сохраняя приложения, файлы и параметры, как и в предыдущей версии Windows. Если пользовательская установка Windows выполняется вместо обновления, приложения и параметры не поддерживаются. Личные файлы и все файлы и каталоги Windows перемещаются в папку **Windows.old** . Доступ к данным можно получить в папке **Windows.old** после завершения установки Windows.

Перенос файлов и параметров

Средство миграции пользовательской среды (USMT) доступно для передачи параметров:

- Между двумя компьютерами под управлением Windows, также известная как *параллельная* миграция.
- На одном компьютере выполняется обновление версии Windows, если не используется обновление на месте, также известное как *очистка и загрузка* или *обновление* миграции.

USMT передает только параметры программы, но не сами программы. USMT — это приложение, предназначенное для администраторов, выполняющих крупномасштабные автоматизированные развертывания, но его также можно использовать при небольших миграциях.

Миграция с помощью средства миграции пользовательской среды

USMT можно использовать для автоматизации миграции во время крупных развертываний операционной системы Windows. USMT использует XML-файлы, определяющие правила миграции. Правила миграции можно настроить для управления тем, что именно выполняет миграция USMT и как она переносит элементы. Например, USMT может выполнять миграцию:

- Учетные записи пользователей, включая конкретные учетные записи для миграции.
- Пользовательские файлы, включая конкретные файлы для переноса.
- Параметры операционной системы, включая параметры конкретной операционной системы для переноса.
- Параметры для некоторых приложений, включая параметры конкретного приложения для миграции.

USMT можно использовать в следующих сценариях:

- **Параллельно** — миграция, при которой одно устройство заменяется другим устройством.
- **Очистка и загрузка/refresh** — миграция, в которой Windows обновляется на одном устройстве.

> ⓘ **Внимание**
>
> USMT поддерживает только устройства, присоединенные к локальному домену Active Directory. USMT не поддерживает Microsoft Entra присоединенных устройств.

Рекомендации по обновлению и миграции

При обновлении или переходе на новую версию Windows учитывайте следующие проблемы и рекомендации.

Совместимость приложений

Дополнительные сведения о совместимости приложений в Windows см. в разделе Совместимость для Windows 11.

Обновления многоязычных образов Windows

USMT не поддерживает обновления между языками при выполнении многоязычных обновлений Windows. При обновлении или переносе операционной системы с несколькими установленными языковыми пакетами можно обновить или перенести только язык пользовательского интерфейса системы по умолчанию. Например, если по

умолчанию используется английский язык, но установлен испанский языковой пакет, можно обновить или перенести только английский язык.

Если одноязычный образ Windows, соответствующий языку пользовательского интерфейса системы по умолчанию многоязычной операционной системы, используется для переноса*обновлениях очисткой и загрузкой*/, миграция работает. Однако все языковые пакеты удаляются. После завершения обновления языковые пакеты потребуется переустановить.

Errorhandler.cmd

При использовании **Errorhandler.cmd** при обновлении с более ранней версии Windows скопируйте **Errorhandler.cmd** в `%WINDIR%\Setup\Scripts` каталог при исходной установке Windows. Копирование **Errorhandler.cmd** в `%WINDIR%\Setup\Scripts` каталог при исходной установке Windows гарантирует, что при возникновении ошибок на этапе начального уровня установки Windows команды **в Errorhandler.cmd** выполняться. Дополнительные сведения см. в статье Запуск скрипта, если программа установки Windows обнаруживает неустранимую ошибку (ErrorHandler.cmd).

Связанное содержимое

- Общие сведения о средстве миграции пользовательской среды (USMT).
- Пути обновления Windows.
- Обновление выпуска Windows.

Last updated on 08.04.2025

Что такое оптимизация доставки?

Применимо к: ✅ Windows 11, ✅ Windows 10

> **Ищете объекты групповая политика?** Ознакомьтесь со справочником по оптимизации доставки или электронной таблицей master, доступной в Центре загрузки для Windows 11 или для Windows 10.

Обновления, обновления и приложения Windows могут содержать пакеты с большими файлами. Скачивание и распространение обновлений может потребовать внушительного объема сетевых ресурсов на обновляемых устройствах. Оптимизация доставки — это надежный загрузчик HTTP с управляемым облаком решением, которое позволяет устройствам Windows при необходимости скачивать эти пакеты из альтернативных источников (например, из других устройств в сети и (или) выделенного сервера кэша) в дополнение к традиционным интернет-серверам (в документах по оптимизации доставки они называются источниками HTTP). Вы можете использовать оптимизацию доставки для снижения потребления пропускной способности путем совместного скачивания этих пакетов между несколькими устройствами в развертывании, однако использование одноранговое подключения является необязательным.

Чтобы использовать одноранговую функцию или функции подключенного кэша (Майкрософт), устройства должны иметь доступ к Интернету и облачным службам оптимизации доставки. Если для оптимизации доставки настроено использование одноранговых узлов и подключенного кэша Майкрософт, для достижения наилучшей возможности доставки содержимого клиент подключается к подключенном кэшу и одноранговым узлам параллельно. Если нужное содержимое не удается получить из подключенного кэша или одноранговых узлов, оптимизация доставки легко вернется к источнику HTTP, чтобы получить запрошенное содержимое.

Вы можете использовать оптимизацию доставки с клиентский компонент Центра обновления Windows, Windows Server Update Services (WSUS), Microsoft Intune/ клиентский компонент Центра обновления Windows политики клиента или Microsoft Configuration Manager (если включена установка Express Обновления).

Сведения о настройке оптимизации доставки, включая советы по лучшим параметрам в различных сценариях, см. в разделе Настройка оптимизации доставки. Полный список всех параметров оптимизации доставки см. в справочнике по оптимизации доставки.

> ⓘ **Заметка**
>
> Службы WSUS также могут использовать BranchCache для кэширования содержимого и предоставления к нему общего доступа. Если оптимизация доставки

включена на устройствах, где используется BranchCache, будет использоваться оптимизация.

Требования

В следующей таблице приведена минимальная версия Windows 10, поддерживающая оптимизацию доставки.

Развернуть таблицу

Тип устройства	Минимальная версия Windows
Компьютеры под управлением Windows 10 или более поздней версии	Windows 10 1511
Windows Server 2019 г. или более поздней версии (в состав серверных ядер)	Windows Server 2019
Устройства Windows IoT	Windows 10 1803

Типы загрузки содержимого, поддерживаемые оптимизацией доставки

Клиент Windows

Развернуть таблицу

Клиент Windows	Минимальная версия Windows	Загрузчик HTTP	Одноранговый узел	Подключенный кэш Майкрософт
клиентский компонент Центра обновления Windows (обновления исправлений компонентов, языковые пакеты, драйверы)	Windows 10 1511, Windows 11	✔	✔	✔

Клиент Windows	Минимальная версия Windows	Загрузчик HTTP	Одноранговый узел	Подключенный кэш Майкрософт
Windows 10/11 приложений магазина UWP	Windows 10 1511, Windows 11	✔	✔	✔
Windows 11 приложений Магазина Win32	Windows 11	✔		
Обновления определений Защитника Windows	Windows 10 1511, Windows 11	✔	✔	✔
приложения Intune Win32	Windows 10 1709, Windows 11	✔ (за исключением облачных сред для государственных организаций)	✔ (за исключением облачных сред для государственных организаций)	✔ (за исключением облачных сред для государственных организаций)
Приложения Microsoft 365 и обновления	Windows 10 1709, Windows 11	✔	✔ (за исключением расширенного канала SAC)	✔
Обновления браузера Edge	Windows 10 1809, Windows 11	✔	✔	✔
Configuration Manager Экспресс-обновления	Windows 10 1709 + Configuration Manager версия 1711, Windows 11	✔	✔	✔
Динамические обновления	Windows 10 1903, Windows 11	✔	✔	✔
Агент MDM	Windows 11	✔		
Xbox Game Pass (ПК)	Windows 10 1809, Windows 11	✔		✔
Диспетчер пакетов	Windows 10 1809, Windows	✔		

Клиент Windows	Минимальная версия Windows	Загрузчик HTTP	Одноранговый узел	Подключенный кэш Майкрософт
Windows	11			
Установщик MSIX	Windows 10 2004, Windows 11	✔		
Обновления Teams	Windows 10 2004, Windows 11	✔	✔ (начиная с версии 25122.1415.3698.6812)	✔ (только по протоколу HTTPS)

Windows Server

Развернуть таблицу

Windows Server	Минимальная версия Windows	Загрузчик HTTP	Одноранговый узел	Подключенный кэш Майкрософт
Центр обновления Windows	Windows Server 2019 (1809)	✔	✔	✔
Обновления браузера Edge	Windows Server 2019 (1809)	✔	✔	✔

Linux (общедоступная предварительная версия)

Развернуть таблицу

Linux (общедоступная предварительная версия)	Версии Linux	Загрузчик HTTP	Одноранговый узел	Подключенный кэш Майкрософт
Обновление устройства для Центр Интернета вещей	Ubuntu 18.04, 20.04 / Debian 9, 10	✔		✔

> **Заметка**
>
> Начиная с Configuration Manager версии 1910, вы можете использовать оптимизацию доставки для распространения всего содержимого обновлений Windows для клиентов, работающих Windows 10 версии 1709 или более поздней, а не только для

файлов экспресс-установки. Дополнительные сведения см. **в статье Оптимизация доставки, начиная с версии 1910**.

В клиентских выпусках Windows Enterprise, Professional и Education оптимизация доставки включена по умолчанию для одноранговового общего доступа в локальной сети (NAT). В частности, все устройства должны находиться за одним и тем же NAT (который включает в себя Ethernet или Wi-Fi), но вы можете настроить его по-разному в групповая политика и решениях управления мобильными устройствами (MDM), таких как Microsoft Intune. Дополнительные сведения см. в разделе Параметры режима загрузки .

Как Майкрософт использует оптимизацию доставки

Чтобы гарантировать, что текущие развертывания не влияют на нашу сеть и не отнимают пропускную способность для других служб, ИТ-служба Майкрософт использует несколько различных стратегий управления пропускной способностью. Оптимизация доставки, одноранговое кэширование, включенное с помощью групповой политики, были внедрены, а затем развернуты на всех управляемых устройствах, на которых используется групповая политика. На основе рекомендаций от команды оптимизации доставки мы использовали конфигурацию "группы", чтобы ограничить общий доступ к содержимому на устройствах, входящих в один домен Active Directory. Содержимое кэшируется на 24 часа. Более 76% содержимого поступает из одноранговых устройств, а не с Интернета.

Использование прокси-сервера с оптимизацией доставки

Если прокси-сервер используется в вашей среде, ознакомьтесь с разделом Использование прокси-сервера с оптимизацией доставки , чтобы понять параметры прокси-сервера, необходимые для правильного использования оптимизации доставки.

Описание взаимодействия клиента и службы оптимизации доставки

Чтобы получить более глубокое представление о рабочем процессе взаимодействия клиента и службы доставки с оптимизацией доставки, см. описание взаимодействия клиента и службы с оптимизацией доставки.

Настройка оптимизации доставки для Windows

Узнайте больше о параметрах оптимизации доставки, чтобы обеспечить правильную настройку в вашей среде.

Справочник по оптимизации доставки

Полный список параметров оптимизации доставки см. в справочнике по оптимизации доставки.

Новые возможности в Windows 10 версии 20H2 и Windows 11

См . новые возможности оптимизации доставки

Last updated on 03.12.2025

Книга по совместимости Windows

Статья20.06.2023

Windows 10, Windows 8, Windows 8.1 и Windows Server 2012 R2 представляют новейшие технологии операционной системы и платформы разработки программного обеспечения для использования разработчиками приложений и предприятиями по всему миру. В рамках дальнейшего повышения безопасности, надежности, производительности и пользовательского интерфейса Windows корпорация Майкрософт представила множество новых функций, улучшила существующие функции и удалила другие.

Хотя целью Windows 10, Windows 8, Windows 8.1 и Windows Server 2012 R2 является обеспечение высокой совместимости с большинством соответствующих приложений, написанных для ранее выпущенных операционных систем, некоторые разрывы совместимости неизбежны из-за инноваций, ужесточения безопасности и повышения надежности. В целом совместимость новых операционных систем с существующими приложениями высока.

Эта *книга состоит* из трех основных разделов, Windows 10, Windows 8.1 и Windows 8:

- Windows 10
- Windows 8.1 и Windows Server 2012 R2
- Windows 8 или Windows Server 2012

Следующие разделы являются новыми в этом выпуске *Cookbook* или обновлены:

- Загрузка файла образа Windows (WimBoot)
- Комплект сертификации приложений для Windows

Мы предлагаем вам ознакомиться с этими разделами, чтобы узнать, как оптимизировать приложения и воспользоваться преимуществами этого новейшего выпуска Windows.

Выпуски Cookbook для обеспечения совместимости Windows, которые предназначены для более ранних версий операционных систем Windows и Windows Server, можно найти в Windows Vista и Windows Server 2008 , Windows 7 и Windows Server 2008 R2.

Подготовка к Windows 11

Статья • 18.03.2023 • Применяется к: ✅ Windows 11, ✅ Windows 10

Windows 10 и Windows 11 предназначены для совместного использования, чтобы вы могли использовать одни и те же привычные средства и процессы для управления обеими операционными системами. Использование единой инфраструктуры управления, поддерживающей распространенные приложения Windows 10 и Windows 11, упрощает процесс миграции. Вы можете анализировать конечные точки, определять совместимость приложений и управлять развертыванием Windows 11 так же, как для Windows 10.

После оценки оборудования на соответствие требованиям Windows 11 самое время проверить инфраструктуру развертывания, средства и общие процессы управления конечными точками и обновлением, а также найти возможности для упрощения и оптимизации. В этой статье содержатся полезные инструкции для выполнения этих задач.

Инфраструктура и средства

Средства, используемые для основных рабочих нагрузок при развертывании Windows 10, по-прежнему можно использовать для Windows 11. Ниже описаны некоторые различия.

> ⓘ **Важно!**
>
> Свяжитесь с поставщиками любых сторонних решений (не Майкрософт), которые вы используете. Проверьте совместимость этих средств с Windows 11, особенно если они предоставляют возможности защиты или предотвращения потери данных.

Локальные решения

- Если вы используете Windows Server Update Services (WSUS), необходимо синхронизировать новую Windows 11 категорию продукта. После синхронизации категории продукта вы увидите Windows 11 в качестве предлагаемого варианта. Если вы хотите проверить Windows 11 до выпуска, вы также можете синхронизировать категорию **Windows Insider Pre-release**.

  > ⓘ **Примечание**

Во время развертывания вам будет предложено согласиться с условиями лицензионного соглашения на использование программного обеспечения корпорации Майкрософт от имени пользователей. Кроме того, вы не увидите вариант x86, так как Windows 11 не поддерживается в 32-разрядной архитектуре.

- Если вы используете Microsoft Configuration Manager, вы можете синхронизировать новый **Windows 11** категории продуктов и начать обновление соответствующих устройств. Если вы хотите проверить Windows 11 до выпуска, вы также можете синхронизировать категорию **Windows Insider Pre-release**.

  > ⓘ **Примечание**
  >
  > Диспетчер конфигураций предложит принять условия лицензионного соглашения на использование программного обеспечения корпорации Майкрософт от имени пользователей в организации.

Облачные решения

- Если вы используете политики Центра обновления Windows для бизнеса, вам нужно будет использовать возможность **целевой версии** (либо через политику, либо через службу развертывания Центра обновления Windows для бизнеса) вместо отсрочки обновлений компонентов для перехода с Windows 10 на Windows 11. Отсрочки обновления компонентов отлично подходят для перехода на более новые версии текущего продукта (например, Windows 10 с версии 20H2 до 21H1), но не будут автоматически перемещать устройства между продуктами (Windows 10 **в Windows 11**).
  - Если вы используете Microsoft Intune и у вас есть лицензия Microsoft 365 E3, вы сможете использовать страницу Развертывание обновлений компонентов, чтобы выбрать **Windows 11 версии 21H2** и обновить устройства с Windows 10 до Windows 11. Вы также можете продолжать использовать те же элементы интерфейса обновления для управления Windows 10 и Windows 11 на странице **Круги обновления** в Intune. Если вы не готовы перейти на Windows 11, установите для версии обновления компонентов значение вашей текущей версии. Когда вы будете готовы к обновлению устройств, измените параметр развертывания обновления компонентов, чтобы указать Windows 11.

- В групповой политике **выбор целевой версии обновления компонентов** включает два поля ввода после установки необязательного обновления от 01.09.2021 (KB5005101) или более позднего обновления: **Версия продукта** и **Целевая версия**.
- В поле версии продукта нужно указать Windows 11, чтобы обновить ОС устройств до Windows 11. Если настроено только поле целевой версии, устройству будут предложены соответствующие версии того же продукта.
- Например, если на устройстве используется *Windows 10 версии 2004* и только целевая версия настроена как 21H1, этому устройству будет предложена *ОС Windows 10 версии 21H1*, даже если несколько продуктов имеют версию 21H1.

- Отсрочка исправлений будет работать так же и в Windows 10, и в Windows 11. Это верно независимо от того, какое средство управления вы используете для настройки политик Центра обновления Windows для бизнеса.
- Если вы используете Microsoft Intune и у вас есть лицензия Microsoft 365 E3, вы сможете использовать развертывание обновлений компонентов для простого обновления устройств с одного выпуска Windows 10 на другой или для перехода с устройств Windows 10 на Windows 11. Вы также можете продолжать использовать те же элементы интерфейса обновления для управления Windows 10 и Windows 11. Если вы не готовы перейти на Windows 11, установите для версии обновления компонентов значение вашей текущей версии. Когда вы будете готовы приступить к обновлению устройств, измените параметр развертывания обновления компонентов, указав **Windows 11**.

  > ⓘ **Примечание**
  >
  > Конечные точки, управляемые Центром обновления Windows для бизнеса, не будут автоматически обновляться до Windows 11, если администратор не настроит **целевую версию** явным образом с помощью параметра TargetReleaseVersion в Windows CSP, профиля обновления компонентов в Intune или параметра Выбрать целевую версию обновления компонентов в групповой политике.

Облачное управление

Если вы еще не используете возможности облачного управления, такие как доступные в Microsoft Intune семействе продуктов, стоит рассмотреть это. Помимо консолидации управления устройствами и безопасности конечных точек в рамках одной платформы, Microsoft Intune может лучше поддерживать разнообразную экосистему by-own-device (BYOD), которая все чаще становится нормой в гибридных сценариях работы. Это также позволяет отслеживать ход выполнения требований и бизнес-целей при защите конфиденциальности пользователей.

Ниже приведены некоторые распространенные варианты использования и соответствующие возможности Microsoft Intune, которые их поддерживают.

- **Подготовка и предварительная настройка новых устройств с Windows 11**. Windows Autopilot позволяет развертывать новые устройства с Windows 11 в состоянии "бизнес-готовности", которое включает в себя нужные приложения, параметры и политики. Его также можно использовать для изменения выпуска Windows. Например, вы можете перейти с выпуска Professional на Enterprise и использовать дополнительные функции. Страница Windows Autopilot диагностика — это новая функция, которая доступна при использовании Windows Autopilot для развертывания Windows 11.
- **Настройка правил и параметров управления для пользователей, приложений и устройств**. При регистрации устройств в Microsoft Intuneадминистраторы получают полный контроль над приложениями, настройками, функциями и безопасностью для Windows 11 и Windows 10. Вы также можете использовать политики защиты приложений, чтобы требовать многофакторную проверку подлинности (MFA) для определенных приложений.
- **Оптимизация управления устройствами для сотрудников без компьютеров, удаленных сотрудников и работников в офисе**. Представленная в Windows 10 облачная конфигурация — это стандартная, простая в управлении конфигурация устройств, оптимизированная для облачного применения пользователями с определенными потребностями рабочего процесса. Его можно развернуть на устройствах с выпусками Pro, Enterprise и Education Windows 11 с помощью Microsoft Intune.

Если вы используете исключительно локальное решение управления устройствами (например, Configuration Manager), вы по-прежнему можете использовать шлюз облачного управления, включить присоединение клиента или включить совместное управление с помощью Microsoft Intune. Эти решения упрощают защиту и обновление устройств.

Обзор подхода и политик обслуживания

Каждая организация переходит на Windows 11 в своем собственном темпе. Корпорация Майкрософт обязуется поддерживать вас в процессе миграции на Windows 11, если вы являетесь ранним последователем или планируете выполнить переход в предстоящие месяцы или годы.

Если вы будете рассматривать обновления операционной системы как непрерывный процесс, вы автоматически улучшите свои возможности развертывания обновлений. Этот подход позволяет поддерживать актуальное состояние с меньшими усилиями и меньшим влиянием на производительность. Для начала подумайте о том, как вы разворачиваете обновления компонентов Windows в настоящее время: на каких устройствах и в каком темпе.

Затем создайте план развертывания для **Windows 11**, который включает группы развертывания, круги, пользователей или устройства. Нет абсолютных правил для точного количества кругов развертывания, но распространена следующая структура:

- Ознакомительный круг (первые пользователи или canary): планирование и разработка
- Ограниченный круг (ранние последователи): пилотное развертывание и проверка
- Широкое использование (пользователи или важные устройства): широкое развертывание

Подробные сведения см. в статье Создание плана развертывания.

Обзор политик

Просмотрите политики, связанные с развертыванием, принимая во внимание цели безопасности организации, сроки обновления для соответствия требованиям и действия на устройствах. Примените изменения, обеспечивающие явное улучшение, особенно в отношении скорости процесса обновления или безопасности.

Проверка приложений и инфраструктуры

Чтобы убедиться, что приложения, инфраструктура и процессы развертывания готовы к Windows 11, присоединитесь к программе предварительной оценки Windows для бизнеса и выберите канал предварительной версии выпуска.

Если вы используете Windows Server Update Services (WSUS), вы можете выполнить развертывание непосредственно из категории предварительной версии

программы предварительной оценки Windows, используя один из следующих процессов:

- Присвойте параметру **Управление предварительными сборками** значение **Release Preview** в Центре обновления Windows для бизнеса.
- Используйте образы виртуального рабочего стола Azure и Azure Marketplace.
- Скачайте и разверните ISO со страницы загрузок Windows ISO программы предварительной оценки Windows от корпорации Майкрософт.

Независимо от выбранного метода вы получаете преимущество бесплатной поддержки Майкрософт при проверке предварительных сборок. Бесплатная поддержка доступна любому коммерческому клиенту, разворачивающему предварительные сборки Windows 10 или Windows 11, когда они становятся доступными в программе предварительной оценки Windows.

Средства аналитики и оценки

Если вы используете Microsoft Intune и подключены устройства к аналитике конечных точек, вы получите доступ к оценке готовности оборудования в конце этого года. Это средство позволяет быстро определить, какие из управляемых устройств позволяют перейти на Windows 11.

Аналитика компьютеров не поддерживает Windows 11. Необходимо использовать аналитику конечных точек.

Подготовка пилотного развертывания

Пилотное развертывание — это подтверждение концепции для развертывания обновления на выбранном количестве устройств в рабочей среде, прежде чем выполнять широкое развертывание в организации.

Состав задач на общем уровне:

1. Назначение группы пользователей или устройств для получения обновления.
2. Реализация обновлений базовых параметров.
3. Реализация операционных обновлений.
4. Проверка процесса развертывания.
5. Развертывание обновления на устройствах.
6. Тестирование и поддержка пилотных устройств.
7. Определение готовности к широкому развертыванию на основе результатов пилотного процесса.

Готовность пользователей

Не забывайте о важности готовности пользователей для эффективного развертывания Windows 11 в рамках всей организации. В Windows 11 используется знакомый дизайн, но пользователи увидят несколько улучшений общего пользовательского интерфейса. Им также потребуется адаптироваться к изменениям в меню и на страницах параметров. Поэтому для подготовки пользователей и сотрудников ИТ-поддержки к Windows 11 рассмотрите следующие задачи:

- Создайте расписание коммуникаций, чтобы предоставлять правильные сообщения в нужное время для нужных групп пользователей в зависимости от того, когда они увидят изменения.
- Создайте черновики кратких сообщений электронной почты, информирующих пользователей о том, какие изменения ожидаются. Предлагайте советы по использованию или настройке интерфейса. Включите сведения о вариантах помощи и технической поддержки.
- Добавьте в руководства службы технической поддержки снимки экранов нового пользовательского интерфейса, интерфейса при первом включении компьютера для новых устройств и интерфейса обновления для существующих устройств.

Подробнее

Ознакомьтесь с схемой обучения "Оставаться в курсе Windows 10 и Приложения Microsoft 365".

- Схема обучения была создана для Windows 10, но основные принципы и задачи, изложенные для этапов планирования, подготовки и развертывания, также применимы к развертыванию Windows 11.

См. также

Планирование Windows 11
Справка по Windows & обучения

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Подготовка к развертыванию Windows

Статья • 18.03.2023

Область применения

- Windows 10
- Windows 11

Проработав действия на этапе планирования, вы должны быть в хорошем состоянии для подготовки среды и процесса развертывания клиента Windows. На этапе планирования вы получите следующие полезные элементы:

- Четкое представление о необходимом персонале и его ролях и критериях оценки готовности приложения
- План тестирования и проверки приложений
- Оценка инфраструктуры развертывания и определений для готовности к работе
- План развертывания, определяющий круги, которые вы хотите использовать.

Теперь вы можете начать вносить изменения в среду, чтобы подготовиться к развертыванию.

Подготовка инфраструктуры и среды

- Развертывание обновлений сервера сайта для Configuration Manager.
- Обновление сторонних средств безопасности, таких как агенты безопасности или серверы.
- Обновление сторонних средств управления, таких как агенты защиты от потери данных.

Ваша инфраструктура, вероятно, включает в себя множество различных компонентов и инструментов. Необходимо убедиться, что на вашу среду не влияют проблемы из-за изменений, внесенных в различные части инфраструктуры. Выполните следующие действия:

1. Просмотрите все изменения инфраструктуры, выявленные в плане. Важно понимать изменения, которые необходимо вносить, и подробно понимать, как их реализовать. Этот процесс позволяет избежать проблем в дальнейшем.

2. Проверьте изменения. Вы проверите изменения для компонентов и средств инфраструктуры, чтобы понять, как изменения могут повлиять на рабочую среду.

3. Реализуйте изменения. После проверки изменений вы можете реализовать изменения в более широкой инфраструктуре.

Вы также должны посмотреть на конфигурацию среды вашей организации и пометить, как вы будете реализовывать все необходимые изменения, ранее определенные на этапе плана для поддержки обновления. Рассмотрите, что необходимо сделать для различных параметров и политик, которые в настоящее время лежат в основе среды. Пример:

- Реализуйте новые черновики рекомендаций по безопасности. Новые версии Windows могут включать новые функции, повышающие безопасность вашей среды. Вашим группам безопасности потребуется внести соответствующие изменения в конфигурации, связанные с безопасностью.

- Обновление базовых показателей безопасности. Группы безопасности понимают соответствующие базовые показатели безопасности и должны будут работать, чтобы убедиться, что все базовые показатели соответствуют рекомендациям, которые они должны соблюдать.

Однако ваша конфигурация будет состоять из множества различных параметров и политик. Важно применять изменения только там, где они необходимы и где вы получаете четкое улучшение. В противном случае в вашей среде могут возникнуть проблемы, которые замедляют процесс обновления. Вы хотите убедиться, что ваша среда не пострадала негативно из-за внесенных изменений. Пример:

1. Просмотрите новые параметры безопасности. Ваша команда безопасности изучит новые параметры безопасности, чтобы понять, как их лучше всего настроить для упрощения обновления, а также исследовать потенциальные последствия, которые они могут оказать на вашу среду.

2. Просмотрите базовые показатели безопасности на наличие изменений. Группы безопасности также проведут проверку всех необходимых базовых показателей безопасности, чтобы убедиться, что изменения могут быть реализованы, и убедиться, что ваша среда будет соответствовать требованиям.

3. Реализуйте и проверяйте параметры безопасности и изменения базовых показателей. Затем ваши группы безопасности реализуют все параметры

безопасности и базовые показатели, устраняя любые потенциальные нерешенные проблемы.

Подготовка приложений и устройств

Ранее вы решили, какие методы проверки следует использовать для проверки приложений на предстоящем этапе пилотного развертывания. Теперь самое время убедиться, что отдельные устройства готовы и могут без труда установить следующее обновление.

Убедитесь, что обновления доступны

Включите службы обновления на устройствах. Убедитесь, что на каждом устройстве работают все службы, от которых клиентский компонент Центра обновления Windows зависит. Иногда пользователи или даже вредоносные программы могут отключить службы, клиентский компонент Центра обновления Windows требуется для правильной работы. Убедитесь, что выполняются следующие службы:

- Фоновая интеллектуальная служба передачи
- Служба инфраструктуры фоновых задач
- BranchCache (если вы используете эту функцию для развертывания обновлений)
- Агент последовательности задач ConfigMgr (если для развертывания обновлений используется Configuration Manager)
- Службы шифрования
- Средство запуска серверных процессов DCOM
- Установка устройства
- Оптимизация доставки
- Диспетчер установки устройств
- Диспетчер лицензий
- Помощник по входу в учетную запись Майкрософт
- Поставщик теневого копирования программного обеспечения Майкрософт
- Удаленный вызов процедуры (RPC)
- Указатель удаленного вызова процедуры (RPC)
- Сопоставитель конечных точек RPC
- Диспетчер управления службами
- Планировщик заданий
- Брокер маркеров
- Обновление службы Orchestrator
- Служба теневого копирования томов

- Служба автоматического обновления Windows
- программа архивации данных
- Брандмауэр Защитника Windows
- Инструментарий управления Windows (WMI)
- Служба управления Windows
- Установщик модулей Windows
- Push-уведомление Windows
- Служба Безопасность Windows
- Служба времени Windows
- Центр обновления Windows
- служба "Клиентский компонент Центра обновления Windows Медик"

Эти службы можно проверка вручную с помощью Services.msc, скриптов PowerShell или других методов.

Конфигурация сети

Убедитесь, что устройства могут достичь необходимые конечные точки Центра обновления Windows через брандмауэр. Например, для Windows 10 версии 2004 следующие протоколы должны иметь возможность достигать следующих конечных точек:

Протокол	URL-адрес конечной точки
TLS 1.2	`*.prod.do.dsp.mp.microsoft.com`
HTTP	`emdl.ws.microsoft.com`
HTTP	`*.dl.delivery.mp.microsoft.com`
HTTP	`*.windowsupdate.com`
HTTPS	`*.delivery.mp.microsoft.com`
TLS 1.2	`*.update.microsoft.com`
TLS 1.2	`tsfe.trafficshaping.dsp.mp.microsoft.com`

> ⓘ **Примечание**
>
> Не используйте протокол HTTPS для конечных точек, которые указывают HTTP, и наоборот. Подключение приведет к ошибке.

Конкретные конечные точки могут отличаться в разных версиях Windows. Для примера см. раздел Конечные точки подключения Windows 10 Корпоративная 2004. Похожие статьи для других версий клиента Windows доступны в содержании рядом.

Оптимизация пропускной способности скачивания

Настройка оптимизации доставки для общего доступа к одноранговой сети или подключенного кэша Майкрософт.

Устранение неработоспособных устройств

В ходе опроса численности устройств вы можете обнаружить устройства с системными проблемами, которые могут мешать установке обновлений. Настало время устранить эти проблемы.

- **Мало места на диске:** Для успешной установки исправлений требуется не менее 2 ГБ. Обновления компонентов требуют от 8 ДО 15 ГБ в зависимости от конфигурации. В Windows 10 версии 1903 и более поздних (и Windows 11) можно заранее использовать функцию "зарезервированного хранилища" (для очистки и загрузки, перестроек и новых сборок), чтобы избежать переполнения дискового пространства. Если вы найдете группу устройств, на которых недостаточно места на диске, часто можно устранить проблему, очислив файлы журнала и попросив пользователей очистить данные при необходимости. Рекомендуется удалить следующие файлы:
  - C:\Windows\temp
  - C:\Windows\cbstemp (хотя этот файл может потребоваться для исследования сбоев обновлений)
  - C:\Windows\WindowsUpdate.log (хотя этот файл может потребоваться для исследования сбоев обновлений)
  - C:\Windows.Old (эти файлы должны автоматически очищаться через 10 дней или могут запрашивать у пользователя устройства разрешение на очистку раньше, когда ограничено место на диске)

Вы также можете создавать и запускать скрипты для выполнения дополнительных действий по очистке на устройствах с правами администратора или использования групповая политика параметров.

- Очистите кэш Магазина Windows, запустив C:\Windows\sytem32\wsreset.exe.
- Оптимизируйте папку WinSxS на клиентском компьютере с помощью **Dism.exe /online /Cleanup-Image /StartComponentCleanup**.

- Сжать операционную систему, запустив **Compact.exe /CompactOS:always**.
- Удалите компоненты Windows по запросу, которые не нужны пользователю. Дополнительные рекомендации см. в разделе Функции по запросу .
- Перемещение известных папок Windows в OneDrive. Дополнительные сведения см. в статье Использование групповая политика для управления параметрами приложение синхронизации OneDrive.
- Очистите папку Распространения программного обеспечения. Попробуйте развернуть следующие команды в виде пакетного файла для запуска на устройствах, чтобы сбросить состояние загрузки windows Обновления:

  Консоль

  ```
  net stop wuauserv
  net stop cryptSvc
  net stop bits
  net stop msiserver
  ren C:\Windows\SoftwareDistribution C:\Windows\SoftwareDistribution.old
  net start wuauserv
  net start cryptSvc
  net start bits
  net start msiserver
  ```

- **Обновления приложений и драйверов:** Устаревшее программное обеспечение приложений или драйверов может препятствовать успешному обновлению устройств. Разверните все обновления от поставщиков для любых проблемных версий приложений или драйверов, чтобы устранить проблемы.
- **Коррупции:** В редких случаях устройство с повторяющимися ошибками установки может быть повреждено таким образом, что система не сможет применить новое обновление. Может потребоваться восстановить хранилище Component-Based из другого источника. Вы можете устранить проблему с помощью средства проверки системных файлов .

Подготовка возможностей

На этапе планирования вы определили конкретные изменения инфраструктуры и конфигурации, которые необходимо было реализовать для добавления новых возможностей в среду. Теперь можно перейти к реализации изменений, определенных на этапе плана. Чтобы получить новые возможности, вам потребуется выполнить следующие задачи более высокого уровня:

- Включите возможности в среде, реализовав изменения. Например, реализуйте обновления соответствующих шаблонов ADMX в Active Directory. Новые версии Windows будут оснащены новыми политиками, которые используются для обновления шаблонов ADMX.
- Проверьте новые изменения, чтобы понять, как они влияют на более широкую среду.
- Устраните все потенциальные проблемы, обнаруженные в результате проверки.

Подготовка пользователей

Пользователи часто чувствуют, что они вынуждены обновлять свои устройства случайным образом. Они часто не понимают, почему требуется обновление, и не знают, когда обновления будут применены к их устройствам заранее. Лучше всего обеспечить четкое информирование о предстоящих обновлениях с соответствующим предупреждением.

Для достижения этой цели можно использовать различные меры, например:

- Отправьте сообщение электронной почты с обзором обновления и о том, как оно будет развернуто во всей организации.
- Отправляйте пользователям персонализированные сообщения электронной почты об обновлении с конкретными сведениями.
- Установите крайний срок отказа для сотрудников, которые должны оставаться в текущей версии немного дольше из-за бизнес-потребности.
- Предоставление возможности добровольного обновления в удобное для пользователей время.
- Сообщите пользователям об обязательной дате установки обновления на всех устройствах.

Политики для соответствия требованиям обновлений, действий и взаимодействия с пользователем

Применяется к: ✅ Windows 11, ✅ Windows 10

Поддержание устройств в актуальном состоянии — лучший способ обеспечить их бесперебойную и безопасную работу.

Крайние сроки соответствия обновлений

Вы можете контролировать, как строго устройства должны надежно соответствовать требуемому расписанию обновлений, используя политики крайних сроков обновления. Компоненты Windows адаптируются в соответствии с этими крайними сроками. Кроме того, они могут найти компромисс между взаимодействием с пользователем и скоростью, чтобы соответствовать требуемым крайним срокам обновления. Например, они могут определять приоритеты взаимодействия с пользователем задолго до наступления крайнего срока, а затем определять приоритет скорости по мере приближения крайнего срока, при этом предоставляя пользователю некоторые возможности контроля.

Сроки

Начиная с Windows 10 версии 1903 и обновления для системы безопасности за август 2019 г. для Windows 10 версии 1709 и более поздних версий (включая Windows 11), была введена новая политика для **замены старых политик, похожих на крайний срок: укажите крайние сроки для автоматических обновлений и перезапусков**.

Старые политики начали применять крайние сроки после того, как устройство достигло `restart pending` состояния для обновления. Новая политика начинает обратный отсчет для крайнего срока установки обновления с момента публикации обновления и любой отсрочки. Кроме того, эта политика включает настраиваемый льготный период и возможность отказаться от автоматических перезапусков до достижения крайнего срока (хотя мы рекомендуем всегда разрешать автоматические перезапуски для максимальной скорости обновления).

Мы рекомендуем установить крайние сроки следующим образом:

- Крайний срок обновления качества в днях: 2
- Крайний срок обновления компонентов в днях: 2

Уведомления автоматически предоставляются пользователю в соответствующее время, и пользователи могут напомнить позже, перепланировать или немедленно перезапустить в зависимости от того, насколько истек крайний срок. Рекомендуется **не** задавать политики уведомлений, так как они автоматически настраиваются с соответствующими значениями по умолчанию. Исключением является использование киосков или цифровых вывесок.

Хотя мы рекомендуем три дня для обновлений качества и семь дней для обновлений компонентов, вы можете решить, что хотите больше или меньше, в зависимости от вашей организации и ее требований, и эта политика настраивается как минимум до двух дней.

> ⓘ **Внимание**
>
> Если устройству не удается подключиться к Интернету, оно не может определить, когда корпорация Майкрософт опубликовала обновление, поэтому оно не сможет применить крайний срок. Узнайте больше об устройствах с низкой активностью.

Льготные периоды

Вы можете задать период в днях для Windows, чтобы найти минимальное время автоматического перезапуска до принудительного перезапуска. Это особенно полезно в тех случаях, когда пользователь не был в течение многих дней (например, в отпуске), чтобы устройство не было вынуждено немедленно обновиться при возвращении пользователя.

Рекомендуется задать следующие параметры:

- Льготный период в днях: 5

После истечения крайнего срока и льготного периода обновления применяются автоматически, и перезапуск происходит независимо от времени активности.

Разрешить Windows выбрать время перезапуска

Windows может использовать взаимодействие с пользователем для динамического определения наименьшего прерывания автоматического перезапуска. Чтобы воспользоваться этой функцией, убедитесь, что параметр **ConfigureDeadlineNoAutoReboot** имеет значение **Отключено**.

Политики действий устройств

Для успешного завершения обновления системы Windows обычно требуется, чтобы устройство было активным и подключено к Интернету в течение по крайней мере шести часов с по крайней мере двумя непрерывными действиями. Устройство может иметь другие физические обстоятельства, которые препятствуют успешной установке обновления, например, если ноутбук работает от батареи, или пользователь выключил устройство до окончания часы активности и устройство не может соответствовать крайнему сроку.

Вы можете использовать параметры, приведенные в этом разделе, чтобы убедиться, что устройства доступны для установки обновлений в течение периода соответствия обновлений.

Часы активности

"Часы активности" определяют период времени, когда устройство должно использоваться. Как правило, перезапуски происходят вне этих часов. Windows 10 версии 1903 появились "интеллектуальные часы активности", которые позволяют системе изучать часы активности на основе действий пользователя, а не вам как администратору, который принимает решения для вашей организации или позволяет пользователю выбирать часы активности, которые сводят к минимуму период, когда система может установить обновление.

> ⓘ **Внимание**
>
> Если вы использовали параметр **Настроить часы активности** в предыдущих версиях Windows 10, эти параметры должны быть **отключены**, чтобы воспользоваться преимуществами интеллектуального времени активности.

Если вы все же настроили часы активности, рекомендуется задать для следующих политик значение **Отключено** , чтобы увеличить скорость обновления:

- Задержка автоматической перезагрузки. Хотя можно настроить для системы задержку перезапусков для пользователей, которые вошли в систему, этот параметр может отложить обновление на неопределенный срок, если пользователь всегда входил в систему или завершал работу. Вместо этого рекомендуется задать для следующих политик значение **Отключено**:
  - **Отключение автоматического перезапуска в часы активности**
  - **Нет автоматического перезапуска для пользователей, вошедшего в систему для запланированных автоматических обновлений**

> ⓘ **Примечание.**

> Политика **автоматической перезагрузки без входа пользователей для установки запланированных автоматических обновлений** никогда не создавалась в качестве CSP. В групповая политика эта политика работает не в точности согласно описанию. Эта политика не может привести к периоду перезагрузки качественных обновлений, учитывая, что многие пользователи никогда не выходить из системы. Вместо этого рекомендуется использовать крайний срок соответствия требованиям, а затем настроить без автоматической перезагрузки, чтобы предотвратить перезагрузку, не относясь к пользователю, до достижения крайнего срока. Для серверных устройств используйте параметр Настроить автоматическую Обновления 7 — уведомление об установке и уведомление о перезагрузке.

- Ограничение задержек перезапуска. Используя крайние сроки соответствия требованиям, пользователи получают уведомления о том, что будут происходить обновления, поэтому рекомендуется задать для этой политики значение **Отключено**, чтобы обеспечить соблюдение крайних сроков, чтобы исключить возможность задержки перезапуска пользователя за пределами параметров крайнего срока соответствия.

- **Не разрешайте пользователям утверждать обновления и перезагрузки**. Предоставление пользователям утверждения или участия в процессе обновления за пределами политик крайнего срока снижает скорость обновления и повышает риск. Для этих политик необходимо задать значение **Отключено**:
  - Update/RequireUpdateApproval
    - Эта политика является устаревшей и неприменима для Windows 11. Устаревшие политики могут быть удалены в будущем выпуске.
  - Update/EngagedRestartDeadline
    - Эта политика является устаревшей и неприменима для Windows 11. Устаревшие политики могут быть удалены в будущем выпуске.
  - Update/EngagedRestartDeadlineForFeatureUpdates
    - Эта политика является устаревшей и неприменима для Windows 11. Устаревшие политики могут быть удалены в будущем выпуске.
  - Update/EngagedRestartSnoozeSchedule
    - Эта политика является устаревшей и неприменима для Windows 11. Устаревшие политики могут быть удалены в будущем выпуске.
  - Update/EngagedRestartSnoozeScheduleForFeatureUpdates
    - Эта политика является устаревшей и неприменима для Windows 11. Устаревшие политики могут быть удалены в будущем выпуске.
  - Update/EngagedRestartTransitionSchedule
    - Эта политика является устаревшей и неприменима для Windows 11. Устаревшие политики могут быть удалены в будущем выпуске.

- Настройте автоматическое обновление. Правильно настроив политики для настройки автоматических обновлений, вы можете увеличить скорость обновления за счет обращения клиентов к серверу Windows Server Update Services (WSUS), чтобы он смог управлять ими. Рекомендуется задать для этой политики значение **Отключено**. Однако если вам нужно указать значения, убедитесь, что загрузка устанавливается автоматически, задав для групповая политика**значение 4**. Если вы используете Microsoft Intune, установите значение Сброс по умолчанию.

- **Разрешить автоматическую загрузку клиентский компонент Центра обновления Windows через лимитные сети**. Так как все больше устройств в основном используют передачу данных сотовой связи и не имеют доступа к Wi-Fi, рассмотрите возможность автоматического скачивания обновлений из сети с лимитным тарифом. Хотя параметр по умолчанию не разрешает загрузку по лимитной сети, установка этого значения **1** может увеличить скорость, позволяя пользователям получать обновления независимо от того, подключены они к Интернету или нет, при условии, что у них есть сотовая связь.

> ⓘ **Внимание**
>
> Более старые версии Windows не поддерживают интеллектуальные часы активности. Если на устройстве установлена версия Windows до Windows 10 версии 1903, рекомендуется задать следующие политики:
>
> - Настройте часы активности. Начиная с Windows 10 версии 1703, можно указать максимальный диапазон активных часов, который рассчитывается из времени начала активных часов. Рекомендуется задать для этого значения **значение 10**.
> - Запланируйте установку обновлений. В параметрах **Настройка автоматического Обновления** есть два способа управления принудительным перезапуском после указанного времени установки. Если вы используете **установку обновления по расписанию**, не включайте оба параметра, так как они, скорее всего, будут конфликтовать.
>   - **Укажите время автоматического обслуживания**. Этот параметр позволяет задать более широкие периоды обслуживания обновлений и гарантирует, что это расписание не конфликтует с активными часами. Рекомендуется задать для этого значения **значение 3** (соответствует 3:00). Если в середине рабочей смены находится 3:00, выберите другое время, по крайней мере за пару часов до начала запланированного рабочего времени.
>   - **Запланируйте время установки**. Этот параметр позволяет запланировать время установки для перезапуска. *Не* рекомендуется задавать значение

Отключено, так как это может конфликтовать с активными часами.

Политики питания

Для обновления устройства должны быть доступны в неактивные часы. Они не могут сделать это, если политики власти мешают им просыпаться. В нашей организации мы стремимся установить баланс между безопасностью и экологически чистыми конфигурациями. Мы рекомендуем следующие параметры, чтобы достичь того, что мы считаем подходящим компромиссом:

Для пользователя устройство либо включено, либо выключено, но для Windows существуют состояния, которые позволяют выполнять обновление (активно), а состояния, которые не выполняются (неактивно). Некоторые состояния считаются активными (спящий режим), но пользователь может подумать, что устройство выключено. Кроме того, существуют состояния питания (подключено к батарее), которые Windows проверяет перед запуском обновления.

Вы можете переопределить параметры по умолчанию и запретить пользователям изменять их, чтобы обеспечить доступность устройств для обновлений в неактивные часы.

> ⓘ **Примечание.**
>
> Один из способов убедиться, что устройства могут устанавливать обновления при необходимости, — научить пользователей поддерживать подключение устройств в неактивные часы. Даже с лучшими политиками устройство, которое не подключено, не будет обновляться даже в спящем режиме.

Мы рекомендуем следующие параметры управления питанием:

- Режим спящего режима (S1 или S0 с низким энергопотреблением в режиме простоя или современный режим ожидания). Когда устройство находится в спящем режиме, система, кажется, отключена, но если доступно обновление, оно может разбудить устройство, чтобы принять обновление. Энергопотребление в спящем режиме находится между работой (система полностью используется) и гибернации (S4 — самый низкий уровень питания перед завершением работы). Если устройство не используется, система, как правило, переходит в спящий режим, прежде чем перейти в режим гибернации. Проблемы с скоростью возникают, когда время между спящего режима и гибернации слишком короткое, а Windows не успеет завершить обновление. Спящий режим является важным параметром, так как

система может вывести систему из спящего режима, чтобы запустить процесс обновления, при условии, что достаточно энергии.

Задайте для следующих политик **значение Включить** или **Не настраивать** , чтобы разрешить устройству использовать спящий режим:

- Power/AllowStandbyStatesWhenSleepingOnBattery
- Power/AllowStandbyWhenSleepingPluggedIn

Задайте для следующих политик **значение 1 (спящий режим),** чтобы при закрытии пользователем крышки устройства система переходит в спящий режим и устройство имеет возможность выполнить обновление:

- Power/SelectLidCloseActionOnBattery
- Power/SelectLidCloseActionPluggedIn
- **Гибернации**. Когда устройство в режиме гибернации, энергопотребление низкое, и система не может проснуться без вмешательства пользователя, например нажатием кнопки питания. Если устройство находится в этом состоянии, оно не может быть обновлено, если оно не поддерживает устройство времени и сигнализации ACPI (TAD). При этом, если устройство, поддерживающее традиционный спящий режим (S3), подключено и доступно обновление Windows, состояние гибернации откладывается до завершения обновления.

> ⓘ **Примечание.**
>
> Это не относится к устройствам, поддерживающим современный режим ожидания (S0 с низким энергопотреблением). Чтобы проверка, какое состояние спящего режима системы (S3 или S0 с низким энергопотреблением) поддерживает устройство, можно запустить `powercfg /a` в командной строке. Дополнительные сведения см. в разделе **Параметры Powercfg**.

Время ожидания по умолчанию на устройствах, поддерживающих традиционный спящий режим, равно 3 часам. Рекомендуется не уменьшать эти политики, чтобы разрешить клиентский компонент Центра обновления Windows возможность перезагрузить устройство перед отправкой в гибернацию:

- Power/HibernateTimeoutOnBattery
- Power/HibernateTimeoutPluggedIn

Старые или конфликтующие политики

Каждый выпуск клиента Windows может вводить новые политики, чтобы улучшить работу как для администраторов, так и для их организаций. При выпуске новой клиентской политики мы либо выпускаем ее исключительно для этого выпуска и более поздних версий, либо вернемся к ней, чтобы сделать ее доступной в более ранних версиях.

> ⓘ **Внимание**
>
> Если вы используете групповая политика, обратите внимание, что мы не обновляем старые шаблоны ADMX, и для использования новой политики необходимо использовать более новый шаблон ADMX (1903). Кроме того, если вы используете средство MDM (Майкрософт или не майкрософт), вы не сможете использовать новую политику, пока она не будет доступна в интерфейсе средства.

Как администраторы, вы настроили и ожидаете определенное поведение, поэтому мы явно не удаляем старые политики, так как они были настроены для ваших конкретных вариантов использования. Однако если задать новую политику без отключения аналогичной более старой политики, может возникнуть конфликтное поведение, а обновления могут работать не так, как ожидалось.

> ⓘ **Внимание**
>
> Иногда администраторы настраивают устройства для получения групповая политика параметров и параметров MDM с сервера MDM, например Microsoft Intune. Конфликты политик обрабатываются по-разному в зависимости от того, как они в конечном итоге настроены:
>
> - Обновления Windows: параметры групповая политика имеют приоритет над MDM.
> - Microsoft Intune. Если задать разные значения для одной политики в двух разных группах, вы получите оповещение, и ни одна из политик не будет задана до устранения конфликта. Очень важно отключить конфликтующие политики, чтобы устройства в вашей организации следовало принимать обновления должным образом. Например, если устройство не реагирует на изменения политики MDM, проверка, чтобы узнать, задана ли аналогичная политика в групповая политика с разным значением. Если вы обнаружите, что скорость обновления не так высока, как ожидалось, или если некоторые устройства работают медленнее, чем другие, может потребоваться очистить все политики и

параметры и указать только рекомендуемые политики обновления. Сводный список рекомендуемых политик см. в справочнике по политикам и параметрам.

Ниже приведены политики, которые может потребоваться отключить, так как они могут снизить скорость обновления или существуют более удобные политики, которые могут конфликтовать.

- **Отложить период Обновления компонентов в днях**. Для максимальной скорости обновления лучше задать значение **0** (без отсрочки), чтобы можно было завершить обновление компонентов и предложить ежемесячные обновления для системы безопасности снова. Даже если требуется срочное обновление качества, которое необходимо быстро развернуть, лучше использовать **функцию приостановки Обновления**, а не устанавливать политику отсрочки. Вы можете выбрать более длительный период, если не хотите быть в курсе последних обновлений компонентов.
- **Отложить период Обновления качества в днях**. Чтобы свести к минимуму риск и увеличить скорость обновления, максимальное время, которое может потребоваться учитывать при оценке обновления с помощью другого круга устройств, составляет два-три дня.
- **Приостановить Обновления время начала компонента**. Установите значение **Отключено,** если не существует известной проблемы, требующей времени для ее решения.
- **Приостановите время начала Обновления качества**. Установите значение **Отключено,** если не существует известной проблемы, требующей времени на ее решение.
- **Крайний срок без автоматической перезагрузки**. Значение по умолчанию **отключено — задайте значение 0** . Рекомендуется автоматически пытаться перезапустить устройства при получении обновления. Windows использует взаимодействие с пользователем для динамического определения наименьшего прерывания перезапуска.

Существуют также дополнительные политики, которые больше не поддерживаются или заменены.

Last updated on 26.09.2025

Обновление базового плана

Статья • 18.03.2023

Область применения: Windows 10

> ⓘ **Примечание**
>
> Обновление базовых показателей в настоящее время недоступно для Windows 11.

Благодаря большому количеству различных политик, предлагаемых для клиента Windows, обновление базовых показателей предоставляет четкий список рекомендуемых параметров политики клиентский компонент Центра обновления Windows для ИТ-администраторов, которым требуется оптимальное взаимодействие с пользователем, а также достижение своих целей по обеспечению соответствия ежемесячным обновлениям. Полный список конфигураций политик см. в разделе Политики, включенные в базовый план обновления .

Зачем нужен базовый план обновления?

Обновление базовых показателей — это проверенное в отрасли решение, которое повышает скорость внедрения обновлений, а также обеспечивает высокое качество взаимодействия с пользователем. Независимо от того, только начинаете ли вы или настраиваете политики в течение многих лет, обновление базовых показателей поможет вам получить известное хорошее состояние с отличным взаимодействием с пользователем. Применение базовых показателей особенно полезно для организаций с многолетней конфигурацией политик, чтобы удалить затяжные ошибки конфигурации.

Обновление базовых показателей можно использовать для:

- для обеспечения соответствия параметрам конфигурации пользователей и устройств;
- для настройки параметров конфигурации. С помощью групповая политика можно настроить устройство со значениями параметров, указанными в базовом плане.

Базовый план обновления не влияет на политики предложения, независимо от того, используете ли вы отсрочки или целевую версию для управления тем, какие обновления предлагаются на устройствах и когда.

Политики, включенные в базовый план обновления

Базовый план обновления настраивает параметры в следующих групповая политика областях:

- Управление системой и питанием
- Компоненты Windows и оптимизация доставки
- Компоненты и клиентский компонент Центра обновления Windows Windows

Полный подробный список всех параметров и их значений см. в файле msft Windows Update.htm в наборе средств Update Baseline в Центре загрузки.

Разделы справки начать?

Набор средств Для обновления базовых показателей упрощает процесс, предоставляя ИТ-администраторам одну команду для загрузки базовых параметров в консоль управления групповая политика. Вы можете получить набор средств "Базовый план обновления " (входит в состав набора средств для обеспечения соответствия требованиям безопасности) в Центре загрузки.

В настоящее время набор средств "Базовый план обновления" доступен только для использования с групповая политика.

Настройка оптимизации доставки (DO) для Windows

Применяется к: ✅ Windows 11, ✅ Windows 10, ✅ Delivery Optimization

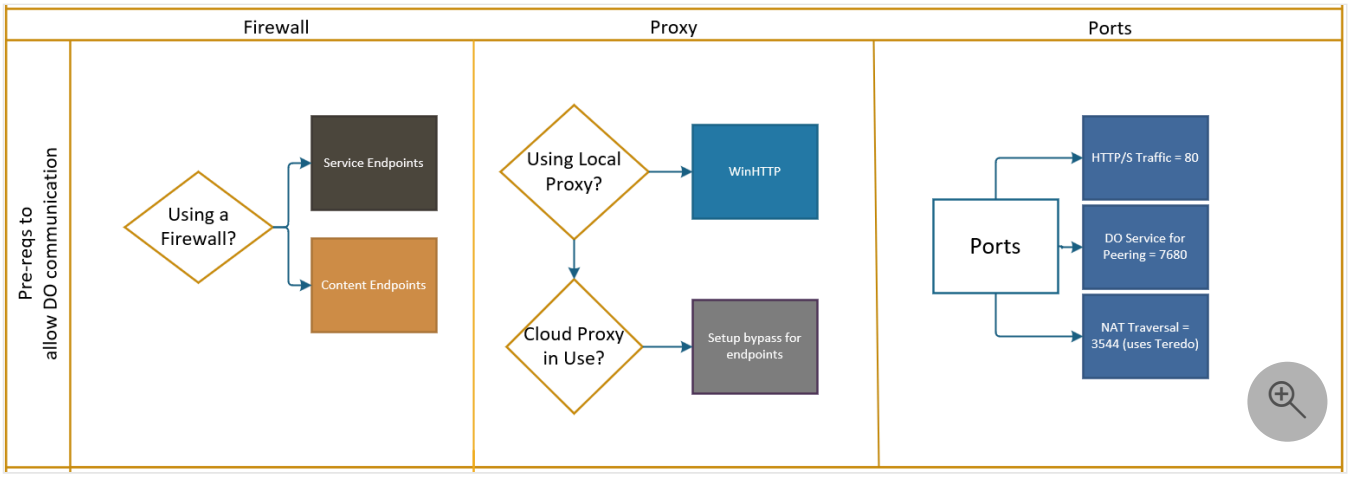
В этой статье описываются различные рекомендации по настройке оптимизации доставки (DO) в вашей среде.

Рекомендации по настройке оптимизации доставки

Используйте этот контрольный список, чтобы ознакомиться с различными аспектами при изменении конфигураций оптимизации доставки для вашей среды.

1. Предварительные требования для разрешения обмена данными по оптимизации доставки
2. Оцените политики оптимизации доставки на основе следующих элементов:
    - Топология сети
    - Размер организации
    - Системные ресурсы
    - Повышение эффективности P2P
3. Использование подключенного кэша Майкрософт
4. Выбор места для установки политик оптимизации доставки

1. Предварительные требования для разрешения обмена данными по оптимизации доставки



Оптимизация доставки (DO) используется для скачивания содержимого Майкрософт из разных источников (источника HTTP, одноранговых узлов и /или выделенного решения кэша). Для поиска лучших и надежных источников контента требуется взаимодействие между клиентом DO и службами. Чтобы эта технология работала, клиент DO, работающий на устройстве с Windows, должен иметь возможность связаться с облачной службой DO.

Узнайте больше о требованиях к параметрам брандмауэра, прокси-сервера и порта, чтобы включить обмен данными по оптимизации доставки.

Брандмауэр

Существуют конечные точки службы, которые необходимо разрешить через брандмауэр для взаимодействия со службой оптимизации доставки. Проверьте полный список разрешенных конечных точек.

Прокси-сервер

Чтобы обеспечить правильную работу одноранговых подключений (P2P), необходимо разрешить прямые вызовы к службе оптимизации доставки с устройств. При использовании прокси-сервера необходимо обойти вызовы из службы оптимизации доставки (*.prod.do.dsp.mp.microsoft.com).

Локальный прокси-сервер

Для скачивания из источников HTTP оптимизация доставки может использовать функцию автоматического обнаружения прокси-сервера WinHttp для обработки связи с прокси-сервером. Важно знать, что оптимизация доставки использует запросы диапазона байтов, поэтому вы захотите убедиться, что прокси-сервер разрешает эту возможность. Дополнительные сведения об использовании оптимизации доставки с прокси-сервером.

Облачный прокси-сервер

Если вы используете облачный прокси-сервер, вызовы к службе DO передаются через облачный прокси-сервер, а общедоступный IP-адрес устройств изменяется, что предотвращает правильную работу P2P. Чтобы избежать проблем, следует настроить его так, чтобы разрешить трафику оптимизации доставки обходить прокси-сервер. В противном случае может возникнуть снижение производительности и увеличение потребления пропускной способности.

Порты

Для оптимизации доставки требуется использование определенных портов для доставки содержимого. Убедитесь, что все необходимые порты открыты, чтобы оптимизация доставки работала без проблем.

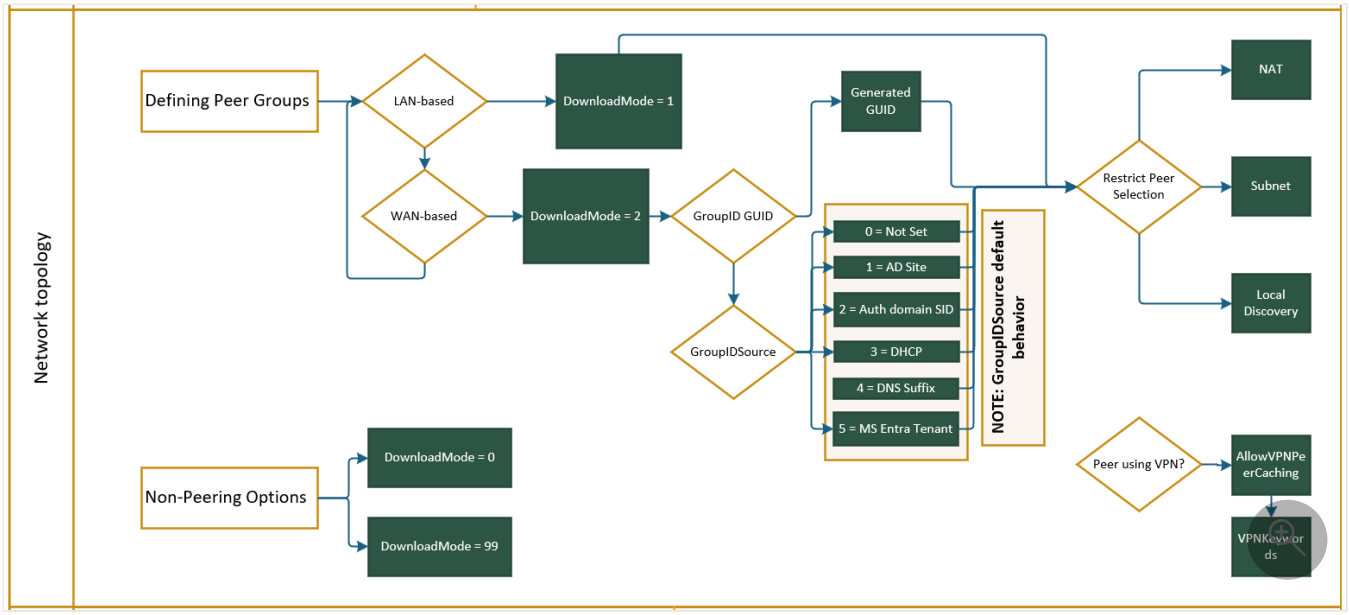
Развернуть таблицу

Port	Протокол	Функция
7680	TCP/IP	Прослушивание P2P с помощью TCP/IP
3544	UDP	Используйте Teredo для обнаружения и подключения к одноранговым узлам в разных NAT. Дополнительные сведения см. в документации по Teredo.
443	HTTPS/ TLS 1.2	Использование для обмена данными о клиенте и службе оптимизации доставки

2. Оценка политик оптимизации доставки

Существует ряд параметров оптимизации доставки для удовлетворения потребностей вашей среды. Чтобы в полной мере использовать оптимизацию доставки, следует сосредоточиться на ключевых областях, чтобы определить наиболее подходящие параметры для вашей уникальной среды.

2a. Топология сети



Одноранговые группы можно определить в разделе Оптимизация доставки с помощью сочетания параметров, таких как DODownloadMode, DOGroupID, DOGroupIDSource и DORestrictPeerSelection. *Сочетание используемых параметров зависит от нужных одноранговых групп и топологии сети.*

Параметры настройки пиринга

Оптимизация доставки может использовать P2P для повышения эффективности пропускной способности. В этом разделе описываются различные параметры, доступные для определения одноранговых групп для вашей среды.

Локальная сеть (LAN)

Чтобы определить группу одноранговых узлов, ограниченную локальной сетью, выберите DODownloadMode (1), режим локальной сети. Этот параметр режима загрузки включает все устройства, которые используют один и тот же общедоступный IP-адрес при подключении к Интернету (за тем же NAT) в одной одноранговой группе.

> ⓘ **Примечание.**
>
> Рассмотрите возможность использования режима загрузки групп и (или) ограничения выбора одноранговых узлов для подсети, если топология сети является звездообразной и периферийной.

Глобальная сеть (WAN)

Чтобы создать одноранговые группы между nat на одном сайте, через глобальную сеть или получить больший контроль в локальной среде, используйте режим скачивания "2", групповой режим. Режим загрузки групп позволяет определить уникальный идентификатор группы GUID или использовать существующие логические группы (например, сайт AD) на предприятии с параметром DOGroupIDSource для идентификации одноранговой группы.

Поведение По умолчанию GroupIDSource

Существует несколько вариантов идентификации идентификатора группы с помощью DOGroupIDSource. Поведение по умолчанию, если политики DOGroupID или DOGroupIDSource не заданы, заключается в определении идентификатора группы с помощью сайта AD (1), идентификатора домена с проверкой подлинности (2) или Microsoft Entra идентификатора клиента (5). Узнайте больше обо всех доступных параметрах DOGroupIDSource.

> ⓘ **Примечание.**
>
> Если одноранговая группа охватывает несколько nat, служба Teredo будет использоваться на порту 3544.
>
> Для Configuration Manager пользователей рекомендуется использовать существующие **группы границ** для определения одноранговых групп.

Ограничение выбора однорангового узла

Если вашей среде требуется более детализированный подход, можно использовать параметр ограничения обнаружения одноранговых узлов вместе с режимом загрузки, чтобы получить больше контроля. Например, если за одним NAT стоит несколько разных подсетей, но вы хотите ограничить группы одноранговых узлов одной подсетью, выберите DODownloadMode (1) и DORestrictPeerSelection (Подсеть). Этот параметр можно использовать в любом из одноранговых режимов загрузки (1, 2 или 3).

Параметры, не относящиеся к числу

Существует два допустимых режима загрузки, в которых не используются функции P2P для доставки содержимого; режимы скачивания (0) и (99). В режиме загрузки (0) используются дополнительные метаданные, предоставляемые службами оптимизации доставки, для однорангового, надежного и эффективного процесса скачивания. Режим

загрузки (99) обеспечивает надежную загрузку по протоколу HTTP из исходного источника загрузки или майкрософт без других проверок.

Пиринг с ПОМОЩЬЮ VPN

По умолчанию, если оптимизация доставки обнаруживает VPN, пиринг не используется. Чтобы изменить это поведение, используйте политику DOAllowVPNPeerCaching . Клиент оптимизации доставки ищет в строках "Description" и "FriendlyName" сетевого адаптера, чтобы определить использование VPN. Чтобы обеспечить большую гибкость для идентификации VPN, используйте DOVpnKeywords , чтобы добавить дескрипторы для определенного VPN, используемого в вашей организации.

> ⓘ **Примечание.**
>
> Список ключевое слово по умолчанию — "VPN", "Secure" и "Виртуальная частная сеть". Например, "MYVPN" соответствует ключевое слово "VPN" и будет обнаружен как VPN-подключение.

2b. Размер организации

Оптимизация доставки предназначена для оптимальной работы в крупномасштабной среде с большим количеством устройств. В зависимости от размера среды следует оценить значение DOMinFileSizeToCache для оптимизации пиринга.

Минимальный размер файла для кэширования

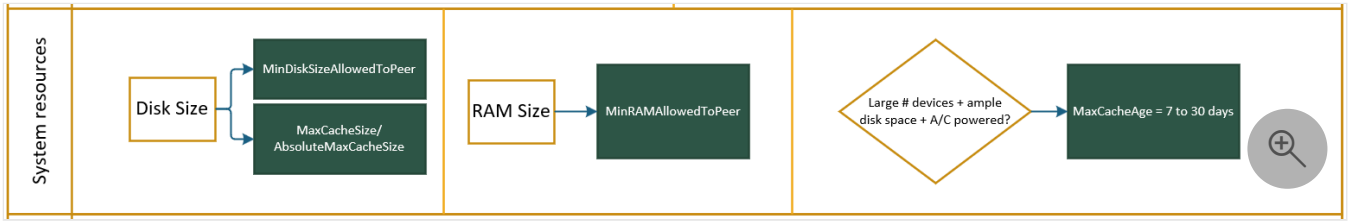
Пиринг содержимого имеет ограниченное количество слотов, доступных в любой момент времени. По умолчанию для пиринга можно использовать только файлы содержимого размером не более 50 МБ. В среде с более чем 30 устройствами измените doMinFileSizeToCache на меньшее значение (10 МБ), чтобы предоставить больше

содержимого для пиринга, которое можно распределить между многими устройствами. Для еще большего числа устройств (>100) этот параметр можно увеличить до (1 МБ).

Мобильные устройства

По умолчанию возможности P2P не включены для устройств, использующих батарею. Если в вашей среде много мобильных устройств, попробуйте включить политику DOMinBatteryPercentageAllowedToUpload до 60 %, чтобы использовать пиринг от аккумулятора.

2c. Системные ресурсы



Существуют некоторые конфигурации оптимизации доставки, которые могут повлиять на доступность различных системных ресурсов.

Размер диска

Измените минимальный размер диска (по умолчанию — 32 ГБ). Устройство должно использовать пиринг с параметром DOMinDiskSizeAllowedToPeer .

Оптимизация размера кэша

Вы также можете управлять объемом пространства, используемого кэшем оптимизации доставки, используя следующие параметры: DOMaxCacheSize (по умолчанию — 20 %) и DOAbsoluteMaxCacheSize (по умолчанию не настроено).

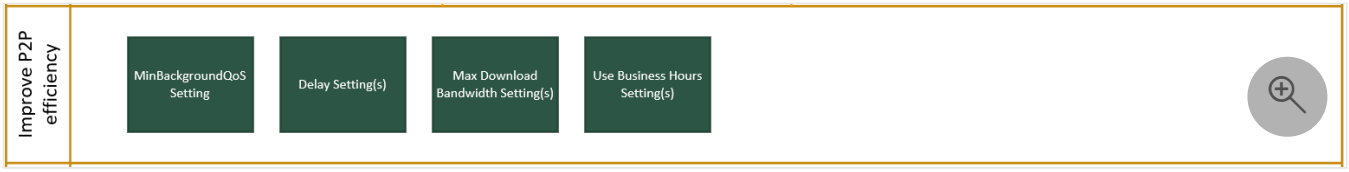
Размер ОЗУ

Управляйте минимальным объемом ОЗУ (включительно), разрешенным для использования однорангового кэширования (по умолчанию — 4 ГБ), с помощью DOMinRAMAllowedToPeer.

Большое количество устройств с неактивными системными ресурсами

В среде с подключенными устройствами и имеющими достаточно свободного места на диске, попробуйте увеличить интервал истечения срока действия содержимого DOMaxCacheAge до семи или более (до 30 дней). Вы можете воспользоваться преимуществами этих устройств, используя их в качестве отличных источников отправки для отправки большего количества содержимого в течение более длительного периода времени.

2d. Повышение эффективности P2P



Хотите повысить эффективность P2P? Ниже перечислены некоторые из наиболее эффективных параметров, которые можно изменить, которые могут оказать значительное влияние на вашу среду:

- Помогите оптимизировать одноранговое подключение через HTTP-подключения с помощью политики DOMinBackgroundQoS . Хорошее значение для политики DOMinBackgroundQoS — это то, что ниже средней скорости скачивания, наблюдаемой в вашей сети. Например, если средняя скорость составляет 1000 КБ/с, установите для этой политики значение 500 КБ/с.

- Повысьте вероятность скачивания с одноранговых узлов и (или) сервера кэша, отложив время попыток DO для создания подключений, прежде чем вернуться к источнику HTTP. К набору политик, связанных с задержками, относятся:
  - DODelayBackgroundDownloadFromHttp
  - DODelayForegroundDownloadFromHttp

  Чтобы повысить эффективность одноранговых узлов или выделенного сервера кэша, хорошей отправной точкой является 60 секунд для фоновых параметров и 30 секунд для параметров переднего плана.

> ⓘ **Примечание.**
>
> Не все типы контента доступны для P2P. Дополнительные сведения см. в **полном списке** .

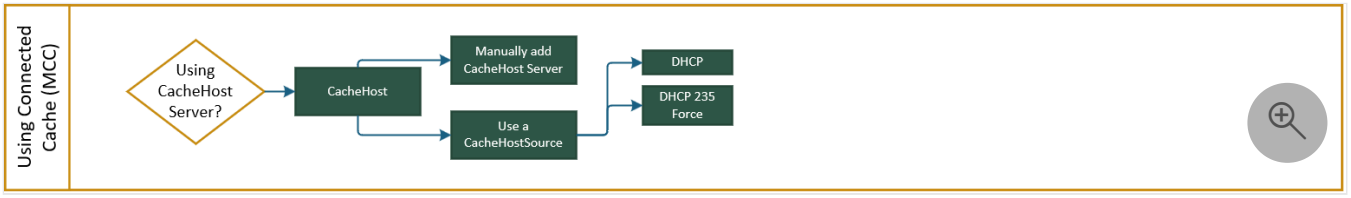
Параметры регулирования пропускной способности

Независимо от P2P, рекомендуется задать следующие политики, чтобы избежать нарушения работы сети.

- Управление использованием сети в виде процентного или абсолютного значения. К этим политикам относятся:
  - DOPercentageMaxBackgroundBandwidth
  - DOPercentageMaxForegroundBandwidth
  - DOMaxBackgroundDownloadBandwidth
  - DOMaxForegroundDownloadBandwidth
- Уменьшите количество сбоев, регулируя их по-разному в разное время суток с помощью следующих политик рабочего времени:
  - DOSetHoursToLimitBackgroundDownloadBandwidth
  - DOSetHoursToLimitForegroundDownloadBandwidth.

> ⓘ **Примечание.**
>
> Абсолютные политики рекомендуются в средах с низкой пропускной способностью.

3. Использование подключенного кэша

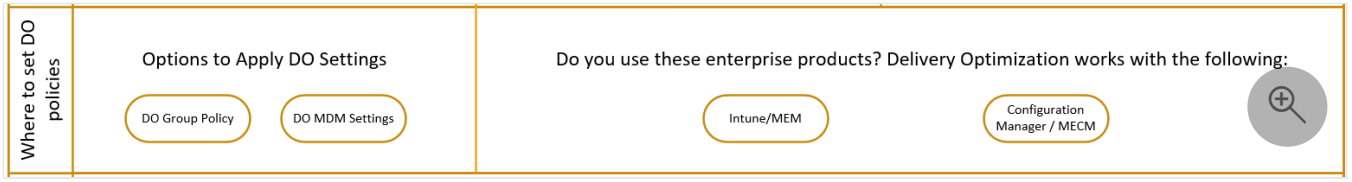


> ⓘ **Примечание.**
>
> Если настроено несколько серверов подключенного кэша, клиент оптимизации доставки подключается к ним в том порядке, в который они отображаются в списке. Если вы включили параметры задержки для резервного размещения сервера кэша, задержка источника отката к HTTP применяется к каждому скачиванию нового файла. Эта задержка не привязана ни к одному конкретному серверу кэша.

- DOCacheHost — это список имен серверов узла кэша, разделенных запятыми.
- DOCacheHostSource можно использовать для динамического обнаружения серверов узлов кэша в сети с помощью DHCP.
- DelayCacheServerFallbackBackground и DelayCacheServerFallbackForeground — это политики задержки, помогающие повысить вероятность извлечения содержимого с серверов узла кэша сети. (См. рекомендуемые значения в разделе Повышение эффективности P2P выше).

- DODisallowCacheServerDownloadsOnVPN позволяет управлять сервером узла кэша для предоставления содержимого, если устройство подключено к VPN-подключению.

4. Выбор места для установки политик оптимизации доставки



Групповые политики

Используйте групповая политика для управления параметрами оптимизации доставки.

`Computer Configuration\Administrative Templates\Windows Components\Delivery Optimization`

Политики MDM

Используйте MDM для управления параметрами оптимизации доставки.

`.Vendor/MSFT/Policy/Config/DeliveryOptimization/`

Оптимизация доставки интегрирована как с Microsoft Endpoint Manager, так и с Configuration Manager.

- Microsoft Endpoint Manager (MEM)
- Microsoft Endpoint Configuration Manager (MECM)

Сводка основных рекомендаций по настройке

Развернуть таблицу

Вариант использования	Политика	Рекомендуемое значение
Использование P2P	DownloadMode	1 или 2
Не используйте P2P	DownloadMode	0

Вариант использования	Политика	Рекомендуемое значение
Количество устройств в организации	MinFileSizeToCache	1 МБ для одноранговой группы > 100 устройств
Неактивные системные ресурсы	MaxCacheAge	7 дней (604800 секунд)
Повышение эффективности P2P	MinBackgroundQoS и DelayBackgroundDownloadFromHttp / DelayForegroundDownloadFromHttp	500 КБ/с и 60/30 секунд
Использование подключенного кэша	DelayCacheServerFallbackBackground / DelayCacheServerFallbackForeground	60/30 секунд

Корпоративный, использующий Intune

Чтобы легко узнать о настройке оптимизации доставки в Intune, проверка в этом руководстве, ориентированном на предприятия, с полезными рекомендациями.

Мониторинг оптимизации доставки

Независимо от того, выбираете ли вы конфигурации оптимизации доставки по умолчанию или настраиваете их в соответствии с вашей средой, вы захотите отслеживать результаты, чтобы увидеть, как они повышают эффективность. Для мониторинга оптимизации доставки доступны следующие параметры:

- На клиентах просмотрите монитор активности, в котором отображается разбивка загрузок по источникам, средняя скорость и статистика загрузки за текущий месяц.
  - **Windows 11**: Параметры > клиентский компонент Центра обновления Windows > Монитор действий оптимизации > доставки дополнительных параметров >
  - **Windows 10**: Параметры > Обновление & монитора активности оптимизации > доставки безопасности >
- Отчеты клиентский компонент Центра обновления Windows для бизнеса предлагают отчет по оптимизации доставки. Дополнительные сведения см. в разделе Мониторинг оптимизации доставки.

Устранение неполадок с оптимизацией доставки

Может быть много разных причин, по которым оптимизация доставки не работает в вашей среде. Узнайте больше о средстве устранения неполадок DO и распространенных проблемах и решениях, которые помогут улучшить работу с оптимизацией доставки.

Оптимизация доставки тестов

Узнайте больше о руководстве по базовым сценариям тестирования, чтобы узнать, как работает оптимизация доставки.

Last updated on 04.08.2025

Настройка BranchCache для обновлений клиентов Windows

Статья • 17.11.2023 • Применяется к: ✅ Windows 10

> **Ищете информацию для потребителей?** См. раздел Центр обновления Windows: вопросы и ответы

BranchCache — это компонент для оптимизации пропускной способности, впервые появившийся в операционных системах Windows Server 2008 R2 и Windows 7. Каждый клиент имеет кэш и выполняет роль альтернативного источника содержимого, которое запрашивают устройства в собственной сети этого клиента. Windows Server Update Services (WSUS) и Microsoft Configuration Manager могут использовать BranchCache для оптимизации пропускной способности сети во время развертывания обновлений, и это легко настроить для любого из них. BranchCache может работать в двух режимах: режим распределенного кэша и режим размещенного кэша.

- Режим распределенного кэша работает аналогично функции оптимизации доставки в клиенте Windows: каждый клиент содержит кэшированную версию запрашиваемых файлов с поддержкой BranchCache и выступает в качестве распределенного кэша для других клиентов, запрашивающих тот же файл.

  > **Совет**
  >
  > Режим распределенного кэша предпочтителен, чем режим размещенного кэша для обновлений клиентов Windows, чтобы получить максимальную выгоду от одноранговой распределения.

- В режиме размещенного кэша определенные серверы в определенных расположениях выполняют роль кэша для файлов, запрашиваемых локальными клиентами. Затем не клиенты получают файлы из скрытого источника, а сервер размещенного кэша предоставляет содержимое от своего имени.

Подробнее о принципах работы режимов распределенного и размещенного кэша см. в разделе Обзор BranchCache.

Настройка клиентов для BranchCache

Независимо от того, используете ли вы BranchCache с Configuration Manager или WSUS, каждый клиент, использующий BranchCache, необходимо соответствующим образом настроить. Обычно настройка выполняется через групповую политику. Пошаговые инструкции по настройке BranchCache для клиентов Windows с помощью групповая политика см. в разделе Конфигурация клиента в руководстве По раннему внедрению BranchCache.

В Windows 10 версии 1607 агент Центра обновления Windows использует оптимизацию доставки по умолчанию, даже при получении обновлений от WSUS. При использовании BranchCache с клиентом Windows задайте **для параметра Режим загрузки** оптимизации доставки значение "100" (обход), чтобы клиенты могли использовать вместо этого протокол фоновой интеллектуальной службы передачи (BITS) с BranchCache. Инструкции по использованию BranchCache в режиме распределенного кэша с WSUS см. в разделе "WSUS и Configuration Manager с BranchCache в режиме распределенного кэша".

> ⓘ **Примечание**
>
> Параметр "**Режим загрузки**" 100 (обход) доступен только в Windows 10 версии 1607 и более поздних, но не в Windows 11. BranchCache не поддерживается для Windows 11.

Настройка серверов для BranchCache

Вы можете использовать WSUS и Configuration Manager с BranchCache в режиме распределенного кэша. BranchCache в режиме распределенного кэша легко настроить как для WSUS, так и для Microsoft Configuration Manager.

Пошаговое руководство по настройке BranchCache на устройствах с Windows Server см. в руководстве по развертыванию BranchCache (Windows Server 2012) или руководстве по развертыванию BranchCache (Windows Server 2016).

В дополнение к этим шагам существует одно требование для wsus, чтобы иметь возможность использовать BranchCache в любом режиме работы: сервер WSUS должен быть настроен для загрузки обновлений локально на сервере в общую папку. Так вы сможете выбрать публикацию BranchCache для общей папки. Что касается Configuration Manager, то вы можете включить BranchCache на точках распределения. Для режима распределенного кэша не требуется дополнительной настройки сервера.

Примечание

Configuration Manager поддерживает только режим распределенного кэша.

Проверка работоспособности выпуска Windows

Статья • 04.06.2024 • Применяется к: ✅ Windows 11, ✅ Windows 10

Страница работоспособности выпуска Windows в Центре администрирования Microsoft 365 позволяет просматривать последние сведения об известных проблемах с ежемесячными обновлениями Windows и обновлениями компонентов. Известная проблема — это проблема, которая влияет на устройства Windows и которая была обнаружена в ежемесячном обновлении Windows или обновлении компонентов. Страница работоспособности выпуска Windows предназначена для информирования об известных проблемах. Эти сведения можно использовать для устранения проблем, с которыми могут столкнуться пользователи. Вы также можете определить, когда и в каком масштабе развертывать обновление в организации.

Если вам не удается войти на портал администрирования Microsoft 365, проверьте страницу состояния работоспособности службы Microsoft 365 , чтобы проверить наличие известных проблем, не мешающих входу в клиент.

Чтобы получать информацию о последних обновлениях и выпусках, следите за @WindowsUpdate в Twitter.

Предварительные условия

Убедитесь, что для отображения страницы работоспособности выпуска Windows в Центре администрирования Microsoft 365 выполнены следующие предварительные требования:

- Одна из следующих лицензий:
  - Windows 10/11 Корпоративная E3 или E5 (входит в состав Microsoft 365 F3, E3 или E5)
  - Windows 10/11 для образовательных учреждений A3 или A5 (входит в состав Microsoft 365 A3 или A5)

- Войдите в Центр администрирования Microsoft 365 с помощью роли администратора.
  - Большинство ролей, содержащих это слово, `administrator` предоставляют доступ к странице работоспособности выпуска Windows, например администратор службы поддержки и администратор службы поддержки.

Дополнительные сведения см. в статье Назначение ролей администратора в Центре администрирования Microsoft 365.

> **Примечание**
>
> В настоящее время работоспособность выпуска Windows доступна для клиентов GCC Community Cloud (GCC), но недоступна для GCC High и DoD.

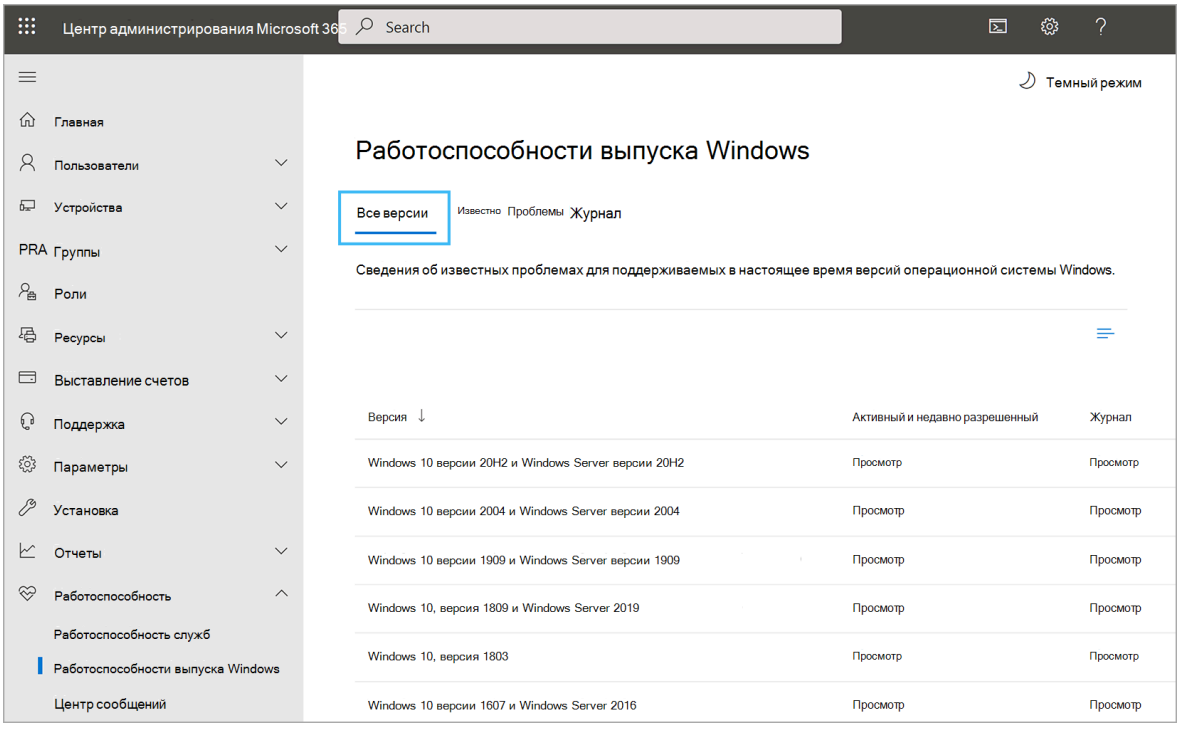
Просмотр сведений о работоспособности выпуска Windows

1. Перейдите в Центр администрирования Microsoft 365 и войдите с учетной записью администратора.

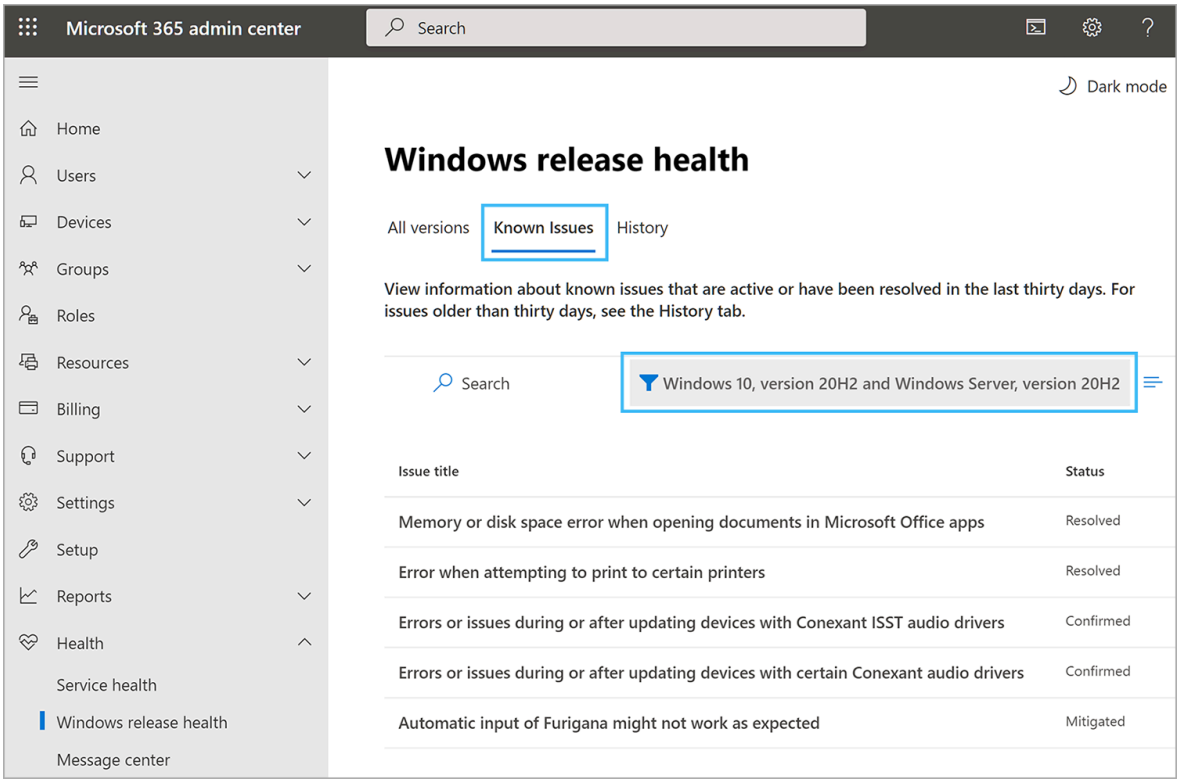
2. Чтобы просмотреть работоспособности выпуска Windows в Центре администрирования Microsoft 365, перейдите в раздел **Работоспособности** > **выпуска Windows**.

3. На странице **работоспособности выпуска Windows** у вас есть доступ к известной проблеме для всех поддерживаемых версий операционной системы Windows.

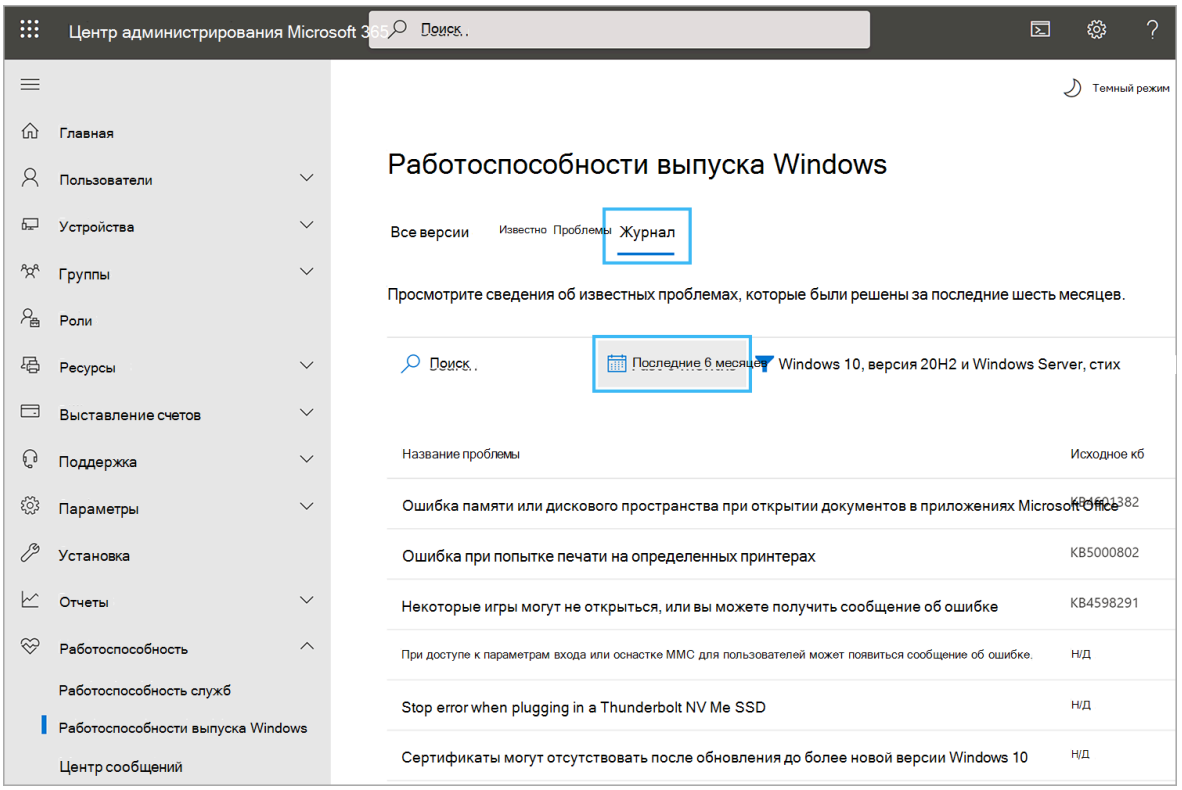
   На **вкладке Все версии** (представление по умолчанию) отображаются все продукты Windows с доступом к опубликованным известным проблемам.



Известная проблема — это проблема, которая была обнаружена в ежемесячном обновлении Windows или обновлении компонентов, влияющих на устройства Windows. В столбце **Активный и недавно разрешенный** столбец содержит ссылку на вкладку **Известные проблемы** , отфильтрованную по выбранной версии. На вкладке **Известные проблемы** отображаются известные проблемы, активные или разрешенные в течение последних 30 дней.



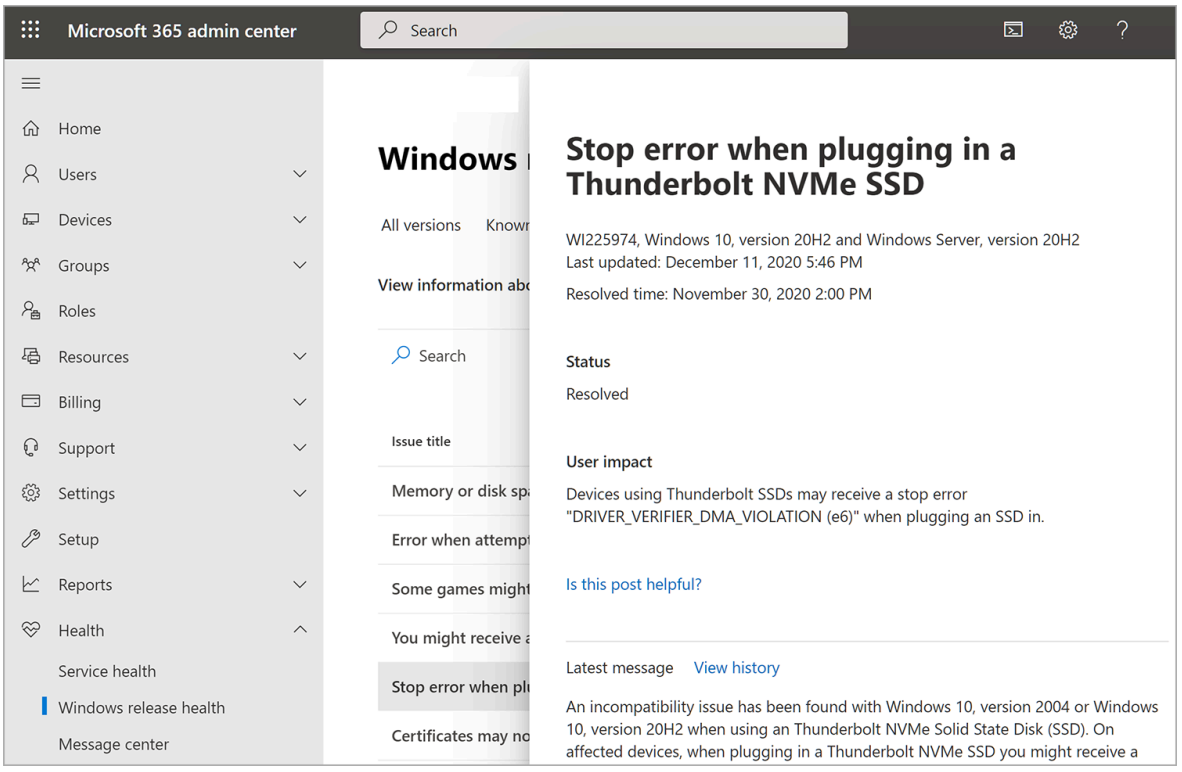
На вкладке **Журнал** отображается журнал известных проблем, которые были решены в течение 6 месяцев.



В сводке по известной проблеме содержатся следующие сведения:

- **Заголовок** — сводка по проблеме.
- **Версия** — имя затронутой версии продукта Windows.
- **Состояние** — текущее состояние проблемы.
- **Исходная база знаний** — номер базы знаний, в котором была впервые обнаружена проблема.
- **Исходная сборка** — номер сборки для базы знаний.

Выберите **заголовок Проблемы** , чтобы получить доступ к дополнительным сведениям, включая ссылку на журнал всех обновлений состояния, опубликованных во время работы над решением. Пример:



Регистрация для получения уведомлений по электронной почте

Вы можете зарегистрироваться для получения уведомлений по электронной почте об известных проблемах Windows и информационных обновлениях. Уведомления включают изменения в состоянии проблемы, новые обходные пути и решения проблем. Чтобы подписаться на уведомления, выполните приведенные далее действия.

1. Перейдите на страницу работоспособности выпуска Windows .
2. Выберите **Параметры**>**Электронная почта**, а затем выберите **Отправить мне уведомления по электронной почте о работоспособности выпуска Windows**.
3. Укажите следующие сведения:

    - Адрес электронной почты для уведомлений
        - Каждая учетная запись администратора может указать до двух адресов электронной почты в параметрах электронной почты.
    - Версии Windows, о которые необходимо получать уведомления

4. Нажмите **кнопку Сохранить** , когда вы закончите указывать адреса электронной почты и версии Windows. Чтобы эти изменения вступили в силу, может потребоваться до 8 часов.

> ⓘ **Примечание**

Если одна известная проблема затрагивает несколько версий Windows, вы получите только одно уведомление по электронной почте, даже если вы выбрали уведомления для нескольких версий. Повторяющиеся сообщения электронной почты не отправляются.

Работа с API обновлений Windows в Microsoft Graph

Если вы хотите разработать альтернативный способ получения сведений об известных проблемах, описанных в разделе Работоспособность выпуска Windows в Центре администрирования, можно использовать API обновлений Windows в Microsoft Graph.

API обновлений Windows содержит текущие и исторические известные данные о проблемах для любого поддерживаемого продукта Windows. Вы можете проверить, подтверждена ли проблема и доступно ли решение, прежде чем обращаться в службу поддержки или тратить время на устранение неполадок.

API обновлений Windows также содержит сведения о жизненном цикле продукта. Например, можно найти даты окончания обслуживания для всех поддерживаемых версий и выпусков Windows, которыми вы управляете в организации. Дополнительные сведения о том, как получить доступ к этим известным данным о проблемах и жизненном цикле, см. в разделе Тип ресурса продукта Microsoft Graph.

Примечание

Эти наборы данных Windows в настоящее время находятся в **справочнике по бета-версии конечной точки REST API Microsoft Graph**.

Определения состояния

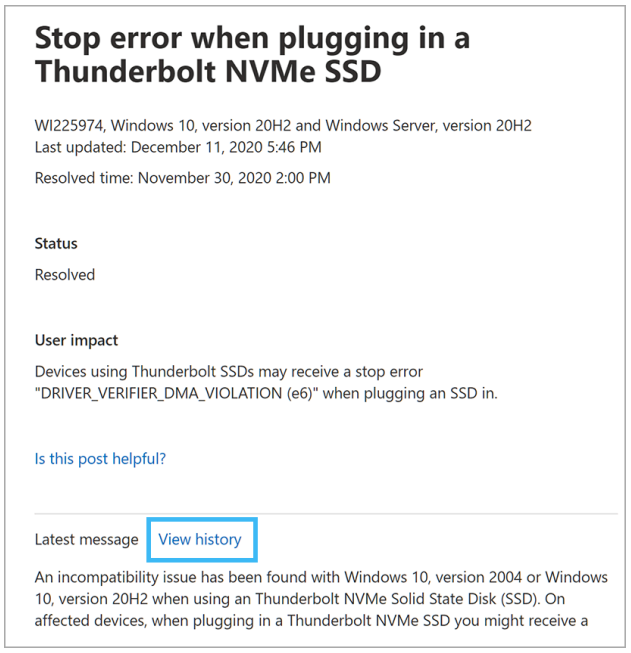
В интерфейсе **работоспособности выпуска Windows** каждой известной проблеме присваивается состояние. Эти состояния определяются следующим образом:

Развернуть таблицу

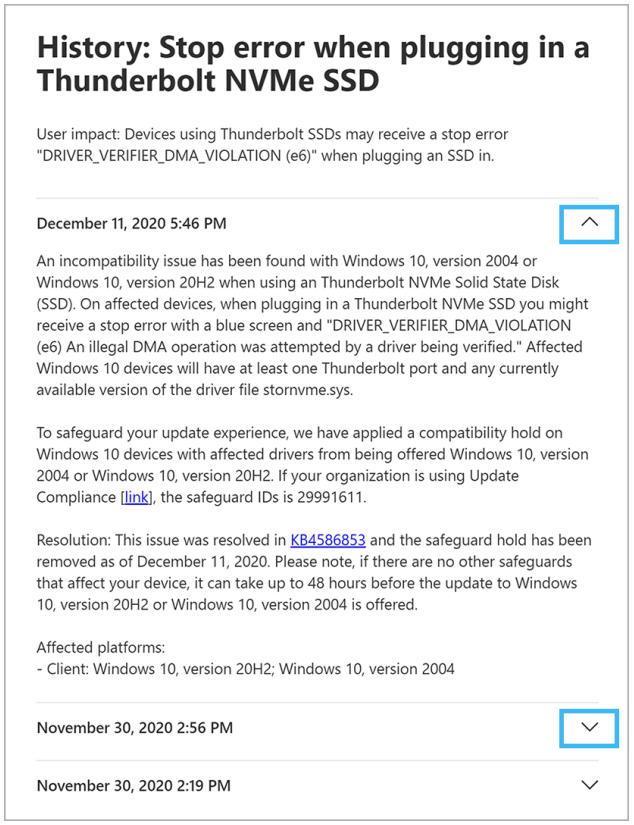
Состояние	Определение
Сообщили	Проблема была доведена до сведения команд Windows. На этом этапе нет подтверждения того, что это касается пользователей.
Исследование	Предполагается, что эта проблема затрагивает пользователей, и предпринимаются усилия по сбору дополнительных сведений о масштабах проблемы, шагах по ее устранению и первопричине.
Подтверждено	После тщательной проверки корпорация Майкрософт определила, что проблема влияет на пользователей Windows, и выполняется прогресс по шагам по устранению рисков и первопричине.
Устранены последствия	Решение доступно и сообщается клиентам Windows по известной проблеме. Известная проблема остается в этом состоянии до тех пор, пока корпорация Майкрософт не выпустит статью базы знаний для устранения известной проблемы.
Устранено: внешний	Решение доступно и сообщается клиентам Windows для известной проблемы, вызванной программным обеспечением или драйвером от стороннего производителя программного обеспечения или устройства. Известная проблема остается в этом состоянии до тех пор, пока не будет решена корпорацией Майкрософт или сторонним поставщиком.
Устранено	Решение было выпущено корпорацией Майкрософт и описано в статье базы знаний, которая устраняет известную проблему после его развертывания в среде клиента.
Устранено: внешний	Решение было выпущено корпорацией Майкрософт или сторонним поставщиком, которое устраняет известную проблему после развертывания в среде клиента.

Известный журнал проблем

На странице работоспособности выпуска Windows можно просмотреть журнал всех обновлений состояния, опубликованных для конкретной известной проблемы. Чтобы просмотреть все последние обновления, опубликованные для данной проблемы, выберите **Просмотр журнала** на странице сведений о проблеме.



Отобразится список всех обновлений состояния, опубликованных за выбранный период времени. Вы можете развернуть любую строку, чтобы просмотреть конкретные сведения, указанные в этом обновлении состояния.



Вопросы и ответы

Охват работоспособности выпусков Windows

- **Что такое работоспособности выпуска Windows?** Работоспособность выпуска Windows — это информационная служба Майкрософт, созданная для информирования лицензированных клиентов Windows об обнаруженных известных проблемах и важных объявлениях.

- **Содержимое о работоспособности службы Microsoft 365 относится к моим клиентам и службам. Является ли содержимое в работоспособности выпуска Windows специфичным для моей среды Windows?**
  Работоспособности выпуска Windows не отслеживает пользовательские среды и не собирает сведения о среде клиента. В системе работоспособности выпусков Windows все известные сведения о проблемах во всех поддерживаемых версиях Windows публикуются для всех подписываемых клиентов. Будущие итерации решения могут быть ориентированы на содержимое в зависимости от расположения клиента, отрасли или версии Windows.

- **Где найти работоспособности выпуска Windows?**
  После входа в Центр администрирования Microsoft 365 разверните меню слева, используя **... Показать все**, выберите **Работоспособности** , чтобы открыть меню **Работоспособности выпуска Windows** .

- **Содержимое о работоспособности выпуска Windows, опубликованное в Центре администрирования Microsoft 365, совпадает с содержимым о работоспособности выпуска Windows в Microsoft Learn?**
  Нет. Хотя содержимое похоже, вы можете увидеть больше проблем и больше технических сведений, опубликованных в windows release health в Центре администрирования Microsoft 365, чтобы улучшить поддержку ИТ-администратора. Например, вы найдете сведения, помогающие диагностировать проблемы в среде, шаги по устранению проблем и анализ первопричин.

- **Как часто будет обновляться содержимое?**
  Чтобы клиенты Windows получили важную информацию как можно скорее, все основные известные проблемы передаются клиентам Windows в Microsoft Learn и в Центре администрирования Microsoft 365. Мы также можем обновить сведения о работоспособности выпусков Windows в Центре администрирования Microsoft 365, если у нас есть дополнительные сведения об обходных решениях, первопричине или других сведениях, которые помогут вам спланировать обновления и устранить проблемы в вашей среде.

- **Можно ли предоставить общий доступ к этому содержимому или другим пользователям Windows?**

Работоспособности выпуска Windows предоставляется вам как лицензированному клиенту Windows и не предоставляется для общего доступа.

- **Является ли содержимое избыточным? Как упорядочено содержимое на разных вкладках?**
  Работоспособности выпуска Windows предоставляет три вкладки. Вкладка **"Все версии** " позволяет выбрать определенную версию Windows. На **вкладке Известные проблемы** отображается список проблем, которые были активны или устранены за последние 30 дней. На вкладке **Журнал** отображается шестимесячный журнал известных проблем, которые были устранены.

- **Как найти сведения о версиях Windows, которые я управляем?**
  На вкладке **Все версии** можно выбрать любую версию Windows. Это действие переведет вас на вкладку **Известные проблемы** , отфильтрованную по выбранной версии. На **вкладке Известные проблемы** представлен список активных известных проблем и проблем, устраненных за последние 30 дней. Этот выбор сохраняется на протяжении всего сеанса, пока не изменится. На вкладке **Журнал** можно просмотреть список разрешенных проблем для этой версии. Чтобы изменить версии, используйте фильтр на вкладке .

Функции Центра администрирования Microsoft 365

- **Как лучше всего найти проблемы, влияющие на мою среду?**
  Вы можете искать страницы Центра администрирования Microsoft 365 с помощью ключевых слов. Для работоспособности выпуска Windows перейдите на нужную страницу продукта и выполните поиск по номерам базы знаний, номерам сборки или ключевым словам.

- **Как добавить других администраторов Windows?**
  В меню слева перейдите в раздел Пользователи, выберите вкладку Активные пользователи и следуйте инструкциям, чтобы добавить нового пользователя или назначить существующего пользователя **роль администратора службы поддержки**.

- **Почему не удается щелкнуть статью базы знаний на вкладках Известные проблемы или Журнал?**
  В описании проблемы вы найдете ссылки на статьи базы знаний. На вкладках "Известные проблемы" и "Журнал" вся строка является записью, доступной для перехода в область сведений о проблеме.

- **В Центре администрирования Microsoft 365 есть мобильное приложение, но я не вижу работоспособности выпуска Windows в меню Работоспособности. Это открытая проблема?**
  Мы работаем над созданием работоспособности выпусков Windows на мобильных устройствах в будущем выпуске.

Справка и поддержка

- **Что делать, если у меня возникла проблема с Windows, о ней не сообщается в работоспособности выпуска Windows?**
  Обратитесь за помощью в службу поддержки Premier, на веб-сайте службы поддержки Майкрософт или свяжитесь с обычными каналами поддержки Windows.

- **Когда они обратились в службу поддержки, они попросили у меня идентификатор консультанта. Что это такое и где это можно?**
  Идентификатор рекомендации можно найти в левом верхнем углу области сведений об известной проблеме. Чтобы найти ее, выберите известную проблему, по которую вы ищете помощь, выберите область **Сведения** , и вы найдете идентификатор под названием проблемы. Идентификатор — это буквы `WI` , за которыми следует число, аналогичное `WI123456`.

- **Как узнать больше о расширении использования Центра администрирования Microsoft 365?** Дополнительные сведения см. в документации по Центру администрирования Microsoft 365.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Документация по Windows Autopilot

Подготовка устройств Windows Autopilot и Windows Autopilot — это набор технологий, используемых для настройки и предварительной настройки новых устройств, подготовки их к продуктивному использованию.

Решения Windows Autopilot

НАЧАЛО РАБОТЫ

Сравнение подготовки устройств Windows Autopilot и Windows Autopilot

Общие сведения о подготовке устройства Windows Autopilot

ОБЗОР

Общие сведения о подготовке устройства Windows Autopilot

Требования

Отчеты и мониторинг

Общие сведения о Windows Autopilot

ОБЗОР

Обзор Windows Autopilot

Требования

Обзор регистрации устройств

Страница состояния регистрации

Регистрация устройств вручную

Учебники

УЧЕБНИК

Сценарии Windows Autopilot

Сценарии подготовки устройств Windows Autopilot

Сценарии и средства развертывания Windows

Статья • 01.09.2024

Чтобы успешно развернуть операционную систему и приложения Windows для вашей организации, важно понимать доступные средства, которые помогут в этом процессе. В этой статье рассматриваются наиболее часто используемые средства для развертывания Windows 10.

Корпорация Майкрософт предоставляет множество инструментов, служб и решений. К этим средствам относятся службы развертывания Windows (WDS), средство управления активацией корпоративных лицензий (VAMT), средство миграции пользовательской среды (USMT), диспетчер системных образов Windows (Windows SIM), среда предустановки Windows (Windows PE) и среда восстановления Windows (Windows RE). Эти средства сами по себе не являются полноценным решением. Объедините эти средства с такими решениями, как Configuration Manager, чтобы получить полное решение для развертывания.

В этой статье также рассматриваются различные типы эталонных образов, которые можно создавать, и почему эталонные образы полезны для большинства организаций.

Комплект средств для развертывания и оценки Windows

Пакет средств оценки и развертывания Windows (Windows ADK) содержит основные средства и технологии для оценки и развертывания, включая:

- Обслуживание образов развертывания и управление ими (DISM).
- Designer конфигурации Windows.
- Диспетчер системных образов Windows (Windows SIM).
- Средство миграции пользовательской среды (USMT).
- средство управления активацией корпоративных лицензий (VAMT).
- Среда предустановки Windows (Windows PE).
- Набор средств оценки Windows.
- Набор средств для повышения производительности Windows (WPT).

Дополнительные сведения доступны в следующих статьях.

- Скачайте и установите Windows ADK.

- Windows ADK для сценариев Windows для ИТ-специалистов.
- Общие сведения о наборах и средствах.

Обслуживание образов развертывания и управление ими (DISM)

DISM — это одно из средств развертывания, входящих в состав Windows ADK. Он используется для записи, обслуживания и развертывания загрузочных образов и образов операционной системы.

Сетевые и автономные образы служб DISM. Например, с помощью DISM можно установить microsoft платформа .NET Framework, пока Windows подключена. Это означает, что вы можете запустить установку в работающей операционной системе. Параметр `/LimitAccess` настраивает DISM для получения файлов только из локального источника. Пример:

Командная строка Windows

```
Dism.exe /Online /Enable-Feature /FeatureName:NetFX3 /All
/Source:D:\Sources\SxS /LimitAccess
```

Windows PowerShell можно использовать в Windows для многих функций, выполняемых **DISM.exe**. Эквивалентная команда в Windows с помощью PowerShell:

PowerShell

```
Enable-WindowsOptionalFeature -Online -FeatureName NetFx3 -All
-Source D:\Sources\SxS -LimitAccess
```

Дополнительные сведения о DISM см. в техническом справочнике по DISM.

Средство миграции пользовательской среды (USMT)

USMT — это средство резервного копирования и восстановления, которое позволяет переносить состояние пользователя, данные и параметры из одной установки в другую. Microsoft Configuration Manager использует USMT в процессе развертывания операционной системы.

USMT включает несколько средств командной строки, наиболее важными из которых являются **ScanState** и **LoadState**:

- **ScanState.exe**. Это средство выполняет резервное копирование пользовательского состояния.
- **LoadState.exe**. Это средство выполняет восстановление пользовательского состояния.
- **UsmtUtils.exe**: это средство дополняет функциональные возможности **вScanState.exe** и **LoadState.exe**.

Помимо этих средств, существуют также шаблоны XML, которые управляют переносимые данные. Вы можете настроить шаблоны или создать новые, чтобы управлять процессом резервного копирования с высоким уровнем детализации. USMT использует следующие термины для своих шаблонов:

- **Шаблоны миграции**. Шаблоны по умолчанию в USMT.
- **Пользовательские шаблоны**. Пользовательские шаблоны, которые вы создаете.
- **Шаблон конфигурации**. Необязательный шаблон **с именемConfig.xml** который можно использовать для исключения или включения компонентов при миграции без изменения других стандартных шаблонов XML.

USMT поддерживает сбор и восстановление данных и параметров из поддерживаемых в настоящее время версий Windows. Он также поддерживает миграцию с 32-разрядной операционной системы на 64-разрядную операционную систему, но не наоборот. Например, можно использовать USMT для миграции с Windows 10 x86 на Windows 11 x64.

По умолчанию USMT переносит множество параметров, большинство из которых связаны с профилем пользователя, а также с панель управления конфигурациями, типами файлов и т. д. Шаблоны по умолчанию, используемые в развертываниях Windows, — **этоMigUser.xml** и **MigApp.xml**. Эти два шаблона по умолчанию переносятся следующие данные и параметры:

- Папки из каждого профиля, включая папки из профилей пользователей, а также общие и общедоступные профили. Например, следующие папки:
  - Документы.
  - Видео.
  - Музыка.
  - Живопись.
  - Настольные ПК.

- Следующие типы файлов:

  `.accdb`, `.ch3`, `.csv`, `.dif`, `.doc*`, `.dot*`, `.dqy`, `.iqy`, `.mcw`, `.mdb*`, `.mpp`, `.one*`, `.oqy`, `.or6`, `.pot*`, `.ppa`, `.pps*`, `.ppt*`, `.pre`, `.pst`, `.pub`, `.qdf`, `.qel`, `.qph`, `.qsd`,

`.rqy`, `.rtf`, `.scd`, `.sh3`, `.slk`, `.txt`, `.vl*`, `.vsd`, `.wk*`, `.wpd`, `.wps`, `.wq1`, `.wri`, `.xl*`, `.xla`, `.xlb`, `.xls*`

> ⓘ **Примечание**
>
> - Звездочка (`*`) означает ноль или больше символов.
> - Расширения OpenDocument (`*.odt`, , `*.ods`), используемые приложениями Microsoft Office, `*.odp` по умолчанию не переносятся.

- Параметры компонентов операционной системы.
- Параметры приложения.

Эти параметры переносятся с помощью **шаблонов по** умолчаниюMigUser.xmlи **MigApp.xml** . Дополнительные сведения см. в статье Что выполняет миграция USMT? Дополнительные общие сведения о USMT см. в статье Общие сведения о средстве миграции пользовательской среды (USMT).

Конструктор конфигураций Windows

Конфигурация Windows Designer — это средство, предназначенное для создания пакетов подготовки, которые можно использовать для динамической настройки устройства Windows. Это средство полезно для настройки новых устройств без необходимости повторного создания образа устройства с помощью пользовательского образа.

Дополнительные сведения см. в разделе Пакеты подготовки для Windows.

Диспетчер системных образов Windows (Windows SIM)

Диспетчер системных образов Windows (Windows SIM) — это средство разработки **дляUnattend.xml** файлов. Sim-карта Windows обычно не требуется при использовании Microsoft Configuration Manager. Microsoft Configuration Manager автоматически создает и обновляет файл **Unattend.xml** на основе параметров, указанных в последовательности задач, главным образом в задаче **Применить параметры Windows**. Автоматизация в Microsoft Configuration Manager значительно упрощает общий процесс.

Дополнительные сведения см. в техническом справочнике по диспетчеру системных образов Windows.

средство управления активацией корпоративных лицензий (VAMT)

Если службы управления ключами (KMS) не используются, можно централизованно управлять несколькими ключами активации (MAK) с помощью средство управления активацией корпоративных лицензий (VAMT). Используйте это средство для установки ключей продуктов и управления ими в организации. VAMT также может активироваться от имени клиентов без доступа к Интернету, выступая в качестве прокси-сервера MAK.

VAMT также можно использовать для создания отчетов, переключения с MAK на KMS, управления активацией на основе Active Directory и управления активацией корпоративных лицензий Office. VAMT также поддерживает PowerShell. Например, чтобы получить сведения из базы данных VAMT, введите:

```
PowerShell

Get-VamtProduct
```

Дополнительные сведения о VAMT см. в следующих статьях:

- средство управления активацией корпоративных лицензий (VAMT).
- Технический справочник по VAMT.

Среда предустановки Windows (Windows PE)

Windows PE — это облегченная версия Windows, используемая в качестве платформы развертывания.

Среда предустановки Windows, как и любая другая операционная система, требует драйверов. Однако для этого не требуется полный набор драйверов. Для развертывания Windows требуется только минималистский набор драйверов. Обычно требуются только сетевые драйверы и драйверы хранилища. Среда предустановки Windows уже включает набор драйверов из коробки, поэтому большинство устройств работают без необходимости добавлять дополнительные драйверы.

Дополнительные сведения о Среде предустановки Windows см. в статье Windows PE (WinPE).

Среда восстановления Windows

Среда восстановления Windows (Windows RE) — это диагностика и набор средств восстановления, включенный в поддерживаемые в настоящее время версии Windows. Windows RE основана на Среде предустановки Windows. При необходимости Windows RE также можно расширить с помощью пользовательских средств. Если windows не запускается и Windows RE установлена, происходит автоматическая отработка отказа в Windows RE.

Дополнительные сведения о Windows RE см. в статье Среда восстановления Windows.

Службы развертывания Windows

Ниже перечислены main функции служб развертывания Windows (WDS).

- Поддержка загрузки PXE.
- Многоадресная рассылка.
- Разблокировка сети BitLocker.

При использовании WDS для развертывания операционной системы следует учитывать следующие рекомендации.

- WDS можно настроить для автономного режима или для интеграции с Active Directory. В большинстве сценариев рекомендуется использовать режим интеграции Active Directory.

- WDS имеет возможность управлять драйверами. Однако управление драйверами с помощью Microsoft Configuration Manager больше подходит для развертывания из-за его гибкости.

- WDS может предварительно подготовить неизвестные устройства как известный компьютер в Active Directory. Однако Microsoft Configuration Manager также имеет возможность промежуточного хранения неизвестных устройств как известных устройств в базе данных. В большинстве сценариев Microsoft Configuration Manager является лучшим решением для предварительно промежуточных устройств, так как он обеспечивает больший контроль и управление.

- С помощью WDS можно настроить параметры размера блока и размера окон по протоколу TFTP, чтобы повысить производительность и скорость скачивания во время загрузки PXE. Однако, хотя увеличение параметров TFTP может повысить производительность и скорость скачивания, это также может снизить надежность и вызвать сбои, включая снижение скорости скачивания. При определении параметров TFTP задействовано множество переменных,

включая сетевое оборудование, конфигурацию сети и совместимость устройств.

Для автономных WDS параметры TFTP можно настроить в консоли WDS на вкладке **TFTP** в свойствах сервера WDS. Сведения о Microsoft Configuration Manager см . в статье Настройка размеров блоков и окон RamDisk TFTP в точках распространения с поддержкой PXE.

Службы Windows Server Update Services

WSUS — это роль сервера в Windows Server, которая включает локальный репозиторий обновлений Майкрософт. После этого Центр обновления Майкрософт можно распространить с сервера WSUS на устройства в среде организации, не переходя на общедоступный сайт Центра обновления Майкрософт. WSUS предлагает контроль утверждения и отчеты о состоянии обновления в среде.

Дополнительные сведения о WSUS см. в разделе Windows Server Update Services (WSUS).

Единый расширяемый интерфейс встроенного ПО

Для инициализации и загрузки устройства используется единый расширяемый интерфейс встроенного ПО (**UEFI**). Это преемник BIOS, метод, используемый в течение многих лет для инициализации и загрузки устройства.

В этом разделе описаны преимущества UEFI по сравнению с BIOS, их отличия и влияние на развертывание операционной системы.

Введение в UEFI

Хотя BIOS успешно использовался на устройствах в течение многих лет, он имеет некоторые ограничения. Пример:

- 16-разрядный код
- 1 МБ адресного пространства
- Низкая производительность при инициализации ПЗУ
- Максимальный размер загрузочного диска MBR 2,2 ТБ

В качестве замены BIOS, UEFI имеет много функций, которых нет в BIOS. Windows может использовать многие из этих функций UEFI. UEFI имеет следующие функции, недоступные в BIOS:

- **Поддержка больших дисков** . Для UEFI требуется диск на основе таблицы разделов GUID (GPT). GPT поддерживает диски размером около 16,8 миллиона ТБ. GPT также поддерживает более 100 основных дисков.

- **Более быстрое время загрузки** . UEFI заменяет вызов прерывания BIOS INT 13h, что улучшает время загрузки, особенно при возобновлении гибернации.

- **Развертывание многоадресной рассылки** . Встроенное ПО UEFI может использовать многоадресную рассылку непосредственно при загрузке. В таких решениях, как WDS и Microsoft Configuration Manager, поддержка многоадресной рассылки доступна только при первой загрузке в Windows PE. С помощью UEFI многоадресная рассылка может выполняться непосредственно из UEFI.

- **Совместимость с более ранней версией BIOS** . Более старые устройства с UEFI имели реализацию UEFI, которая включала модуль поддержки совместимости (CSM), эмулирующий BIOS. Однако из-за широкой поддержки UEFI современные устройства, как правило, не имеют CSM и поэтому не совместимы с BIOS. Например, Windows 11 и более новые версии не поддерживают BIOS, поэтому работает только на современных устройствах с UEFI.

- **Архитектура, независимая от ЦП** . BIOS может работать как с 32-разрядной, так и с 64-разрядной версиями встроенного ПО. Однако все драйверы устройств встроенного ПО в системах BIOS должны быть 16-разрядными. Это ограничение влияет на производительность, и можно устранить только 64 КБ памяти. UEFI устраняет эти ограничения.

- **Драйверы, независимые от ЦП** . В системах BIOS дополнительные карты PCI должны содержать ПЗУ, который содержит отдельный драйвер для всех поддерживаемых архитектур ЦП. Это ограничение не требуется для UEFI, так как UEFI имеет возможность использовать образы кода байтов EFI (EBC). Образы EBC позволяют создать среду драйвера устройства, не зависят от процессора.

- **Гибкая среда предварительной операционной системы** . UEFI поддерживает приложение UEFI, которое может выполняться до загрузки ОС. Приложения UEFI обеспечивают множество дополнительных функций, таких как

диагностика, автоматическое исправление и возможность вызова домой для сообщения об ошибках.

- **Безопасная загрузка** . В настоящее время поддерживаемые версии Windows используют процесс проверки встроенного ПО UEFI, называемый безопасной загрузкой. При использовании безопасной загрузки UEFI гарантирует, что запускается только проверенный загрузчик операционной системы и что вредоносная программа не может переключить загрузчик.

Поддержка оборудования для UEFI

Что касается UEFI, оборудование делится на четыре класса устройств:

- **Устройства класса 0.** Устройствами этого класса являются BIOS или устройства, отличные от UEFI.
- **Устройства класса 1.** Устройства в этом классе ведут себя как стандартное устройство BIOS, но они работают внутри EFI. Они должны рассматриваться как обычные компьютеры на основе BIOS. Устройства класса 1 используют CSM для эмуляции BIOS.
- **Устройства класса 2.** Устройства в этом классе могут работать как устройство BIOS или как устройство UEFI. Процесс загрузки или конфигурация встроенного ПО устройства определяет режим. Устройства класса 2 используют CSM для эмуляции BIOS.
- **Устройства класса 3.** Устройства в этом классе являются устройствами только UEFI. Они не имеют обратной совместимости с BIOS. Устройства в этом классе должны работать под управлением операционной системы, поддерживающей UEFI. Все поддерживаемые в настоящее время версии Windows поддерживают UEFI. Устройства класса 3 не имеют CSM для эмуляции BIOS.

Как правило, все современные устройства относятся к устройствам класса 3. Устройства класса 0, класса 1 и класса 2 являются более старыми и больше не производятся.

Поддержка UEFI в Windows

- Windows 10 поддерживает версии UEFI для x86 и x64.
- Windows 11 и более поздних версий поддерживает только 64-разрядные версии UEFI.

- UEFI не поддерживает кроссплатформенную загрузку.
  - Устройства UEFI x64 могут работать только под управлением 64-разрядной операционной системы. Большинство современных устройств UEFI — x64.
  - Устройства UEFI x86 могут работать только под управлением 32-разрядной операционной системы. Для Windows только Windows 10 x86 поддерживает UEFI x86. Windows 11 и более поздних версий не поддерживает UEFI x86. Отсутствие поддержки UEFI x86 в Windows 11 обычно не является проблемой, так как устройства UEFI x86 встречаются редко.

Рекомендации по UEFI для развертывания операционной системы

Существует много вещей, которые влияют на развертывание операционной системы сразу после запуска на оборудовании на основе UEFI или EFI. Ниже приведены рекомендации, которые следует учитывать при работе с устройствами UEFI.

- Устройства класса 2 могут переключаться между BIOS и UEFI через встроенное ПО устройства. Убедитесь, что в встроенном ПО устройства выбран нужный режим для устройства. Корпорация Майкрософт рекомендует использовать устройства класса 2 в режиме UEFI из-за дополнительных преимуществ и безопасности, предоставляемых UEFI.

  При переключении устройства класса 2 с BIOS на UEFI необходимо выполнить одно из следующих двух действий:

  - Диск необходимо преобразовать из MBR в GPT, а затем секционировать соответствующим образом для поддержки UEFI. Это преобразование можно выполнить с помощью средства, например diskpart. Например, в то время как windows, работающей в BIOS, требуется только один раздел, который может быть FAT32 или NTFS, для Windows, работающей на устройстве UEFI, требуются следующие разделы:
    - Загрузочный/системный раздел FAT32.
    - Раздел ОС NTFS.
    - Раздел , зарезервированный майкрософт (MSR) (уникальный для Windows).
    - Раздел восстановления (необязательно).

    Так как существующий диск очищается в рамках этого процесса, необходимо выполнить следующие действия:
    - Windows необходимо переустановить.
    - Приложения необходимо переустановить.

    - Необходимо создать резервную копию и восстановить данные и параметры.

    Дополнительные сведения см. в разделе Разделы жесткого диска на основе UEFI/GPT.

  - Средство MBR2GPT.EXE можно использовать для преобразования диска из MBR в GPT для использования с UEFI неразрушающим способом. **MBR2GPT.EXE** также перенастраивает секционирование на диске с правильным секционированием, чтобы Windows запускала в UEFI. Преимущество использования **MBR2GPT.EXE** заключается в том, что он преобразует диск и повторно секционирует его без очистки диска и без потери данных. Так как диск не очищается и данные не будут потеряны, выполнять следующие действия не требуется:
    - Windows не требуется переустанавливать.
    - Приложения не нужно переустанавливать.
    - Резервное копирование и восстановление данных и параметров не требуется.

- При развертывании устройства класса 2 убедитесь, что для параметра загрузки задано правильное загрузочное устройство (жесткий диск, флэш-накопитель, PXE и т. д.). Параметры загрузки, доступные на устройствах класса 2, могут отличаться в режимах BIOS и UEFI.

- Когда устройство UEFI загружается с носителя, носитель должен быть FAT32. UEFI поддерживает загрузку только из разделов FAT32, поэтому загрузочный/системный раздел на диске — FAT32. Кроме того, FAT32 имеет ограничение размера файла в 4 ГБ. Образы ОС размером более 4 ГБ необходимо разделить с помощью такого средства, как DISM. Дополнительные сведения см. в разделе Split-WindowsImage или /Split-Image.

- UEFI не поддерживает загрузку между архитектурами. Устройствам x64 требуется загрузочный носитель x64, а устройствам x86 — загрузочный носитель x86.

- Большинство современных устройств UEFI — x64. Устройства UEFI x86 встречаются редко.

Дополнительные сведения о UEFI см. в обзоре встроенного ПО UEFI и связанных ресурсах.

Связанное содержимое

- Windows ADK для сценариев Windows для ИТ-специалистов.
- MBR2GPT.EXE.
- Разделы жесткого диска на основе UEFI/GPT.
- Встроенное ПО UEFI.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Назначение устройств каналам обслуживания для обновлений Windows

Статья • 19.10.2023 • Применяется к: ✅ Windows 11, ✅ Windows 10

> **Ищете информацию для потребителей?** См. раздел Центр обновления Windows: вопросы и ответы

Совет

Если вы не знакомы с каналами обслуживания или выпуска, сначала прочитайте **статью Каналы обслуживания** .

Канал общедоступной доступности — это канал обслуживания по умолчанию для всех Windows 10 и Windows 11 устройств, кроме устройств с установленным выпуском LTSC. В следующей таблице показаны каналы обслуживания, доступные для каждого выпуска.

Выпуск	Канал общей доступности	Long-Term Servicing Channel	Программа предварительной оценки
Домашняя	Нет	Нет	Да
Pro	Да	Нет	Да
Корпоративная	Да	Нет	Да
Корпоративная LTSC	Нет	Да	Нет
Pro для образовательных учреждений	Да	Нет	Да
Для образовательных учреждений	Да	Нет	Да

Примечание

Выпуск LTSC доступен только в **Центре корпоративного лицензирования Майкрософт**.

> **Примечание**
>
> Устройства будут автоматически получать обновления из канала общедоступной доступности, если только они не настроены на получение обновлений предварительной версии через программу предварительной оценки Windows.

Регистрация устройств в программе предварительной оценки Windows

Чтобы начать работу с программой предварительной оценки Windows для бизнеса, выполните следующие действия.

1. На веб-сайте программы предварительной оценки Windows выберите **Зарегистрировать**, чтобы зарегистрировать учетную запись Microsoft Entra организации.
2. Следуйте инструкциям, чтобы зарегистрировать клиент.
   Примечание: Для регистрации пользователя, выполнившего вход, необходимо быть **глобальным администратором** домена Microsoft Entra.
3. Убедитесь, что для параметра **Разрешить телеметрию** задано значение **2** или выше.
4. Для устройств Windows настройте политики для управления предварительными сборками и их доставкой:

Параметр **Управление предварительными сборками** позволяет администраторам включать и отключать установку предварительных сборок на устройстве. Можно также остановить предварительные сборки после официального выпуска.

- Групповая политика: **Конфигурация компьютера** > **Административные шаблоны** > **Компоненты Windows** > **Центр обновления Windows** > **Центр обновления Windows для бизнеса** - *Управление предварительными сборками*
- MDM: **Update/ManagePreviewBuilds**

Параметры **Уровня готовности ветви** позволяют выбирать между кругами предварительного просмотра и позволяют отложить или приостановить доставку обновлений.

- групповая политика: **Конфигурация компьютера/Административные шаблоны/Компоненты Windows/клиентский компонент Центра обновления Windows/ клиентский компонент Центра обновления Windows для бизнеса** - *Выберите, когда используются предварительные сборки и обновления компонентов Получил*
- MDM: **Update/BranchReadinessLevel**

Подробнее: Программа предварительной оценки Windows для бизнеса.

Блокирование доступа к программе предварительной оценки Windows

Чтобы предотвратить регистрацию устройств в организации в программе предварительной оценки для ранних выпусков Windows 10:

- групповая политика: Конфигурация компьютера\Административные шаблоны\Компоненты Windows\Сбор данных и предварительный просмотр сборок**Переключить пользовательский контроль над сборками предварительной оценки**
- MDM: поставщик служб конфигурации политики — System/AllowBuildPreview

> ⓘ **Важно!**
>
> Начиная с Windows 10 версия 1709 эта политика заменена на политику **Управление предварительными сборками**.
>
> - Групповая политика: **Конфигурация компьютера > Административные шаблоны > Компоненты Windows > Центр обновления Windows > Центр обновления Windows для бизнеса** - *Управление предварительными сборками*
> - MDM: **Update/ManagePreviewBuilds**

Развертывание обновлений клиента Windows с помощью служб Windows Server Update Services (WSUS)

Применяется к: ✅ Windows 11, ✅ Windows 10, ✅ WSUS

> **Ищете информацию для потребителей?** См. раздел Центр обновления Windows: вопросы и ответы

WSUS – это роль сервера Windows, доступная в операционной системе Windows Server. Это единый центр обновлений Windows в организации. WSUS позволяет компаниям не только откладывать обновления, но и выборочно утверждать их, выбирать, когда они будут доставлены, и определять, какие отдельные устройства или группы устройств получают их. СЛУЖБЫ WSUS обеспечивают дополнительный контроль над клиентский компонент Центра обновления Windows клиентскими политиками, но не предоставляют все параметры планирования и гибкости развертывания, предоставляемые Microsoft Configuration Manager.

При выборе WSUS в качестве источника обновлений Windows используется групповая политика для указания клиентских устройств Windows на сервер WSUS для их обновлений. Отсюда обновления периодически загружаются на сервер WSUS, где с помощью консоли администрирования или групповой политики осуществляется утверждение, развертывание и управление ими, тем самым оптимизируя управление обновлениями в организации. Если в настоящее время вы используете WSUS для управления обновлениями Windows в своей среде, вы можете продолжать делать это в Windows 11.

> ⓘ **Примечание.**
>
> СЛУЖБЫ WSUS устарели и больше не добавляют новые функции. Однако он по-прежнему поддерживается для производственных развертываний и получает обновления безопасности и качества в рамках жизненного цикла продукта. Дополнительные сведения см. в разделе Функции, удаленные или не разработанные в Windows Server.

Требования к обслуживанию клиентов Windows с помощью WSUS

Чтобы иметь возможность использовать WSUS для управления обновлениями компонентов Windows и их развертывания, необходимо использовать поддерживаемые службы WSUS в поддерживаемой версии операционной системы:

- Роль WSUS в Windows Server 2016
- Роль WSUS в Windows Server 2019 г.
- Роль WSUS в Windows Server 2022 г.
- Роль WSUS в Windows Server 2025

Дополнительные сведения о развертывании роли WSUS см. в статье Общие сведения о Windows Server Update Services (WSUS).

Масштабируемость WSUS

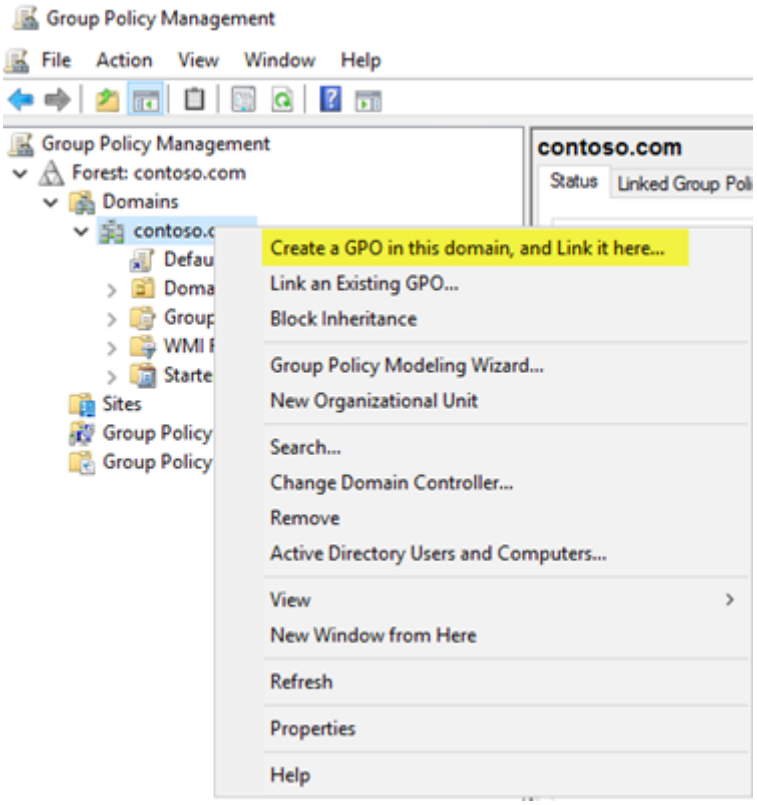
Чтобы использовать WSUS для управления всеми обновлениями Windows, некоторым организациям потребуется доступ к WSUS из сети периметра, либо придется реализовать какой-нибудь другой сложный сценарий. WSUS — это решение с широкими возможностями масштабирования и настройки для организаций любого масштаба, с любой структурой сайтов. Конкретные сведения о масштабировании WSUS, включая конфигурацию вышестоящий и подчиненных серверов, филиалы, балансировку нагрузки WSUS и другие сложные сценарии, см. в статье Развертывание Windows Server Update Services.

Настройка автоматических обновлений и обновление расположения службы

При использовании WSUS для управления обновлениями на клиентских устройствах Windows начните с настройки параметров групповых политик **Настройка автоматических обновлений** и **Размещение службы обновлений Майкрософт в интрасети** в своей среде. Это заставляет затронутые клиенты обращаться к серверу WSUS, чтобы он мог осуществлять управление ими. Следующий процесс описывает, как задать эти параметры и развернуть их на всех устройствах домена.

Настройка параметров групповых политик "Настройка автоматических обновлений" и "Размещение службы обновлений Майкрософт в интрасети" в вашей среде

1. Откройте консоль управления групповая политика (gpmc.msc).
2. Разверните *узел Лес\Домены\Your_Domain*.
3. Щелкните правой кнопкой мыши **Your_Domain**, а затем выберите **Создать объект групповой политики в этом домене и связать его здесь**.



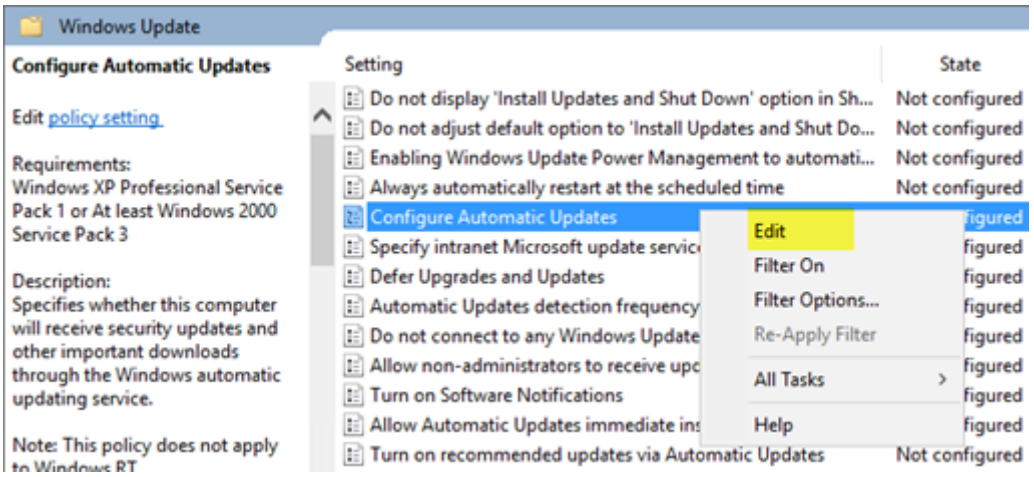
> ⓘ **Примечание.**
>
> В этом примере параметры групповых политик **Настройка автоматического обновления** и **Размещение службы обновлений Майкрософт в интрасети** указаны для всего домена. Это не обязательно; Эти параметры можно нацелить на любую группу безопасности с помощью фильтра безопасности или определенного подразделения.

4. В диалоговом окне **Новый объект групповой политики** назовите новый объект групповой политики **WSUS — автоматическое Обновления и расположение службы обновления интрасети**.

5. Щелкните правой кнопкой мыши объект групповой политики **WSUS — авто Обновления и расположение службы обновления интрасети**, а затем выберите **изменить**.

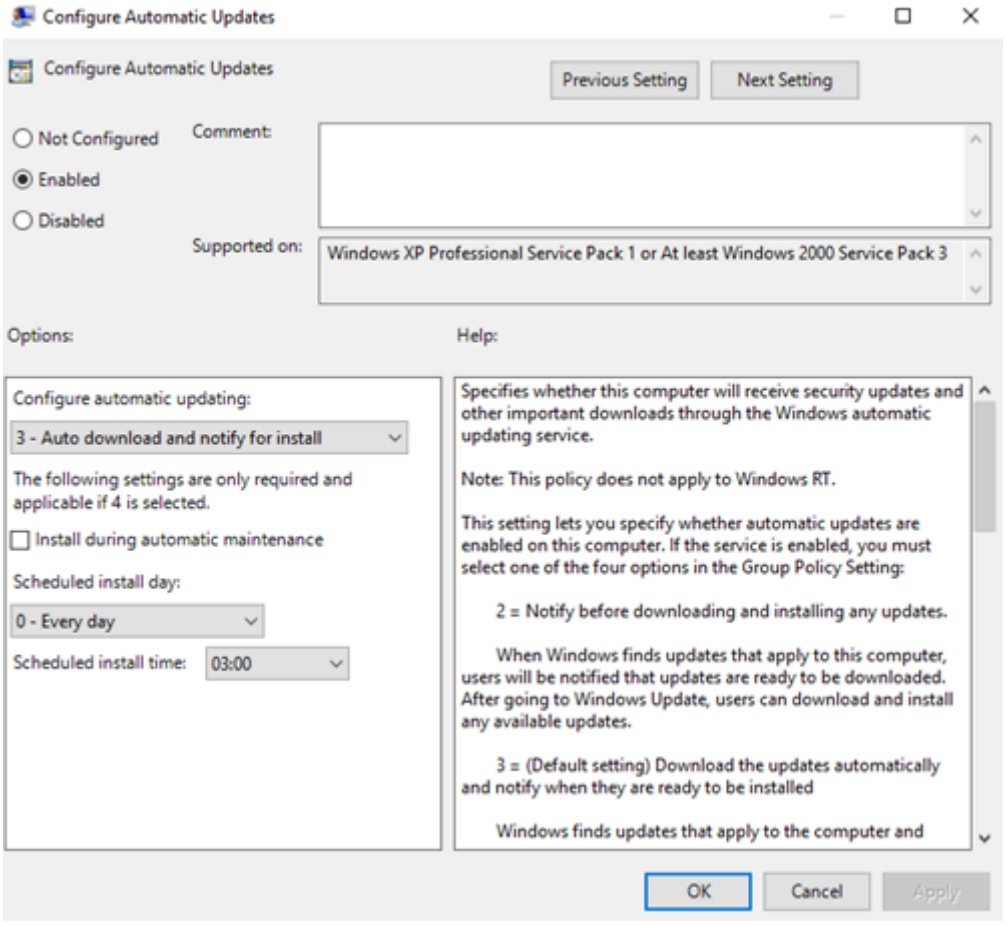
6. В редакторе управления групповыми политиками выберите Конфигурация компьютера\Политики\Административные шаблоны\Компоненты Windows\Центр обновления Windows.

7. Щелкните правой кнопкой мыши параметр **Настроить автоматический Обновления** и выберите **изменить**.



8. В диалоговом окне **Настройка автоматических обновлений** выберите **Включить**.

9. В разделе **Параметры** в списке **Настройка автоматического обновления** выберите **3 — Автоматическое скачивание и уведомление об установке**, а затем нажмите **кнопку ОК**.



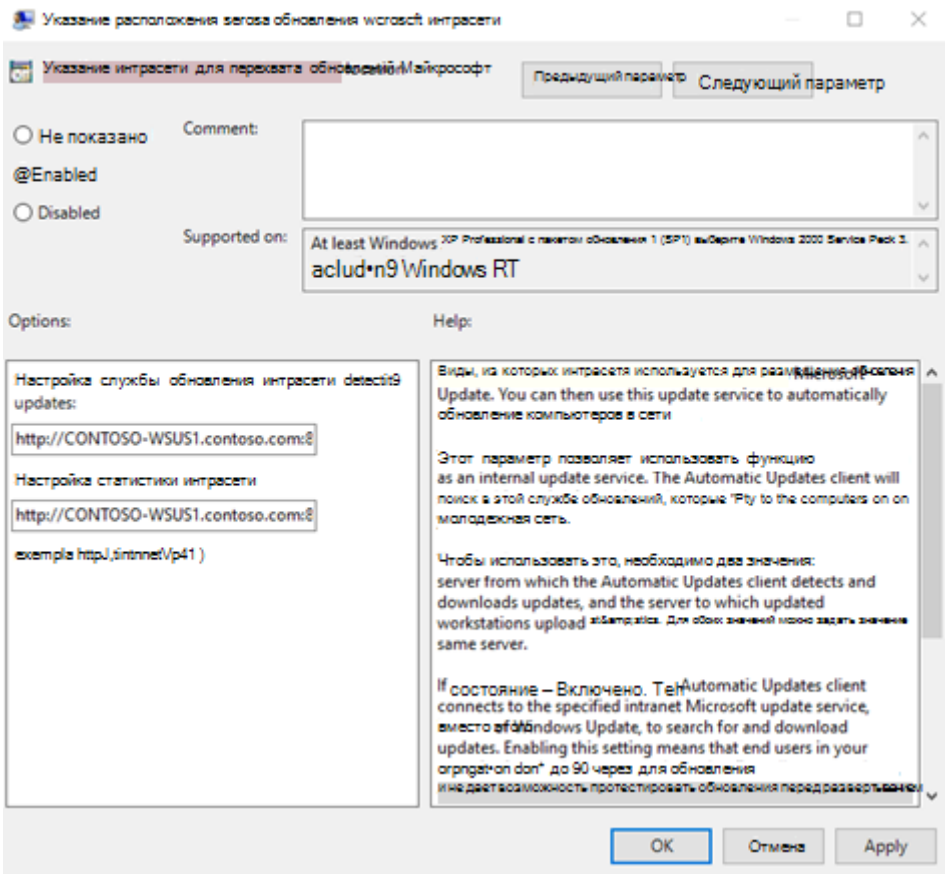
> **ⓘ Внимание**
>
> - Используйте Regedit.exe, чтобы проверка, что следующий ключ не включен, так как он может нарушить подключение к Магазину Windows: Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\DoNotConnectToWindowsUpdateInternetLocations

- Существуют три других параметра для автоматического скачивания и установки обновлений. В данном случае этот параметр используется исключительно для примера. Другие примеры контроля автоматических обновлений и других связанных политик см. в разделе [Настройка автоматических обновлений с использованием групповой политики](#).

10. Щелкните правой кнопкой мыши параметр **Указать расположение службы обновления Майкрософт в интрасети** и выберите **изменить**.

11. В диалоговом окне **Указать размещение службы обновлений Майкрософт в интрасети** выберите **Включить**.

12. В разделе **Параметры** в разделе **Настройка службы обновления интрасети для обнаружения обновлений** и **Настройка параметров сервера статистики интрасети** введите `http://Your_WSUS_Server_FQDN:PortNumber`, а затем нажмите **кнопку ОК**.



> ⓘ **Примечание.**
>
> - URL-адрес `http://Your_WSUS_Server_FQDN:PortNumber` на следующем рисунке приведен в качестве примера. В своей среде обязательно укажите имя сервера и номер порта для соответствующего экземпляра WSUS.

- HTTP-порт по умолчанию для WSUS — 8530, а HTTPS-порт по умолчанию — 8531. (Другие варианты — 80 и 443, другие порты не поддерживаются.)

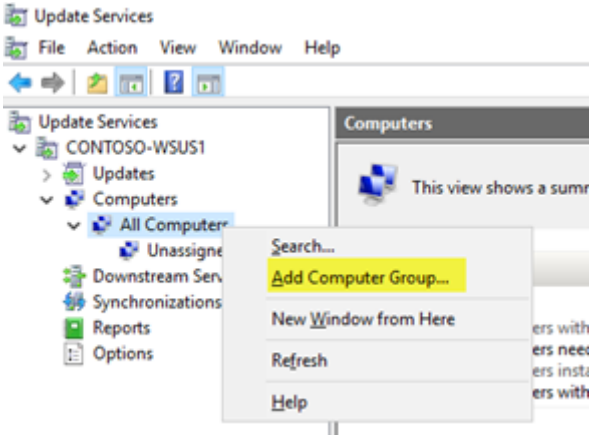
По мере того как клиенты Windows обновляют политики на своих компьютерах (по умолчанию групповая политика обновляется каждые 90 минут и при перезапуске), компьютеры начинают отображаться в WSUS. Теперь когда клиенты взаимодействуют с сервером WSUS, создайте группы компьютеров, соответствующие вашим кругам развертывания.

Создание групп компьютеров на консоли администрирования WSUS

Группы компьютеров можно использовать, чтобы применить ту или иную политику к подмножеству устройств с определенными исправлениями и обновлениями компонентов. Эти группы представляют ваши круги развертывания, контролируемые WSUS. Эти группы можно заполнить вручную с помощью консоли администрирования WSUS или автоматически с использованием групповой политики. Независимо от выбранного метода сначала нужно создать группы на консоли администрирования WSUS.

Создание групп компьютеров на консоли администрирования WSUS

1. Откройте консоль администрирования WSUS.
2. Выберите *Server_Name*\Computers\All Computers и выберите **Добавить группу компьютеров**.



3. Введите **Ring 2 Pilot Business Users** в поле имя и нажмите кнопку **Добавить**.
4. Повторите эти действия для групп **Круг 3 — широкая группа ИТ-пользователей** и **Круг 4 — широкая группа бизнес-пользователей**. По завершении должно быть три группы кругов развертывания.

Создав группы, добавьте компьютеры в группы компьютеров, соответствующие нужным кругам развертывания. Для этого можно воспользоваться групповой политикой или выполнить это вручную с помощью консоли администрирования WSUS.

Использование консоли администрирования WSUS для заполнения кругов развертывания

Добавить компьютеры в группы компьютеров на консоли администрирования WSUS очень просто, но это может занять намного больше времени, чем при использовании групповой политики, особенно если нужно добавить много компьютеров. Добавление компьютеров в группы компьютеров на консоли администрирования WSUS называется *указание на стороне сервера*.

В этом примере компьютеры добавляются в группы компьютеров двумя способами: назначая неназначенные компьютеры вручную и выполняя поиск нескольких компьютеров.

Назначение неназначенных компьютеров группам вручную

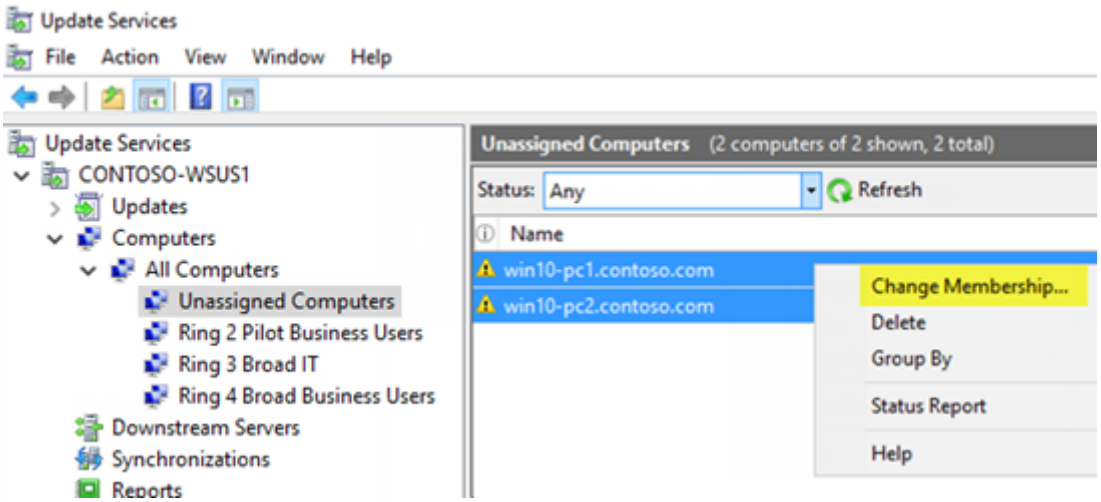
Когда новые компьютеры обмениваются данными с WSUS, они отображаются в группе **Неназначенные компьютеры**. Для добавления компьютеров в нужные группы на этом этапе можно использовать следующую процедуру. В этих примерах для добавления компьютеров в группы компьютеров используются два ПК Windows 10 (WIN10-PC1 и WIN10-PC2).

Назначение компьютеров вручную

1. На консоли администрирования WSUS перейдите в раздел *Имя_сервера*\Компьютеры\Все компьютеры\Неназначенные компьютеры.

   Здесь отображаются новые компьютеры, которые получили созданный в предыдущем разделе объект групповой политики и начали обмен данными с WSUS. В этом примере имеется только два компьютера; В зависимости от того, насколько широко развернута политика, у вас, скорее всего, будет много компьютеров.

2. Выберите оба компьютера, щелкните их правой кнопкой мыши и выберите **команду Изменить членство**.



3. В диалоговом окне **Настройка членства в группах компьютеров** выберите круг **развертывания Пилотные бизнес-пользователи круг 2** , а затем нажмите **кнопку ОК**.

   Так как они были назначены группе, эти компьютеры больше не относятся к группе **Неназначенные компьютеры**. Если выбрать группу **компьютеров Круг 2 пилотных бизнес-пользователей** , вы увидите оба компьютера.

Поиск нескольких компьютеров для добавления в группы

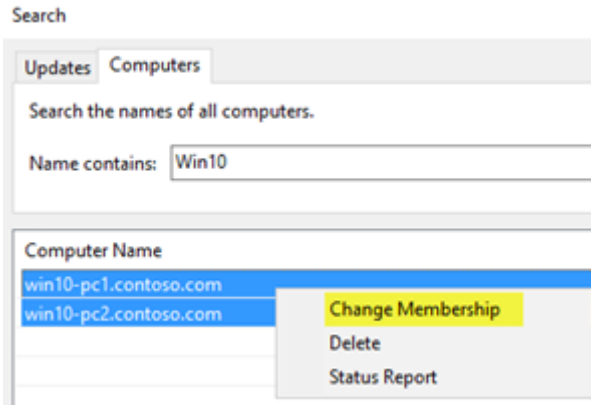
Кроме того, чтобы добавить несколько компьютеров в круг развертывания на консоли администрирования WSUS, можно воспользоваться функцией поиска.

Поиск нескольких компьютеров

1. В консоли администрирования WSUS перейдите в *раздел Server_Name*\Computers\All Computers, щелкните правой кнопкой мыши **Все компьютеры** и выберите **Поиск**.

2. В поле поиска введите **WIN10**.

3. В результатах поиска выберите компьютеры, щелкните их правой кнопкой мыши и выберите **команду Изменить членство**.



4. Выберите круг **"Круг 3" Расширенное ИТ-развертывание** , а затем нажмите **кнопку ОК**.

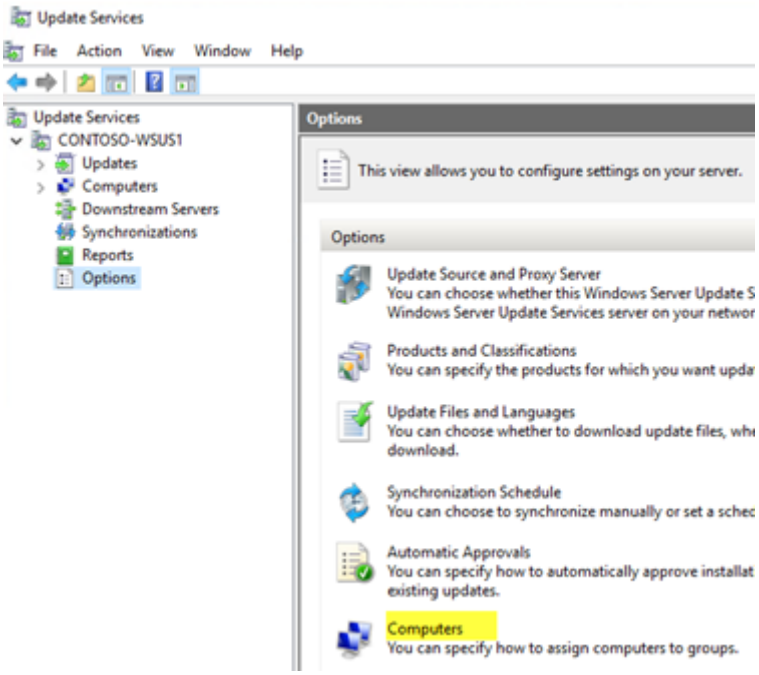
Теперь эти компьютеры отображаются в группе компьютеров **Круг 3 — широкая группа ИТ-пользователей**.

Использование групповой политики для заполнения кругов развертывания

Консоль администрирования WSUS предоставляет удобный интерфейс, с помощью которого можно управлять исправлениями и обновлениями компонентов Windows. Если требуется добавить в соответствующий круг развертывания WSUS достаточно много компьютеров, выполнение этой операции вручную с использованием консоли администрирования WSUS может занять много времени. В таких случаях целесообразно использовать для выбора нужных компьютеров групповую политику, которая автоматически добавит их в нужный круг развертывания WSUS в зависимости от их группы безопасности Active Directory. Эта процедура называется *указание на стороне клиента*. Прежде чем включать в групповой политике указание на стороне клиента необходимо настроить принятие назначений компьютеров в WSUS с помощью групповой политики

Настройка WSUS для указания на стороне клиента с использованием групповой политики

1. Откройте консоль администрирования WSUS, перейдите в *раздел Server_Name*\Параметры, а затем выберите **Компьютеры**.



2. В диалоговом окне **Компьютеры** выберите **Использовать групповая политика или параметры реестра на компьютерах**, а затем нажмите **кнопку OK**.

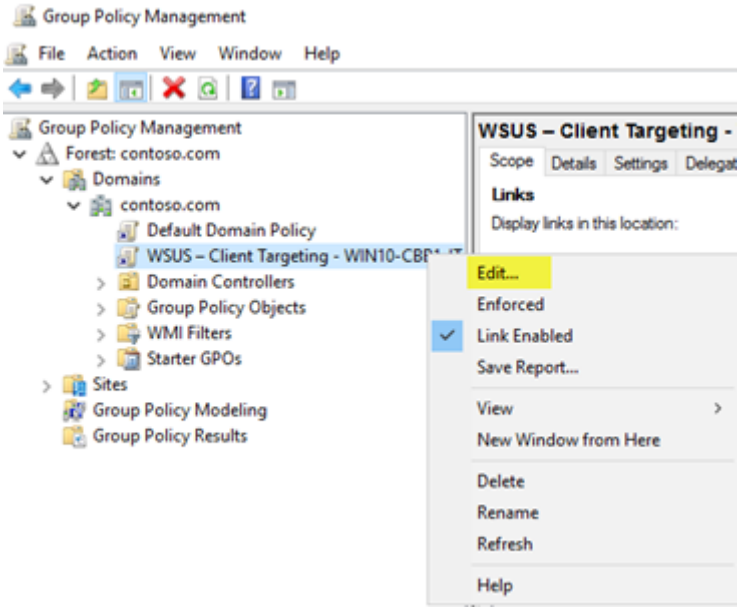
   > ⓘ **Примечание.**
   >
   > Этот параметр можно задать только по принципу «или — или». Если вы включаете в WSUS использование групповой политики для назначения групп, вы больше не сможете вручную добавлять компьютеры на консоли администрирования WSUS до тех пор, пока не вернете первоначальные настройки.

Подготовив WSUS к указанию на стороне клиента, выполните следующие шаги, чтобы использовать групповую политику для настройки указания на стороне клиента.

Настройка указания на стороне клиента

> 💡 **Совет**
>
> При использовании указания на стороне клиента целесообразно присвоить группам безопасности те же имена, что и кругам развертывания. Это упрощает процесс создания политики и гарантирует, что компьютеры не добавляются в неправильные круги.

1. Откройте консоль управления групповая политика (gpmc.msc).
2. Разверните узел Лес\Домены*Your_Domain*.
3. Щелкните правой кнопкой мыши *Your_Domain*, а затем выберите **Создать объект групповой политики в этом домене и связать его здесь**.
4. В диалоговом окне **Новый объект групповой политики** введите **WSUS — Целевой клиент — Круг 4 расширенных бизнес-пользователей** в качестве имени нового объекта групповой политики.
5. Щелкните правой кнопкой мыши объект групповой политики **WSUS — targeting client — Ring 4 Broad Business Users (Широкий круг бизнес-пользователей)** и выберите **команду Изменить**.

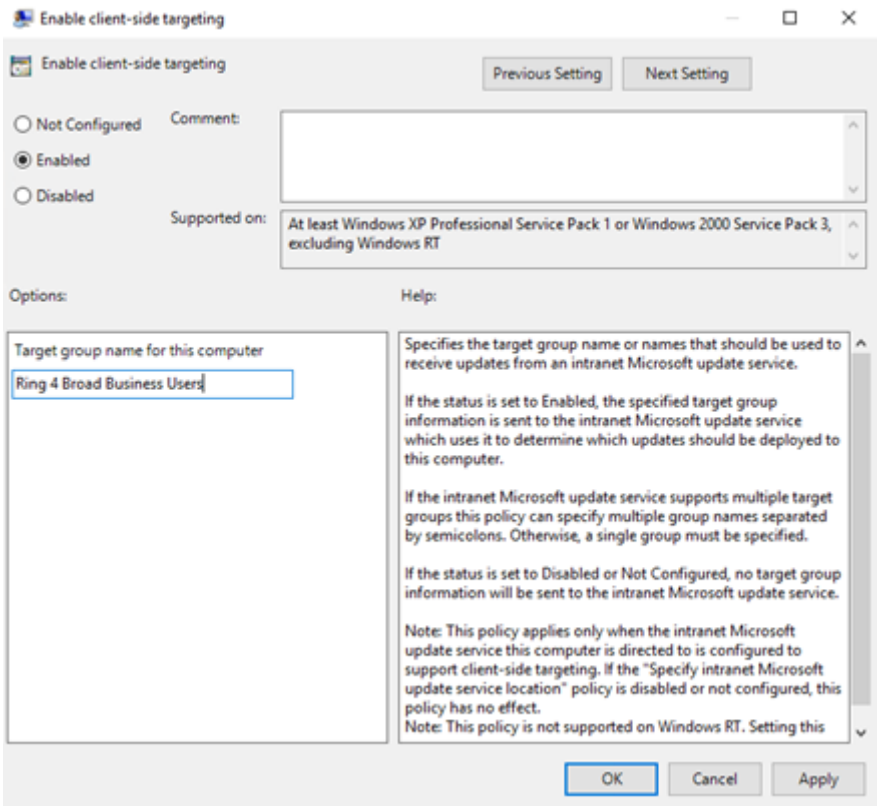


6. В редакторе управления групповыми политиками выберите Конфигурация компьютера\Политики\Административные шаблоны\Компоненты Windows\Центр обновления Windows.

7. Щелкните правой кнопкой мыши **Включить нацеливание на стороне клиента** и выберите **изменить**.

8. В диалоговом окне **Включение указания на стороне клиента** выберите **Включить**.

9. В поле **Имя целевой группы для данного компьютера** введите *Круг 4 — широкая группа бизнес-пользователей*. Это имя круга развертывания в WSUS, в который будут добавлены эти компьютеры.



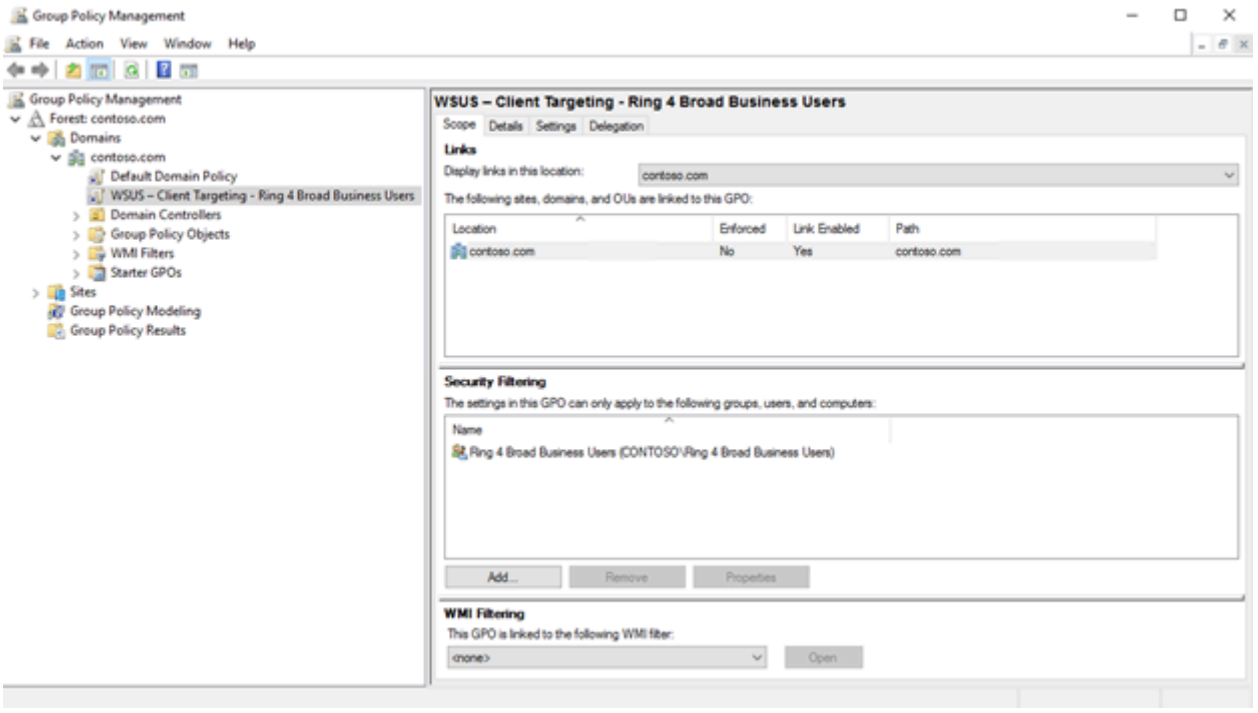
> ⚠ **Предупреждение**
>
> Имя целевой группы должно соответствовать имени группы компьютеров.

10. Закройте редактор управления групповыми политиками.

Теперь вы готовы развернуть этот объект групповой политики в правильной группе безопасности компьютеров для круга развертывания **Круг 4 Для широких бизнес-пользователей** .

Указание группы в качестве области действия объекта групповой политики

1. В GPMC выберите политику **WSUS — targeting Client Targeting — Ring 4 (Широкая группа бизнес-пользователей**).
2. Перейдите на вкладку **Область** .
3. В разделе **Фильтры безопасности** удалите группу безопасности по умолчанию **ПРОШЕДШИЕ ПРОВЕРКУ**, а затем добавьте группу **Круг 4 — широкая группа бизнес-пользователей**.



В следующий раз, когда клиенты в группе безопасности **Круг 4 "Широкая группа бизнес-пользователей** " получат политику компьютера и обращаются к WSUS, они будут добавлены в круг развертывания **круг 4 "Широкие бизнес-пользователи** ".

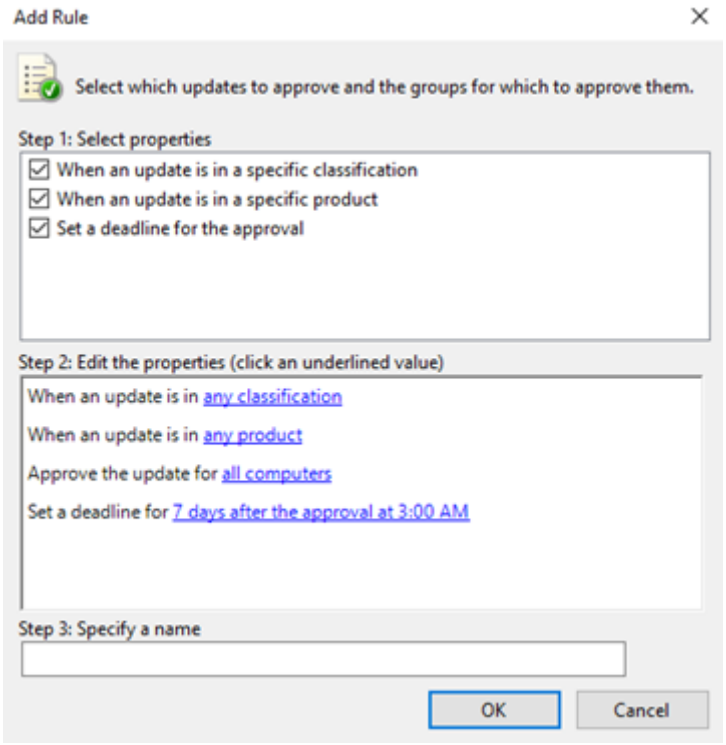
Автоматическое утверждение и развертывание обновлений компонентов

Для клиентов, для которых обновления компонентов должны быть утверждены, как только они будут доступны, можно настроить правила автоматического утверждения в WSUS.

> ⓘ **Примечание.**
>
> WSUS учитывает ветвь обслуживания клиентского устройства. Если вы утверждаете обновление компонентов, пока оно находится в одной ветви, например в предварительной версии программы предварительной оценки, службы WSUS установят обновление только на устройствах, которые находятся в этой ветви обслуживания. Когда корпорация Майкрософт выпускает сборку для **канала общедоступной доступности**, устройства в ней будут устанавливать ее. параметры ветви клиентский компонент Центра обновления Windows клиентских политик не применяются к обновлениям компонентов через WSUS.

Настройка правила автоматического утверждения для обновлений клиентских компонентов Windows и утверждение их для круга расширенного ИТ-развертывания круга 3 В этом примере используется Windows 10, но процесс одинаков для Windows 11.

1. В консоли администрирования WSUS перейдите в раздел Update Services*Server_Name*\Options, а затем выберите **Автоматические утверждения**.
2. На вкладке **Обновить правила** выберите **Создать правило**.
3. В диалоговом окне **Добавление правила** установите флажки **Когда обновление затрагивает конкретный класс**, **Когда обновление затрагивает конкретный продукт** и **Установить крайний срок для утверждения**.



4. В области **Изменить свойства** щелкните **любая классификация**. Очистите все, кроме **обновлений**, а затем нажмите **кнопку ОК**.

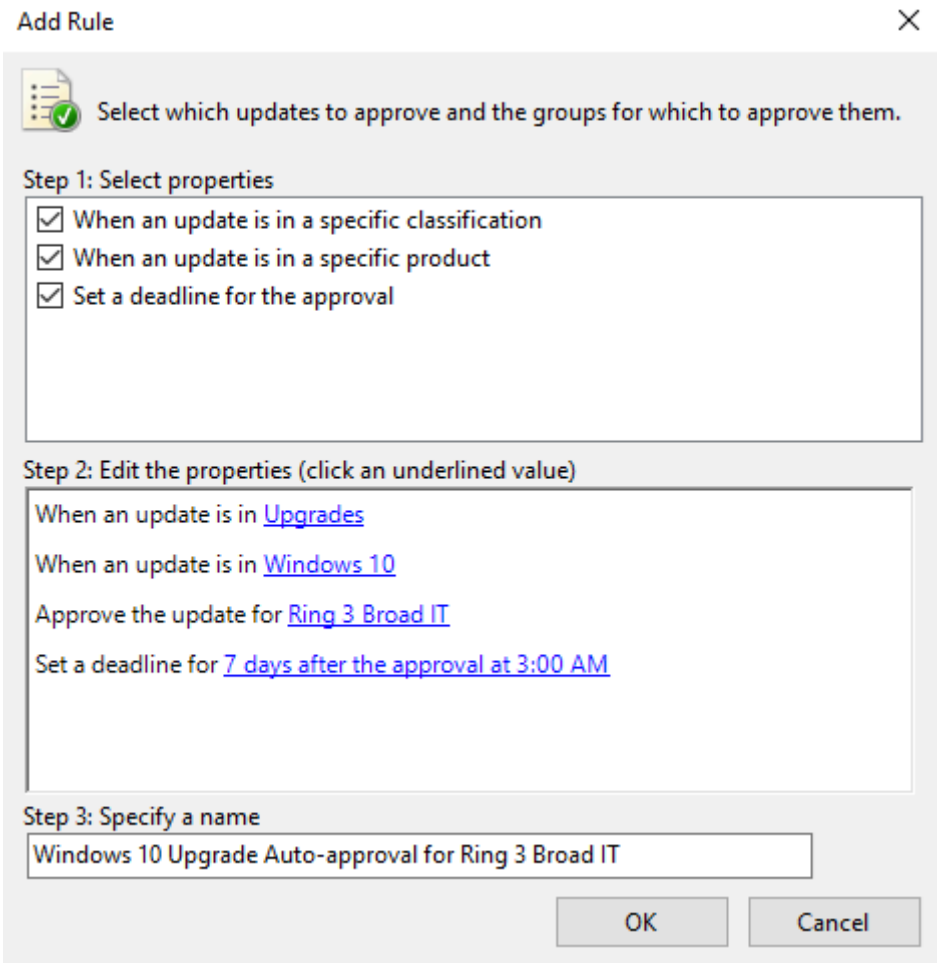
5. В **области Изменение свойств** выберите ссылку **на любой продукт** . Очистите все поля проверка, кроме **Windows 10**, а затем нажмите **кнопку ОК**.

   Windows 10 находится в разделе Все продукты\Microsoft\Windows.

6. В области **Изменить свойства** выберите ссылку **Все компьютеры** . Очистите все поля группы компьютеров проверка, кроме **круга 3 Broad IT**, а затем нажмите **кнопку ОК**.

7. Оставьте заданный срок: **7 дней после утверждения в 3:00**.

8. В поле **Шаг 3. Укажите имя** введите **Windows 10 Автоматическое утверждение обновления для круга 3 Расширенный ИТ и** нажмите **кнопку ОК**.



9. В диалоговом окне **Автоматические утверждения** нажмите **кнопку OK**.

> ⓘ **Примечание.**
>
> Службы WSUS не учитывают существующие параметры отсрочки по месяцам, **неделям и дням**. При этом, если вы используете политики клиентский компонент Центра обновления Windows клиентов для компьютера, для которого WSUS также управляет обновлениями, когда WSUS утвердит обновление, оно будет установлено на компьютере независимо от того, настроено ли групповая политика для ожидания.

Теперь при публикации обновлений компонентов клиента Windows в WSUS они автоматически утверждаются для круга **широкого ИТ-развертывания круга 3** с крайним сроком установки в 1 неделю.

> ⚠ **Предупреждение**
>
> Правило автоматического утверждения запускается после синхронизации. Это означает, что *следующее* обновление для каждой версии клиента Windows будет утверждено. Если выбрать **Запустить правило**, будут утверждены все возможные обновления, соответствующие условиям, потенциально включая старые обновления,

которые вам не нужны, что может стать проблемой, если размер загрузки очень велик.

Утверждение и развертывание обновлений компонентов вручную

Можно вручную утвердить обновления и установить сроки для установки на консоли администрирования WSUS. Возможно, лучше утвердить правила обновления вручную после обновления пилотного развертывания.

Чтобы упростить процесс утверждения вручную, начните с создания представления обновления программного обеспечения, содержащего только Windows 10 (в этом примере) обновлений. Для обновлений Windows 11 происходит то же самое.

> ⓘ **Примечание.**
>
> При утверждении нескольких обновлений компонентов для компьютера может возникнуть ошибка с клиентом. Утвердить только одно обновление компонентов на компьютер.

Утверждение и развертывание обновлений компонентов вручную

1. В консоли администрирования WSUS выберите Update Services*Server_Name*\Обновления. В области **Действие** выберите **Создать представление обновления**.

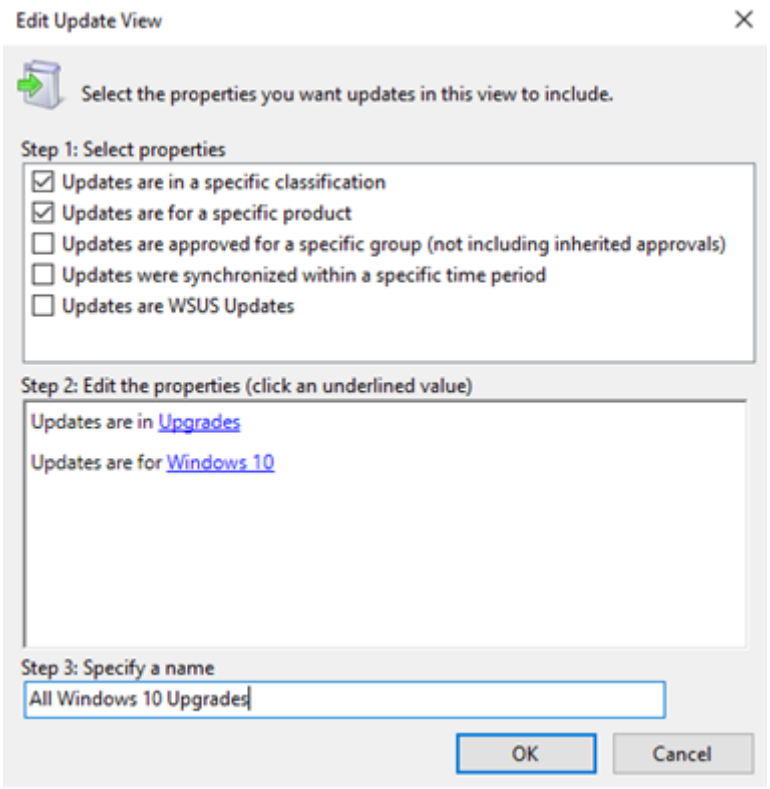
2. В диалоговом окне **Добавление режима просмотра обновлений** выберите **Обновления принадлежат конкретному классу** и **Обновления предназначены для конкретного продукта**.

3. В **разделе Шаг 2. Изменение свойств** выберите **любую классификацию**. Очистите все поля проверка, кроме **обновлений**, и нажмите **кнопку ОК**.

4. В **разделе Шаг 2. Изменение свойств** выберите **любой продукт**. Очистите все поля проверка, кроме **Windows 10**, а затем нажмите **кнопку ОК**.

   Windows 10 находится в разделе Все продукты\Microsoft\Windows.

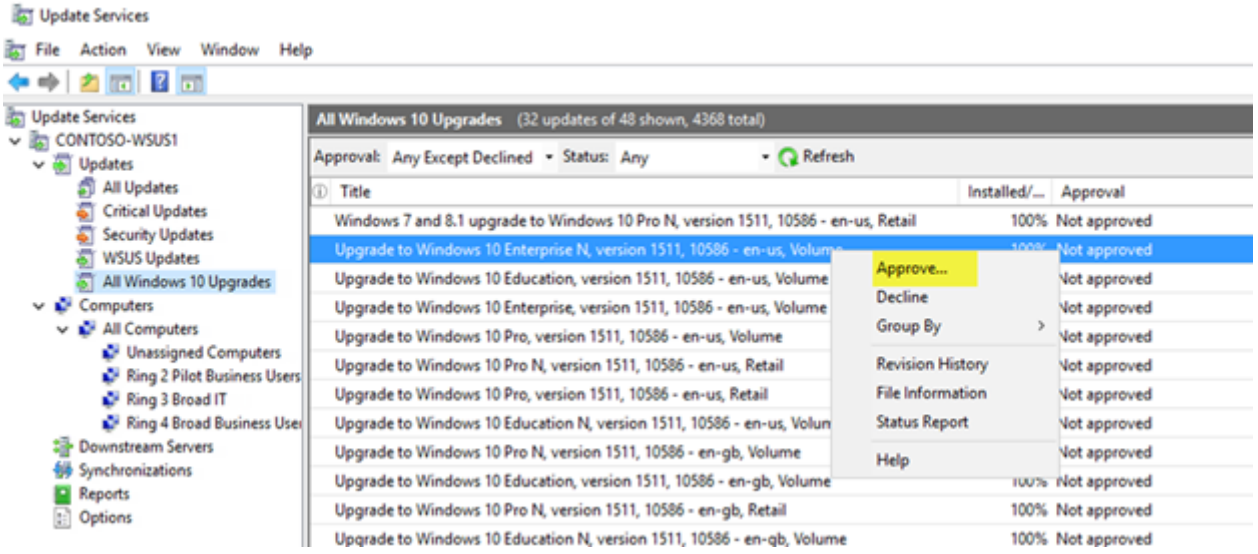
5. В поле **Шаг 3. Указание имени** введите **Все обновления Windows 10**, а затем нажмите **кнопку ОК**.



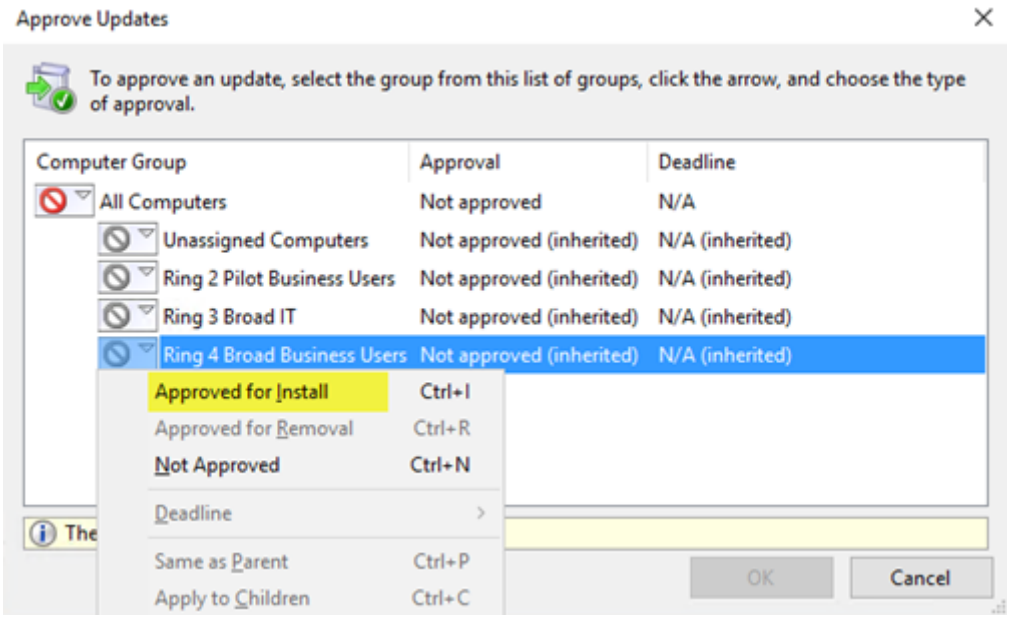
Теперь, когда у вас есть представление **Все обновления Windows 10**, выполните следующие действия, чтобы вручную утвердить обновление для круга развертывания **Круг 4 широких бизнес-пользователей**:

1. В консоли администрирования WSUS выберите Update Services*Server_Name*\Обновления\All Windows 10 Upgrades.

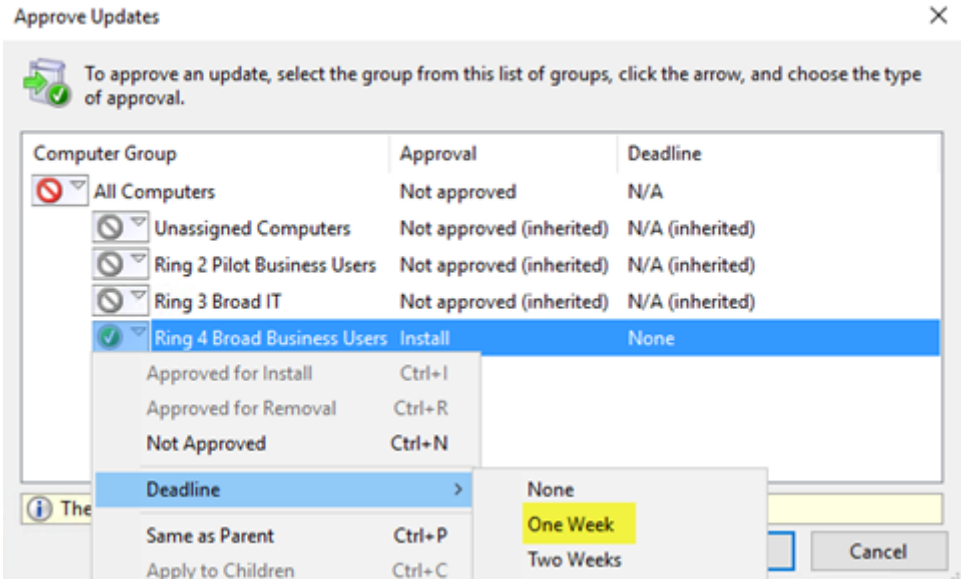
2. Щелкните правой кнопкой мыши обновление компонентов, которое требуется развернуть, и выберите **утвердить**.



3. В диалоговом окне **Утверждение обновлений** в списке **Круг 4 — широкая группа бизнес-пользователей** выберите **Утверждено для установки**.

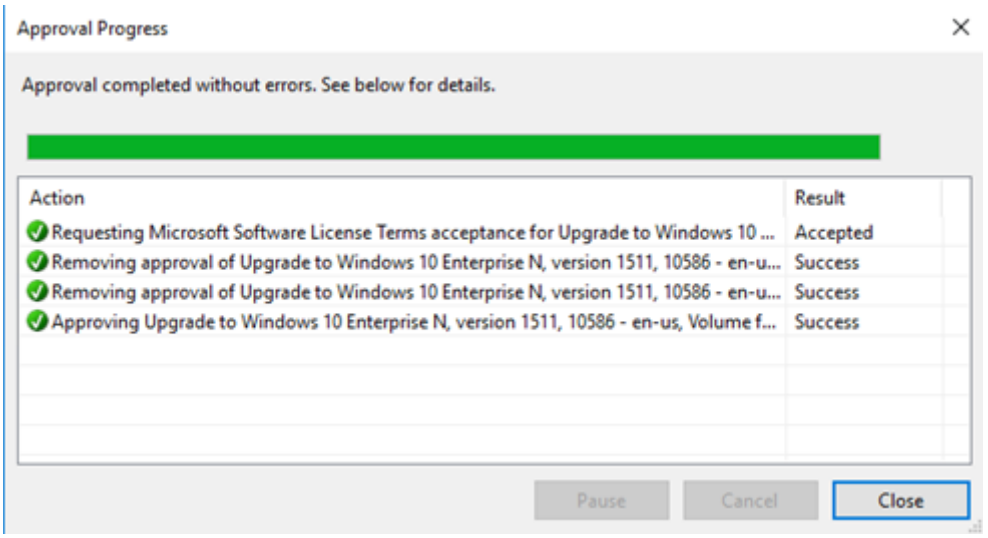


4. В диалоговом окне **Утверждение Обновления** в списке **Круг 4 широких бизнес-пользователей** выберите **Крайний срок**, **выберите Одна неделя**, а затем нажмите **кнопку ОК**.



5. Если откроется диалоговое окно **Условия лицензионного соглашения на использование программного обеспечения Майкрософт** , выберите **Принять**.

   Если развертывание завершено успешно, вы получите отчет об успешном выполнении операции.



6. В диалоговом окне **Ход утверждения** выберите **Закрыть**.

Last updated on 17.06.2025

Обновление установочного носителя Windows с помощью динамического обновления

Применяется к: ✅ Windows 11, ✅ Windows 10, ✅ Windows Server

В этой статье объясняется, как получать и применять пакеты динамического обновления к существующим *образам Windows перед развертыванием*, а также содержатся Windows PowerShell скрипты, которые можно использовать для автоматизации этого процесса.

Корпоративный носитель доступен для каждого выпуска Windows в Центре обслуживания корпоративного лицензирования (VLSC) и других соответствующих каналах, таких как политики клиентский компонент Центра обновления Windows клиентов, Windows Server Update Services (WSUS) и Подписки Visual Studio. Вы можете использовать динамическое обновление, чтобы обеспечить наличие на устройствах Windows последних пакетов обновления компонентов в рамках обновления на месте при сохранении языковых пакетов и компонентов по запросу (FOD), которые могли быть установлены ранее. Динамическое обновление также устраняет необходимость установки отдельного обновления качества в рамках процесса обновления на месте.

Динамическое обновление

При каждом запуске установки обновления компонентов (с носителя или среды, подключенной к клиентский компонент Центра обновления Windows), одним из первых шагов является *динамическое обновление*. Программа установки Windows связывается с конечной точкой Майкрософт для получения пакетов динамического обновления, а затем применяет эти обновления к установочному носителю операционной системы. Пакеты обновлений включают следующие типы обновлений:

- Обновления для Setup.exe двоичных файлов или других файлов, используемых программой установки для обновления компонентов
- Обновления для "безопасной операционной системы" (SafeOS), используемой для среды восстановления Windows
- Обновления в стек обслуживания, необходимый для завершения обновления компонентов Дополнительные сведения см. в разделе Обновления стека обслуживания.
- Последнее накопительное (качественное) обновление
- Обновления к применимым драйверам, уже опубликованным производителями, специально предназначенными для динамического обновления

Динамическое обновление сохраняет языковые пакеты и пакеты компонентов по запросу, повторно запрашивая их.

Устройства должны иметь возможность подключения к Интернету, чтобы получить динамические Обновления. В некоторых средах это не вариант для получения динамической Обновления. Вы по-прежнему можете выполнить обновление компонентов на основе мультимедиа, получив пакеты динамического обновления и применив его к образу перед запуском установки на устройстве.

Получение пакетов динамического обновления

Пакеты динамического обновления можно получить из каталога Центра обновления Майкрософт. На этом сайте используйте строку поиска в правом верхнем углу, чтобы найти пакеты динамического обновления для определенного выпуска. Различные пакеты динамического обновления могут не присутствовать в результатах одного поиска, поэтому вам может потребоваться выполнить поиск с разными ключевыми словами, чтобы найти все обновления. Проверьте различные части результатов, чтобы убедиться, что вы определили необходимые файлы. В следующих таблицах показаны ключевые значения для поиска или поиска в результатах.

Пакеты динамического обновления Windows Server 2025 г.

Заголовок может различать каждый динамический пакет. В последние накопительные обновления внедрен стек обслуживания. Стек обслуживания публикуется только при необходимости для данного накопительного обновления.

Развернуть таблицу

Обновление пакетов	Title
Безопасное динамическое обновление ОС	ГГГ-ММ Безопасное динамическое обновление ОС для серверной операционной системы Майкрософт версии 24H2
Настройка динамического обновления	ГгГГ-ММ: динамическое обновление для операционной системы сервера Майкрософт версии 24H2
Последнее накопительное обновление	ГГГГ-ММ накопительное обновление для серверной операционной системы Майкрософт версии 24H2
Динамическое обновление стека обслуживания	Обновление стека обслуживания ггГГ-ММ для серверной операционной системы Майкрософт версии 24H2

пакеты динамического обновления Windows Server версии 23H2

Заголовок может различать каждый динамический пакет. В последние накопительные обновления внедрен стек обслуживания. Стек обслуживания публикуется только при необходимости для данного накопительного обновления. Azure Stack HCI версии 23H2 имеет аналогичный формат.

Развернуть таблицу

Обновление пакетов	Title
Безопасное динамическое обновление ОС	YYYY-MM Безопасное динамическое обновление ОС для серверной операционной системы Майкрософт версии 23H2
Настройка динамического обновления	ГгГГ-ММ: динамическое обновление установки для операционной системы сервера Майкрософт версии 23H2
Последнее накопительное обновление	ГгГГ-ММ накопительное обновление для серверной операционной системы Майкрософт версии 23H2
Динамическое обновление стека обслуживания	ГгГГ-ММ обновление стека обслуживания для серверной операционной системы Майкрософт версии 23H2

Пакеты динамического обновления Azure Stack HCI версии 22H2

Для различения каждого динамического пакета требуется название, **продукт** и **описание** . В последнее накопительное обновление внедрен стек обслуживания. Стек обслуживания публикуется отдельно, только если это необходимо в качестве необходимого условия для данного накопительного обновления.

Развернуть таблицу

Обновление пакетов	Title	Продукт	Описание
Безопасное динамическое обновление ОС	Динамическое обновление ггГГ-ММ для серверной операционной системы Майкрософт, версия 22H2	Динамическое обновление безопасной ОС Windows	ComponentUpdate
Настройка динамического обновления	Динамическое обновление ггГГ-ММ для серверной	динамическое обновление Windows	SetupUpdate

Обновление пакетов	Title	Продукт	Описание
	операционной системы Майкрософт, версия 22H2	10 и более поздних версий	
Последнее накопительное обновление	ГГГГ-ММ накопительное обновление для серверной операционной системы Майкрософт, версия 22H2		
Динамическое обновление стека обслуживания	Обновление стека обслуживания ггГГ-ММ для серверной операционной системы Майкрософт, версия 22H2		

Windows Server 2022 более поздних пакетов динамического обновления

Для различения каждого динамического пакета требуется название, **продукт** и **описание** . В последнее накопительное обновление внедрен стек обслуживания. Стек обслуживания публикуется отдельно, только если это необходимо в качестве необходимого условия для данного накопительного обновления.

Развернуть таблицу

Обновление пакетов	Title	Продукт	Описание
Безопасное динамическое обновление ОС	Динамическое обновление ГГГГ-ММ для серверной операционной системы Майкрософт, версия 21H2	Динамическое обновление безопасной ОС Windows	ComponentUpdate
Настройка динамического обновления	Динамическое обновление ГГГГ-ММ для серверной операционной системы Майкрософт, версия 21H2	динамическое обновление Windows 10 и более поздних версий	SetupUpdate
Последнее накопительное обновление	ГгГГ-ММ Накопительное обновление для серверной операционной системы Майкрософт, версия 21H2		

Обновление пакетов	Title	Продукт	Описание
Динамическое обновление стека обслуживания	Обновление стека обслуживания ггГГ-ММ для серверной операционной системы Майкрософт, версия 21H2		

пакеты динамического обновления Windows 11 версии 22H2 и более поздних версий

Заголовок может различать каждый динамический пакет. В последние накопительные обновления внедрен стек обслуживания. Стек обслуживания публикуется только при необходимости для данного накопительного обновления. Следующие заголовки предназначены для Windows 11 версии 22H2. Windows 11 версии 23H2 и версии 24H2 имеют аналогичный формат:

Развернуть таблицу

Обновление пакетов	Title
Безопасное динамическое обновление ОС	YYYY-MM Безопасное динамическое обновление ОС для Windows 11 версии 22H2
Настройка динамического обновления	Динамическое обновление установки ггГГ-ММ для Windows 11 версии 22H2
Последнее накопительное обновление	ГгГГ-ММ накопительное обновление для Windows 11 версии 22H2
Динамическое обновление стека обслуживания	Обновление стека обслуживания ггГГ-ММ для Windows 11 версии 22H2

пакеты динамического обновления Windows 11 версии 21H2

Для различения каждого динамического пакета требуется название, **продукт** и **описание** . В последнее накопительное обновление внедрен стек обслуживания. Стек обслуживания публикуется отдельно, только если это необходимо в качестве необходимого условия для данного накопительного обновления.

Развернуть таблицу

Обновление пакетов	Title	Продукт	Описание
Безопасное динамическое обновление ОС	Динамическое обновление ггГГ-ММ для Windows 11	Динамическое обновление безопасной ОС Windows	ComponentUpdate
Настройка динамического обновления	Динамическое обновление ггГГ-ММ для Windows 11	динамическое обновление Windows 10 и более поздних версий	SetupUpdate
Последнее накопительное обновление	Накопительное обновление ггГГ-ММ для Windows 11		
Динамическое обновление стека обслуживания	Обновление стека обслуживания ггГГ-ММ для Windows 11 версии 21H2		

пакеты динамического обновления Windows 10 версии 22H2

Для различения каждого динамического пакета требуется название, **продукт** и **описание** . В последнее накопительное обновление внедрен стек обслуживания. Стек обслуживания публикуется отдельно, только если это необходимо в качестве необходимого условия для данного накопительного обновления.

Развернуть таблицу

Обновление пакетов	Title	Продукт	Описание
Безопасное динамическое обновление ОС	Динамическое обновление ГГГГ-ММ для Windows 10 версии 22H2	Динамическое обновление безопасной ОС Windows	ComponentUpdate
Настройка динамического обновления	Динамическое обновление ГГГГ-ММ для Windows 10 версии 22H2	динамическое обновление Windows 10 и более поздних версий	SetupUpdate
Последнее накопительное обновление	Накопительное обновление ггГГ-ММ для Windows 10 версии 22H2		
Динамическое обновление стека обслуживания	Обновление стека обслуживания ггГГ-ММ для Windows 10 версии 22H2		

Если вы хотите настроить образ с помощью дополнительных языков или функций по запросу, скачайте дополнительные ISO-файлы мультимедиа из Центра обслуживания корпоративного лицензирования. Например, если динамическое обновление будет отключено для ваших устройств и пользователям требуются определенные функции по запросу, их можно предварительно включить в образ.

Обновление установочного носителя Windows

Правильное обновление установочного носителя включает в себя множество действий, выполняемых с несколькими разными целевыми объектами (файлами образов). Некоторые действия повторяются в разных целевых объектах. К целевым файлам образов относятся:

- Среда предустановки Windows (WinPE): небольшая операционная система, используемая для установки, развертывания и восстановления операционных систем Windows.
- Среда восстановления Windows (WinRE): исправит распространенные причины незагрузимых операционных систем. WinRE основан на WinPE и может быть настроен с помощью дополнительных драйверов, языков, необязательных пакетов и других средств для устранения неполадок или диагностики.
- Операционная система Windows: один или несколько выпусков Windows, хранящихся в \sources\install.wim
- Установочный носитель Windows: полная коллекция файлов и папок на установочном носителе Windows. Например, папка \sources, папка \boot, Setup.exe и т. д.

В этой таблице показана правильная последовательность для применения различных задач к файлам. Например, полная последовательность начинается с добавления обновления стека обслуживания в WinRE (1) и завершается добавлением диспетчера загрузки из WinPE на новый носитель (28).

Развернуть таблицу

Задача	WinRE (winre.wim)	Операционная система (install.wim)	WinPE (boot.wim)	Новый носитель
Добавление обновления стека обслуживания с помощью последнего накопительного обновления	1	9	17	
Добавление языкового пакета	2	10	18	

Задача	WinRE (winre.wim)	Операционная система (install.wim)	WinPE (boot.wim)	Новый носитель
Добавление локализованных необязательных пакетов	3		19	
Добавление поддержки шрифтов	4		20	
Добавление преобразования текста в речь	5		21	
Обновление Lang.ini			22	
Добавление функций по запросу		11		
Добавление необязательных компонентов		12		
Добавление безопасного динамического обновления ОС	6			
Добавление динамического обновления установки				26
Добавление Setup.exe и setuphost.exe из WinPE				27
Добавление диспетчера загрузки из WinPE				28
Добавление последнего накопительного обновления		13	23	
Очистка изображения	7	14	24	
Добавление накопительных обновлений .NET и .NET		15		
Экспорт изображения	8	16	25	

ⓘ Примечание.

- Начиная с февраля 2021 г. последнее накопительное обновление и обновление стека обслуживания объединяется и распространяется в каталоге Центра обновления Майкрософт в виде нового объединенного накопительного обновления. Для шагов 1, 9 и 17, требующих обновления стека обслуживания для обновления установочного носителя, следует использовать объединенное

накопительное обновление. Дополнительные сведения о объединенном накопительном обновлении см. в разделе **Обновления стека обслуживания**. При получении пакетов динамического обновления убедитесь, что пакеты соответствуют тому же месяцу, что и последнее накопительное обновление. Если, например, динамическое обновление SafeOS или динамическое обновление установки недоступно в течение того же месяца, что и последнее накопительное обновление, используйте последнюю опубликованную версию каждого из них.

- Корпорация Майкрософт удаляет компонент Flash из Windows через **KB4577586: Обновление для удаления Adobe Flash Player**. Вы также можете удалить Flash в любое время, развернув обновление в KB4577586 (доступно в каталоге) между шагами 20 и 21. Начиная с июля 2021 года, KB4577586, "Обновление для удаления Adobe Flash Player" будет включено в последнее накопительное обновление для Windows 10 версии 1607 и 1507. Обновление также будет включено в ежемесячный накопительный пакет и обновление только для системы безопасности для Windows 8.1, Windows Server 2012 и Windows Embedded 8 Standard. Дополнительные сведения см. в разделе **Обновление окончания поддержки Adobe Flash Player**.

Несколько выпусков Windows

Файл операционной системы main (install.wim) может содержать несколько выпусков Windows. Возможно, для его развертывания на основе индекса требуется только обновление для определенного выпуска. Или может потребоваться обновление для всех выпусков. Кроме того, убедитесь, что языки установлены перед компонентом по запросу, а последнее накопительное обновление всегда применяется последним.

Дополнительные языки и функции

Вам не нужно добавлять в образ дополнительные языки и функции, чтобы выполнить обновления, но это возможность настроить образ с дополнительными языками, дополнительными компонентами и функциями по запросу, помимо того, что находится в начальном образе. При добавлении дополнительных языков и функций важно внести эти изменения в правильном порядке: сначала применить обновления стека обслуживания, а затем добавить язык, затем добавить компоненты и, наконец, последнее накопительное обновление. Предоставленный пример скрипта устанавливает второй язык (в данном случае японский (ja-JP)). Так как этот язык поддерживается lp.cab, добавлять языковой

пакет не требуется. Японский язык добавляется как в main операционную систему, так и в среду восстановления, чтобы позволить пользователю просматривать экраны восстановления на японском языке. Сюда входит добавление локализованных версий пакетов, установленных в данный момент в образе восстановления.

Необязательные компоненты вместе с функцией .NET можно установить в автономном режиме. Однако при этом создаются ожидающие операции, требующие перезапуска устройства. В результате вызов для очистки образа завершится ошибкой. Существует два способа избежать сбоя очистки. Один из вариантов — пропустить шаг очистки образа, хотя это приводит к большему размеру install.wim. Другой вариант — установить .NET и необязательные компоненты на шаге после очистки, но перед экспортом. Это параметр в примере скрипта. Это позволит вам начать с исходного файла install.wim (без ожидающих действий) при следующем обслуживании или обновлении образа (например, в следующем месяце).

Накопительные обновления контрольных точек

Начиная с Windows 11 версии 24H2 и Windows Server 2025, последнее накопительное обновление может иметь обязательное накопительное обновление, которое необходимо установить в первую очередь. Эти обновления называются накопительными обновлениями контрольных точек. В этих случаях различия на уровне файлов накопительного обновления основаны на предыдущем накопительном обновлении, а не на выпуске Windows RTM. Преимущество заключается в меньшем пакете обновления и более быстрой установке. При получении последнего накопительного обновления из каталога Центра обновления Майкрософт накопительные обновления контрольных точек доступны с помощью кнопки скачивания. Кроме того, дополнительные сведения содержатся в статье база знаний накопительного обновления.

Чтобы установить контрольные точки при обслуживании ОС Windows (шаги 9 & 12) и WinPE (шаги 17 & 23), вызовите `Add-WindowsPackage` целевое накопительное обновление. Папка из `-PackagePath` используется для обнаружения и установки одной или нескольких контрольных точек при необходимости. В папке должны находиться только целевые накопительные обновления и накопительные обновления контрольных `-PackagePath` точек. Пакеты накопительного обновления с редакцией <= целевое накопительное обновление обрабатываются. Если вы не настраиваете образ с дополнительными языками и (или) дополнительными функциями, то для шагов 9 & 17 выше можно использовать отдельные вызовы (`Add-WindowsPackage` сначала накопительные обновления контрольных точек). Отдельные вызовы нельзя использовать для шагов 12 и 23.

Windows PowerShell скрипты для применения динамической Обновления к существующему образу

Эти примеры предназначены только для иллюстрации и поэтому не обрабатывают ошибки. Сценарий предполагает, что следующие пакеты хранятся локально в этой структуре папок:

Развернуть таблицу

Папка	Описание
C:\mediaRefresh	Родительская папка, содержащая скрипт PowerShell
C:\mediaRefresh\oldMedia	Папка, содержащая исходный носитель, который будет обновлен. Например, содержит Setup.exe и папку \sources.
C:\mediaRefresh\newMedia	Папка, которая будет содержать обновленный носитель. Он копируется из \oldMedia, а затем используется в качестве целевого объекта для всех операций обновления и очистки.

Get started

Скрипт начинается с объявления глобальных переменных и создания папок для подключения образов. Затем создайте копию исходного носителя из \oldMedia в \newMedia, сохраняя исходный носитель на случай ошибки скрипта и необходимо начать с известного состояния. Кроме того, он предоставляет сравнение старых и новых носителей для оценки изменений. Чтобы убедиться, что новые обновления мультимедиа не доступны только для чтения. Скрипт также демонстрирует добавление дополнительных языков, функций по запросу и дополнительных компонентов. Они не являются обязательными, но добавляются для выделения, когда они должны быть добавлены в последовательности. Начиная с Windows 11 версии 21H2, ISO-файл языкового пакета (LANGPACK) заменен ISO-файлом "Компоненты по запросу". Языковые пакеты и пакеты среды предустановки \Windows являются частью ISO функций по запросу. Кроме того, путь к языку ос main и дополнительным функциям перемещен в папку \LanguagesAndOptionalFeatures, а не в корневой каталог. Если вы используете этот скрипт для Windows 10, измените его для подключения и использования ISO языкового пакета (LANGPACK).

PowerShell

```
#Requires -RunAsAdministrator

function Get-TS { return "{0:HH:mm:ss}" -f [DateTime]::Now }

Write-Output "$(Get-TS): Starting media refresh"

# Declare Dynamic Update packages. A dedicated folder is used for the latest
cumulative update, and as needed
# checkpoint cumulative updates.
$LCU_PATH        = "C:\mediaRefresh\packages\CU\LCU.msu"
$SETUP_DU_PATH   = "C:\mediaRefresh\packages\Other\Setup_DU.cab"
$SAFE_OS_DU_PATH = "C:\mediaRefresh\packages\Other\SafeOS_DU.cab"
$DOTNET_CU_PATH  = "C:\mediaRefresh\packages\Other\DotNet_CU.msu"

# Declare media for FOD and LPs
$FOD_ISO_PATH    = "C:\mediaRefresh\packages\CLIENT_LOF_PACKAGES_OEM.iso"

# Array of Features On Demand for main OS
# This is optional to showcase where these are added
$FOD = @(
'XPS.Viewer~~~~0.0.1.0'
)

# Array of Legacy Features for main OS
# This is optional to showcase where these are added
$OC = @(
'MediaPlayback'
'WindowsMediaPlayer'
)

# Mount the Features on Demand ISO
Write-Output "$(Get-TS): Mounting FOD ISO"
$FOD_ISO_DRIVE_LETTER = (Mount-DiskImage -ImagePath $FOD_ISO_PATH -ErrorAction stop
| Get-Volume).DriveLetter
$FOD_PATH = $FOD_ISO_DRIVE_LETTER + ":\LanguagesAndOptionalFeatures"

# Declare language for showcasing adding optional localized components
$LANG  = "ja-jp"
$LANG_FONT_CAPABILITY = "jpan"

# Declare language related cabs
$WINPE_OC_PATH              = "$FOD_ISO_DRIVE_LETTER`:\Windows Preinstallation
Environment\x64\WinPE_OCs"
$WINPE_OC_LANG_PATH         = "$WINPE_OC_PATH\$LANG"
$WINPE_OC_LANG_CABS         = Get-ChildItem $WINPE_OC_LANG_PATH -Name
$WINPE_OC_LP_PATH           = "$WINPE_OC_LANG_PATH\lp.cab"
$WINPE_FONT_SUPPORT_PATH    = "$WINPE_OC_PATH\WinPE-FontSupport-$LANG.cab"
$WINPE_SPEECH_TTS_PATH      = "$WINPE_OC_PATH\WinPE-Speech-TTS.cab"
$WINPE_SPEECH_TTS_LANG_PATH = "$WINPE_OC_PATH\WinPE-Speech-TTS-$LANG.cab"
$OS_LP_PATH                 = "$FOD_PATH\Microsoft-Windows-Client-Language-
Pack_x64_$LANG.cab"

# Declare folders for mounted images and temp files
$MEDIA_OLD_PATH  = "C:\mediaRefresh\oldMedia\Ge\client_professional_en-us"
```

```
$MEDIA_NEW_PATH  = "C:\mediaRefresh\newMedia"
$WORKING_PATH    = "C:\mediaRefresh\temp"
$MAIN_OS_MOUNT   = "C:\mediaRefresh\temp\MainOSMount"
$WINRE_MOUNT     = "C:\mediaRefresh\temp\WinREMount"
$WINPE_MOUNT     = "C:\mediaRefresh\temp\WinPEMount"

# Create folders for mounting images and storing temporary files
New-Item -ItemType directory -Path $WORKING_PATH -ErrorAction Stop | Out-Null
New-Item -ItemType directory -Path $MAIN_OS_MOUNT -ErrorAction stop | Out-Null
New-Item -ItemType directory -Path $WINRE_MOUNT -ErrorAction stop | Out-Null
New-Item -ItemType directory -Path $WINPE_MOUNT -ErrorAction stop | Out-Null

# Keep the original media, make a copy of it for the new, updated media.
Write-Output "$(Get-TS): Copying original media to new media path"
Copy-Item -Path $MEDIA_OLD_PATH"\*" -Destination $MEDIA_NEW_PATH -Force -Recurse -
ErrorAction stop | Out-Null
Get-ChildItem -Path $MEDIA_NEW_PATH -Recurse | Where-Object { -not $_.PSIsContainer
-and $_.IsReadOnly } | ForEach-Object { $_.IsReadOnly = $false }
```

Обновление WinRE и каждой main ос Windows

Скрипт обновляет каждый выпуск Windows в файле операционной системы main (install.wim). Для каждого выпуска подключен образ ОС main.

Для первого образа Winre.wim копируется в рабочую папку и подключается. Затем он применяет стек обслуживания через последнее накопительное обновление, так как его компоненты используются для обновления других компонентов. В зависимости от выпуска Windows, который вы обновляете, существует два разных подхода к обновлению стека обслуживания. Первый подход заключается в использовании объединенного накопительного обновления. Это относится к выпускам Windows, которые предоставляют объединенное накопительное обновление, включающее обновления стека обслуживания (то есть объединяются SSU и LCU). примерами являются Windows 11 версии 21H2 и Windows 11 версии 22H2. В этих случаях обновление стека обслуживания не публикуется отдельно; На этом шаге следует использовать объединенное накопительное обновление. Однако в редких случаях может произойть критическое изменение в объединенном формате накопительного обновления, что требует публикации автономного обновления стека обслуживания и установки сначала перед установкой объединенного накопительного обновления. Так как скрипт при необходимости добавляет японский язык, он добавляет языковой пакет в образ и устанавливает японские версии всех дополнительных пакетов, уже установленных в Winre.wim. Затем применяется пакет динамического обновления безопасной ОС. Она завершается очисткой и экспортом образа, чтобы уменьшить размер изображения.

Затем для подключенного образа ОС скрипт запускается с применением стека обслуживания с помощью последнего накопительного обновления. Затем добавляется

поддержка японского языка, а затем функции японского языка. В отличие от пакетов динамического обновления, он использует для `Add-WindowsCapability` добавления этих функций. Полный список таких функций и связанные с ними имена возможностей см. в разделе Доступные функции по запросу. Настало время включить другие необязательные компоненты или добавить другие функции по запросу. Если с такой функцией связано накопительное обновление (например, .NET), это время для его применения. Затем скрипт пытается очистить образ, а затем последний шаг для применения последнего накопительного обновления. Важно применить последнее накопительное обновление, чтобы убедиться, что функции по запросу, необязательные компоненты и языки обновляются с исходного состояния выпуска. Функция .NET — это исключение, которое добавляется вместе с накопительным обновлением. Наконец, скрипт экспортирует изображение.

Этот процесс повторяется для каждого выпуска Windows в файле операционной системы main. Чтобы уменьшить размер, файл Winre.wim с первого образа сохраняется и используется для обновления каждого последующего выпуска Windows. Это уменьшает окончательный размер install.wim.

PowerShell

```
#
# Update each main OS Windows image including the Windows Recovery Environment
(WinRE)
#

# Get the list of images contained within the main OS
$WINOS_IMAGES = Get-WindowsImage -ImagePath $MEDIA_NEW_PATH"\sources\install.wim"

Foreach ($IMAGE in $WINOS_IMAGES)
{

    # first mount the main OS image
    Write-Output "$(Get-TS): Mounting main OS, image index $($IMAGE.ImageIndex)"
    Mount-WindowsImage -ImagePath $MEDIA_NEW_PATH"\sources\install.wim" -Index
$IMAGE.ImageIndex -Path $MAIN_OS_MOUNT -ErrorAction stop| Out-Null

    if ($IMAGE.ImageIndex -eq "1")
    {

        #
        # update Windows Recovery Environment (WinRE) within this OS image
        #
        Copy-Item -Path $MAIN_OS_MOUNT"\windows\system32\recovery\winre.wim" -
Destination $WORKING_PATH"\winre.wim" -Force -ErrorAction stop | Out-Null
        Write-Output "$(Get-TS): Mounting WinRE"
        Mount-WindowsImage -ImagePath $WORKING_PATH"\winre.wim" -Index 1 -Path
$WINRE_MOUNT -ErrorAction stop | Out-Null

        # Add servicing stack update (Step 1 from the table)
```

```
        Write-Output "$(Get-TS): Adding package $LCU_PATH to WinRE"
        try
        {
            Add-WindowsPackage -Path $WINRE_MOUNT -PackagePath $LCU_PATH | Out-Null
        }
        Catch
        {
            $theError = $_
            Write-Output "$(Get-TS): $theError"

            if ($theError.Exception -like "*0x8007007e*")
            {
                Write-Warning "$(Get-TS): Failed with error 0x8007007e. This failure
is a known issue with combined cumulative update, we can ignore."
            }
            else
            {
                throw
            }
        }

        #
        # Optional: Add the language to recovery environment
        #

        # Install lp.cab cab
        Write-Output "$(Get-TS): Adding package $WINPE_OC_LP_PATH to WinRE"
        Add-WindowsPackage -Path $WINRE_MOUNT -PackagePath $WINPE_OC_LP_PATH -
ErrorAction stop | Out-Null

        # Install language cabs for each optional package installed
        $WINRE_INSTALLED_OC = Get-WindowsPackage -Path $WINRE_MOUNT
        Foreach ($PACKAGE in $WINRE_INSTALLED_OC)
        {
            if ( ($PACKAGE.PackageState -eq "Installed") -and
($PACKAGE.PackageName.startsWith("WinPE-")) -and ($PACKAGE.ReleaseType -eq
"FeaturePack") )
            {
                $INDEX = $PACKAGE.PackageName.IndexOf("-Package")
                if ($INDEX -ge 0)
                {
                    $OC_CAB = $PACKAGE.PackageName.Substring(0, $INDEX) + "_" +
$LANG + ".cab"
                    if ($WINPE_OC_LANG_CABS.Contains($OC_CAB))
                    {
                        $OC_CAB_PATH = Join-Path $WINPE_OC_LANG_PATH $OC_CAB
                        Write-Output "$(Get-TS): Adding package $OC_CAB_PATH to
WinRE"
                        Add-WindowsPackage -Path $WINRE_MOUNT -PackagePath
$OC_CAB_PATH -ErrorAction stop | Out-Null
                    }
                }
            }
        }
```

```
        # Add font support for the new language
        if ( (Test-Path -Path $WINPE_FONT_SUPPORT_PATH) )
        {
            Write-Output "$(Get-TS): Adding package $WINPE_FONT_SUPPORT_PATH to
WinRE"
            Add-WindowsPackage -Path $WINRE_MOUNT -PackagePath
$WINPE_FONT_SUPPORT_PATH -ErrorAction stop | Out-Null
        }

        # Add TTS support for the new language
        if (Test-Path -Path $WINPE_SPEECH_TTS_PATH)
        {
            if ( (Test-Path -Path $WINPE_SPEECH_TTS_LANG_PATH) )
            {
                Write-Output "$(Get-TS): Adding package $WINPE_SPEECH_TTS_PATH to
WinRE"
                Add-WindowsPackage -Path $WINRE_MOUNT -PackagePath
$WINPE_SPEECH_TTS_PATH -ErrorAction stop | Out-Null

                Write-Output "$(Get-TS): Adding package $WINPE_SPEECH_TTS_LANG_PATH
to WinRE"
                Add-WindowsPackage -Path $WINRE_MOUNT -PackagePath
$WINPE_SPEECH_TTS_LANG_PATH -ErrorAction stop | Out-Null
            }
        }

        # Add Safe OS
        Write-Output "$(Get-TS): Adding package $SAFE_OS_DU_PATH to WinRE"
        Add-WindowsPackage -Path $WINRE_MOUNT -PackagePath $SAFE_OS_DU_PATH -
ErrorAction stop | Out-Null

        # Perform image cleanup
        Write-Output "$(Get-TS): Performing image cleanup on WinRE"
        DISM /image:$WINRE_MOUNT /cleanup-image /StartComponentCleanup /ResetBase
/Defer | Out-Null
        if ($LastExitCode -ne 0)
        {
            throw "Error: Failed to perform image cleanup on WinRE. Exit code:
$LastExitCode"
        }

        # Dismount
        Dismount-WindowsImage -Path $WINRE_MOUNT  -Save -ErrorAction stop | Out-Null

        # Export
        Write-Output "$(Get-TS): Exporting image to $WORKING_PATH\winre.wim"
        Export-WindowsImage -SourceImagePath $WORKING_PATH"\winre.wim" -SourceIndex
1 -DestinationImagePath $WORKING_PATH"\winre2.wim" -ErrorAction stop | Out-Null

    }

    Copy-Item -Path $WORKING_PATH"\winre2.wim" -Destination
$MAIN_OS_MOUNT"\windows\system32\recovery\winre.wim" -Force -ErrorAction stop | Out-
Null
```

```
    #
    # update Main OS
    #

    # Add servicing stack update (Step 17 from the table). Unlike WinRE and WinPE,
we don't need to check for error 0x8007007e
    Write-Output "$(Get-TS): Adding package $LCU_PATH to main OS, index
$($IMAGE.ImageIndex)"
    Add-WindowsPackage -Path $MAIN_OS_MOUNT -PackagePath $LCU_PATH | Out-Null


    # Optional: Add language to main OS and corresponding language experience
Features on Demand
    Write-Output "$(Get-TS): Adding package $OS_LP_PATH to main OS, index
$($IMAGE.ImageIndex)"
    Add-WindowsPackage -Path $MAIN_OS_MOUNT -PackagePath $OS_LP_PATH -ErrorAction
stop | Out-Null

    Write-Output "$(Get-TS): Adding language FOD: Language.Fonts.Jpan~~~und-
JPAN~0.0.1.0 to main OS, index $($IMAGE.ImageIndex)"
    Add-WindowsCapability -Name
"Language.Fonts.$LANG_FONT_CAPABILITY~~~und-$LANG_FONT_CAPABILITY~0.0.1.0" -Path
$MAIN_OS_MOUNT -Source $FOD_PATH -ErrorAction stop | Out-Null

    Write-Output "$(Get-TS): Adding language FOD: Language.Basic~~~$LANG~0.0.1.0 to
main OS, index $($IMAGE.ImageIndex)"
    Add-WindowsCapability -Name "Language.Basic~~~$LANG~0.0.1.0" -Path
$MAIN_OS_MOUNT -Source $FOD_PATH -ErrorAction stop | Out-Null

    Write-Output "$(Get-TS): Adding language FOD: Language.OCR~~~$LANG~0.0.1.0 to
main OS, index $($IMAGE.ImageIndex)"
    Add-WindowsCapability -Name "Language.OCR~~~$LANG~0.0.1.0" -Path $MAIN_OS_MOUNT
-Source $FOD_PATH -ErrorAction stop | Out-Null

    Write-Output "$(Get-TS): Adding language FOD:
Language.Handwriting~~~$LANG~0.0.1.0 to main OS, index $($IMAGE.ImageIndex)"
    Add-WindowsCapability -Name "Language.Handwriting~~~$LANG~0.0.1.0" -Path
$MAIN_OS_MOUNT -Source $FOD_PATH -ErrorAction stop | Out-Null

    Write-Output "$(Get-TS): Adding language FOD:
Language.TextToSpeech~~~$LANG~0.0.1.0 to main OS, index $($IMAGE.ImageIndex)"
    Add-WindowsCapability -Name "Language.TextToSpeech~~~$LANG~0.0.1.0" -Path
$MAIN_OS_MOUNT -Source $FOD_PATH -ErrorAction stop | Out-Null

    Write-Output "$(Get-TS): Adding language FOD: Language.Speech~~~$LANG~0.0.1.0 to
main OS, index $($IMAGE.ImageIndex)"
    Add-WindowsCapability -Name "Language.Speech~~~$LANG~0.0.1.0" -Path
$MAIN_OS_MOUNT -Source $FOD_PATH -ErrorAction stop | Out-Null

    # Optional: Add additional Features On Demand
    For ( $index = 0; $index -lt $FOD.count; $index++)#
    {
        Write-Output "$(Get-TS): Adding $($FOD[$index]) to main OS, index
$($IMAGE.ImageIndex)"
        Add-WindowsCapability -Name $($FOD[$index]) -Path $MAIN_OS_MOUNT -Source
```

```
$FOD_PATH -ErrorAction stop | Out-Null
    }

    # Optional: Add Legacy Features
    For ( $index = 0; $index -lt $OC.count; $index++)
    {
        Write-Output "$(Get-TS): Adding $($OC[$index]) to main OS, index
$($IMAGE.ImageIndex)"
        DISM /Image:$MAIN_OS_MOUNT /Enable-Feature /FeatureName:$($OC[$index]) /All
| Out-Null
        if ($LastExitCode -ne 0)
        {
            throw "Error: Failed to add $($OC[$index]) to main OS, index
$($IMAGE.ImageIndex). Exit code: $LastExitCode"
        }
    }

    # Add latest cumulative update
    Write-Output "$(Get-TS): Adding package $LCU_PATH to main OS, index
$($IMAGE.ImageIndex)"
    Add-WindowsPackage -Path $MAIN_OS_MOUNT -PackagePath $LCU_PATH -ErrorAction stop
| Out-Null

    # Perform image cleanup. Some Optional Components might require the image to be
booted, and thus
    # image cleanup may fail. We'll catch and handle as a warning.
    Write-Output "$(Get-TS): Performing image cleanup on main OS, index
$($IMAGE.ImageIndex)"
    DISM /image:$MAIN_OS_MOUNT /cleanup-image /StartComponentCleanup | Out-Null
    if ($LastExitCode -ne 0)
    {
        if ($LastExitCode -eq -2146498554)
        {
            # We hit 0x800F0806 CBS_E_PENDING. We will ignore this with a warning
            # This is likely due to legacy components being added that require
online operations.
            Write-Warning "$(Get-TS): Failed to perform image cleanup on main OS,
index $($IMAGE.ImageIndex). Exit code: $LastExitCode. The operation cannot be
performed until pending servicing operations are completed. The image must be booted
to complete the pending servicing operation."
        }
        else
        {
            throw "Error: Failed to perform image cleanup on main OS, index
$($IMAGE.ImageIndex). Exit code: $LastExitCode"
        }
    }

    # Finally, we'll add .NET 3.5 and the .NET cumulative update
    Write-Output "$(Get-TS): Adding NetFX3~~~~ to main OS, index
$($IMAGE.ImageIndex)"
    Add-WindowsCapability -Name "NetFX3~~~~" -Path $MAIN_OS_MOUNT -Source $FOD_PATH
-ErrorAction stop | Out-Null

    # Add .NET Cumulative Update
```

```
    Write-Output "$(Get-TS): Adding package $DOTNET_CU_PATH to main OS, index
$($IMAGE.ImageIndex)"
    Add-WindowsPackage -Path $MAIN_OS_MOUNT -PackagePath $DOTNET_CU_PATH -
ErrorAction stop | Out-Null

    # Dismount
    Dismount-WindowsImage -Path $MAIN_OS_MOUNT -Save -ErrorAction stop | Out-Null

    # Export
    Write-Output "$(Get-TS): Exporting image to $WORKING_PATH\install2.wim"
    Export-WindowsImage -SourceImagePath $MEDIA_NEW_PATH"\sources\install.wim" -
SourceIndex $IMAGE.ImageIndex -DestinationImagePath $WORKING_PATH"\install2.wim" -
ErrorAction stop | Out-Null
}

Move-Item -Path $WORKING_PATH"\install2.wim" -Destination
$MEDIA_NEW_PATH"\sources\install.wim" -Force -ErrorAction stop | Out-Null
```

Обновление WinPE

Этот скрипт аналогичен тому, который обновляет WinRE, но вместо этого он подключает Boot.wim, применяет пакеты с последним накопительным обновлением и сохраняет. Он повторяет это для всех образов внутри Boot.wim, обычно двух образов. Он начинается с применения динамического обновления стека обслуживания. Так как скрипт настраивает этот носитель на японском языке, он устанавливает языковой пакет из папки WinPE в ISO-файле языкового пакета. Кроме того, он добавляет поддержку шрифтов и текста в речь (TTS). Так как скрипт добавляет новый язык, он перестраивает lang.ini, используемый для идентификации языков, установленных в образе. Для второго образа мы сохраняем setup.exe и setuphost.exe для последующего использования, чтобы убедиться, что эти версии соответствуют \sources\setup.exe и \sources\setuphost.exe версии с установочного носителя. Если эти двоичные файлы не идентичны, программа установки Windows завершится ошибкой во время установки. Мы также сохраним обслуживаемые файлы диспетчера загрузки для последующего использования в скрипте. Наконец, скрипт очищает и экспортирует Boot.wim и копирует его обратно на новый носитель.

PowerShell

```
#
# update Windows Preinstallation Environment (WinPE)
#

# Get the list of images contained within WinPE
$WINPE_IMAGES = Get-WindowsImage -ImagePath $MEDIA_NEW_PATH"\sources\boot.wim"

Foreach ($IMAGE in $WINPE_IMAGES)
{
```

```
    # update WinPE
    Write-Output "$(Get-TS): Mounting WinPE, image index $($IMAGE.ImageIndex)"
    Mount-WindowsImage -ImagePath $MEDIA_NEW_PATH"\sources\boot.wim" -Index
$IMAGE.ImageIndex -Path $WINPE_MOUNT -ErrorAction stop | Out-Null

    # Add servicing stack update (Step 9 from the table)
    try
    {
        Write-Output "$(Get-TS): Adding package $LCU_PATH to WinPE, image index
$($IMAGE.ImageIndex)"
        Add-WindowsPackage -Path $WINPE_MOUNT -PackagePath $LCU_PATH | Out-Null
    }
    Catch
    {
        $theError = $_
        Write-Output "$(Get-TS): $theError"
        if ($theError.Exception -like "*0x8007007e*")
        {
            Write-Warning "$(Get-TS): Failed with error 0x8007007e. This failure is
a known issue with combined cumulative update, we can ignore."
        }
        else
        {
            throw
        }
    }

    # Install lp.cab cab
    Write-Output "$(Get-TS): Adding package $WINPE_OC_LP_PATH to WinPE, image index
$($IMAGE.ImageIndex)"
    Add-WindowsPackage -Path $WINPE_MOUNT -PackagePath $WINPE_OC_LP_PATH -
ErrorAction stop | Out-Null

    # Install language cabs for each optional package installed
    $WINPE_INSTALLED_OC = Get-WindowsPackage -Path $WINPE_MOUNT
    Foreach ($PACKAGE in $WINPE_INSTALLED_OC)
    {
        if ( ($PACKAGE.PackageState -eq "Installed") -and
($PACKAGE.PackageName.startsWith("WinPE-")) -and ($PACKAGE.ReleaseType -eq
"FeaturePack") )
        {
            $INDEX = $PACKAGE.PackageName.IndexOf("-Package")
            if ($INDEX -ge 0)
            {
                $OC_CAB = $PACKAGE.PackageName.Substring(0, $INDEX) + "_" + $LANG +
".cab"
                if ($WINPE_OC_LANG_CABS.Contains($OC_CAB))
                {
                    $OC_CAB_PATH = Join-Path $WINPE_OC_LANG_PATH $OC_CAB

                    Write-Output "$(Get-TS): Adding package $OC_CAB_PATH to WinPE,
image index $($IMAGE.ImageIndex)"
                    Add-WindowsPackage -Path $WINPE_MOUNT -PackagePath $OC_CAB_PATH
-ErrorAction stop | Out-Null
                }
```

```
            }
        }
    }

    # Add font support for the new language
    if ( (Test-Path -Path $WINPE_FONT_SUPPORT_PATH) )
    {
        Write-Output "$(Get-TS): Adding package $WINPE_FONT_SUPPORT_PATH to WinPE,
image index $($IMAGE.ImageIndex)"
        Add-WindowsPackage -Path $WINPE_MOUNT -PackagePath $WINPE_FONT_SUPPORT_PATH
-ErrorAction stop | Out-Null
    }

    # Add TTS support for the new language
    if (Test-Path -Path $WINPE_SPEECH_TTS_PATH)
    {
        if ( (Test-Path -Path $WINPE_SPEECH_TTS_LANG_PATH) )
        {
            Write-Output "$(Get-TS): Adding package $WINPE_SPEECH_TTS_PATH to WinPE,
image index $($IMAGE.ImageIndex)"
            Add-WindowsPackage -Path $WINPE_MOUNT -PackagePath
$WINPE_SPEECH_TTS_PATH -ErrorAction stop | Out-Null

            Write-Output "$(Get-TS): Adding package $WINPE_SPEECH_TTS_LANG_PATH to
WinPE, image index $($IMAGE.ImageIndex)"
            Add-WindowsPackage -Path $WINPE_MOUNT -PackagePath
$WINPE_SPEECH_TTS_LANG_PATH -ErrorAction stop | Out-Null
        }
    }

    # Generates a new Lang.ini file which is used to define the language packs
inside the image
    if ( (Test-Path -Path $WINPE_MOUNT"\sources\lang.ini") )
    {
        Write-Output "$(Get-TS): Updating lang.ini"
        DISM /image:$WINPE_MOUNT /Gen-LangINI /distribution:$WINPE_MOUNT | Out-Null
        if ($LastExitCode -ne 0)
        {
            throw "Error: Failed to update lang.ini. Exit code: $LastExitCode"
        }
    }

    # Add latest cumulative update
    Write-Output "$(Get-TS): Adding package $LCU_PATH to WinPE, image index
$($IMAGE.ImageIndex)"
    Add-WindowsPackage -Path $WINPE_MOUNT -PackagePath $LCU_PATH -ErrorAction stop |
Out-Null

    # Perform image cleanup
    Write-Output "$(Get-TS): Performing image cleanup on WinPE, image index
$($IMAGE.ImageIndex)"
    DISM /image:$WINPE_MOUNT /cleanup-image /StartComponentCleanup /ResetBase /Defer
| Out-Null
    if ($LastExitCode -ne 0)
    {
```

```
        throw "Error: Failed to perform image cleanup on WinPE, image index
$($IMAGE.ImageIndex). Exit code: $LastExitCode"
    }

    if ($IMAGE.ImageIndex -eq "2")
    {
        # Save setup.exe for later use. This will address possible binary mismatch
with the version in the main OS \sources folder
        Copy-Item -Path $WINPE_MOUNT"\sources\setup.exe" -Destination
$WORKING_PATH"\setup.exe" -Force -ErrorAction stop | Out-Null

        # Save setuphost.exe for later use. This will address possible binary
mismatch with the version in the main OS \sources folder
        # This is only required starting with Windows 11 version 24H2
        $TEMP = Get-WindowsImage -ImagePath $MEDIA_NEW_PATH"\sources\boot.wim" -
Index $IMAGE.ImageIndex
        if ([System.Version]$TEMP.Version -ge [System.Version]"10.0.26100")
        {
            Copy-Item -Path $WINPE_MOUNT"\sources\setuphost.exe" -Destination
$WORKING_PATH"\setuphost.exe" -Force -ErrorAction stop | Out-Null
        }
        else
        {
            Write-Output "$(Get-TS): Skipping copy of setuphost.exe; image version
$($TEMP.Version)"
        }

        # Save serviced boot manager files later copy to the root media.
        Copy-Item -Path $WINPE_MOUNT"\Windows\boot\efi\bootmgfw.efi" -Destination
$WORKING_PATH"\bootmgfw.efi" -Force -ErrorAction stop | Out-Null
        Copy-Item -Path $WINPE_MOUNT"\Windows\boot\efi\bootmgr.efi" -Destination
$WORKING_PATH"\bootmgr.efi" -Force -ErrorAction stop | Out-Null
    }

    # Dismount
    Dismount-WindowsImage -Path $WINPE_MOUNT -Save -ErrorAction stop | Out-Null

    #Export WinPE
    Write-Output "$(Get-TS): Exporting image to $WORKING_PATH\boot2.wim"
    Export-WindowsImage -SourceImagePath $MEDIA_NEW_PATH"\sources\boot.wim" -
SourceIndex $IMAGE.ImageIndex -DestinationImagePath $WORKING_PATH"\boot2.wim" -
ErrorAction stop | Out-Null
}

Move-Item -Path $WORKING_PATH"\boot2.wim" -Destination
$MEDIA_NEW_PATH"\sources\boot.wim" -Force -ErrorAction stop | Out-Null
```

Обновление оставшихся файлов мультимедиа

Эта часть скрипта обновляет файлы установки. Он просто копирует отдельные файлы из пакета динамического обновления установки на новый носитель. На этом шаге по мере

необходимости будут добавлены обновленные файлы установки, а также последняя база данных совместимости и манифесты компонентов замены. Этот скрипт также выполняет окончательную замену файлов setup.exe, setuphost.exe и диспетчера загрузки с использованием ранее сохраненных версий из WinPE.

PowerShell

```
#
# update remaining files on media
#

# Add Setup DU by copy the files from the package into the newMedia
Write-Output "$(Get-TS): Adding package $SETUP_DU_PATH"
cmd.exe /c $env:SystemRoot\System32\expand.exe $SETUP_DU_PATH -F:*
$MEDIA_NEW_PATH"\sources" | Out-Null
if ($LastExitCode -ne 0)
{
    throw "Error: Failed to expand $SETUP_DU_PATH. Exit code: $LastExitCode"
}

# Copy setup.exe from boot.wim, saved earlier.
Write-Output "$(Get-TS): Copying $WORKING_PATH\setup.exe to
$MEDIA_NEW_PATH\sources\setup.exe"
Copy-Item -Path $WORKING_PATH"\setup.exe" -Destination
$MEDIA_NEW_PATH"\sources\setup.exe" -Force -ErrorAction stop | Out-Null

# Copy setuphost.exe from boot.wim, saved earlier.
if (Test-Path -Path $WORKING_PATH"\setuphost.exe")
{
    Write-Output "$(Get-TS): Copying $WORKING_PATH\setuphost.exe to
$MEDIA_NEW_PATH\sources\setuphost.exe"
    Copy-Item -Path $WORKING_PATH"\setuphost.exe" -Destination
$MEDIA_NEW_PATH"\sources\setuphost.exe" -Force -ErrorAction stop | Out-Null
}

# Copy bootmgr files from boot.wim, saved earlier.
$MEDIA_NEW_FILES = Get-ChildItem $MEDIA_NEW_PATH -Force -Recurse -Filter b*.efi

Foreach ($File in $MEDIA_NEW_FILES)
{
    if (($File.Name -ieq "bootmgfw.efi") -or ($File.Name -ieq "bootx64.efi") -or
($File.Name -ieq "bootia32.efi") -or ($File.Name -ieq "bootaa64.efi"))
    {
        Write-Output "$(Get-TS): Copying $WORKING_PATH\bootmgfw.efi to
$($File.FullName)"
        Copy-Item -Path $WORKING_PATH"\bootmgfw.efi" -Destination $File.FullName -
Force -ErrorAction stop | Out-Null
    }
    elseif ($File.Name -ieq "bootmgr.efi")
    {
        Write-Output "$(Get-TS): Copying $WORKING_PATH\bootmgr.efi to
$($File.FullName)"
        Copy-Item -Path $WORKING_PATH"\bootmgr.efi" -Destination $File.FullName -
```

```
Force -ErrorAction stop | Out-Null
    }
}
```

Завершить

В качестве последнего шага скрипт удаляет рабочую папку временных файлов и отключает наш языковой пакет и компоненты по запросу ISOS.

PowerShell

```
#
# Perform final cleanup
#

# Remove our working folder
Remove-Item -Path $WORKING_PATH -Recurse -Force -ErrorAction stop | Out-Null

# Dismount ISO images
Write-Output "$(Get-TS): Dismounting ISO images"
Dismount-DiskImage -ImagePath $FOD_ISO_PATH -ErrorAction stop | Out-Null

Write-Output "$(Get-TS): Media refresh completed!"
```

Last updated on 27.06.2025

Перенос и получение дополнительного содержимого Windows во время обновлений

Статья • 22.04.2024 • Применяется к: ✅ Windows 11, ✅ Windows 10

В этой статье приведены некоторые сведения о проблеме сохранения языковых ресурсов и функций по запросу во время обновлений операционной системы, а также рекомендации, которые помогут вам двигаться вперед в краткосрочной перспективе и подготовиться к долгосрочной перспективе.

При обновлении операционной системы важно сохранить языковые ресурсы и функции по запросу (FOD). Многие коммерческие организации используют Configuration Manager или другие средства управления для распространения и оркестрации установки клиента Windows с помощью локального образа Windows или *WIM-файла (обновление на основе мультимедиа* или *последовательности задач*). Другие пользователи выполняют обновления на месте с помощью утвержденного обновления компонентов клиента Windows с помощью Windows Server Update Services (WSUS), Configuration Manager или эквивалентных средств (обновление *на основе обслуживания*).

Ни один из подходов не содержит полный набор дополнительных функций Windows, которые могут потребоваться устройству пользователя, поэтому эти функции не переносятся в новую операционную систему. В прошлом эти функции не были доступны в Configuration Manager и WSUS для локального приобретения после обновления компонентов.

Что такое необязательное содержимое?

Дополнительное содержимое включает следующие элементы:

- Общие функции по запросу, также называемые FOD (например, Windows Mixed Reality)
- Языковые и региональные FOD (например, Language.Basic~~ja-jp~0.0.1.0)
- Пакеты локального интерфейса
- Языковые пакеты

Необязательное содержимое не включается по умолчанию в файл образа Windows, который является частью носителя операционной системы, доступного в Центре обслуживания корпоративного лицензирования (VLSC). Вместо этого он

выпускается в виде дополнительного ISO-файла в VLSC. Доставка этих функций с носителя операционной системы и их отдельная доставка сокращает дисковое пространство Windows. Такой подход предоставляет больше места для данных пользователя. Это также сокращает время, необходимое для обслуживания операционной системы, будь то установка ежемесячного обновления качества или обновление до более новой версии. Меньший образ Windows по умолчанию также означает меньше данных для передачи по сети.

Почему получение дополнительного содержимого является сложной задачей?

Проблемы, связанные с дополнительным содержимым, обычно делятся на две группы:

Неполные обновления операционной системы

Первая проблема связана с переносом содержимого во время обновления компонентов. Когда программа установки Windows выполняет обновление на месте, новая операционная система записывается на диск пользователя вместе со старой версией во временной папке, где устанавливается вторая чистая операционная система и подготавливается к *переходу* пользователя. При выполнении операции программа установки Windows перечисляет дополнительное содержимое, установленное уже в текущей версии, и планирует установить новую версию этого содержимого в новой операционной системе.

Программе установки Windows требуется доступ к необязательному содержимому. Так как необязательное содержимое по умолчанию не содержится в образе Windows, программа установки Windows должна искать в другом месте, чтобы получить пакеты Windows, подготовить их к этапу, а затем установить их в новой операционной системе. Если содержимое не удается найти, результатом является обновление, в результате чего отсутствуют функции на устройстве, разочарованный конечный пользователь и, скорее всего, звонок в службу поддержки. Эту болевую точку иногда называют *неудачей при переносе необязательного содержимого во время обновления*. Для обновлений на основе мультимедиа Windows автоматически попытается повторить попытку после загрузки новой операционной системы. Мы называем это *скрытым приобретением*.

Сбой при получении компонентов, инициированных пользователем

Вторая проблема связана с неспособностью получить функции, когда пользователь запрашивает их. Представьте себе пользователя, работающего на устройстве с новой версией клиента Windows, с помощью чистой установки или обновления на месте. Пользователь посещает **параметры** и пытается установить второй язык, дополнительные функции языкового интерфейса или другое необязательное содержимое. Опять же, так как эти функции отсутствуют в операционной системе, пакеты необходимо получить. Для обычного пользователя с доступом к Интернету Windows приобретает функции из соседней сети доставки содержимого Майкрософт, и все работает по плану. Для коммерческих пользователей некоторые из них могут не иметь доступа к Интернету или иметь политики для предотвращения приобретения через Интернет. В таких ситуациях Windows должна получать содержимое из другого расположения. Если содержимое не удается найти, пользователи расстроены, и может возникнуть другой звонок в службу поддержки. Эту болевую точку иногда называют *неспособностью получить необязательное содержимое*.

Параметры получения дополнительного содержимого

Большинство коммерческих организаций понимают описанные выше проблемы, и обсуждения обычно начинаются с вопроса о том, какие планы доступны для решения этих проблем. В следующей таблице приведено несколько вариантов, которые следует рассмотреть в зависимости от того, как вы сейчас развертываете клиент Windows. В заголовках таблицы используются следующие определения:

- **Миграция**. Поддерживает необязательную миграцию содержимого во время обновления.
- **Приобретение**: поддерживает необязательный сбор содержимого (т. е. инициированный пользователем).
- **Мультимедиа**: применимо к развертываниям на основе мультимедиа.
- **Обслуживание**: применимо к развертываниям на основе обслуживания.

Развернуть таблицу

Метод	Миграция	Приобретение	Носители	Обслуживание
Вариант 1. Использование клиентский компонент Центра	Да	Да	Нет	Да

Метод	Миграция	Приобретение	Носители	Обслуживание
обновления Windows				
Вариант 2. Использование WSUS с интеграцией UUP	Да	Да	Нет	Да
Вариант 3. Включение динамического обновления	Да	Нет	Да	Да
Вариант 4. Настройка образа Windows перед развертыванием	Да	Нет	Да	Нет
Вариант 5. Установка языковых компонентов во время развертывания	Частично	Нет	Да	Нет
Вариант 6. Установка дополнительного содержимого после развертывания	Да	Нет	Да	Да
Вариант 7. Настройка альтернативного источника для функций по запросу	Нет	Частично	Да	Да

Вариант 1. Использование клиентский компонент Центра обновления Windows

клиентский компонент Центра обновления Windows для бизнеса решает необязательную проблему с содержимым. Дополнительное содержимое публикуется и доступно для приобретения программой установки Windows из ближайшей сети доставки содержимого Майкрософт и приобретается с помощью единой платформы обновлений. Необязательные сценарии миграции и получения содержимого работают только тогда, когда устройство подключено к службе обновлений, которая использует единую платформу обновлений, например клиентский компонент Центра обновления Windows или клиентский компонент Центра обновления Windows для бизнеса. Если по какой-либо причине языковой пакет не удается установить во время обновления, обновление автоматически откатится.

Единая платформа обновлений — это усовершенствование базовой технологии обновления Windows, которая приводит к уменьшению размеров загрузки и более эффективному протоколу для проверки наличия обновлений, получения и установки необходимых пакетов и получения актуальной информации за один шаг

обновления. Эта технология *является унифицированной* , так как она объединяет стек обновлений для клиента Windows, Windows Server и других продуктов, таких как HoloLens.

Рассмотрите возможность перехода на клиентский компонент Центра обновления Windows для бизнеса. Необязательный сценарий содержимого будет работать не только без проблем (как это делается сегодня для потребительских устройств), но вы также получите все преимущества загрузки меньшего размера. Кроме того, устройства не подвержены проблеме обновления Windows, когда язык установки операционной системы непреднамеренно изменяется на новый. В противном случае любые будущие обновления компонентов на основе носителя могут завершиться ошибкой, если установочный носитель имеет другой язык установки. Дополнительные сведения об этой проблеме см. в статье Обновление Windows 10 устройств с установочным носителем, отличным от исходного языка установки ОС.

Вариант 2. Использование WSUS с интеграцией UUP

Начиная с марта 2023 г., UUP интегрируется с WSUS и Configuration Manager, чтобы обеспечить в локальных решениях по управлению те же дополнительные преимущества содержимого и приобретения, что и клиентский компонент Центра обновления Windows. Пример

- FoD и языки будут автоматически переноситься для устройств, которые выполняют обновление на месте с помощью утвержденного обновления функций клиента Windows 11 версии 22H2 из WSUS. Аналогичным образом, обновления, такие как объединенное накопительное обновление, обновления установки и обновления безопасной ОС, включаются и актуальны в зависимости от месяца утверждения обновления компонентов.

- Устройства, которые обновляются с помощью локального образа Windows, но используют WSUS или Configuration Manager для утверждения объединенного накопительного обновления, будут иметь поддержку дополнительного получения содержимого в обновленной ОС Windows, а также самостоятельного восстановления ОС.

Содержимое, необходимое для включения этой функции, будет получаться через WSUS или Configuration Manager без подключения к Интернету для конечных точек клиента. Чтобы включить это улучшение, один раз за основной выпуск Windows требуется значительное скачивание в каталог содержимого WSUS или точку распространения. Сюда входят пакеты для поддержки FOD и приобретения языка,

а также пакеты для обеспечения самовосстановления ОС из-за повреждения. Дополнительные сведения см. в статье Планирование развертывания WSUS.

Вариант 3. Включение динамического обновления

Если вы не готовы перейти на клиентский компонент Центра обновления Windows, другой вариант — включить динамическое обновление во время обновления компонентов. Как только запускается обновление компонентов Windows, будь то с помощью обновления на основе мультимедиа или обновления компонентов на основе WSUS, динамическое обновление является одним из первых этапов вызова. Программа установки Windows подключается к URL-адресу для доступа к Интернету, размещенного корпорацией Майкрософт, для получения содержимого динамического обновления, а затем применяет эти обновления к установочному носителю операционной системы. Полученное содержимое включает следующее:

- **Обновления установки**. Исправления для Setup.exe двоичных файлов или файлов, используемых программой установки для обновления компонентов.
- **Безопасные обновления ОС**: исправления для *безопасной ОС* , которые используются для обновления среды восстановления Windows (WinRE).
- **Обновления стека обслуживания**. Исправления, необходимые для решения проблемы с стека обслуживания Windows и, следовательно, необходимые для завершения обновления компонентов.
- **Последнее накопительное обновление**. Устанавливает последнее накопительное обновление качества.
- **Обновления драйверов**. Последняя версия применимых драйверов, которые уже были опубликованы производителями в клиентский компонент Центра обновления Windows и предназначены специально для динамического обновления.

В дополнение к этим обновлениям для новой операционной системы динамическое обновление получает необязательное содержимое во время процесса обновления, чтобы гарантировать наличие этого содержимого на устройстве по завершении обновления. Таким образом, хотя устройство не подключено к клиентский компонент Центра обновления Windows, оно получает содержимое из соседней сети загрузки содержимого Майкрософт (CDN). Этот подход устраняет первую боль с необязательным содержимым, но не с инициированным пользователем приобретением. По умолчанию динамическое обновление включается программой установки Windows. Динамическое обновление можно включить или отключить с помощью параметра /DynamicUpdate в программе установки Windows. Если используется подход на основе обслуживания, это значение можно задать с `setupconfig.ini` помощью .

Дополнительные сведения см. в статье Общие сведения об автоматизации установки Windows .

Динамическое обновление можно настроить с помощью дополнительных параметров. Например, вы можете воспользоваться преимуществами необязательной миграции содержимого без автоматического получения последнего обновления качества. Это можно сделать с помощью параметра /DynamicUpdate NoLCU программы установки Windows. После этого вы будете отдельно следовать существующему процессу тестирования и утверждения ежемесячных обновлений. Недостатком этого подхода является повторная перезагрузка устройства для последнего накопительного обновления, так как оно было недоступно во время обновления компонентов.

При использовании динамического обновления следует учитывать влияние на сеть. Одним из основных блокировщиков этого подхода является забота о том, что каждое устройство будет получать это содержимое отдельно от корпорации Майкрософт. Программа установки скачивает содержимое динамического обновления с помощью оптимизации доставки, если это доступно. Для устройств, которые не подключены к Интернету, подмножество содержимого динамического обновления доступно с помощью WSUS и каталога Майкрософт.

Вариант 4. Настройка образа Windows перед развертыванием

Во многих организациях рабочий процесс развертывания включает Configuration Manager последовательность задач, которая выполняет обновление на основе мультимедиа. Некоторые клиенты либо не имеют подключения к Интернету, либо подключение плохое, поэтому они не могут включить динамическое обновление. В таких случаях рекомендуется установить дополнительное содержимое перед развертыванием. Это действие иногда называют настройкой установочного носителя.

Образ Windows можно настроить следующими способами:

- Применение накопительного обновления
- Применение обновлений к стеку обслуживания
- Применение обновлений к двоичным `Setup.exe` файлам или другим файлам, которые программа установки использует для обновления компонентов
- Применение обновлений для *безопасной операционной системы* (SafeOS), используемой для среды восстановления Windows
- Добавление или удаление языков
- Добавление или удаление компонентов по запросу

Преимущество этого параметра заключается в том, что образ Windows может включать эти дополнительные языки, функции языкового интерфейса и другие функции по запросу путем однократных обновлений образа. Затем их можно использовать в существующей последовательности задач или настраиваемом развертывании, где `Setup.exe` они задействованы. Недостатком этого подхода является то, что он требует предварительной подготовки образа, включая создание скриптов с помощью DISM для установки дополнительных пакетов. Это также означает, что образ одинаков для всех устройств, которые его используют и может содержать больше функций, чем требуется некоторым пользователям. Дополнительные сведения о настройке носителя см. в разделе Обновление Windows 10 мультимедиа с помощью пакетов динамического обновления. Кроме того, как и в случае с динамическим обновлением, у вас по-прежнему есть решение для переноса необязательного содержимого, но не поддерживается инициированное пользователем необязательное получение содержимого. Кроме того, существует вариант этого параметра, в котором носитель обновляется *на устройстве* непосредственно перед установкой. Этот параметр позволяет настроить образ для конкретного устройства в зависимости от установленных в настоящее время.

Вариант 5. Установка языковых компонентов во время развертывания

Частичное решение для решения первой проблемной точки, когда не удалось перенести необязательное содержимое во время обновления, заключается в внедрении подмножества необязательного содержимого во время процесса обновления. Этот подход использует параметр установки Windows /InstallLangPacks для добавления языковых пакетов и языковых возможностей, таких как распознавание текста в речь, из папки, содержащей пакеты. Такой подход позволяет ИТ-специалисту взять подмножество дополнительного содержимого и подготовить его в своей сети. Если вы используете подход на основе обслуживания, вы можете настроить InstallLangPacks с помощью `setupconfig.ini`. Дополнительные сведения см. в статье Общие сведения об автоматизации установки Windows.

При запуске программа установки внедряет эти пакеты в новую операционную систему во время установки. Это может быть альтернативой включению динамического обновления или настройке образа операционной системы перед развертыванием. При таком подходе необходимо соблюдать осторожность, так как пакеты не могут быть переименованы. Кроме того, содержимое поступает от двух отдельных носителей isos. Ключ заключается в том, чтобы скопировать пакеты FOD

и метаданные FOD .cab из FOD ISO в папку, а языковой пакет для конкретной архитектуры .cab файлы из ISO-файла LPLIP. Мы обрабатываем сбои InstallLangPacks как неустранимые и откатаем все обновление. Идея заключается в том, чтобы не оставлять пользователя в плохом состоянии, так как обновления на основе мультимедиа не переносят FOD и языки (если динамическое обновление не включено).

Этот подход имеет некоторые интересные преимущества. Исходный образ Windows не требуется изменять, что позволяет сэкономить время и создание скриптов.

Вариант 6. Установка дополнительного содержимого после развертывания

Этот параметр похож на вариант 4 в том, что после его развертывания вы настраиваете образ операционной системы с дополнительным содержимым. ИТ-специалисты могут расширить поведение программы установки Windows, выполняя собственные пользовательские сценарии действий во время и после обновления компонентов. Дополнительные сведения см. в статье Выполнение пользовательских действий во время обновления компонентов . При таком подходе можно создать миграцию необязательного содержимого для конкретного устройства, запечатав необязательное содержимое, установленное в операционной системе, а затем сохранив этот список, чтобы установить то же необязательное содержимое в новой операционной системе. Как и в варианте 5, вы будете внутренне размещать сетевую папку, содержащую источник необязательных пакетов содержимого. Затем во время выполнения программы установки на устройстве запишите список установленного дополнительного содержимого из исходной операционной системы и сохраните. Позже, после завершения установки, вы используете список для установки дополнительного содержимого, которое оставляет устройство пользователя без потери функциональности.

Вариант 7. Настройка альтернативного источника для необязательного содержимого

Несколько вариантов позволяют устранить необязательные проблемы миграции содержимого во время обновления на месте. Чтобы устранить вторую проблемную точку легкого получения необязательного содержимого в инициированном пользователем случае, можно настроить каждое устройство с помощью групповая политика Указание параметров для установки необязательных

компонентов и восстановления компонентов. Этот параметр политики определяет сетевые расположения, которые будут использоваться для устранения повреждений операционной системы и включения дополнительных функций, для которых были удалены файлы полезных данных. Этот подход имеет недостаток большего количества содержимого для размещения в сети (в дополнение к образу операционной системы, который вы все еще развертываете на некоторых клиентах), но имеет преимущество получения содержимого в сети. Некоторые напоминания об этой политике:

- Путь к файлу к альтернативному источнику должен быть полным путем. Несколько расположений можно разделить точкой с запятой.
- Этот параметр не поддерживает установку языковых пакетов из альтернативного пути к исходному файлу, только функции по запросу. Если политика настроена для получения содержимого из клиентский компонент Центра обновления Windows, будут получены языковые пакеты.
- Если этот параметр не настроен или отключен, файлы скачиваются из расположения по умолчанию клиентский компонент Центра обновления Windows, например клиентский компонент Центра обновления Windows для бизнеса или WSUS.

Дополнительные сведения см. в разделах Настройка источника восстановления Windows и Как сделать функции по запросу и языковые пакеты доступными при использовании WSUS или Configuration Manager.

Дополнительные ресурсы

Дополнительные сведения о единой платформе обновлений и подходах, описанных в этой статье, см. в следующих ресурсах:

- Планирование развертывания WSUS
- /InstallLangPacks
- /DynamicUpdate
- Настройка источника восстановления Windows
- Выполнение пользовательских действий во время обновления компонентов
- Единая платформа обновлений
- Обновление установочного носителя Windows с помощью пакетов динамического обновления
- Обзор автоматизации установки Windows

Образцы сценариев

Варианты 4 и 6 предполагают наибольшее использование скриптов. Примеры скриптов для варианта 4 уже существуют, поэтому давайте рассмотрим примеры скриптов для варианта 6: установка дополнительного содержимого после развертывания.

Создание необязательного репозитория содержимого

Чтобы приступить к работе, мы создадим репозиторий с дополнительным содержимым и размещением в общей сетевой папке. Это подмножество содержимого из ОБЪЕКТОВ ISOS FOD и языковых пакетов, которые поставляются с каждым выпуском. Мы настраиваем этот репозиторий или репозиторий только с теми FOD, которые нужны нашей организации, с помощью DISM /Export. Например, надмножество, основанное на инвентаризации дополнительных компонентов, установленных на существующих устройствах. В этом случае мы исключаем функцию Windows Mixed Reality. Кроме того, мы копируем все языковые пакеты в корень репозитория.

PowerShell

```
# Declare media for FOD and LPs
$LP_ISO_PATH = "C:\_IMAGE\2004_ISO\CLIENTLANGPACKDVD_OEM_MULTI.iso"
$FOD_ISO_PATH = "C:\_IMAGE\2004_ISO\FOD-PACKAGES_OEM_PT1_amd64fre_MULTI.iso"

# Declare folders
$WORKING_PATH = "C:\_IMAGE\BuildRepo"
$MEDIA_PATH = "C:\_IMAGE\2004_SETUP"

$MAIN_OS_MOUNT = $WORKING_PATH + "\MainOSMount"
$REPO_PATH = $WORKING_PATH + "\Repo"

# Create folders for mounting image optional content repository
if (Test-Path $MAIN_OS_MOUNT) {
    Remove-Item -Path $MAIN_OS_MOUNT -Force -Recurse -ErrorAction stop| Out-
Null
}

if (Test-Path $REPO_PATH) {
    Remove-Item -Path $REPO_PATH -Force -Recurse -ErrorAction stop| Out-Null
}

New-Item -ItemType Directory -Force -Path $MAIN_OS_MOUNT -ErrorAction stop|
Out-Null
New-Item -ItemType Directory -Force -Path $REPO_PATH -ErrorAction stop| Out-
Null

# Mount the main OS, I'll use this throughout the script
Write-Host "Mounting main OS"
Mount-WindowsImage -ImagePath $MEDIA_PATH"\sources\install.wim" -Index 1 -
Path $MAIN_OS_MOUNT -ErrorAction stop| Out-Null
```

```
# Mount the LP ISO
Write-Host "Mounting LP ISO"
$LP_ISO_DRIVE_LETTER = (Mount-DiskImage -ImagePath $LP_ISO_PATH -ErrorAction
stop | Get-Volume).DriveLetter

# Declare language related cabs
$OS_LP_PATH = $LP_ISO_DRIVE_LETTER + ":\x64\langpacks\" + "*.cab"

# Mount the FOD ISO
Write-Host "Mounting FOD ISO"
$FOD_ISO_DRIVE_LETTER = (Mount-DiskImage -ImagePath $FOD_ISO_PATH -
ErrorAction stop | Get-Volume).DriveLetter
$FOD_PATH = $FOD_ISO_DRIVE_LETTER + ":\"

# Export the FODs from the ISO that we are interested in
Write-Host "Exporting FODs to Repo"
DISM /image:$MAIN_OS_MOUNT /export-source /source:$FOD_PATH
/target:$REPO_PATH `
    /capabilityname:Accessibility.Braille~~~~0.0.1.0 `
    /capabilityname:App.StepsRecorder~~~~0.0.1.0 `
    /capabilityname:App.WirelessDisplay.Connect~~~~0.0.1.0 `
    /capabilityname:Browser.InternetExplorer~~~~0.0.11.0 `
    /capabilityname:DirectX.Configuration.Database~~~~0.0.1.0 `
    /capabilityname:Language.Basic~~~af-za~0.0.1.0 `
    /capabilityname:Language.Basic~~~ar-sa~0.0.1.0 `
    /capabilityname:Language.Basic~~~as-in~0.0.1.0 `
    /capabilityname:Language.Basic~~~az-latn-az~0.0.1.0 `
    /capabilityname:Language.Basic~~~ba-ru~0.0.1.0 `
    /capabilityname:Language.Basic~~~be-by~0.0.1.0 `
    /capabilityname:Language.Basic~~~bg-bg~0.0.1.0 `
    /capabilityname:Language.Basic~~~bn-bd~0.0.1.0 `
    /capabilityname:Language.Basic~~~bn-in~0.0.1.0 `
    /capabilityname:Language.Basic~~~bs-latn-ba~0.0.1.0 `
    /capabilityname:Language.Basic~~~ca-es~0.0.1.0 `
    /capabilityname:Language.Basic~~~cs-cz~0.0.1.0 `
    /capabilityname:Language.Basic~~~cy-gb~0.0.1.0 `
    /capabilityname:Language.Basic~~~da-dk~0.0.1.0 `
    /capabilityname:Language.Basic~~~de-ch~0.0.1.0 `
    /capabilityname:Language.Basic~~~de-de~0.0.1.0 `
    /capabilityname:Language.Basic~~~el-gr~0.0.1.0 `
    /capabilityname:Language.Basic~~~en-au~0.0.1.0 `
    /capabilityname:Language.Basic~~~en-ca~0.0.1.0 `
    /capabilityname:Language.Basic~~~en-gb~0.0.1.0 `
    /capabilityname:Language.Basic~~~en-in~0.0.1.0 `
    /capabilityname:Language.Basic~~~en-us~0.0.1.0 `
    /capabilityname:Language.Basic~~~es-es~0.0.1.0 `
    /capabilityname:Language.Basic~~~es-mx~0.0.1.0 `
    /capabilityname:Language.Basic~~~es-us~0.0.1.0 `
    /capabilityname:Language.Basic~~~et-ee~0.0.1.0 `
    /capabilityname:Language.Basic~~~eu-es~0.0.1.0 `
    /capabilityname:Language.Basic~~~fa-ir~0.0.1.0 `
    /capabilityname:Language.Basic~~~fi-fi~0.0.1.0 `
    /capabilityname:Language.Basic~~~fil-ph~0.0.1.0 `
    /capabilityname:Language.Basic~~~fr-be~0.0.1.0 `
```

```
    /capabilityname:Language.Basic~~~fr-ca~0.0.1.0 `
    /capabilityname:Language.Basic~~~fr-ch~0.0.1.0 `
    /capabilityname:Language.Basic~~~fr-fr~0.0.1.0 `
    /capabilityname:Language.Basic~~~ga-ie~0.0.1.0 `
    /capabilityname:Language.Basic~~~gd-gb~0.0.1.0 `
    /capabilityname:Language.Basic~~~gl-es~0.0.1.0 `
    /capabilityname:Language.Basic~~~gu-in~0.0.1.0 `
    /capabilityname:Language.Basic~~~ha-latn-ng~0.0.1.0 `
    /capabilityname:Language.Basic~~~haw-us~0.0.1.0 `
    /capabilityname:Language.Basic~~~he-il~0.0.1.0 `
    /capabilityname:Language.Basic~~~hi-in~0.0.1.0 `
    /capabilityname:Language.Basic~~~hr-hr~0.0.1.0 `
    /capabilityname:Language.Basic~~~hu-hu~0.0.1.0 `
    /capabilityname:Language.Basic~~~hy-am~0.0.1.0 `
    /capabilityname:Language.Basic~~~id-id~0.0.1.0 `
    /capabilityname:Language.Basic~~~ig-ng~0.0.1.0 `
    /capabilityname:Language.Basic~~~is-is~0.0.1.0 `
    /capabilityname:Language.Basic~~~it-it~0.0.1.0 `
    /capabilityname:Language.Basic~~~ja-jp~0.0.1.0 `
    /capabilityname:Language.Basic~~~ka-ge~0.0.1.0 `
    /capabilityname:Language.Basic~~~kk-kz~0.0.1.0 `
    /capabilityname:Language.Basic~~~kl-gl~0.0.1.0 `
    /capabilityname:Language.Basic~~~kn-in~0.0.1.0 `
    /capabilityname:Language.Basic~~~kok-deva-in~0.0.1.0 `
    /capabilityname:Language.Basic~~~ko-kr~0.0.1.0 `
    /capabilityname:Language.Basic~~~ky-kg~0.0.1.0 `
    /capabilityname:Language.Basic~~~lb-lu~0.0.1.0 `
    /capabilityname:Language.Basic~~~lt-lt~0.0.1.0 `
    /capabilityname:Language.Basic~~~lv-lv~0.0.1.0 `
    /capabilityname:Language.Basic~~~mi-nz~0.0.1.0 `
    /capabilityname:Language.Basic~~~mk-mk~0.0.1.0 `
    /capabilityname:Language.Basic~~~ml-in~0.0.1.0 `
    /capabilityname:Language.Basic~~~mn-mn~0.0.1.0 `
    /capabilityname:Language.Basic~~~mr-in~0.0.1.0 `
    /capabilityname:Language.Basic~~~ms-bn~0.0.1.0 `
    /capabilityname:Language.Basic~~~ms-my~0.0.1.0 `
    /capabilityname:Language.Basic~~~mt-mt~0.0.1.0 `
    /capabilityname:Language.Basic~~~nb-no~0.0.1.0 `
    /capabilityname:Language.Basic~~~ne-np~0.0.1.0 `
    /capabilityname:Language.Basic~~~nl-nl~0.0.1.0 `
    /capabilityname:Language.Basic~~~nn-no~0.0.1.0 `
    /capabilityname:Language.Basic~~~nso-za~0.0.1.0 `
    /capabilityname:Language.Basic~~~or-in~0.0.1.0 `
    /capabilityname:Language.Basic~~~pa-in~0.0.1.0 `
    /capabilityname:Language.Basic~~~pl-pl~0.0.1.0 `
    /capabilityname:Language.Basic~~~ps-af~0.0.1.0 `
    /capabilityname:Language.Basic~~~pt-br~0.0.1.0 `
    /capabilityname:Language.Basic~~~pt-pt~0.0.1.0 `
    /capabilityname:Language.Basic~~~rm-ch~0.0.1.0 `
    /capabilityname:Language.Basic~~~ro-ro~0.0.1.0 `
    /capabilityname:Language.Basic~~~ru-ru~0.0.1.0 `
    /capabilityname:Language.Basic~~~rw-rw~0.0.1.0 `
    /capabilityname:Language.Basic~~~sah-ru~0.0.1.0 `
    /capabilityname:Language.Basic~~~si-lk~0.0.1.0 `
    /capabilityname:Language.Basic~~~sk-sk~0.0.1.0 `
```

```
    /capabilityname:Language.Basic~~~sl-si~0.0.1.0 `
    /capabilityname:Language.Basic~~~sq-al~0.0.1.0 `
    /capabilityname:Language.Basic~~~sr-cyrl-rs~0.0.1.0 `
    /capabilityname:Language.Basic~~~sr-latn-rs~0.0.1.0 `
    /capabilityname:Language.Basic~~~sv-se~0.0.1.0 `
    /capabilityname:Language.Basic~~~sw-ke~0.0.1.0 `
    /capabilityname:Language.Basic~~~ta-in~0.0.1.0 `
    /capabilityname:Language.Basic~~~te-in~0.0.1.0 `
    /capabilityname:Language.Basic~~~tg-cyrl-tj~0.0.1.0 `
    /capabilityname:Language.Basic~~~th-th~0.0.1.0 `
    /capabilityname:Language.Basic~~~tk-tm~0.0.1.0 `
    /capabilityname:Language.Basic~~~tn-za~0.0.1.0 `
    /capabilityname:Language.Basic~~~tr-tr~0.0.1.0 `
    /capabilityname:Language.Basic~~~tt-ru~0.0.1.0 `
    /capabilityname:Language.Basic~~~ug-cn~0.0.1.0 `
    /capabilityname:Language.Basic~~~uk-ua~0.0.1.0 `
    /capabilityname:Language.Basic~~~ur-pk~0.0.1.0 `
    /capabilityname:Language.Basic~~~uz-latn-uz~0.0.1.0 `
    /capabilityname:Language.Basic~~~vi-vn~0.0.1.0 `
    /capabilityname:Language.Basic~~~wo-sn~0.0.1.0 `
    /capabilityname:Language.Basic~~~xh-za~0.0.1.0 `
    /capabilityname:Language.Basic~~~yo-ng~0.0.1.0 `
    /capabilityname:Language.Basic~~~zh-cn~0.0.1.0 `
    /capabilityname:Language.Basic~~~zh-hk~0.0.1.0 `
    /capabilityname:Language.Basic~~~zh-tw~0.0.1.0 `
    /capabilityname:Language.Basic~~~zu-za~0.0.1.0 `
    /capabilityname:Language.Fonts.Arab~~~und-Arab~0.0.1.0 `
    /capabilityname:Language.Fonts.Beng~~~und-Beng~0.0.1.0 `
    /capabilityname:Language.Fonts.Cans~~~und-Cans~0.0.1.0 `
    /capabilityname:Language.Fonts.Cher~~~und-Cher~0.0.1.0 `
    /capabilityname:Language.Fonts.Deva~~~und-Deva~0.0.1.0 `
    /capabilityname:Language.Fonts.Ethi~~~und-Ethi~0.0.1.0 `
    /capabilityname:Language.Fonts.Gujr~~~und-Gujr~0.0.1.0 `
    /capabilityname:Language.Fonts.Guru~~~und-Guru~0.0.1.0 `
    /capabilityname:Language.Fonts.Hans~~~und-Hans~0.0.1.0 `
    /capabilityname:Language.Fonts.Hant~~~und-Hant~0.0.1.0 `
    /capabilityname:Language.Fonts.Hebr~~~und-Hebr~0.0.1.0 `
    /capabilityname:Language.Fonts.Jpan~~~und-Jpan~0.0.1.0 `
    /capabilityname:Language.Fonts.Khmr~~~und-Khmr~0.0.1.0 `
    /capabilityname:Language.Fonts.Knda~~~und-Knda~0.0.1.0 `
    /capabilityname:Language.Fonts.Kore~~~und-Kore~0.0.1.0 `
    /capabilityname:Language.Fonts.Laoo~~~und-Laoo~0.0.1.0 `
    /capabilityname:Language.Fonts.Mlym~~~und-Mlym~0.0.1.0 `
    /capabilityname:Language.Fonts.Orya~~~und-Orya~0.0.1.0 `
    /capabilityname:Language.Fonts.PanEuropeanSupplementalFonts~~~0.0.1.0 `
    /capabilityname:Language.Fonts.Sinh~~~und-Sinh~0.0.1.0 `
    /capabilityname:Language.Fonts.Syrc~~~und-Syrc~0.0.1.0 `
    /capabilityname:Language.Fonts.Taml~~~und-Taml~0.0.1.0 `
    /capabilityname:Language.Fonts.Telu~~~und-Telu~0.0.1.0 `
    /capabilityname:Language.Fonts.Thai~~~und-Thai~0.0.1.0 `
    /capabilityname:Language.Handwriting~~~af-za~0.0.1.0 `
    /capabilityname:Language.Handwriting~~~bs-latn-ba~0.0.1.0 `
    /capabilityname:Language.Handwriting~~~ca-es~0.0.1.0 `
    /capabilityname:Language.Handwriting~~~cs-cz~0.0.1.0 `
    /capabilityname:Language.Handwriting~~~cy-gb~0.0.1.0 `
```

```
    /capabilityname:Language.Handwriting~~~da-dk~0.0.1.0 `
    /capabilityname:Language.Handwriting~~~de-de~0.0.1.0 `
    /capabilityname:Language.Handwriting~~~el-gr~0.0.1.0 `
    /capabilityname:Language.Handwriting~~~en-gb~0.0.1.0 `
    /capabilityname:Language.Handwriting~~~en-us~0.0.1.0 `
    /capabilityname:Language.Handwriting~~~es-es~0.0.1.0 `
    /capabilityname:Language.Handwriting~~~es-mx~0.0.1.0 `
    /capabilityname:Language.Handwriting~~~eu-es~0.0.1.0 `
    /capabilityname:Language.Handwriting~~~fi-fi~0.0.1.0 `
    /capabilityname:Language.Handwriting~~~fr-fr~0.0.1.0 `
    /capabilityname:Language.Handwriting~~~ga-ie~0.0.1.0 `
    /capabilityname:Language.Handwriting~~~gd-gb~0.0.1.0 `
    /capabilityname:Language.Handwriting~~~gl-es~0.0.1.0 `
    /capabilityname:Language.Handwriting~~~hi-in~0.0.1.0 `
    /capabilityname:Language.Handwriting~~~hr-hr~0.0.1.0 `
    /capabilityname:Language.Handwriting~~~id-id~0.0.1.0 `
    /capabilityname:Language.Handwriting~~~it-it~0.0.1.0 `
    /capabilityname:Language.Handwriting~~~ja-jp~0.0.1.0 `
    /capabilityname:Language.Handwriting~~~ko-kr~0.0.1.0 `
    /capabilityname:Language.Handwriting~~~lb-lu~0.0.1.0 `
    /capabilityname:Language.Handwriting~~~mi-nz~0.0.1.0 `
    /capabilityname:Language.Handwriting~~~ms-bn~0.0.1.0 `
    /capabilityname:Language.Handwriting~~~ms-my~0.0.1.0 `
    /capabilityname:Language.Handwriting~~~nb-no~0.0.1.0 `
    /capabilityname:Language.Handwriting~~~nl-nl~0.0.1.0 `
    /capabilityname:Language.Handwriting~~~nn-no~0.0.1.0 `
    /capabilityname:Language.Handwriting~~~nso-za~0.0.1.0 `
    /capabilityname:Language.Handwriting~~~pl-pl~0.0.1.0 `
    /capabilityname:Language.Handwriting~~~pt-br~0.0.1.0 `
    /capabilityname:Language.Handwriting~~~pt-pt~0.0.1.0 `
    /capabilityname:Language.Handwriting~~~rm-ch~0.0.1.0 `
    /capabilityname:Language.Handwriting~~~ro-ro~0.0.1.0 `
    /capabilityname:Language.Handwriting~~~ru-ru~0.0.1.0 `
    /capabilityname:Language.Handwriting~~~rw-rw~0.0.1.0 `
    /capabilityname:Language.Handwriting~~~sk-sk~0.0.1.0 `
    /capabilityname:Language.Handwriting~~~sl-si~0.0.1.0 `
    /capabilityname:Language.Handwriting~~~sq-al~0.0.1.0 `
    /capabilityname:Language.Handwriting~~~sr-cyrl-rs~0.0.1.0 `
    /capabilityname:Language.Handwriting~~~sr-latn-rs~0.0.1.0 `
    /capabilityname:Language.Handwriting~~~sv-se~0.0.1.0 `
    /capabilityname:Language.Handwriting~~~sw-ke~0.0.1.0 `
    /capabilityname:Language.Handwriting~~~tn-za~0.0.1.0 `
    /capabilityname:Language.Handwriting~~~tr-tr~0.0.1.0 `
    /capabilityname:Language.Handwriting~~~wo-sn~0.0.1.0 `
    /capabilityname:Language.Handwriting~~~xh-za~0.0.1.0 `
    /capabilityname:Language.Handwriting~~~zh-cn~0.0.1.0 `
    /capabilityname:Language.Handwriting~~~zh-hk~0.0.1.0 `
    /capabilityname:Language.Handwriting~~~zh-tw~0.0.1.0 `
    /capabilityname:Language.Handwriting~~~zu-za~0.0.1.0 `
    /capabilityname:Language.LocaleData~~~zh-tw~0.0.1.0 `
    /capabilityname:Language.OCR~~~ar-sa~0.0.1.0 `
    /capabilityname:Language.OCR~~~bg-bg~0.0.1.0 `
    /capabilityname:Language.OCR~~~bs-latn-ba~0.0.1.0 `
    /capabilityname:Language.OCR~~~cs-cz~0.0.1.0 `
    /capabilityname:Language.OCR~~~da-dk~0.0.1.0 `
```

```
    /capabilityname:Language.OCR~~~de-de~0.0.1.0 `
    /capabilityname:Language.OCR~~~el-gr~0.0.1.0 `
    /capabilityname:Language.OCR~~~en-gb~0.0.1.0 `
    /capabilityname:Language.OCR~~~en-us~0.0.1.0 `
    /capabilityname:Language.OCR~~~es-es~0.0.1.0 `
    /capabilityname:Language.OCR~~~es-mx~0.0.1.0 `
    /capabilityname:Language.OCR~~~fi-fi~0.0.1.0 `
    /capabilityname:Language.OCR~~~fr-ca~0.0.1.0 `
    /capabilityname:Language.OCR~~~fr-fr~0.0.1.0 `
    /capabilityname:Language.OCR~~~hr-hr~0.0.1.0 `
    /capabilityname:Language.OCR~~~hu-hu~0.0.1.0 `
    /capabilityname:Language.OCR~~~it-it~0.0.1.0 `
    /capabilityname:Language.OCR~~~ja-jp~0.0.1.0 `
    /capabilityname:Language.OCR~~~ko-kr~0.0.1.0 `
    /capabilityname:Language.OCR~~~nb-no~0.0.1.0 `
    /capabilityname:Language.OCR~~~nl-nl~0.0.1.0 `
    /capabilityname:Language.OCR~~~pl-pl~0.0.1.0 `
    /capabilityname:Language.OCR~~~pt-br~0.0.1.0 `
    /capabilityname:Language.OCR~~~pt-pt~0.0.1.0 `
    /capabilityname:Language.OCR~~~ro-ro~0.0.1.0 `
    /capabilityname:Language.OCR~~~ru-ru~0.0.1.0 `
    /capabilityname:Language.OCR~~~sk-sk~0.0.1.0 `
    /capabilityname:Language.OCR~~~sl-si~0.0.1.0 `
    /capabilityname:Language.OCR~~~sr-cyrl-rs~0.0.1.0 `
    /capabilityname:Language.OCR~~~sr-latn-rs~0.0.1.0 `
    /capabilityname:Language.OCR~~~sv-se~0.0.1.0 `
    /capabilityname:Language.OCR~~~tr-tr~0.0.1.0 `
    /capabilityname:Language.OCR~~~zh-cn~0.0.1.0 `
    /capabilityname:Language.OCR~~~zh-hk~0.0.1.0 `
    /capabilityname:Language.OCR~~~zh-tw~0.0.1.0 `
    /capabilityname:Language.Speech~~~da-dk~0.0.1.0 `
    /capabilityname:Language.Speech~~~de-de~0.0.1.0 `
    /capabilityname:Language.Speech~~~en-au~0.0.1.0 `
    /capabilityname:Language.Speech~~~en-ca~0.0.1.0 `
    /capabilityname:Language.Speech~~~en-gb~0.0.1.0 `
    /capabilityname:Language.Speech~~~en-in~0.0.1.0 `
    /capabilityname:Language.Speech~~~en-us~0.0.1.0 `
    /capabilityname:Language.Speech~~~es-es~0.0.1.0 `
    /capabilityname:Language.Speech~~~es-mx~0.0.1.0 `
    /capabilityname:Language.Speech~~~fr-ca~0.0.1.0 `
    /capabilityname:Language.Speech~~~fr-fr~0.0.1.0 `
    /capabilityname:Language.Speech~~~it-it~0.0.1.0 `
    /capabilityname:Language.Speech~~~ja-jp~0.0.1.0 `
    /capabilityname:Language.Speech~~~pt-br~0.0.1.0 `
    /capabilityname:Language.Speech~~~zh-cn~0.0.1.0 `
    /capabilityname:Language.Speech~~~zh-hk~0.0.1.0 `
    /capabilityname:Language.Speech~~~zh-tw~0.0.1.0 `
    /capabilityname:Language.TextToSpeech~~~ar-eg~0.0.1.0 `
    /capabilityname:Language.TextToSpeech~~~ar-sa~0.0.1.0 `
    /capabilityname:Language.TextToSpeech~~~bg-bg~0.0.1.0 `
    /capabilityname:Language.TextToSpeech~~~ca-es~0.0.1.0 `
    /capabilityname:Language.TextToSpeech~~~cs-cz~0.0.1.0 `
    /capabilityname:Language.TextToSpeech~~~da-dk~0.0.1.0 `
    /capabilityname:Language.TextToSpeech~~~de-at~0.0.1.0 `
    /capabilityname:Language.TextToSpeech~~~de-ch~0.0.1.0 `
```

```
    /capabilityname:Language.TextToSpeech~~~de-de~0.0.1.0 `
    /capabilityname:Language.TextToSpeech~~~el-gr~0.0.1.0 `
    /capabilityname:Language.TextToSpeech~~~en-au~0.0.1.0 `
    /capabilityname:Language.TextToSpeech~~~en-ca~0.0.1.0 `
    /capabilityname:Language.TextToSpeech~~~en-gb~0.0.1.0 `
    /capabilityname:Language.TextToSpeech~~~en-ie~0.0.1.0 `
    /capabilityname:Language.TextToSpeech~~~en-in~0.0.1.0 `
    /capabilityname:Language.TextToSpeech~~~en-us~0.0.1.0 `
    /capabilityname:Language.TextToSpeech~~~es-es~0.0.1.0 `
    /capabilityname:Language.TextToSpeech~~~es-mx~0.0.1.0 `
    /capabilityname:Language.TextToSpeech~~~fi-fi~0.0.1.0 `
    /capabilityname:Language.TextToSpeech~~~fr-ca~0.0.1.0 `
    /capabilityname:Language.TextToSpeech~~~fr-ch~0.0.1.0 `
    /capabilityname:Language.TextToSpeech~~~fr-fr~0.0.1.0 `
    /capabilityname:Language.TextToSpeech~~~he-il~0.0.1.0 `
    /capabilityname:Language.TextToSpeech~~~hi-in~0.0.1.0 `
    /capabilityname:Language.TextToSpeech~~~hr-hr~0.0.1.0 `
    /capabilityname:Language.TextToSpeech~~~hu-hu~0.0.1.0 `
    /capabilityname:Language.TextToSpeech~~~id-id~0.0.1.0 `
    /capabilityname:Language.TextToSpeech~~~it-it~0.0.1.0 `
    /capabilityname:Language.TextToSpeech~~~ja-jp~0.0.1.0 `
    /capabilityname:Language.TextToSpeech~~~ko-kr~0.0.1.0 `
    /capabilityname:Language.TextToSpeech~~~ms-my~0.0.1.0 `
    /capabilityname:Language.TextToSpeech~~~nb-no~0.0.1.0 `
    /capabilityname:Language.TextToSpeech~~~nl-be~0.0.1.0 `
    /capabilityname:Language.TextToSpeech~~~nl-nl~0.0.1.0 `
    /capabilityname:Language.TextToSpeech~~~pl-pl~0.0.1.0 `
    /capabilityname:Language.TextToSpeech~~~pt-br~0.0.1.0 `
    /capabilityname:Language.TextToSpeech~~~pt-pt~0.0.1.0 `
    /capabilityname:Language.TextToSpeech~~~ro-ro~0.0.1.0 `
    /capabilityname:Language.TextToSpeech~~~ru-ru~0.0.1.0 `
    /capabilityname:Language.TextToSpeech~~~sk-sk~0.0.1.0 `
    /capabilityname:Language.TextToSpeech~~~sl-si~0.0.1.0 `
    /capabilityname:Language.TextToSpeech~~~sv-se~0.0.1.0 `
    /capabilityname:Language.TextToSpeech~~~ta-in~0.0.1.0 `
    /capabilityname:Language.TextToSpeech~~~th-th~0.0.1.0 `
    /capabilityname:Language.TextToSpeech~~~tr-tr~0.0.1.0 `
    /capabilityname:Language.TextToSpeech~~~vi-vn~0.0.1.0 `
    /capabilityname:Language.TextToSpeech~~~zh-cn~0.0.1.0 `
    /capabilityname:Language.TextToSpeech~~~zh-hk~0.0.1.0 `
    /capabilityname:Language.TextToSpeech~~~zh-tw~0.0.1.0 `
    /capabilityname:MathRecognizer~~~~0.0.1.0 `
    /capabilityname:Microsoft.Onecore.StorageManagement~~~~0.0.1.0 `
    /capabilityname:Microsoft.WebDriver~~~~0.0.1.0 `
    /capabilityname:Microsoft.Windows.MSPaint~~~~0.0.1.0 `
    /capabilityname:Microsoft.Windows.Notepad~~~~0.0.1.0 `
    /capabilityname:Microsoft.Windows.PowerShell.ISE~~~~0.0.1.0 `
    /capabilityname:Microsoft.Windows.StorageManagement~~~~0.0.1.0 `
    /capabilityname:Microsoft.Windows.WordPad~~~~0.0.1.0 `
    /capabilityname:Msix.PackagingTool.Driver~~~~0.0.1.0 `
    /capabilityname:NetFX3~~ `
    /capabilityname:Network.Irda~~~~0.0.1.0 `
    /capabilityname:OneCoreUAP.OneSync~~~~0.0.1.0 `
    /capabilityname:OpenSSH.Client~~~~0.0.1.0 `
    /capabilityname:OpenSSH.Server~~~~0.0.1.0 `
```

```
    /capabilityname:Print.EnterpriseCloudPrint~~~~0.0.1.0 `
    /capabilityname:Print.Fax.Scan~~~~0.0.1.0 `
    /capabilityname:Print.Management.Console~~~~0.0.1.0 `
    /capabilityname:Print.MopriaCloudService~~~~0.0.1.0 `
    /capabilityname:RasCMAK.Client~~~~0.0.1.0 `
    /capabilityname:RIP.Listener~~~~0.0.1.0 `
    /capabilityname:Rsat.ActiveDirectory.DS-LDS.Tools~~~~0.0.1.0 `
    /capabilityname:Rsat.BitLocker.Recovery.Tools~~~~0.0.1.0 `
    /capabilityname:Rsat.CertificateServices.Tools~~~~0.0.1.0 `
    /capabilityname:Rsat.DHCP.Tools~~~~0.0.1.0 `
    /capabilityname:Rsat.Dns.Tools~~~~0.0.1.0 `
    /capabilityname:Rsat.FailoverCluster.Management.Tools~~~~0.0.1.0 `
    /capabilityname:Rsat.FileServices.Tools~~~~0.0.1.0 `
    /capabilityname:Rsat.GroupPolicy.Management.Tools~~~~0.0.1.0 `
    /capabilityname:Rsat.IPAM.Client.Tools~~~~0.0.1.0 `
    /capabilityname:Rsat.LLDP.Tools~~~~0.0.1.0 `
    /capabilityname:Rsat.NetworkController.Tools~~~~0.0.1.0 `
    /capabilityname:Rsat.NetworkLoadBalancing.Tools~~~~0.0.1.0 `
    /capabilityname:Rsat.RemoteAccess.Management.Tools~~~~0.0.1.0 `
    /capabilityname:Rsat.RemoteDesktop.Services.Tools~~~~0.0.1.0 `
    /capabilityname:Rsat.ServerManager.Tools~~~~0.0.1.0 `
    /capabilityname:Rsat.Shielded.VM.Tools~~~~0.0.1.0 `
    /capabilityname:Rsat.StorageMigrationService.Management.Tools~~~~0.0.1.0
`
    /capabilityname:Rsat.StorageReplica.Tools~~~~0.0.1.0 `
    /capabilityname:Rsat.SystemInsights.Management.Tools~~~~0.0.1.0 `
    /capabilityname:Rsat.VolumeActivation.Tools~~~~0.0.1.0 `
    /capabilityname:Rsat.WSUS.Tools~~~~0.0.1.0 `
    /capabilityname:ServerCore.AppCompatibility~~~~0.0.1.0 `
    /capabilityname:SNMP.Client~~~~0.0.1.0 `
    /capabilityname:Tools.DeveloperMode.Core~~~~0.0.1.0 `
    /capabilityname:Tools.Graphics.DirectX~~~~0.0.1.0 `
    /capabilityname:Windows.Client.ShellComponents~~~~0.0.1.0 `
    /capabilityname:Windows.Desktop.EMS-SAC.Tools~~~~0.0.1.0 `
    /capabilityname:WMI-SNMP-Provider.Client~~~~0.0.1.0 `
    /capabilityname:XPS.Viewer~~~~0.0.1.0

    # This one is large, lets skip for now
    #/capabilityname:Analog.Holographic.Desktop~~~~0.0.1.0 `


# Copy language caps to the repo
Copy-Item -Path $OS_LP_PATH -Destination $REPO_PATH -Force -ErrorAction stop
| Out-Null

# Dismount OS image
Dismount-WindowsImage -Path $MAIN_OS_MOUNT -Discard -ErrorAction ignore |
Out-Null

# Dismount ISO images
Write-Host "Dismounting ISO images"
Dismount-DiskImage -ImagePath $LP_ISO_PATH -ErrorAction ignore | Out-Null
Dismount-DiskImage -ImagePath $FOD_ISO_PATH -ErrorAction ignore | Out-Null
```

Сохранение необязательного содержимого в исходной операционной системе

Чтобы сохранить необязательное состояние содержимого в исходной операционной системе, мы создадим скрипт пользовательского действия, который будет выполняться перед установкой операционной системы. В этом сценарии мы сохраняем дополнительные функции и языковые ресурсы в файл. Кроме того, мы создаем локальную копию репозитория с необходимыми файлами на основе языков, установленных в исходной операционной системе. Это действие ограничивает копирование файлов.

PowerShell

```
$OUTPUT_PATH = "C:\TEMP\"
$LOG_PATH = $OUTPUT_PATH + "log.txt"
$OUTPUT_PATH = "C:\TEMP\"
$LOG_PATH = $OUTPUT_PATH + "log.txt"
$LANG_PATH = $OUTPUT_PATH + "sourceLang.txt"
$CAP_PATH = $OUTPUT_PATH + "sourceCapability.txt"
$OSVERSION_PATH = $OUTPUT_PATH + "sourceVersion.txt"
$REPO_PATH = "Z:\Repo\"
$LOCAL_REPO_PATH = $OUTPUT_PATH + "Local_Repo\"

Function Get-TS { return "{0:HH:mm:ss}" -f (Get-Date) }

Function Log
{
    param (
        [Parameter(Mandatory=$True)]
        [string]$MESSAGE
    )

    $M = "$(Get-TS): PreInstall: $MESSAGE"
    Write-Host $M
    Add-Content -Path $LOG_PATH -Value $M

 }

Function IsLangFile
{
    param (
        [Parameter(Mandatory=$True)]
        [string]$PATH
    )

    if (($PATH -match '[-_~]ar[-_~]') -or ($PATH -match '[-_~]bg[-_~]') -or
($PATH -match '[-_~]cs[-_~]') -or `
        ($PATH -match '[-_~]da[-_~]') -or ($PATH -match '[-_~]de[-_~]') -or
($PATH -match '[-_~]el[-_~]') -or `
        ($PATH -match '[-_~]en[-_~]') -or ($PATH -match '[-_~]es[-_~]') -or
($PATH -match '[-_~]et[-_~]') -or `
```

```
        ($PATH -match '[-_~]fi[-_~]') -or ($PATH -match '[-_~]fr[-_~]') -or
($PATH -match '[-_~]he[-_~]') -or `
        ($PATH -match '[-_~]hr[-_~]') -or ($PATH -match '[-_~]hu[-_~]') -or
($PATH -match '[-_~]it[-_~]') -or `
        ($PATH -match '[-_~]ja[-_~]') -or ($PATH -match '[-_~]ko[-_~]') -or
($PATH -match '[-_~]lt[-_~]') -or `
        ($PATH -match '[-_~]lv[-_~]') -or ($PATH -match '[-_~]nb[-_~]') -or
($PATH -match '[-_~]nl[-_~]') -or `
        ($PATH -match '[-_~]pl[-_~]') -or ($PATH -match '[-_~]pt[-_~]') -or
($PATH -match '[-_~]ro[-_~]') -or `
        ($PATH -match '[-_~]ru[-_~]') -or ($PATH -match '[-_~]sk[-_~]') -or
($PATH -match '[-_~]sl[-_~]') -or `
        ($PATH -match '[-_~]sv[-_~]') -or ($PATH -match '[-_~]th[-_~]') -or
($PATH -match '[-_~]tr[-_~]') -or `
        ($PATH -match '[-_~]uk[-_~]') -or ($PATH -match '[-_~]zh[-_~]') -or
($PATH -match '[-_~]sr[-_~]')) {
        return $True
    }
    else {
        return $False
    }
 }

# Remove the log
Remove-Item -Path $LOG_PATH -Force -ErrorAction ignore | Out-Null
Log "Starting"

# Remove state files, keep repo if it exists
Remove-Item -Path $LANG_PATH -Force -ErrorAction ignore | Out-Null
Remove-Item -Path $CAP_PATH -Force -ErrorAction ignore | Out-Null
Remove-Item -Path $OSVERSION_PATH -Force -ErrorAction ignore | Out-Null

# Get OS version, to use later for detecting compat scans versus OS
installation
$OSINFO = Get-CimInstance Win32_OperatingSystem
Log "OS Version: $($OSINFO.Version)"
Add-Content -Path $OSVERSION_PATH -Value $OSINFO.Version

# Get installed languages from international settings
$INTL = DISM.exe /Online /Get-Intl /English

# Save only output lines with installed languages
$LANGUAGES = $INTL | Select-String -SimpleMatch 'Installed language(s)'

# Replace with null so we have a simple list of language codes
$LANGUAGES = $LANGUAGES | ForEach-Object {$_.Line.Replace("Installed
language(s): ","")}

# Save System Language, save only output line with default system language
$SYSLANG = $INTL | Select-String -SimpleMatch 'Default system UI language'

# Replace with null so we have the language code
$SYSLANG = $SYSLANG | ForEach-Object {$_.Line.Replace("Default system UI
language : ","")}
```

```
# Save these languages
Log "Default system UI language on source OS: $($SYSLANG)"
ForEach ($ITEM in $LANGUAGES) {
    Log "Installed language on source OS: $($ITEM)"
    Add-Content -Path $LANG_PATH -Value $ITEM
}

# Get and save installed packages, we'll use this for debugging
$PACKAGES = Get-WindowsPackage -Online
ForEach ($ITEM in $PACKAGES) {
    if($ITEM.PackageState -eq "Installed") {
        Log "Package $($ITEM.PackageName) is installed"
    }
}

# Get and save capabilities
$CAPABILITIES = Get-WindowsCapability -Online
ForEach ($ITEM in $CAPABILITIES) {
    if($ITEM.State -eq "Installed") {
        Log "Capability $($ITEM.Name) is installed"
        Add-Content -Path $CAP_PATH -Value $ITEM.Name
    }
}

# Copy a subset of the Repo files locally, all neutral files and the
languages needed
$REPO_FILES = Get-ChildItem $REPO_PATH -file -Recurse
ForEach ($FILE in $REPO_FILES) {
    $PATH = ($FILE.DirectoryName + "\") -Replace
[Regex]::Escape($REPO_PATH), $LOCAL_REPO_PATH
    If (!(Test-Path $Path)) {
        New-Item -ItemType Directory -Path $PATH -Force | Out-Null
    }
    If ((IsLangFile $FILE.Name)) {

        # Only copy those files where we need the primary languages from the
source OS
        ForEach ($ITEM in $LANGUAGES) {
            if ($FILE.Name -match $Item) {

                If (!(Test-Path (Join-Path $Path $File.Name))) {
                    Copy-Item $FILE.FullName -Destination $PATH -Force
                    Log "Copied file $($FILE.FullName) to local repository"
                }
                else {
                    Log "File $($FILE.Name) already exists in local
repository"
                }
            }
        }
    } Else {

        # Copy all 'neutral files' and those language specific that are not
in the core 38
        If (!(Test-Path (Join-Path $Path $File.Name))) {
```

```
            Copy-Item $FILE.FullName -Destination $PATH -Force
            Log "Copied file $($FILE.FullName) to local repository"
        }
        else {
            Log "File $($FILE.Name) already exists in local repository"
        }
    }
}

Log ("Exiting")
```

Добавление дополнительного содержимого в целевую операционную систему

После успешного завершения установки мы используем success.cmd для получения необязательного состояния содержимого из исходной операционной системы и установки в новой операционной системе только в том случае, если оно отсутствует. Затем примените последнее ежемесячное обновление в качестве последнего шага.

PowerShell

```
$OUTPUT_PATH = "C:\TEMP\"
$LOG_PATH = $OUTPUT_PATH + "log.txt"
$LANG_PATH = $OUTPUT_PATH + "sourceLang.txt"
$CAP_PATH = $OUTPUT_PATH + "sourceCapability.txt"
$OSVERSION_PATH = $OUTPUT_PATH + "sourceVersion.txt"
$LOCAL_REPO_PATH = $OUTPUT_PATH + "Local_Repo\"
$LCU_PATH = $OUTPUT_PATH + "Windows10.0-KB4565503-x64_PSFX.cab"
$PENDING = $false

Function Get-TS { return "{0:HH:mm:ss}" -f (Get-Date) }

Function Log
{
    param (
        [Parameter(Mandatory=$True)]
        [string]$MESSAGE
    )

    $M = "$(Get-TS): PostInstall: $MESSAGE"
    Write-Host $M
    Add-Content -Path $LOG_PATH -Value $M

 }

Log "Starting"

# Get OS version
```

```
$OSINFO = Get-CimInstance Win32_OperatingSystem
Log "OS Version: $($OSINFO.Version)"

# Check for source OS state, just to be sure
if (!(Test-Path $LANG_PATH) -or !(Test-Path $CAP_PATH) -or !(Test-Path
$OSVERSION_PATH) ) {
    Log "Source OS state is missing."
}

# If this script is executing and the OS version hasn't changed, let's exit
out.
else {

    # Retrive OS version from source OS
    $SOURCE_OSVERSION  = Get-Content -Path $OSVERSION_PATH
    if ($OSINFO.Version -eq $SOURCE_OSVERSION) {
        Log "OS Version hasn't changed."
    }

    else {

        # Retrive language list from source OS
        $SOURCE_LANGUAGES  = Get-Content -Path $LANG_PATH

        # Get installed languages from International Settings
        $INTL = DISM.exe /Online /Get-Intl /English

        # Save System Language, save only output line with default system
language
        $SYS_LANG = $INTL | Select-String -SimpleMatch 'Default system UI
language'

        # Replace with null so we have the language code
        $SYS_LANG = $SYS_LANG | ForEach-Object {$_.Line.Replace("Default
system UI language : ","")}

        # Get and save installed packages, we'll use this for debugging
        $PACKAGES = Get-WindowsPackage -Online
        ForEach ($ITEM in $PACKAGES) {
            if($ITEM.PackageState -eq "Installed") {
                Log "Package $($ITEM.PackageName) is installed"
            }
        }

        # Loop through source OS languages, and install if missing on target
OS
        ForEach ($SOURCE_ITEM in $SOURCE_LANGUAGES) {
            if ($SOURCE_ITEM -ne $SYS_LANG) {

                # add missing languages except the system language
                Log "Adding language Microsoft-Windows-Client-Language-
Pack_x64_$($SOURCE_ITEM).cab"
                try {
                    Add-WindowsPackage -Online -PackagePath
"$($LOCAL_REPO_PATH)\Microsoft-Windows-Client-Language-
```

```
Pack_x64_$($SOURCE_ITEM).cab" -ErrorAction stop | Out-Null
                }
                catch {
                    Log $_.Exception.Message
                }
            }
        }

        # Retrieve capabilities from source OS and target OS
        $SOURCE_CAPABILITIES  = Get-Content -Path $CAP_PATH
        $CAPABILITIES = Get-WindowsCapability -Online

        # Loop through source OS capabilities, and install if missing on
target OS
        ForEach ($SOURCE_ITEM in $SOURCE_CAPABILITIES) {
            $INSTALLED = $false
            ForEach ($ITEM in $CAPABILITIES) {
                if ($ITEM.Name -eq $($SOURCE_ITEM)) {
                    if ($ITEM.State -eq "Installed") {
                        $INSTALLED = $true
                        break
                    }
                }
            }

            # Add if not already installed
            if (!($INSTALLED)) {
                Log "Adding capability $SOURCE_ITEM"
                try {
                    Add-WindowsCapability -Online -Name $SOURCE_ITEM -Source
$LOCAL_REPO_PATH -ErrorAction stop | Out-Null
                }
                catch {
                    Log $_.Exception.Message
                }
            }
            else {
                Log "Capability $SOURCE_ITEM is already installed"
            }
        }

        # Add LCU, this is required after adding FODs and languages
        Log ("Adding LCU")
        Add-WindowsPackage -Online -PackagePath $LCU_PATH -NoRestart

        # Get packages, we'll use this for debugging and to see if we need
to restart to install
        $PACKAGES = Get-WindowsPackage -Online
        ForEach ($ITEM in $PACKAGES) {
            Log "Package $($ITEM.PackageName) is $($ITEM.PackageState)"
            if ($ITEM.PackageState -eq "InstallPending") {
                $PENDING = $true
            }
        }
    }
```

```
}

# Remove local repository and state files
Remove-Item -Path $LANG_PATH -Force -ErrorAction ignore | Out-Null
Remove-Item -Path $CAP_PATH -Force -ErrorAction ignore | Out-Null
Remove-Item -Path $OSVERSION_PATH -Force -ErrorAction ignore | Out-Null
Remove-Item -Path $LOCAL_REPO_PATH -Force -Recurse -ErrorAction ignore |
Out-Null

# Restarting the computer to let setup process to exit cleanly
if ($PENDING) {
    Log ("Install pending packages exists, restarting in 10 seconds")
    Start-Process -FilePath cmd -ArgumentList "/C shutdown /r /t 10 /f"
}

Log ("Exiting")
```

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Развертывание обновлений компонентов для установок, инициированных пользователем (в течение фиксированного периода службы)

Статья • 18.03.2023 • Применяется к: ✅ Windows 10, ✅ Microsoft Configuration Manager

Выполните следующие действия, чтобы развернуть обновление компонентов для установки, инициированной пользователем.

Подготовка к развертыванию обновлений компонентов

Шаг 1. Включение одноранговой кэша

Использование **одноранговой кэша** для управления развертыванием содержимого на клиентах в удаленных расположениях. Одноранговый кэш — это встроенное решение Configuration Manager, которое позволяет клиентам обмениваться содержимым с другими клиентами непосредственно из локального кэша.

Включите Configuration Manager клиент в полной ОС для предоставления общего доступа к содержимому, если у вас есть клиенты в удаленных расположениях, для которых было бы полезно скачивать содержимое обновления компонентов из одноранговой узла, а не из точки распространения (или Центра обновления Майкрософт).

Шаг 2. Переопределение приоритета установки Windows по умолчанию (Windows 10 версии 1709 и более поздних версий)

При развертывании **обновления компонентов в Windows 10 версии 1709** или более поздней по умолчанию части установки настраиваются для запуска с более низким приоритетом. Это может привести к большему общему времени установки обновления компонентов. При развертывании в течение периода обслуживания

рекомендуется переопределить это поведение по умолчанию, чтобы сократить общее время установки. Чтобы переопределить приоритет по умолчанию, создайте файл с именем SetupConfig.ini на каждом компьютере, который будет обновляться в расположении ниже, в котором указан один раздел.

%systemdrive%\Users\Default\AppData\Local\Microsoft\Windows\WSUS\SetupConfig.ini

```
[SetupConfig]
Priority=Normal
```

Новую функцию запуска скриптов можно использовать для запуска скрипта PowerShell, как показано в примере ниже, чтобы создать SetupConfig.ini на целевых устройствах.

```
#Parameters
Param(
  [string] $PriorityValue = "Normal"
  )

#Variable for ini file path
$iniFilePath =
"$env:SystemDrive\Users\Default\AppData\Local\Microsoft\Windows\WSUS\SetupCo
nfig.ini"

#Variables for SetupConfig
$iniSetupConfigSlogan = "[SetupConfig]"
$iniSetupConfigKeyValuePair =@{"Priority"=$PriorityValue;}

#Init SetupConfig content
$iniSetupConfigContent = @"
$iniSetupConfigSlogan
"@

#Build SetupConfig content with settings
foreach ($k in $iniSetupConfigKeyValuePair.Keys)
{
    $val = $iniSetupConfigKeyValuePair[$k]

    $iniSetupConfigContent =
$iniSetupConfigContent.Insert($iniSetupConfigContent.Length, "`r`n$k=$val")
}

#Write content to file
New-Item $iniFilePath -ItemType File -Value $iniSetupConfigContent -Force
```

```
<#
Disclaimer
Sample scripts are not supported under any Microsoft standard support
program or service. The sample scripts is
provided AS IS without warranty of any kind. Microsoft further disclaims all
implied warranties including, without
limitation, any implied warranties of merchantability or of fitness for a
particular purpose. The entire risk
arising out of the use or performance of the sample script and documentation
remains with you. In no event shall
Microsoft, its authors, or anyone else involved in the creation, production,
or delivery of the scripts be liable
for any damages whatsoever (including, without limitation, damages for loss
of business profits, business interruption,
loss of business information, or other pecuniary loss) arising out of the
use of or inability to use the sample script
or documentation, even if Microsoft has been advised of the possibility of
such damages.
#>
```

> ⓘ **Примечание**
>
> Если вы решили не переопределять приоритет установки по умолчанию, вам потребуется увеличить **максимальное значение времени выполнения** для обновления компонентов до Windows 10 версии 1709 или выше с 60 минут по умолчанию. Может потребоваться значение 240 минут. Не забудьте убедиться, что продолжительность периода обслуживания больше заданного максимального значения времени выполнения.

Развертывание обновлений компонентов вручную в установке, инициированной пользователем

В следующих разделах приведены инструкции по развертыванию обновления компонентов вручную.

Шаг 1. Указание условий поиска для обновлений компонентов

В консоли Configuration Manager может отображаться не более тысячи обновлений функций. Первым шагом в рабочем процессе для развертывания обновления компонентов вручную является определение обновлений компонентов, которые требуется развернуть.

1. В консоли Configuration Manager выберите **Библиотека программного обеспечения**.

2. В рабочей области Библиотека программного обеспечения разверните **узел Windows 10 Обслуживание** и выберите **Все Windows 10 Обновления**. Отобразятся синхронизированные обновления компонентов.

3. В области поиска выполните фильтрацию, чтобы определить необходимые обновления компонентов, выполнив один или оба следующих шага:

    - В текстовом поле **поиска** введите строку поиска, которая фильтрует обновления компонентов. Например, введите номер версии для конкретного обновления компонентов или введите строку, которая будет отображаться в заголовке обновления компонентов.
    - Выберите **Добавить критерии**, выберите критерии, которые нужно использовать для фильтрации обновлений программного обеспечения, нажмите **кнопку Добавить**, а затем укажите значения для условий. Например, заголовок содержит значение 1803, **обязательное** значение больше или равно 1, а **значение Language** равно английскому языку.

4. Сохраните поиск для дальнейшего использования.

Шаг 2. Скачивание содержимого для обновлений компонентов

Перед развертыванием обновлений компонентов можно скачать содержимое в виде отдельного шага. Выполните это скачивание, чтобы убедиться, что содержимое доступно на точках распространения, прежде чем развертывать обновления компонентов. Скачивание сначала помогает избежать непредвиденных проблем с доставкой содержимого. Используйте следующую процедуру, чтобы скачать содержимое для обновлений компонентов перед созданием развертывания.

1. В консоли Configuration Manager перейдите в раздел **Библиотека > программного обеспечения Windows 10 обслуживание**.

2. Выберите обновления компонентов для скачивания с помощью сохраненных условий поиска. Выберите одно или несколько возвращенных обновлений компонентов, щелкните правой кнопкой мыши и выберите **Скачать**.

    Откроется **мастер загрузки программного обеспечения Обновления**.

3. На странице **Пакет развертывания** настройте следующие параметры: **Создать новый пакет развертывания**. Выберите этот параметр, чтобы создать новый пакет развертывания для обновлений программного обеспечения, которые находятся в развертывании. Настройте следующие параметры:

   - **Имя**: указывает имя пакета развертывания. Пакет должен иметь уникальное имя, кратко описывающее содержимое пакета. Он ограничен 50 символами.

   - **Описание**: указывает описание пакета развертывания. Описание пакета содержит сведения о содержимом пакета и ограничено 127 символами.

   - **Источник пакета**. Указывает расположение исходных файлов обновления компонентов. Введите сетевой путь для исходного расположения, например \\server\sharename\path, или нажмите кнопку **Обзор** , чтобы найти сетевое расположение. Перед переходом к следующей странице необходимо создать общую папку для исходных файлов пакета развертывания.

     > ⓘ **Важно!**
     > - Указанное исходное расположение пакета развертывания не может использоваться другим пакетом развертывания программного обеспечения.
     > - Учетная запись компьютера поставщика SMS и пользователь, запускающий мастер загрузки обновлений компонентов, должны иметь разрешения NTFS на запись в расположении скачивания. Следует тщательно ограничить доступ к расположению загрузки, чтобы снизить риск изменения злоумышленниками исходных файлов обновления компонентов.
     > - Вы можете изменить расположение источника пакета в свойствах пакета развертывания после Configuration Manager создания пакета развертывания. Но в этом случае необходимо сначала скопировать содержимое из исходного источника пакета в новое расположение исходного пакета.

   Выберите **Далее**.

4. На странице **Точки распространения** укажите точки распространения или группы точек распространения, в которых будут размещаться файлы обновления компонентов, а затем нажмите кнопку **Далее**. Дополнительные

сведения о точках распространения см. в разделе Конфигурации точек распространения.

> ⓘ **Примечание**
>
> Страница "Точки распространения" доступна только при создании пакета развертывания обновления программного обеспечения.

5. На странице **Параметры распространения** укажите следующие параметры:

   - **Приоритет распространения**. Используйте этот параметр, чтобы указать приоритет распространения для пакета развертывания. Приоритет распространения применяется, когда пакет развертывания отправляется в точки распространения на дочерних сайтах. Пакеты развертывания отправляются в порядке приоритета: **Высокий**, **Средний** или **Низкий**. Пакеты с одинаковыми приоритетами отправляются в том порядке, в котором они были созданы. Если невыполненная работа отсутствует, пакет обрабатывается немедленно, независимо от его приоритета. По умолчанию пакеты отправляются с использованием среднего приоритета.

   - **Включить распространение по запросу**. Используйте этот параметр, чтобы включить распространение содержимого по запросу в предпочтительные точки распространения. Если этот параметр включен, точка управления создает триггер для диспетчера распространения для распространения содержимого во все предпочтительные точки распространения, когда клиент запрашивает содержимое для пакета, а содержимое недоступно ни в каких предпочтительных точках распространения. Дополнительные сведения о предпочтительных точках распространения и содержимом по запросу см. в статье Сценарии расположения источника контента.

   - **Параметры предварительно подготовленной точки распространения**. Используйте этот параметр, чтобы указать способ распространения содержимого в предварительно подготовленные точки распространения. Выберите один из следующих вариантов:
     - **Автоматическое скачивание содержимого при назначении пакетов точкам распространения**. Используйте этот параметр, чтобы игнорировать параметры предварительной подготовки и распространить содержимое в точку распространения.

- **Скачивание только изменений содержимого в точку распространения**. Используйте этот параметр, чтобы предварительно настроить начальное содержимое в точку распространения, а затем распространить изменения содержимого в точку распространения.
- **Копирование содержимого в этом пакете вручную в точку распространения**. Используйте этот параметр для постоянной подготовки содержимого в точке распространения. Этот параметр используется по умолчанию.

Дополнительные сведения о предварительной подготовке содержимого к точкам распространения см. в разделе Использование предварительно подготовленного содержимого. Выберите **Далее**.

6. На странице **Расположение загрузки** укажите расположение, которое Configuration Manager будет использовать для скачивания исходных файлов обновлений программного обеспечения. При необходимости используйте следующие параметры:

   - **Скачивание обновлений программного обеспечения из Интернета**. Выберите этот параметр, чтобы скачать обновления программного обеспечения из расположения в Интернете. Этот параметр устанавливается по умолчанию.

   - **Скачивание обновлений программного обеспечения из расположения в локальной сети**. Выберите этот параметр, чтобы скачать обновления программного обеспечения из локальной или общей сетевой папки. Используйте этот параметр, если компьютер, на котором запущен мастер, не имеет доступа к Интернету.

     > ⓘ **Примечание**
     >
     > При использовании этого параметра скачайте обновления программного обеспечения с любого компьютера с доступом к Интернету, а затем скопируйте обновления программного обеспечения в расположение в локальной сети, доступное с компьютера, на котором запущен мастер.

   Выберите **Далее**.

7. На странице **Выбор языка** укажите языки, для которых будут загружены выбранные обновления компонентов, а затем нажмите кнопку **Далее**. Убедитесь, что выбранный язык соответствует языкам обновлений

компонентов, выбранных для скачивания. Например, если вы выбрали для скачивания обновления компонентов на английском и немецком языках, выберите те же языки на странице выбора языка.

8. На странице **Сводка** проверьте параметры, выбранные в мастере, и нажмите кнопку **Далее** , чтобы скачать обновления программного обеспечения.

9. На странице **Завершение** убедитесь, что обновления программного обеспечения успешно загружены, и нажмите кнопку **Закрыть**.

Мониторинг состояния содержимого

1. Чтобы отслеживать состояние содержимого обновлений компонентов, выберите **Мониторинг** в консоли Configuration Manager.
2. В рабочей области Мониторинг разверните узел **Состояние распространения**, а затем выберите **Состояние содержимого**.
3. Выберите пакет обновления компонентов, который вы определили ранее, чтобы скачать обновления компонентов.
4. На вкладке **Главная** в группе Содержимое выберите **Просмотреть состояние**.

Шаг 3. Развертывание обновлений компонентов

После определения обновлений компонентов, которые планируется развернуть, можно вручную развернуть обновления компонентов. Используйте следующую процедуру, чтобы вручную развернуть обновления компонентов.

1. В консоли Configuration Manager выберите **Библиотека программного обеспечения**.

2. В рабочей области Библиотека программного обеспечения разверните **узел Windows 10 Обслуживание** и выберите **Все Windows 10 Обновления**.

3. Выберите обновления компонентов для развертывания с помощью сохраненных условий поиска. Выберите одно или несколько возвращенных обновлений компонентов, щелкните правой кнопкой мыши и выберите **Развернуть**.

   Откроется **мастер развертывания Обновления программного обеспечения**.

4. На странице Общие настройте следующие параметры:

   - **Имя**. Укажите имя развертывания. Развертывание должно иметь уникальное имя, описывающее назначение развертывания и

отличающее его от других развертываний на Configuration Manager сайте. По умолчанию Configuration Manager автоматически предоставляет имя для развертывания в следующем формате: **Microsoft Software Обновления — <дата><и время>**.

- **Описание**. Укажите описание развертывания. В описании содержится обзор развертывания и любая другая важная информация, которая помогает определить и дифференцировать развертывание среди других на Configuration Manager сайте. Поле описания является необязательным, имеет ограничение в 256 символов и имеет пустое значение по умолчанию.
- **Обновление программного обеспечения или группа обновлений программного обеспечения**. Убедитесь, что отображаемая группа обновлений программного обеспечения или обновления программного обеспечения является правильной.
- **Выберите Шаблон развертывания**: укажите, следует ли применять ранее сохраненный шаблон развертывания. Вы можете настроить шаблон развертывания так, чтобы он содержал несколько общих свойств развертывания обновлений программного обеспечения, а затем применить шаблон при развертывании последующих обновлений программного обеспечения, чтобы обеспечить согласованность в аналогичных развертываниях и сэкономить время.
- **Коллекция**. Укажите коллекцию для развертывания, если применимо. Члены коллекции получают обновления компонентов, определенные в развертывании.

5. На странице Параметры развертывания настройте следующие параметры:

- **Тип развертывания**. Укажите тип развертывания для развертывания обновлений программного обеспечения. Выберите **Обязательный,** чтобы создать обязательное развертывание обновлений программного обеспечения, в котором обновления компонентов автоматически устанавливаются на клиентах до установленного крайнего срока установки.

  > ⓘ **Важно!**
  >
  > После создания развертывания обновления программного обеспечения вы не сможете изменить тип развертывания.

  > ⓘ **Примечание**

Группа обновлений программного обеспечения, развернутая в качестве **обязательной** , будет загружена в фоновом режиме и учитывать параметры BITS, если это настроено.

- **Использование пробуждения по локальной сети для пробуждения клиентов для необходимых развертываний**. Укажите, следует ли включить пробуждение по локальной сети в крайнем сроке для отправки пакетов пробуждения на компьютеры, которым требуется одно или несколько обновлений программного обеспечения в развертывании. Все компьютеры, которые находятся в спящем режиме в течение крайнего срока установки, будут пробуждаются, чтобы можно было инициировать установку обновления программного обеспечения. Клиенты, которые находятся в спящем режиме, для которых не требуются обновления программного обеспечения в развертывании, не запускаются. По умолчанию этот параметр не включен и доступен только в том случае, если **для параметра Тип развертывания** задано значение **Обязательный**.

  ⚠ **Предупреждение**

  Прежде чем использовать этот параметр, компьютеры и сети должны быть настроены для пробуждения по локальной сети.

- **Уровень сведений**. Укажите уровень детализации для сообщений о состоянии, сообщаемых клиентскими компьютерами.

6. На странице Планирование настройте следующие параметры:

   - **Планирование оценки**. Укажите, оценивается ли доступное время и крайний срок установки в соответствии с UTC или местным временем компьютера, на котором запущена консоль Configuration Manager.

   - **Время доступности программного обеспечения**. Выберите **Конкретное время** , чтобы указать, когда обновления программного обеспечения будут доступны клиентам:
     - **Определенное время**. Выберите этот параметр, чтобы сделать обновление компонентов в развертывании доступным для клиентов в определенную дату и время. Укажите дату и время, соответствующие началу фиксированного периода обслуживания. При создании развертывания политика клиента обновляется, и клиенты получают сведения о развертывании во время следующего цикла опроса

политики клиента. Однако обновление компонентов в развертывании недоступно для установки до тех пор, пока не будут достигнуты указанные дата и время и не будет загружено необходимое содержимое.

- **Крайний срок установки**. Выберите **Конкретное время** , чтобы указать крайний срок установки обновлений программного обеспечения в развертывании.

  > ⓘ **Примечание**
  >
  > Параметр крайнего срока установки можно настроить только в том случае, если для **параметра Тип развертывания** задано значение **Обязательный** на странице Параметры развертывания.

  - **Определенное время**. Выберите этот параметр, чтобы автоматически установить обновления программного обеспечения в развертывании в определенную дату и время. Однако для целей фиксированного периода обслуживания установите дату и время установки в будущем значение, за пределами фиксированного периода обслуживания.

  Необходимые развертывания для обновлений программного обеспечения могут воспользоваться функциями, называемыми расширенной загрузкой. По достижении времени, доступного по программному обеспечению, клиенты начинают скачивать содержимое на основе случайного времени. Обновление компонентов не будет отображаться в Центре программного обеспечения для установки до полного скачивания содержимого. Это гарантирует, что установка обновления компонентов начнется сразу после запуска.

7. На странице Взаимодействие с пользователем настройте следующие параметры:

   - **Уведомления пользователей**: укажите **отображение в Центре программного обеспечения и отобразите все уведомления**.

   - **Поведение крайних сроков**. Доступно, только если на странице Параметры **развертывания для параметра типа развертывания** задано значение **Обязательный** . Укажите поведение, которое будет происходить при достижении крайнего срока развертывания обновлений программного обеспечения. Укажите, следует ли устанавливать обновления программного обеспечения в развертывании. Также укажите, следует ли выполнять перезагрузку системы после

установки обновления программного обеспечения независимо от настроенного периода обслуживания.

> ⓘ **Примечание**
>
> Помните, что дата и время установки будут в будущем, чтобы обеспечить много времени для установки, инициированной пользователем, в течение фиксированного периода обслуживания.

- **Поведение перезапуска устройства**. Доступно только в том случае, если для **параметра Тип развертывания** задано значение **Обязательный** на странице Параметры развертывания. Укажите, следует ли отключить перезапуск системы на серверах и рабочих станциях после установки обновлений программного обеспечения, а для завершения установки требуется перезагрузка системы.

  > ⓘ **Важно!**
  >
  > Отключение перезапусков системы может быть полезно в серверных средах или в случаях, когда компьютеры, устанавливающие обновления программного обеспечения, не должны перезапускаться по умолчанию. Однако это может привести к тому, что компьютеры будут в небезопасном состоянии, в то время как принудительная перезагрузка помогает обеспечить немедленное завершение установки обновления программного обеспечения.

- **Обработка фильтра записи для устройств Windows Embedded**. При развертывании обновлений программного обеспечения на устройствах Windows Embedded с включенным фильтром записи можно указать установку обновления программного обеспечения на временном наложении и либо зафиксировать изменения позже, либо зафиксировать изменения в крайнем сроке установки или во время периода обслуживания. При фиксации изменений в крайний срок установки или во время периода обслуживания требуется перезагрузка, а изменения сохраняются на устройстве.

  > ⓘ **Примечание**

При развертывании обновления программного обеспечения на устройстве Windows Embedded убедитесь, что устройство является членом коллекции с настроенным периодом обслуживания.

- **Поведение повторной оценки развертывания обновлений программного обеспечения при перезапуске**. Начиная с Configuration Manager версии 1606, выберите этот параметр, чтобы настроить развертывания обновлений программного обеспечения, чтобы клиенты запускали проверку соответствия обновлений программного обеспечения сразу после установки и перезапуска клиента. Это позволяет клиенту проверка дополнительных обновлений программного обеспечения, которые становятся применимыми после перезапуска клиента, а затем установить их (и стать совместимыми) в течение того же периода обслуживания.

8. На странице Оповещения настройте, как Configuration Manager и System Center Operations Manager создают оповещения для этого развертывания. Оповещения можно настроить только в том случае, если для **параметра Тип развертывания** задано значение **Обязательный** на странице Параметры развертывания.

> ⓘ **Примечание**
>
> Оповещения о последних обновлениях программного обеспечения можно просмотреть в узле **Обновления программного обеспечения** в рабочей области **Библиотека программного обеспечения**.

9. На странице Скачивание параметров настройте следующие параметры:

   - Укажите, будет ли клиент загружать и устанавливать обновления программного обеспечения, когда клиент подключен к медленной сети или использует резервное расположение содержимого.

   - Укажите, следует ли клиенту загружать и устанавливать обновления программного обеспечения из резервной точки распространения, если содержимое обновлений программного обеспечения недоступно в предпочтительной точке распространения.

   - **Разрешить клиентам делиться содержимым с другими клиентами в той же подсети**. Укажите, следует ли включить использование BranchCache для скачивания содержимого. Дополнительные сведения о BranchCache см. в разделе Основные понятия для управления содержимым.

- **Если обновления программного обеспечения недоступны в точке распространения в текущих, соседних группах или группах сайтов, скачайте содержимое из Microsoft Обновления**. Выберите этот параметр, чтобы клиенты, подключенные к интрасети, загружали обновления программного обеспечения из Центра обновления Майкрософт, если обновления программного обеспечения недоступны в точках распространения. Интернет-клиенты всегда могут перейти в Центр обновления Майкрософт для получения содержимого обновлений программного обеспечения.

- Укажите, следует ли разрешать клиентам скачивание после крайнего срока установки при использовании лимитных подключений к Интернету. Интернет-провайдеры иногда взимают плату за объем данных, которые вы отправляете и получаете, когда вы используете лимитное подключение к Интернету.

  > ⓘ **Примечание**
  >
  > Клиенты запрашивают расположение содержимого из точки управления для обновлений программного обеспечения в развертывании. Поведение скачивания зависит от того, как вы настроили точку распространения, пакет развертывания и параметры на этой странице. Дополнительные сведения см. в статье Сценарии расположения источника содержимого.

10. На странице Сводка просмотрите параметры. Чтобы сохранить параметры в шаблоне развертывания, выберите **Сохранить как шаблон**, введите имя и выберите параметры, которые нужно включить в шаблон, а затем нажмите кнопку **Сохранить**. Чтобы изменить настроенный параметр, выберите соответствующую страницу мастера и измените параметр.

11. Нажмите **кнопку Далее** , чтобы развернуть обновления компонентов.

Шаг 4. Мониторинг состояния развертывания

После развертывания обновлений компонентов можно отслеживать состояние развертывания. Чтобы отслеживать состояние развертывания, выполните следующую процедуру:

1. В консоли Configuration Manager перейдите в раздел **Мониторинг** > **Обзор** > **развертываний**.

2. Выберите группу обновлений программного обеспечения или обновление программного обеспечения, для которых требуется отслеживать состояние развертывания.
3. На вкладке **Главная** в группе **Развертывание** выберите **Просмотреть состояние**.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Меры защиты

Статья • 18.03.2023

Область применения

- Windows 10
- Windows 11

Корпорация Майкрософт использует данные о качестве и совместимости для выявления проблем, которые могут привести к сбою или откату обновления клиентских компонентов Windows. Когда мы обнаруживаем такую проблему, мы можем применить защитные удержания к службе обновления, чтобы предотвратить установку обновления на затронутых устройствах, чтобы защитить их от таких возможностей. Мы также используем удержания защиты, когда клиент, партнер или внутренняя проверка Майкрософт обнаруживает проблему, которая может привести к серьезным последствиям (например, откат обновления, потеря данных, потеря подключения или потеря ключевых функциональных возможностей) и когда обходной путь недоступен сразу.

Удержания защиты не позволяют устройству с известной проблемой предложить новую версию операционной системы. Мы продлеваем предложение после того, как будет найдено и проверено исправление. Мы используем удержания, чтобы клиенты успешно работали, когда их устройство переходит на новую версию клиента Windows.

Срок действия гарантии зависит от времени, необходимого для изучения и устранения проблемы. В течение этого времени корпорация Майкрософт тщательно работает над приобретением, разработкой и проверкой исправления, а затем предлагает его затронутым устройствам. Мы отслеживаем данные о качестве и совместимости, чтобы убедиться, что исправление завершено, прежде чем освободить удержание защиты. Как только мы отпустим удержание защиты, клиентский компонент Центра обновления Windows возобновит предлагать устройствам новые версии операционной системы.

Удержания защиты влияют только на устройства, которые используют службу клиентский компонент Центра обновления Windows для обновлений. Мы рекомендуем ИТ-администраторам, которые управляют обновлениями на устройствах через другие каналы (например, установки мультимедиа или обновления, поступающие из Windows Server Update Services), оставаться в курсе известных проблем, которые также могут присутствовать в их средах.

ИТ-администраторы, управляющие обновлениями с помощью службы развертывания клиентский компонент Центра обновления Windows для бизнеса, также получают преимущество от удержания средств защиты на устройствах, на которых, скорее всего, повлияет проблема. Дополнительные сведения см. в статье Защита от вероятных и известных проблем.

Влияет ли на меня удержание?

ИТ-администраторы могут использовать отчеты клиентский компонент Центра обновления Windows для бизнеса для мониторинга различных метрик работоспособности обновлений для устройств в своей организации. В отчетах содержится список активных удержаний для защиты, чтобы получить представление о удержаниях, которые препятствуют обновлению или обновлению устройств.

Отчеты клиентский компонент Центра обновления Windows для бизнеса определяют удержания по 8-значным идентификаторам. Дополнительные сведения об этой проблеме можно найти на панели мониторинга работоспособности выпуска Windows , выполнив поиск идентификатора удержания защиты на странице **Известные проблемы** для соответствующего выпуска.

На устройствах, использующих клиентский компонент Центра обновления Windows (но не клиентский компонент Центра обновления Windows для бизнеса), **клиентский компонент Центра обновления Windows** на странице в приложении "Параметры" отображается сообщение о том, что обновление находится на пути, но не готово для устройства. Вместо параметра скачивания и установки обновления пользователи увидят следующее сообщение:

Это сообщение означает, что устройство защищено одним или несколькими защитными удержаниями. Если проблема устранена и обновление безопасно установить, мы снимем удержание защиты, и обновление может возобновиться безопасно.

Как поступить в этом случае?

Рекомендуется не пытаться вручную обновить до тех пор, пока проблемы не будут устранены и не будут освобождены.

> ⊗ **Внимание!**
>
> Отказ от удержания защиты может поставить устройства под угрозу из-за известных проблем с производительностью. Мы настоятельно рекомендуем провести надежное тестирование, чтобы убедиться, что влияние является приемлемым, прежде чем отказаться от него.

Учитывая это, ИТ-администраторы, которые остаются в курсе клиентский компонент Центра обновления Windows отчетов для бизнеса и панели мониторинга работоспособности выпусков Windows, могут временно отказаться от защиты всех удержаний и разрешить обновление. Рекомендуется отказаться только в ИТ-среде и в целях проверки. Если вы откажетесь от удержания, это условие является временным. После завершения обновления защита удержаний автоматически восстанавливается.

Отказ от мер безопасности

Статья • 21.12.2023 • Применяется к: ✅ Windows 11, ✅ Windows 10

Удержания защиты не позволяют устройству с известной проблемой совместимости предлагать новое обновление функций клиента Windows с помощью клиентский компонент Центра обновления Windows. Мы используем защитные удержания, чтобы защитить устройство и пользователя от неудачного или плохого обновления. Мы продлеваем предложение после того, как исправление будет выдано и проверено на затронутом устройстве. Дополнительные сведения об удержании средств защиты см. в разделе Удержание защиты.

Как отказаться от удержания средств защиты?

ПРИ необходимости ИТ-администраторы могут отказаться от защиты устройств с помощью политики отключения мер безопасности. В средстве mobile Управление устройствами (MDM) используйте CSP **update/DisableWUfBSafeguards**. В групповая политика используйте групповая политика **Отключить меры безопасности для Обновления компонентов**. Эта политика доступна для клиентский компонент Центра обновления Windows для устройств для бизнеса под управлением следующих операционных систем:

- Windows 11
- Windows 10, версия 1809 или более поздней версии с обновлением для системы безопасности за октябрь 2020 г.

> ⊗ **Внимание!**
>
> Отказ от удержания защиты может поставить устройства под угрозу из-за известных проблем с производительностью.

Рекомендуется отказаться только в ИТ-среде и в целях проверки. Вы также можете проверить предстоящую версию клиентского обновления компонентов Windows без применения мер безопасности с помощью канала Release Preview программы предварительной оценки Windows для бизнеса.

Отключение мер безопасности не гарантирует, что устройство сможет успешно обновиться. Обновление может по-прежнему завершиться ошибкой и, скорее

всего, приведет к плохому взаимодействию, так как вы обходите защиту от известных проблем.

> **Примечание**
>
> После того как устройство установит новую версию клиента Windows, параметр **Отключить меры безопасности для Обновления компонентов** групповая политика будет отменить изменения **значение Не настроено**, даже если она была включена ранее. Это делается для того, чтобы администратор сознательно отключит защиту майкрософт по умолчанию от известных проблем для каждого нового обновления компонентов.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Управление перезапусками устройства после обновлений

Применяется к: ✅ Windows 11, ✅ Windows 10

> **Ищете информацию для потребителей?** См. раздел Центр обновления Windows: вопросы и ответы

Вы можете использовать параметры групповой политики, управление мобильными устройствами (MDM) или реестр Windows, чтобы настроить время перезапуска устройств после установки обновления Windows. Вы можете запланировать установку обновлений и задать политики для перезапуска, настроить часы активности, когда перезапуски не должны происходить, или вы можете сделать и то, и другое.

> **Примечание.**
>
> Прямое редактирование реестра Windows не рекомендуется.

Планирование установки обновлений

В групповой политике в разделе **Настройка автоматического Обновления** можно настроить принудительную перезагрузку после указанного времени установки.

Чтобы задать время, перейдите в **раздел Настройка автоматического Обновления**, выберите вариант **4 — Автоматическое скачивание и запланируйте установку**, а затем введите **время запланированной установки**. Кроме того, можно указать, что установка происходит во время автоматического обслуживания. Чтобы настроить этот альтернативный метод, используйте **конфигурацию компьютера\Административные шаблоны\Компоненты Windows\Планировщик обслуживания**.

Параметр **Всегда автоматически перезапускается в запланированное время** , принуждает перезапуск после указанного времени установки. Он позволяет настроить таймер, чтобы предупредить пользователя, выполнившего вход, о том, что произойдет перезагрузка. Эта политика является устаревшей и неприменима для Windows 11. Устаревшие политики могут быть удалены в будущем выпуске.

Хотя это не рекомендуется, вы можете достичь того же результата с помощью реестра Windows. В `HKLM\Software\Policies\Microsoft\Windows\WindowsUpdate\AU` параметре задайте значение `AuOptions` `4` и задайте время установки с `ScheduledInstallTime` помощью . Включите `AlwaysAutoRebootAtScheduledTime` и укажите задержку в минутах до

`AlwaysAutoRebootAtScheduledTimeMinutes`. Как и в случае с групповой политикой, `AlwaysAutoRebootAtScheduledTimeMinutes` задает таймер для предупреждения пользователя, выполнившего вход, о том, что произойдет перезагрузка.

Подробное описание этих разделов реестра см. в разделе Разделы реестра, используемые для управления перезагрузкой.

Задержка автоматического перезапуска

При включении **настройки автоматического Обновления** в групповой политике можно также включить одну из следующих политик для задержки автоматического перезапуска после установки обновления:

- **Отключить автоматический перезапуск при обновлении в период активности** — предотвращает автоматический перезапуск в период активности.
- **Не выполнять автоматическую перезагрузку при автоматической установке обновлений, если в системе работают пользователи** — предотвращает автоматический перезапуск, если пользователь выполнил вход в систему. Если пользователь планирует перезапуск в уведомлении об обновлении, устройство перезапускается в момент, когда пользователь указывает, даже если пользователь вошел в систему в это время. Эта политика применяется только в том случае, если для **параметра Настройка автоматического Обновления** задано значение **4 — автоматическое скачивание и планирование установки**.

> ⓘ **Примечание.**
>
> - При использовании подключений по протоколу удаленного рабочего стола (RDP) только активные сеансы RDP считаются входными пользователями. Устройства, у которых нет локальных пользователей или активных сеансов RDP, перезапускаются.
> - Политика **автоматической перезагрузки без входа пользователей для установки запланированных автоматических обновлений** никогда не создавалась в качестве CSP. В групповая политика эта политика работает не в точности согласно описанию. Эта политика не может привести к периоду перезагрузки качественных обновлений, учитывая, что многие пользователи никогда не выходить из системы. Вместо этого рекомендуется использовать крайний срок соответствия требованиям, а затем настроить без автоматической перезагрузки, чтобы предотвратить перезагрузку, не относясь к пользователю, до достижения крайнего срока. Для серверных устройств используйте параметр

Настроить автоматическую Обновления 7 — уведомление об установке и уведомление о перезагрузке.

Вы также можете использовать реестр Windows, чтобы предотвратить автоматические перезапуски при входе пользователя. В разделе `HKLM\Software\Policies\Microsoft\Windows\WindowsUpdate\AU` задайте значение `4` `AuOptions` и включите `NoAutoRebootWithLoggedOnUsers`. Как и в случае с групповой политикой, если пользователь планирует перезапуск в уведомлении об обновлении, он переопределяет этот параметр.

Подробное описание этих разделов реестра см. в разделе Разделы реестра, используемые для управления перезагрузкой.

Настройка периода активности

Период активности — это период, когда устройство предположительно будет использоваться. Автоматические перезапуски после обновления происходят в нерабочее время.

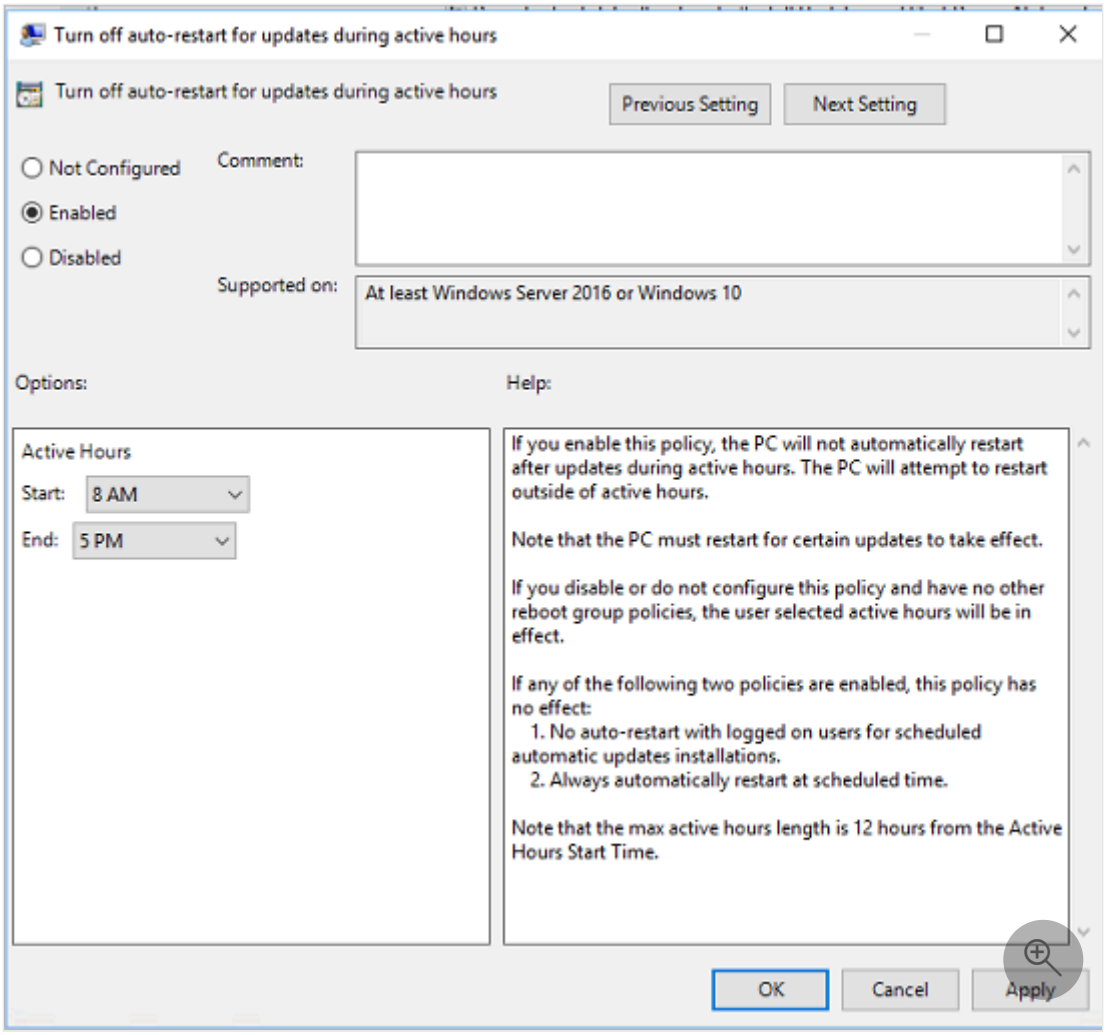
По умолчанию время активности на компьютерах — с 8:00 до 17:00. Пользователи могут вручную изменить часы активности.

Можно также указать диапазон максимального количества активных часов. Указанный диапазон отсчитывается из времени начала активных часов.

> ⓘ **Примечание.**
>
> Максимальная продолжительность активных часов для Windows 10 версии 1607 и Windows Server 2016 — 12. Более поздние версии поддерживают максимальную продолжительность активных часов в 18 часов.

Настройка времени активности с помощью групповой политики

Чтобы настроить часы активности с помощью групповой политики, **перейдите в раздел Конфигурация компьютера\Административные шаблоны\Компоненты Windows\клиентский компонент Центра обновления Windows** и откройте параметр политики **Отключить автоматическую перезагрузку для обновлений во время активности**. Если политика включена, можно задать время начала и окончания периода активности.



Настройка времени активности с помощью MDM

Чтобы настроить часы активности, MDM использует следующие параметры в CSP политики обновления:

- ActiveHoursStart
- ActiveHoursEnd
- ActiveHoursMaxRange

Настройка активных часов с помощью реестра Windows

Этот метод не рекомендуется использовать, и его следует использовать только в том случае, если вы не можете использовать групповую политику или MDM. Все параметры, настроенные в реестре, могут конфликтовать с любой существующей конфигурацией, которая использует любой из других методов.

Настройте часы активности, задав сочетание следующих значений реестра:

В разделе `HKLM\Software\Policies\Microsoft\Windows\WindowsUpdate` Используется `SetActiveHours` для включения или отключения часов активности и

`ActiveHoursStart` `ActiveHoursEnd` для указания диапазона активных часов.

Подробное описание этих разделов реестра см. в разделе Разделы реестра, используемые для управления перезагрузкой.

> **Совет**
>
> Чтобы вручную настроить часы активности на устройстве, перейдите в **раздел Параметры>клиентский компонент Центра обновления Windows>Добавить параметры** и выберите **Активные часы**.

Настройка максимального диапазона активных часов

Можно указать максимальный диапазон активных часов, который могут задать пользователи. Этот параметр позволяет оставить некоторые часы активности на стороне пользователя, а также предоставить достаточно времени для установки обновлений. Максимальный диапазон вычисляется из времени начала активных часов.

Чтобы настроить максимальный диапазон для часов активности с помощью групповой политики, перейдите в раздел **Конфигурация компьютера\Административные шаблоны\Компоненты Windows\клиентский компонент Центра обновления Windows** и откройте параметр **Укажите диапазон активных часов для автоматического перезапуска**.

Чтобы настроить максимальный диапазон для активных часов с помощью MDM, используйте ActiveHoursMaxRange.

Ограничение задержек перезапуска

После установки обновления Windows пытается автоматически перезапустить в нерабочее время. Если перезапуск не выполняется после периода по умолчанию, равного семи дням, пользователь видит уведомление о необходимости перезапуска. Чтобы изменить задержку, используйте параметр **указать крайний срок перед автоматическим перезапуском для установки обновлений**. Минимальное значение — два дня, а максимальное — две недели (14 дней). Эта политика является устаревшей и неприменима для Windows 11. Устаревшие политики могут быть удалены в будущем выпуске.

Управление уведомлениями о перезапуске

Параметры отображения уведомлений об обновлении

Вы можете указать, какие клиентский компонент Центра обновления Windows уведомления отображаются пользователю. Эта политика не определяет, как и когда загружаются и устанавливаются обновления.

Чтобы настроить это поведение с помощью групповой политики, **перейдите в раздел Конфигурация компьютера\Административные шаблоны\Компоненты Windows\клиентский компонент Центра обновления Windows** и выберите политику для **параметра Параметры отображения уведомлений об обновлениях**. Настройте следующие значения:

- `0`(по умолчанию): используйте уведомления по умолчанию клиентский компонент Центра обновления Windows.
- `1`: отключите большинство уведомлений, но оставьте предупреждения о перезапуске.
- `2`: отключите все уведомления, включая предупреждения о перезапуске.

Чтобы настроить это поведение с помощью MDM, используйте UpdateNotificationLevel.

Начиная с Windows 11 версии 22H2, в качестве другого параметра для **отображения параметров уведомлений об обновлении** добавлен параметр **Применить только в часы активности**. При выборе **параметра Применить только в часы активности** уведомления отключаются только в часы активности при использовании параметров `1` или `2`. Чтобы обеспечить обновление устройства, уведомление по-прежнему отображается в часы активности, если выбрано **применить только в часы активности**, а после достижения крайнего срока при настройке указать крайние сроки для автоматических обновлений и перезапусков.

Чтобы настроить это поведение с помощью MDM, используйте UpdateNotificationLevel.

Уведомления об автоматическом перезапуске

Вы можете переопределить поведение по умолчанию для уведомления об обязательном автоматическом перезапуске. По умолчанию это уведомление закрывается автоматически.

- Чтобы настроить это поведение с помощью групповой политики, перейдите в раздел **Конфигурация компьютера\Административные шаблоны\Компоненты Windows\клиентский компонент Центра обновления Windows** и выберите политику **Настройка необходимого уведомления о необходимости автоматического перезапуска для обновлений**. Если выбран параметр **2 - User**

Action, пользователь, который получает это уведомление, должен закрыть его вручную. Эта политика является устаревшей и неприменима для Windows 11. Устаревшие политики могут быть удалены в будущем выпуске.

- Чтобы настроить это поведение с помощью MDM, используйте AutoRestartRequiredNotificationDismissal. Эта политика является устаревшей и неприменима для Windows 11. Устаревшие политики могут быть удалены в будущем выпуске.

Вы также можете настроить период до обновления, которое отображается в этом уведомлении. Значение по умолчанию — 15 минут.

- Чтобы изменить его с помощью групповой политики, выберите **Настроить уведомления об автоматическом перезапуске и напоминания для обновлений** в разделе **Конфигурация компьютера\Административные шаблоны\Компоненты Windows\клиентский компонент Центра обновления Windows** и выберите период в минутах. Эта политика является устаревшей и неприменима для Windows 11. Устаревшие политики могут быть удалены в будущем выпуске.

- Чтобы изменить его с помощью MDM, используйте AutoRestartNotificationSchedule. Эта политика является устаревшей и неприменима для Windows 11. Устаревшие политики могут быть удалены в будущем выпуске.

В некоторых случаях может потребоваться отключить уведомления.

- Для этого с помощью групповой политики **перейдите в раздел Конфигурация компьютера\Административные шаблоны\Компоненты Windows\клиентский компонент Центра обновления Windows** и выберите параметр **Отключить уведомления об автоматическом перезапуске для установки обновлений**. Эта политика является устаревшей и неприменима для Windows 11. Устаревшие политики могут быть удалены в будущем выпуске.

- Для этого с помощью MDM используйте SetAutoRestartNotificationDisable. Эта политика является устаревшей и неприменима для Windows 11. Устаревшие политики могут быть удалены в будущем выпуске.

Предупреждения об автоматическом перезапуске по расписанию

Так как пользователи не могут отложить запланированный перезапуск после достижения крайнего срока, можно настроить предупреждение перед запланированным перезапуском. Вы также можете настроить предупреждение перед перезапуском, чтобы

уведомить пользователей о неминуемом перезапуске и разрешить им сохранить свою работу.

Чтобы настроить оба компонента с помощью групповой политики, найдите параметр **Настройка расписания предупреждений автоматического перезапуска для обновлений** в разделе **Конфигурация компьютера\Административные шаблоны\Компоненты Windows\клиентский компонент Центра обновления Windows**. Напоминание о предупреждении можно настроить с помощью **функции Напоминания (часы),** а предупреждение перед неминуемым автоматическим перезапуском можно настроить с помощью **параметра Warning (mins).** Эта политика является устаревшей и неприменима для Windows 11. Устаревшие политики могут быть удалены в будущем выпуске.

В MDM, чтобы настроить напоминание о предупреждении, используйте ScheduleRestartWarning. Эта политика является устаревшей и неприменима для Windows 11. Устаревшие политики могут быть удалены в будущем выпуске. Чтобы настроить автоматическое предупреждение о неминуемом перезапуске, используйте ScheduleImminentRestartWarning. Эта политика является устаревшей и неприменима для Windows 11. Устаревшие политики могут быть удалены в будущем выпуске.

Управляемый перезапуск

Управляемый перезапуск подразумевает, что пользователям предоставляется период времени, в течение которого они должны запланировать перезапуск. Изначально Windows автоматически перезапускается в нерабочее время. После окончания семидневного периода по умолчанию Windows переходит на запланированные пользователем перезапуски.

Вы можете настроить следующие параметры для включенной перезагрузки:

- Период времени до перехода автоматического перезапуска на задействованный перезапуск.
- количество дней, на которое пользователи могут отложить уведомления с напоминанием об управляемом перезапуске;
- количество дней до автоматического выполнения отложенного перезапуска вне периода активности.

В групповой политике перейдите в раздел **Конфигурация компьютера\Административные шаблоны\Компоненты Windows\клиентский компонент Центра обновления Windows** и используйте параметр **Указать задействованный переход перезапуска и расписание уведомлений об обновлениях**.

Эта политика является устаревшей и неприменима для Windows 11. Устаревшие политики могут быть удалены в будущем выпуске.

В MDM используйте следующие политики:

- EngagedRestartTransitionSchedule
  - Эта политика является устаревшей и неприменима для Windows 11. Устаревшие политики могут быть удалены в будущем выпуске.
- EngagedRestartSnoozeSchedule
  - Эта политика является устаревшей и неприменима для Windows 11. Устаревшие политики могут быть удалены в будущем выпуске.
- EngagedRestartDeadline
  - Эта политика является устаревшей и неприменима для Windows 11. Устаревшие политики могут быть удалены в будущем выпуске.

Параметры групповой политики для перезапуска

В редакторе групповой политики параметры политики для поведения перезапуска находятся в разделе **Конфигурация компьютера\Административные шаблоны\Компоненты Windows\клиентский компонент Центра обновления Windows**. В следующей таблице показано, какие политики применяются к Windows 10.

Развернуть таблицу

Политика	Применяется к Windows 10	Примечания
Отключить автоматический перезапуск при обновлении в период активности	Да	Используйте эту политику, чтобы настроить часы активности, в течение которых устройство не будет перезагружено. Эта политика не имеет эффекта, если включена политика **Не выполнять автоматическую перезагрузку при автоматической установке обновлений, если в системе работают пользователи** или **Всегда автоматически перезагружаться в запланированное время**.
Всегда автоматически перезагружаться в запланированное время	Да	Используйте эту политику для настройки таймера перезагрузки (от 15 до 180 минут), который начнет отсчет сразу после установки Центром обновления Windows важных обновлений. Эта политика не имеет эффекта, если включена политика **Не выполнять автоматическую перезагрузку при автоматической установке обновлений, если в системе работают пользователи**. Эта политика является устаревшей и неприменима для

Политика	Применяется к Windows 10	Примечания
		Windows 11. Устаревшие политики могут быть удалены в будущем выпуске.
Указание срока до автоматического перезапуска после установки обновления	Да	Используйте эту политику, чтобы указать, на сколько дней (от 2 до 14) можно отложить автоматический перезапуск. Эта политика не имеет эффекта, если включена политика **Не выполнять автоматическую перезагрузку при автоматической установке обновлений, если в системе работают пользователи** или **Всегда автоматически перезагружаться в запланированное время**. Эта политика является устаревшей и неприменима для Windows 11. Устаревшие политики могут быть удалены в будущем выпуске.
Не выполнять автоматическую перезагрузку при автоматической установке обновлений, если в системе работают пользователи	Да	Используйте эту политику, чтобы не допустить автоматического перезапуска, если пользователь работает в системе. Эта политика применяется только при настройке политики **для настройки автоматического Обновления** для планирования установки. Политика **автоматической перезагрузки без входа пользователей для установки запланированных автоматических обновлений** никогда не создавалась в качестве CSP. В групповая политика эта политика работает не в точности согласно описанию. Эта политика не может привести к периоду перезагрузки качественных обновлений, учитывая, что многие пользователи никогда не выходить из системы. Вместо этого рекомендуется использовать крайний срок соответствия требованиям, а затем настроить без автоматической перезагрузки, чтобы предотвратить перезагрузку, не относясь к пользователю, до достижения крайнего срока. Для серверных устройств используйте параметр Настроить автоматическую Обновления 7 — уведомление об установке и уведомление о перезагрузке.
Повторный запрос для перезагрузки при запланированных установках	Нет	Эта политика не реализована в Windows 10 и не действует, если задано Windows 10 или Windows 11.
Задержка перезагрузки при запланированных установках	Нет	Эта политика не реализована в Windows 10 и не действует, если задано Windows 10 или Windows 11.
Перенос запланированных автоматических	Нет	Эта политика не реализована в Windows 10 и не действует, если задано Windows 10 или Windows 11.

Политика	Применяется к Windows 10	Примечания
установок обновлений		

Примечание.

- Можно выбрать только один путь для поведения перезагрузки.
- Если настроить конфликтующие политики перезапуска, фактическое поведение перезапуска может отличаться от ожидаемого.
- При использовании RDP только активные сеансы RDP считаются входными пользователями.
- Политика **автоматической перезагрузки без входа пользователей для установки запланированных автоматических обновлений** никогда не создавалась в качестве CSP. В групповая политика эта политика работает не в точности согласно описанию. Эта политика не может привести к периоду перезагрузки качественных обновлений, учитывая, что многие пользователи никогда не выходить из системы. Вместо этого рекомендуется использовать крайний срок соответствия требованиям, а затем настроить без автоматической перезагрузки, чтобы предотвратить перезагрузку, не относясь к пользователю, до достижения крайнего срока. Для серверных устройств используйте параметр Настроить автоматическую Обновления 7 — уведомление об установке и уведомление о перезагрузке.

Разделы реестра, используемые для управления перезагрузкой

В следующих таблицах перечислены значения реестра, соответствующие параметрам групповой политики для управления перезапусками после обновлений в Windows 10.

`HKLM\Software\Policies\Microsoft\Windows\WindowsUpdate`

Развернуть таблицу

Раздел реестра	Тип ключа	Значение
`ActiveHoursEnd`	`REG_DWORD`	`0-23`: задайте для активных часов конец в определенный час. Он начинается с 12:00 (`0`) и заканчивается 23:00 (`23`).
`ActiveHoursStart`	`REG_DWORD`	`0-23`: задайте часы активности, которые будут начинаться с определенного часа. Он начинается с 12:00 (`0`) и заканчивается 23:00 (`23`.)
`SetActiveHours`	`REG_DWORD`	`0`: отключить автоматический перезапуск после обновления в нерабочее время. `1`: включите автоматический перезапуск после обновления в нерабочее время.

`HKLM\Software\Policies\Microsoft\Windows\WindowsUpdate\AU`

Развернуть таблицу

Раздел реестра	Тип ключа	Значение
`AlwaysAutoRebootAtScheduledTime`	`REG_DWORD`	`0`: отключите автоматический перезапуск после установки обновления в запланированное время. `1`: включите автоматический перезапуск после установки обновления в запланированное время.
`AlwaysAutoRebootAtScheduledTimeMinutes`	`REG_DWORD`	`15-180`: настройте автоматическую перезагрузку после указанного количества минут.
`AUOptions`	`REG_DWORD`	`2`: уведомляет о скачивании и уведомляет об установке обновлений. `3`: автоматически скачивает обновления и уведомляет об установке обновлений. `4`: автоматическое скачивание и планирование установки обновлений. `5`: разрешить локальному администратору настроить эти параметры. **Заметка:** Чтобы настроить поведение перезапуска, присвойте этому значению значение `4`.
`NoAutoRebootWithLoggedOnUsers`	`REG_DWORD`	`0`: если пользователи вошли в систему, автоматически перезапустите ("отключить не перезагружайте").

Раздел реестра	Тип ключа	Значение
		`1`: если пользователь вошел в систему, не перезапускайте после установки обновления. **Заметка:** Если параметр отключен (`0`), автоматический Обновления уведомляет пользователя о том, что компьютер планируется автоматически перезапустить через пять минут, чтобы завершить установку.
`ScheduledInstallTime`	`REG_DWORD`	`0-23`: запланируйте время установки обновления на определенный час. Он начинается с 12:00 (`0`) и заканчивается 23:00 (`23`).

Существует три различных сочетания реестра для управления поведением перезапуска:

- Чтобы задать часы активности, выполните приведенные далее действия.
  - `SetActiveHours` значение должно иметь значение `1`.
  - Затем, чтобы определить диапазон времени, используйте `ActiveHoursStart` и `ActiveHoursEnd`.

- Чтобы запланировать определенную установку и время перезапуска, выполните указанные ниже действия.
  - `AUOptions` значение должно иметь значение `4`.
  - `ScheduledInstallTime` должно указать время установки.
  - Задайте значение `AlwaysAutoRebootAtScheduledTime` `1`. Эта политика является устаревшей и неприменима для Windows 11. Устаревшие политики могут быть удалены в будущем выпуске.
  - `AlwaysAutoRebootAtScheduledTimeMinutes` необходимо указать время ожидания в минутах перед перезапуском. Эта политика является устаревшей и неприменима для Windows 11. Устаревшие политики могут быть удалены в будущем выпуске.

- Чтобы отложить перезапуск, если пользователь вошел в систему, выполните приведенные далее действия.
  - `AUOptions` значение должно иметь значение `4`.
  - Задайте значение `NoAutoRebootWithLoggedOnUsers` `1`.

Дополнительные ресурсы

- Обзор модели "Windows как услуга"
- Настройка оптимизации доставки для обновлений Windows

- Настройка политик клиента клиентский компонент Центра обновления Windows
- Пошаговое руководство. Использование групповой политики для настройки клиентский компонент Центра обновления Windows клиентских политик
- Управление обновлениями программного обеспечения Windows в Microsoft Intune

---

Last updated on 06.10.2025

Управление дополнительными параметрами Центра обновления Windows

Статья • 27.12.2024 • Применяется к: ✅ Windows 11, ✅ Windows 10

> **Ищете информацию для потребителей?** См. раздел Центр обновления Windows: вопросы и ответы

Вы можете использовать настройки групповой политики или управление мобильными устройствами (MDM) для настройки поведения центра обновления Windows на ваших устройствах Windows 10. Можно настроить частота обнаружения обновлений, выбрать, когда следует получать обновления, указать размещение службы обновлений и так далее.

Сводка параметров Центра обновления Windows

Развернуть таблицу

Параметр групповой политики	Параметр MDM	Поддерживается с версии
Указать размещение службы обновлений Майкрософт в интрасети	UpdateServiceUrl и UpdateServiceUrlAlternate	Все
Частота поиска автоматических обновлений	DetectionFrequency	1703
Запретить доступ для использования любых средств Центра обновления Windows	Update/SetDisableUXWUAccess	Все
Не подключаться к расположениям		Все

Параметр групповой политики	Параметр MDM	Поддерживается с версии
Центра обновления Windows в Интернете		
Разрешить клиенту присоединение к целевой группе		Все
Разрешить прием содержимого с подписью из службы обновления Майкрософт в интрасети	AllowNonMicrosoftSignedUpdate	Все
Исключать драйверы из обновлений Windows	ExcludeWUDriversInQualityUpdate	1607
Настройка автоматического обновления	AllowAutoUpdate	Все
	клиентский компонент Центра обновления Windows уведомлениях отображается название организации *Название организации отображается по умолчанию. Значение реестра может отключить это поведение.	Windows 11 устройства, присоединенные к Microsoft Entra или зарегистрированные
	Разрешить установку обновлений Windows до первоначального входа пользователя (только для реестра)	Windows 11 версии 22H2 с предварительной версией накопительного обновления 2023-04 или более поздним накопительным обновлением

ⓘ Важно!

Дополнительные сведения о параметрах для управления перезапусками устройств и уведомлениями о перезапуске доступны в разделе **Управление перезапусками устройства после обновлений**.

Дополнительные параметры, которые настраивают при получении обновлений компонентов и качества, см. в **разделе Настройка клиентский компонент Центра обновления Windows для бизнеса**.

Поиск обновлений

Администраторы могут настраивать способ сканирования и получения обновлений устройствами.

Параметр Указать размещение службы обновления Майкрософт в интрасети позволяет администраторам выбрать внутреннее расположение службы обновления Майкрософт для устройств. Параметр Не подключать к расположениям Центра обновления Windows в Интернете позволяет запретить устройствам использование любых служб обновления, кроме этой внутренней службы. Параметр Частота обнаружения автоматических обновлений определяет, насколько часто устройства проверяют наличие обновлений.

Вы можете создать настраиваемые группы устройств, которые работают с внутренней службой обновлений Майкрософт, с помощью параметра Включить нацеливание на стороне клиента. Вы также можете убедиться, что устройства получают обновления, которые не были подписаны корпорацией Майкрософт, из внутренней службы обновлений Майкрософт, с помощью параметра Разрешить подписанные обновления из расположения службы обновлений Майкрософт в интрасети.

Наконец, чтобы убедиться, что процесс обновления полностью контролируется администратором, можно удалить доступ, чтобы использовать все функции клиентский компонент Центра обновления Windows для пользователей.

Дополнительные параметры, которые настраивают при получении обновлений компонентов и качества, см. в разделе Настройка клиентский компонент Центра обновления Windows для бизнеса.

Указать размещение службы обновлений Майкрософт в интрасети

Указывает сервер в интрасети, на котором размещены обновления из центра обновления Майкрософт. Затем можно использовать эту службу обновления для автоматического обновления компьютеров в вашей сети. Этот параметр позволяет указать сервер в вашей сети, который будет функционировать в качестве

внутренней службы обновления. Клиент автоматического Обновления выполняет поиск обновлений, которые применяются к компьютерам в сети.

Чтобы использовать этот параметр в групповой политике, перейдите в расположение **Конфигурация компьютера\Административные шаблоны\Компоненты Windows\Центр обновления Windows\Указать расположение службы Центра обновления Майкрософт в интрасети**. Необходимо задать два значения имени сервера:

- Сервер, с которого клиент автоматического Обновления обнаруживает и скачивает обновления
- Сервер, на который отправляются обновленные рабочие станции статистики. Оба значения можно задать как один и тот же сервер. Можно указать дополнительное значение имени сервера, чтобы агент Центра обновления Windows скачивал обновления с альтернативного сервера скачивания вместо службы обновления в интрасети.

Если задать значение **Включено**, клиент автоматического обновления подключается для поиска и скачивания обновлений к указанной службе обновления Windows в интрасети (или к альтернативному серверу скачивания) вместо центра обновления Windows. Включение этого параметра означает, что конечным пользователям в вашей организации не требуется проходить через брандмауэр, чтобы получить обновления, и дает вам возможность протестировать обновления после их развертывания. Если для параметра **задано значение Отключено** или **Не настроено**, а автоматическое Обновления не отключено политикой или пользовательскими предпочтениями, клиент автоматического Обновления подключается непосредственно к сайту клиентский компонент Центра обновления Windows в Интернете.

Альтернативный сервер скачивания настраивает агент Центра обновления Windows для скачивания файлов с альтернативного сервера скачивания вместо службы обновлений в интрасети. Возможность скачивать файлы с отсутствующими URL-адресами позволяет скачивать содержимое с альтернативного сервера загрузки, если url-адреса для скачивания файлов в метаданных обновления отсутствуют. Этот параметр следует использовать только в том случае, если служба обновления интрасети не предоставляет URL-адреса загрузки в метаданных обновления для файлов, присутствующих на альтернативном сервере загрузки.

> ⓘ **Примечание**
>
> Если политика "Настройка автоматического обновления" выключена, то данная политика не оказывает воздействия.

Если "Альтернативный сервер скачивания" не задан, по умолчанию для скачивания обновлений будет использоваться служба обновлений в интрасети.

Параметр "Скачивать файлы без URL-адреса..." используется, только если задано значение "Альтернативный сервер скачивания".

Чтобы настроить эту политику с помощью MDM, используйте UpdateServiceUrl и UpdateServiceUrlAlternate.

Частота поиска автоматических обновлений

Указывает промежуток времени в часах между поисками доступных обновлений. Истинное время ожидания определяется путем вычитания от 0 до 20 процентов от указанного времени. Например, если в данной политике задается обнаружение с периодом 20 часов, то все клиенты, к которым применяется эта политика, будут проверять наличие обновлений с интервалом 16–20 часов.

Чтобы использовать этот параметр в групповой политике, перейдите в расположение **Конфигурация компьютера\Административные шаблоны\Компоненты Windows\Центр обновления Windows\Частота поиска автоматических обновлений**.

Если параметр имеет значение **Включено**, Windows проверяет наличие доступных обновлений с указанным интервалом. Если для параметра **задано значение Отключено** или **Не настроено**, Windows проверяет наличие доступных обновлений с интервалом по умолчанию в 22 часа.

> ⓘ **Примечание**
>
> Для того чтобы эта политика действовала, должен быть включен параметр "Указать размещение службы обновлений Майкрософт в интрасети".
>
> Если политика "Настройка автоматического обновления" выключена, эта политика не оказывает влияния.

Чтобы настроить эту политику с помощью MDM, используйте DetectionFrequency.

Запретить доступ для использования любых средств Центра обновления Windows

Включив параметр групповой политики в разделе **Конфигурация компьютера\Административные шаблоны\Компоненты Windows\Обновление Windows\Блокировать доступ для использования всех функций Центра обновления Windows**, администраторы могут отключать параметр "Проверка обновления" для пользователей. Все фоновые проверки, загрузки и установки обновлений будут по-прежнему работать в соответствии с настройками.

Не подключаться к расположениям Центра обновления Windows в Интернете

Даже если Центр обновления Windows настроен для получения обновлений из службы обновления в интрасети, он будет периодически получать сведения из общедоступной службы обновления Windows для обеспечения подключений в будущем к Центру обновления Windows и другим службам, таким как Центр обновления Майкрософт или Microsoft Store.

Чтобы включить эту политику, используйте **Конфигурация компьютера\Административные шаблоны\Компоненты Windows\Центр обновления Windows\Не подключаться к расположениям Центра обновления Windows в Интернете**. Если эта политика включена, эта политика отключит описанные выше функции и может привести к прекращению работы подключения к общедоступным службам, таким как Microsoft Store, клиентский компонент Центра обновления Windows для бизнеса и оптимизация доставки.

> ⓘ **Примечание**
>
> Эта политика применяется, только когда устройство настроено для подключения к службе обновления в интрасети с помощью политики "Указать размещение службы обновлений Майкрософт в интрасети".

Разрешить клиенту присоединение к целевой группе

Указывает имя или имена целевой группы, которые должны использоваться для получения обновлений из службы обновления Майкрософт в интрасети. Это позволяет администраторам настраивать группы устройств, которые получают различные обновления из таких источников, как WSUS или Configuration Manager.

Этот параметр групповой политики находится в разделе **Конфигурация компьютера\Административные шаблоны\Компоненты Windows\Обновление Windows\Разрешить клиенту присоединение к целевой группе**. Если для

параметра **задано значение Включено**, сведения о целевой группе отправляются в службу обновления Майкрософт интрасети, которая использует ее для определения обновлений, которые следует развернуть на этом компьютере. Если для параметра **задано значение Отключено** или **Не настроено**, в службу обновления Майкрософт интрасети не отправляются сведения о целевой группе.

Если служба обновлений Майкрософт в интрасети поддерживает несколько целевых групп, эта политика может указать несколько имен групп, разделенных точкой с запятой. В противном случае необходимо указать одну группу.

> ⓘ **Примечание**
>
> Эта политика применяется, только если служба обновления Майкрософт в интрасети, на которую направляется устройство, настроена для поддержки присоединения клиента к целевой группе. Если политика "Указать размещение службы обновлений Майкрософт в интрасети" отключена или не настроена, эта политика не оказывает влияния.

Разрешить прием содержимого с подписью из службы обновления Майкрософт в интрасети

Этот параметр политики позволяет управлять, принимает ли служба автоматических обновлений обновления, подписанные организациями, отличными от Майкрософт, при обнаружении обновления в размещении службы обновлений Майкрософт в интрасети.

Чтобы настроить этот параметр в групповой политике, перейдите в расположение **Конфигурация компьютера\Административные шаблоны\Компоненты Windows\Центр обновления Windows\Разрешить прием содержимого с подписью из службы обновления Майкрософт в интрасети**.

Если этот параметр политики включен, автоматический Обновления принимает обновления, полученные через расположение службы обновлений Майкрософт в интрасети, как указано в разделе Указание расположения службы обновления Майкрософт в интрасети, если они подписаны сертификатом, найденным в хранилище сертификатов "Доверенные издатели" на локальном компьютере. Если этот параметр политики отключен или не настроен, обновления из расположения службы обновлений Майкрософт в интрасети должны быть подписаны корпорацией Майкрософт.

> ⓘ **Примечание**
>
> Обновления от службы, отличной от службы обновлений Майкрософт в интрасети, всегда должны быть подписаны корпорацией Майкрософт и на них не влияет этот параметр политики.

Чтобы настроить эту политику с помощью MDM, используйте AllowNonMicrosoftSignedUpdate.

Установка обновлений

Чтобы повысить гибкость процесса обновления, есть параметры управления установкой обновлений.

Настройка автоматического Обновления предлагает четыре различных варианта автоматической установки обновлений, а не включать драйверы в Windows Обновления гарантирует, что драйверы не установлены вместе с остальными полученными обновлениями.

Исключать драйверы из обновлений Windows

Позволяет администраторам исключать драйверы Центра обновления Windows во время обновлений.

Чтобы настроить этот параметр в групповой политике, используйте пункт **Конфигурация компьютера\Административные шаблоны\Компоненты Windows\Центр обновления Windows\Исключать драйверы из обновлений Windows**. Включите эту политику, чтобы не включать драйверы в исправления Windows. Если эта политика отключена или не настроена, клиентский компонент Центра обновления Windows включает обновления с классификацией драйверов.

Настройка автоматического обновления

Позволяет ИТ-администратору управлять поведением автоматического обновления, чтобы искать, скачивать и устанавливать обновления.

Настройка компонента «Автоматическое обновление» с помощью групповой политики

В разделе **Конфигурация компьютера\Административные шаблоны\Компоненты Windows\Windows Update\Configure Automatic Обновления** необходимо выбрать один из следующих параметров:

2. Уведомление о скачивании и автоматической установке . Когда Windows находит обновления, которые применяются к этому устройству, пользователи получают уведомление о том, что обновления готовы к скачиванию. Перейдя в **раздел Обновление параметров > & клиентский компонент Центра обновления Windows безопасности>**, пользователи смогут скачать и установить любые доступные обновления.

3. Автоматическое скачивание и уведомление для установки . Windows находит обновления, которые применяются к устройству, и загружает их в фоновом режиме (пользователь не уведомляется или прерывается во время этого процесса). По завершении загрузки пользователи будут уведомлены о том, что они готовы к установке. **Перейдя > в раздел Параметры Обновление & клиентский компонент Центра обновления Windows безопасности>**, пользователи смогут установить их.

4 — Автоматически загружать и планировать установку—-укажите расписание с помощью параметров групповой политики. Подробные сведения об этом параметре см. в разделе Планирование установки обновлений.

5. Разрешить локальному администратору выбирать параметры . С помощью этого параметра локальные администраторы могут использовать приложение параметров для выбора выбранного параметра конфигурации. Локальные администраторы не смогут отключить конфигурацию для автоматического Обновления. Этот параметр недоступен ни в одной Windows 10 или более поздних версиях.

7 . Уведомлять об установке и уведомлять о перезапуске (только Windows Server 2016 и более поздних версий). При использовании этого параметра, когда Windows находит обновления, относящиеся к этому устройству, они загружаются, пользователи получают уведомление о том, что обновления готовы к установке. После установки обновлений пользователям отображается уведомление о перезапуске устройства.

Если этот параметр имеет значение **Отключено**, все обновления, доступные в Центре обновления Windows, необходимо скачивать и устанавливать вручную. Для этого пользователи должны перейти в **раздел Параметры > Обновление & клиентский компонент Центра обновления Windows безопасности>**.

Если для этого параметра задано значение **Не настроено**, администратор по-прежнему может настроить автоматическую Обновления с помощью приложения

параметров в разделе **Обновление параметров > & безопасность > клиентский компонент Центра обновления Windows > Дополнительные параметры**.

Настройка автоматического обновления с помощью параметров системного реестра

> ⓘ **Примечание**
>
> Неправильное изменение параметров системного реестра с помощью редактора реестра или любым иным путем может привести к возникновению серьезных неполадок. Эти проблемы могут привести к необходимости переустановки операционной системы. Корпорация Майкрософт не гарантирует, что эти проблемы можно будет устранить. Внося изменения в реестр, вы действуете на свой страх и риск.

В среде, в которой не развернута Служба Active Directory, можно изменить параметры реестра, чтобы настроить групповые политики для автоматического обновления.

Для этого выполните следующие действия:

1. Нажмите кнопку **Пуск**, выполните поиск по запросу "regedit", а затем откройте редактор реестра.
2. Откройте следующий раздел реестра:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU
   ```

3. Для настройки автоматического обновления добавьте одно из следующих значений реестра.
   - NoAutoUpdate (REG_DWORD):
     - **0**: автоматическое обновление включено (по умолчанию).
     - **1**: автоматическое обновление отключено.
   - AUOptions (REG_DWORD):
     - **1**: флажок "Выполнять обновление системы" для компонента "Автоматическое обновление" снят.

- **2**: уведомлять о загрузке и установке.
- **3**: загружать автоматически и уведомлять об установке.
- **4**: загружать автоматически и устанавливать по заданному расписанию.
- **5**. Разрешить локальному администратору выбрать режим конфигурации. Этот параметр недоступен для Windows 10 или более поздних версий.
- **7**. Уведомлять об установке и уведомлять о перезапуске. (только Windows Server 2016 и более поздних версий)

- ScheduledInstallEveryWeek (REG_DWORD):
  - **0**. Не применяйте установку по расписанию раз в неделю.
  - **1**. Принудительная автоматическая установка раз в неделю в указанный день и время. (***Требуется задать ScheduledInstallDay*** и ***ScheduledInstallTime*** .)
- ScheduledInstallDay (REG_DWORD):
  - **0**: ежедневно.
  - С **1** по **7**: дни недели от воскресенья (1) до субботы (7).
- ScheduledInstallTime (REG_DWORD):

  n, где **n** — время суток в 24-часовом формате (0-23).
- UseWUServer (REG_DWORD)

  Установите значение **1**, чтобы указать службе "Автоматического обновления" использовать сервер, на котором запущены службы SUS, вместо Центра обновления Windows.
- RescheduleWaitTime (REG_DWORD)

  m, где **m** — время ожидания от запуска компонента "Автоматическое обновление" до начала установки обновлений в случае, если запланированная установка была пропущена. Это время задается в минутах в пределах от 1 до 60.

  > ⓘ **Примечание**

> Этот параметр вступает в силу лишь в том случае, если установлен клиент SUS с пакетом обновления версии 1 (SP1) или выше.

- NoAutoRebootWithLoggedOnUsers (REG_DWORD):

  0 (ложь) или **1** (истина). Если задано значение **1**, автоматический Обновления не перезагружает компьютер автоматически, пока пользователи вошли в систему.

  > ⓘ **Примечание**
  >
  > Этот параметр вступает в силу, если установлен клиент SUS с пакетом обновления версии 1 (SP1) или выше.

Сведения об использовании автоматического Обновления с сервером, на котором выполняются службы Windows Software Update Services (WSUS), см. в руководстве по развертыванию microsoft Windows Server Update Services.

При настройке параметров автоматического обновления с помощью реестра, параметры политики имеют более высокий приоритет по сравнению с параметрами, заданными локальным пользователем с правами администратора. Если администратор удалит разделы реестра позже, то снова вступят в силу параметры, заданные локальным пользователем с правами администратора.

Чтобы назначить сервер WSUS, к которому остальные серверы и клиентские компьютеры должны обращаться за обновлениями, добавьте в реестр следующие значения:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\
```

- WUServer (REG_SZ)

  Это значение задает сервер WSUS по HTTP-имени (например, http://IntranetSUS).

- WUStatusServer (REG_SZ)

  Это значение задает сервер статистики SUS по http-имени (например, http://IntranetSUS).

Отображение названия организации в уведомлениях клиентский компонент Центра обновления Windows

Если клиенты Windows 11 связаны с клиентом Microsoft Entra, в уведомлениях клиентский компонент Центра обновления Windows отображается название организации. Например, если для клиентский компонент Центра обновления Windows для бизнеса настроен крайний срок соответствия требованиям, в уведомлении пользователя отображается сообщение, аналогичное **contoso, требующее установки важных обновлений**. Название организации также будет отображаться на странице **клиентский компонент Центра обновления Windows** в **разделе Параметры** для Windows 11.

Название организации автоматически отображается для Windows 11 клиентов, связанных с Microsoft Entra ID, любым из следующих способов:

- Microsoft Entra присоединено
- Microsoft Entra зарегистрировано
- Microsoft Entra гибридное присоединение

Чтобы отключить отображение названия организации в уведомлениях клиентский компонент Центра обновления Windows, добавьте или измените следующие значения в реестре:

- **Раздел реестра**: `HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsUpdate\Orchestrator\Configurations`
- **Имя значения DWORD**: UsoDisableAADJAttribution
- **Значения данных:** 1

В качестве примера предоставляется следующий сценарий PowerShell:

PowerShell

```
$registryPath =
"HKLM:\Software\Microsoft\WindowsUpdate\Orchestrator\Configurations"
$Name = "UsoDisableAADJAttribution"
$value = "1"

if (!(Test-Path $registryPath))
{
  New-Item -Path $registryPath -Force | Out-Null
}
```

```
New-ItemProperty -Path $registryPath -Name $name -Value $value -PropertyType
DWORD -Force | Out-Null
```

Разрешить установку обновлений Windows до первоначального входа пользователя

(Начиная с Windows 11 версии 22H2 с предварительной версией накопительного обновления 2023-04 или более поздним накопительным обновлением)

На новых устройствах клиентский компонент Центра обновления Windows не начинает установку фоновых обновлений до тех пор, пока пользователь не завершит процесс запуска (OOBE) и не войдет в систему в первый раз. Во многих случаях пользователь входит в систему сразу после завершения запуска OOBE. Однако некоторые решения на основе виртуальных машин подготавливают устройство и автоматизируют первый пользовательский интерфейс. Эти виртуальные машины могут быть назначены пользователю не сразу, поэтому он не увидит первоначальный вход до нескольких дней спустя.

В сценариях, когда начальный вход задерживается, установка следующих значений реестра позволяет устройствам начать фоновые операции обновления до первого входа пользователя:

- **Раздел реестра**: `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Orchestrator`
- **Имя значения DWORD**: ScanBeforeInitialLogonAllowed
- **Значения данных**: 1

> ⚠ **Предупреждение**
>
> Это значение предназначено для использования только в сценариях с отложенным первоначальным вхохом пользователем. Установка этого значения на устройствах, где первоначальный вход пользователя не задерживается, может негативно сказаться на производительности, так как это может позволить выполнить обновление при первом входе пользователя.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Что такое Центр обновления Windows для бизнеса?

Статья • 16.05.2024 • Применяется к: ✅ Windows 11, ✅ Windows 10

> **Ищете информацию для потребителей?** См. раздел Центр обновления Windows: вопросы и ответы

клиентский компонент Центра обновления Windows для бизнеса — это бесплатная служба, которая доступна для следующих выпусков Windows 10 и Windows 11:

- Pro, включая Pro для рабочих станций
- Education
- Корпоративный, включая Enterprise LTSC, IoT Enterprise и IoT Enterprise LTSC

клиентский компонент Центра обновления Windows для бизнеса позволяет ИТ-администраторам постоянно обновлять клиентские устройства Windows своей организации с помощью последних обновлений системы безопасности и функций Windows, напрямую подключая эти системы к службе клиентский компонент Центра обновления Windows. Для настройки клиентский компонент Центра обновления Windows для бизнеса параметров клиентский компонент Центра обновления Windows для бизнеса можно использовать решения групповая политика или решения для мобильных Управление устройствами (MDM), например Microsoft Intune.

В частности, клиентский компонент Центра обновления Windows для бизнеса позволяет управлять предложениями обновлений и возможностями, чтобы обеспечить надежность и тестирование производительности на подмножестве устройств перед развертыванием обновлений в организации. Она также обеспечивает положительный процесс обновления для сотрудников вашей организации.

Что можно сделать с помощью клиентский компонент Центра обновления Windows для бизнеса?

клиентский компонент Центра обновления Windows для бизнеса позволяет коммерческим клиентам управлять получением Обновления Windows, а также опытом, который устройство получает при их получении.

Вы можете управлять политиками клиентский компонент Центра обновления Windows для бизнеса с помощью средств MDM или управления групповая политика, таких как локальная групповая политика или консоль управления групповая политика (GPMC), а также другие средства управления, отличные от Корпорации Майкрософт. MDM используют политики поставщика служб конфигурации (CSP) вместо групповая политика. Intune также использует облачные политики. Не все политики доступны во всех форматах (CSP, групповая политика или облачная политика).

Управление развертыванием windows Обновления

С помощью клиентский компонент Центра обновления Windows для бизнеса вы можете:

- Управление типами Обновления Windows, предлагаемых устройствам в вашей организации
- Управление применением обновлений к устройствам
- Развертывание обновлений на устройствах в организации волнами

Управление предлагаемыми обновлениями

клиентский компонент Центра обновления Windows для бизнеса позволяет ИТ-администратору получать различные типы Обновления Windows и управлять ими.

Типы обновлений, управляемые клиентский компонент Центра обновления Windows для бизнеса

клиентский компонент Центра обновления Windows для бизнеса предоставляет политики управления для нескольких типов обновлений для Windows 10 устройств:

- **Обновления компонентов:** Обновления компонентов, которые ранее назывались обновлениями, содержат не только исправления безопасности и качества, но и значительные дополнения и изменения функций. Обновления компонентов выпускаются сразу же, как только они становятся доступными. Обновления компонентов недоступны для устройств LTSC.
- **Обновления качества:** Обновления качества — это традиционные обновления операционной системы. Как правило, исправления выпускаются во второй вторник каждого месяца, хотя они могут быть выпущены в любое

время. К ним относятся обновления для системы безопасности, драйверов и критические обновления.
- **Обновления драйверов:** Обновления для драйверов сторонних производителей, относящихся к вашим устройствам. Обновления драйверов включены по умолчанию, но при желании их можно отключить с помощью политик клиентский компонент Центра обновления Windows для бизнеса.
- **Обновления продуктов Майкрософт**: Обновления для других продуктов Майкрософт, например версий Office, установленных с помощью установщика Windows (MSI). Версии Office, установленные с помощью функции "нажми и запускай", не могут быть обновлены с помощью клиентский компонент Центра обновления Windows для бизнеса. Обновления продукта по умолчанию отключены. Их можно включить с помощью политик клиентский компонент Центра обновления Windows для бизнеса.

Жертвоприношение

Вы можете управлять применением обновлений. Например, можно отложить установку обновления на устройстве или путем приостановки обновлений на определенный период.

Управление предложением обновлений

Установку обновлений можно отложить или приостановить на заданный период времени.

Регистрация в предварительных обновлениях

Уровень готовности ветви позволяет администраторам указать канал обновлений компонентов, которые они хотят получать. На сегодняшний день существуют параметры уровня готовности ветви как для предварительной версии, так и для выпущенных обновлений:

- Канал Программы предварительной оценки Windows
- Канал разработки для программы предварительной оценки Windows
- Канал предварительной оценки Windows (бета-версия)
- Канал предварительной версии предварительной оценки Windows

Отложить обновление

Администратор может отложить установку обновлений компонентов и обновлений качества от развертывания на устройствах в течение определенного периода времени в зависимости от того, когда эти обновления впервые становятся доступными в службе клиентский компонент Центра обновления Windows. Эту отсрочку можно использовать, чтобы предоставить время для проверки развертываний при их отправке на устройства. Отсрочки работают, позволяя указать количество дней после выпуска обновления, прежде чем оно будет предложено устройству. То есть, если задать период отсрочки обновления компонентов в 365 дней, устройство не установит обновление компонентов, выпущенное менее 365 дней. Чтобы отложить обновления компонентов, используйте политику **Выбрать, когда предварительные сборки и обновления компонентов получены** .

Развернуть таблицу

Категория	Максимальный период отсрочки
Обновления компонентов	365 дней
Исправления	30 дней
Неизменяемый	нет

Приостановка обновления

При обнаружении проблемы при развертывании компонента или обновления качества можно приостановить обновление на 35 дней с указанной даты начала, чтобы другие устройства не устанавливали его до устранения проблемы. Если вы приостановите обновление компонентов, обновления качества по-прежнему предлагаются устройствам, чтобы обеспечить их безопасность. Период приостановки обновления компонентов и обновлений качества рассчитывается с заданной даты начала.

Чтобы приостановить обновления компонентов, используйте политику **Выбор, когда предварительные версии сборок и обновлений компонентов получены**, а для приостановки обновлений качества используйте политику **Select when Quality Обновления are Received**. Дополнительные сведения см. в разделах Приостановка обновлений компонентов и Приостановка обновлений качества.

Встроенные преимущества. При обновлении с клиентский компонент Центра обновления Windows вы получаете дополнительные преимущества встроенных проверок совместимости, чтобы предотвратить плохое обновление устройства и проверка для предотвращения повторных откатов.

Рекомендации

Для оптимальной работы с клиентский компонент Центра обновления Windows следуйте приведенным ниже рекомендациям.

- Используйте устройства не менее 6 часов в месяц, в том числе не менее 2 часов непрерывного использования.
- Регулярно оплачивайте устройства. Подключение устройств в одночасье позволяет им автоматически обновляться в нерабочее время.
- Убедитесь, что на устройствах есть не менее 10 ГБ свободного места.
- Предоставьте устройствам беспрепятственный доступ к службе клиентский компонент Центра обновления Windows.

Управление взаимодействием с конечными пользователями при получении windows Обновления

клиентский компонент Центра обновления Windows для бизнеса предоставляет средства управления, которые помогают соответствовать стандартам безопасности вашей организации и обеспечивают отличный интерфейс для конечных пользователей. Мы делаем это, позволяя устанавливать автоматические обновления в периоды, которые хорошо работают для сотрудников вашей организации, и устанавливать крайние сроки для обновлений качества и компонентов. Поскольку клиентский компонент Центра обновления Windows включает встроенную аналитику, лучше использовать меньше элементов управления для управления взаимодействием с пользователем.

Рекомендуемые параметры взаимодействия

Такие функции, как часы активности, обеспечивают лучшие возможности для конечных пользователей, обеспечивая при этом устройства более безопасными и актуальными. Чтобы воспользоваться преимуществами этих функций, выполните следующие действия.

1. Автоматическое скачивание, установка и перезапуск (по умолчанию, если политики перезапуска не настроены или не включены).
2. Используйте уведомления по умолчанию.
3. Установите крайние сроки обновления.

Установка крайних сроков

Политика крайних сроков соответствия позволяет задавать отдельные крайние сроки и льготные периоды для обновлений компонентов и качества.

Эта политика позволяет указать количество дней с даты публикации обновления, в течение которых оно должно быть установлено на устройстве. Политика также включает настраиваемый льготный период, указывающий количество дней с момента установки обновления на устройстве до принудительного перезапуска устройства. Этот подход полезен в сценарии отпуска, так как он позволяет, например, пользователям, которые были в отпуске, иметь немного времени, прежде чем они будут вынуждены перезапустить свои устройства по возвращении из отпуска.

Обновление базового плана

> **Примечание**
>
> Набор средств Update Baseline доступен только для групповая политика. Базовый план обновления не влияет на политики предложения, независимо от того, используете ли вы отсрочки или целевую версию для управления тем, какие обновления предлагаются устройствам, когда. Обновление базовых показателей в настоящее время не поддерживается для Windows 11.

Большое количество различных политик, предлагаемых, может оказаться подавляющим. Базовый план обновления содержит четкий список рекомендуемых параметров политики обновления Windows для ИТ-администраторов, которым требуется оптимальное взаимодействие с пользователем, а также достижение своих целей по обеспечению соответствия обновлений. Базовый план обновления для Windows 10 содержит рекомендации по параметрам политики, охватывающие настройку крайних сроков, поведение перезапуска, политики питания и многое другое.

Набор средств "Базовый план обновления" упрощает процесс, предоставляя ИТ-администраторам одну команду для применения базовых показателей обновления к устройствам. Вы можете получить набор средств "Базовый план обновления" в Центре загрузки.

Другие службы клиентский компонент Центра обновления Windows для бизнеса

В семейство продуктов клиентский компонент Центра обновления Windows для бизнеса входят следующие службы:

- Отчеты клиентский компонент Центра обновления Windows для бизнеса — это облачное решение, которое предоставляет сведения о соответствии Microsoft Entra присоединенных устройств обновлениям Windows. Отчеты клиентский компонент Центра обновления Windows для бизнеса предлагаются через портал Azure. Отчеты клиентский компонент Центра обновления Windows для бизнеса помогают:
  - Мониторинг безопасности, качества, драйверов и обновлений компонентов для устройств Windows 11 и Windows 10
  - Отчет об устройствах с проблемами соответствия обновлений
  - Анализ и отображение данных несколькими способами
- Автоматическое исправление Windows — это облачная служба, предназначенная для работы с существующими политиками клиентский компонент Центра обновления Windows для бизнеса. Автопатка Windows обеспечивает дополнительный контроль над утверждением, планированием и защитой обновлений, доставляемых с клиентский компонент Центра обновления Windows на управляемые устройства.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Настройка политик клиента клиентский компонент Центра обновления Windows

Применяется к: ✅ Windows 11, ✅ Windows 10, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

> **Ищете информацию для потребителей?** См. раздел клиентский компонент Центра обновления Windows: вопросы и ответы.

Вы можете использовать групповая политика или службу управления мобильными устройствами (MDM) для настройки клиентский компонент Центра обновления Windows клиентских политик для своих устройств. В разделах этой статьи приведены политики групповая политика и MDM для Windows 10 версии 1511 и более поздних версий, включая Windows 11. Политики MDM используют параметр OMA-URI из раздела Поставщик служб конфигурации политик.

> **Примечание.**
>
> Windows Server *не* получает обновления компонентов от клиентский компонент Центра обновления Windows, поэтому применяются только политики обновления качества. Это поведение не применяется к **гиперконвергентной инфраструктуре Azure Stack (HCI).**

Вы можете использовать политики клиента клиентский компонент Центра обновления Windows независимо от выбранного уровня диагностических данных. Если для уровня диагностических данных задано значение **0 (безопасность),** клиентский компонент Центра обновления Windows клиентские политики по-прежнему соблюдаются. Дополнительные сведения см. в разделе Настройка уровня диагностических данных операционной системы.

> **Совет**
>
> Эта функция ранее называлась *клиентский компонент Центра обновления Windows для бизнеса*.

Первый этап — группировка устройств

Группируя устройства с одинаковыми периодами отсрочки, администраторы могут объединять устройства в группы развертывания или проверки, которые могут быть мерой контроля качества при развертывании обновлений. Благодаря наличию периода отсрочки и возможности приостановки обновлений администраторы могут эффективно контролировать и измерять развертывания обновлений: сначала обновление можно развернуть в небольшом пуле устройств, чтобы проверить качество, а затем продолжить на других устройствах организации.

> **Совет**
>
> Помимо настройки нескольких кругов для развертывания обновлений следует также включить в стратегию развертывания устройства, зарегистрированные в программе предварительной оценки Windows. Это позволит вам не только оценить новые функции, прежде чем они станут широко доступны для широкой общественности, но и увеличить время для предоставления отзывов и влияния на разработку корпорации Майкрософт в отношении функциональных аспектов продукта. Дополнительные сведения о программе предварительной оценки Windows см. в разделе **https://insider.windows.com/**.

Настройка устройств для соответствующего канала службы

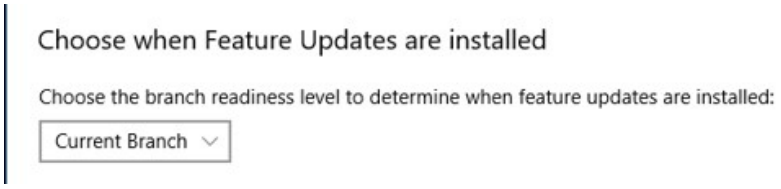
С помощью клиентский компонент Центра обновления Windows клиентских политик можно настроить устройство на Windows Insider Preview или в ветви обслуживания канала доступности общего доступа. Дополнительные сведения об этой модели обслуживания см. в разделе Каналы обслуживания.

Политики ветвей выпусков

Развернуть таблицу

Политика	Устанавливает раздел реестра в HKLM\Software
Объект групповой политики для Windows 10 версии 1607 или более поздней: конфигурация компьютера > Административные шаблоны > Компоненты > Windows клиентский компонент Центра обновления Windows > клиентский компонент Центра обновления Windows для бизнеса >**Выберите время обновления компонентов получено** Эта политика является устаревшей и неприменима для Windows 11. Устаревшие политики могут быть удалены в будущем выпуске.	\Policies\Microsoft\Windows\WindowsUpdate\BranchReadinessLevel
Объект групповой политики для Windows 10 версии 1511. Конфигурация компьютера > Административные шаблоны > Компоненты > Windows клиентский компонент Центра обновления Windows >**Отложить обновления и Обновления** Эта политика является устаревшей и неприменима для Windows 11. Устаревшие политики могут быть удалены в будущем выпуске.	\Policies\Microsoft\Windows\WindowsUpdate\DeferUpgrade
MDM для Windows 10 версии 1607 или более поздней: .. /Vendor/MSFT/Policy/Config/Update/**BranchReadinessLevel** Эта политика является устаревшей и неприменима для Windows 11. Устаревшие политики могут быть удалены в будущем выпуске.	\Microsoft\PolicyManager\default\Update\BranchReadinessLevel
MDM для Windows 10 версии 1511: .. /Vendor/MSFT/Policy/Config/Update/**RequireDeferUpgrade** Эта политика является устаревшей и не применима к Windows 11. Устаревшие политики могут быть удалены в будущем выпуске.	\Microsoft\PolicyManager\default\Update\RequireDeferUpgrade

Начиная с Windows 10 версии 1703, пользователи могут настроить уровень готовности ветви для своего устройства с помощью **параметров > Обновление & безопасности > клиентский компонент Центра обновления Windows > Дополнительные параметры**.



> ⓘ **Примечание.**
>
> Пользователи не могут изменять этот параметр, если он был настроен с помощью политики.

Настройка получения устройств обновлений компонентов

После настройки ветви обслуживания (Windows Insider Preview или канала общедоступной доступности) можно определить, следует ли и на какой срок отложить получение обновлений компонентов после их доступности от Корпорации Майкрософт на клиентский компонент Центра обновления Windows. Вы можете отложить получение этих обновлений компонентов на период до 365 дней с момента их выпуска, задав `DeferFeatureUpdatesPeriodinDays` значение .

Например, устройство на канале `DeferFeatureUpdatesPeriodinDays=30` общедоступной доступности с не установит обновление компонентов, которое впервые станет общедоступным в клиентский компонент Центра обновления Windows сентября, до 30 дней позже, в октябре.

Параметры политики для отсрочки обновлений компонентов

Развернуть таблицу

Политика	Устанавливает раздел реестра в HKLM\Software
Объект групповой политики для Windows 10 версии 1607 или более поздней: конфигурация компьютера > Административные шаблоны > Компоненты > Windows клиентский компонент Центра обновления Windows > клиентский компонент Центра обновления Windows для бизнеса >**Выберите время обновления компонентов получено** Эта политика является устаревшей и неприменима для Windows 11. Устаревшие политики могут быть удалены в будущем выпуске.	\Policies\Microsoft\Windows\WindowsUpdate\DeferFeatureUpdates \Policies\Microsoft\Windows\WindowsUpdate\DeferFeatureUpdatesPeriodInDays
Объект групповой политики для Windows 10 версии 1511. Конфигурация компьютера > Административные шаблоны > Компоненты > Windows клиентский компонент Центра обновления Windows >**Отложить обновления и Обновления** Эта политика является устаревшей и неприменима для Windows 11. Устаревшие политики могут быть удалены в будущем выпуске.	\Policies\Microsoft\Windows\WindowsUpdate\DeferUpgradePeriod
MDM для Windows 10 версии 1607 и более поздних:	\Microsoft\PolicyManager\default\Update\DeferFeatureUpdatesPeriodInDays

Политика	Устанавливает раздел реестра в HKLM\Software
.. /Vendor/MSFT/Policy/Config/Update/**DeferFeatureUpdatesPeriodInDays**	
MDM для Windows 10 версии 1511: .. /Vendor/MSFT/Policy/Config/Update/**DeferUpgrade** Эта политика является устаревшей и неприменимой для Windows 11. Устаревшие политики могут быть удалены в будущем выпуске.	\Microsoft\PolicyManager\default\Update\RequireDeferUpgrade

> ⓘ **Примечание.**
>
> Если политика не настроена, отдельные пользователи могут отложить обновления компонентов с помощью **параметров > Обновление & безопасности > клиентский компонент Центра обновления Windows > Дополнительные параметры**.

Приостановка обновлений компонентов

Вы также можете приостановить получение обновлений компонентов устройством на период до 35 дней с момента установки значения. По истечении 35 дней срок действия параметра приостановки истечет автоматически, и устройство будет проверять клиентский компонент Центра обновления Windows на наличие применимых обновлений компонентов. После этой проверки вы можете снова приостановить обновления компонентов для устройства.

Начиная с Windows 10 версии 1703 при настройке приостановки с помощью политики необходимо задать дату начала приостановки. Период приостановки вычисляется путем добавления 35 дней к этой дате начала.

В случаях, когда политика приостановки сначала применяется после истечения настроенной даты начала, можно продлить период приостановки до 35 дней, настроив более позднюю дату начала.

> ⓘ **Внимание**
>
> В Windows 10 версии 1703 и более поздних можно приостановить обновления компонентов до 35 дней, аналогичное количеству дней для обновлений качества.

Параметры политики для приостановки обновлений компонентов

Развернуть таблицу

Политика	Устанавливает раздел реестра в HKLM\Software
Объект групповой политики для Windows 10 версии 1607 или более поздней: конфигурация компьютера > Административные шаблоны > Компоненты > Windows клиентский компонент Центра обновления Windows > клиентский компонент Центра обновления Windows для бизнеса >**Выберите время обновления компонентов получены**	**1607:** \Policies\Microsoft\Windows\WindowsUpdate\PauseFeatureUpdates **1703 и более поздних версий:** \Policies\Microsoft\Windows\WindowsUpdate\PauseFeatureUpdatesStartTime

Политика	Устанавливает раздел реестра в HKLM\Software
Объект групповой политики для Windows 10 версии 1511. Конфигурация компьютера > Административные шаблоны > Компоненты > Windows клиентский компонент Центра обновления Windows >**Отложить обновления и Обновления** Эта политика является устаревшей и неприменима для Windows 11. Устаревшие политики могут быть удалены в будущем выпуске.	\Policies\Microsoft\Windows\WindowsUpdate\Pause
MDM для Windows 10 версии 1607 или более поздней: .. /Vendor/MSFT/Policy/Config/Update/**PauseFeatureUpdates**	**1607:** \Microsoft\PolicyManager\default\Update\PauseFeatureUpdates **1703 и более поздних версий:** \Microsoft\PolicyManager\default\Update\PauseFeatureUpdatesStartTime
MDM для Windows 10 версии 1511: .. /Vendor/MSFT/Policy/Config/Update/**DeferUpgrade** Эта политика является устаревшей и неприменимой для Windows 11. Устаревшие политики могут быть удалены в будущем выпуске.	\Microsoft\PolicyManager\default\Update\Pause

Вы можете проверка дату приостановки обновлений компонентов, проверив раздел реестра **PausedFeatureDatев разделе HKLM\SOFTWARE\Microsoft\WindowsUpdate\UpdatePolicy\Settings**.

Редактор локальной групповой политики (GPEdit.msc) не будет отражать, истек ли период приостановки обновления компонентов. Хотя устройство автоматически возобновит обновления компонентов через 35 дней, поле приостановки проверка останется выбранным в редакторе политик. Чтобы проверка, возобновляет ли устройство автоматически получать обновления компонентов, проверка раздел реестра состояния **PausedFeatureStatus** в разделе **HKLM\SOFTWARE\Microsoft\WindowsUpdate\UpdatePolicy\Settings** для следующих значений:

Развернуть таблицу

Значение	Состояние
0	обновления компонентов не приостановлены
1	обновления компонентов приостановлены
2	обновления компонентов автоматически возобновляются после приостановки

> ⓘ **Примечание.**
>
> Если политика не настроена, отдельные пользователи могут приостановить обновления компонентов с помощью **параметров > Обновление & безопасности > клиентский компонент Центра обновления Windows > дополнительные параметры**.

Начиная с Windows 10 версии 1703, использование параметров для управления поведением паузы обеспечивает более согласованное взаимодействие, в частности:

- Все активные уведомления о перезапуске очищаются или закрываются.

- Все ожидающие перезапуски отменяется.
- Все ожидающие установки обновлений отменяется.
- Любая установка обновления, выполняемая при активации приостановки, будет пытаться выполнить откат.

Настройка получения устройств обновлений качества

Обновления качества обычно публикуются во второй вторник каждого месяца, хотя они могут быть выпущены в любое время. Вы можете определить, следует ли и на какой срок отложить получение обновлений качества после их доступности. Вы можете отложить получение этих обновлений качества на период до 30 дней с момента их выпуска, задав значение **DeferQualityUpdatesPeriodinDays** .

Вы можете настроить систему на получение обновлений для других продуктов Майкрософт, известных как обновления Майкрософт (например, Microsoft Office, Visual Studio), наряду с обновлениями Windows, задав политику **AllowMUUpdateService** . При этом эти обновления Майкрософт будут следовать тем же правилам отсрочки и приостановки, что и все другие обновления качества. Список других продуктов Майкрософт, которые могут быть обновлены, см. в разделе Обновление других продуктов Майкрософт.

Параметры политики для отсрочки обновлений качества

Развернуть таблицу

Политика	Устанавливает раздел реестра в HKLM\Software
Объект групповой политики для Windows 10 версии 1607 или более поздней: конфигурация компьютера > Административные шаблоны > Компоненты > Windows клиентский компонент Центра обновления Windows > клиентский компонент Центра обновления Windows для бизнеса >**Выберите, когда качество Обновления получены**	\Policies\Microsoft\Windows\WindowsUpdate\DeferQualityUpdates \Policies\Microsoft\Windows\WindowsUpdate\DeferQualityUpdatesPeriodInDays
Объект групповой политики для Windows 10 версии 1511. Конфигурация компьютера > Административные шаблоны > Компоненты > Windows клиентский компонент Центра обновления Windows >**Отложить обновления и Обновления** Эта политика является устаревшей и неприменима для Windows 11. Устаревшие политики могут быть удалены в будущем выпуске.	\Policies\Microsoft\Windows\WindowsUpdate\DeferUpdatePeriod
MDM для Windows 10 версии 1607 или более поздней: .. /Vendor/MSFT/Policy/Config/Update/**DeferQualityUpdatesPeriodInDays**	\Microsoft\PolicyManager\default\Update\DeferQualityUpdatesPeriodInDays
MDM для Windows 10 версии 1511: .. /Vendor/MSFT/Policy/Config/Update/**DeferUpgrade** Эта политика является устаревшей и неприменимой для Windows 11. Устаревшие	\Microsoft\PolicyManager\default\Update\RequireDeferUpdate

Политика	Устанавливает раздел реестра в HKLM\Software
политики могут быть удалены в будущем выпуске.	

> ⓘ **Примечание.**
>
> Если политика не настроена, отдельные пользователи могут отложить обновления качества с помощью **параметров > Обновление & безопасности > клиентский компонент Центра обновления Windows > дополнительные параметры**.

Приостановка исправлений

Вы также можете приостановить получение системой обновлений качества на период до 35 дней с момента установки значения. По истечении 35 дней срок действия параметра приостановки автоматически истечет, и устройство будет проверять клиентский компонент Центра обновления Windows на наличие применимых обновлений качества. После этой проверки вы можете снова приостановить обновления качества для устройства.

Начиная с Windows 10 версии 1703 при настройке приостановки с помощью политики необходимо задать дату начала приостановки. Период приостановки вычисляется путем добавления 35 дней к этой дате начала.

В случаях, когда политика приостановки сначала применяется после истечения настроенной даты начала, можно продлить период приостановки до 35 дней, настроив более позднюю дату начала.

> ⓘ **Примечание.**
>
> Начиная с Windows 10, версия 1809, ИТ-администраторы могут запретить отдельным пользователям приостановку обновлений.

Параметры политики для приостановки обновлений качества

Развернуть таблицу

Политика	Устанавливает раздел реестра в HKLM\Software
Объект групповой политики для Windows 10 версии 1607 или более поздней: конфигурация компьютера > Административные шаблоны > Компоненты > Windows клиентский компонент Центра обновления Windows > клиентский компонент Центра обновления Windows для бизнеса >**Выберите, когда качество Обновления получены**	**1607:** \Policies\Microsoft\Windows\WindowsUpdate\PauseQualityUpdates **1703:** \Policies\Microsoft\Windows\WindowsUpdate\PauseQualityUpdatesStartTime
Объект групповой политики для Windows 10 версии 1511. Конфигурация компьютера > Административные шаблоны > Компоненты > Windows клиентский компонент Центра обновления Windows >**Отложить обновления и Обновления** Эта политика является устаревшей и неприменима для Windows 11. Устаревшие	\Policies\Microsoft\Windows\WindowsUpdate\Pause

Политика	Устанавливает раздел реестра в HKLM\Software
политики могут быть удалены в будущем выпуске.	
MDM для Windows 10 версии 1607 или более поздней: .. /Vendor/MSFT/Policy/Config/Update/**PauseQualityUpdates**	**1607:** \Microsoft\PolicyManager\default\Update\PauseQualityUpdates **1703:** \Microsoft\PolicyManager\default\Update\PauseQualityUpdatesStartTime
MDM для Windows 10 версии 1511: .. /Vendor/MSFT/Policy/Config/Update/**DeferUpgrade** Эта политика является устаревшей и неприменимой для Windows 11. Устаревшие политики могут быть удалены в будущем выпуске.	\Microsoft\PolicyManager\default\Update\Pause

Вы можете проверка дату приостановки обновлений качества, проверив раздел реестра **PausedQualityDateв разделе HKLM\SOFTWARE\Microsoft\WindowsUpdate\UpdatePolicy\Settings**.

Редактор локальной групповой политики (GPEdit.msc) не будет отражать, истек ли период приостановки обновления качества. Хотя устройство автоматически возобновит обновления качества через 35 дней, поле приостановки проверка останется выбранным в редакторе политик. Чтобы проверка, возобновляет ли устройство прием Обновления качества, проверка раздел реестра состояния **PausedQualityStatus** в разделе **HKLM\SOFTWARE\Microsoft\WindowsUpdate\UpdatePolicy\Settings** для следующих значений:

Развернуть таблицу

Значение	Состояние
0	обновления качества не приостановлены
1	исправление обновлений приостановлено
2	обновление качества автоматически возобновляется после приостановки

> ⓘ **Примечание.**
>
> Если политика не настроена, отдельные пользователи могут приостановить обновления качества с помощью **параметра > Обновление & безопасности > клиентский компонент Центра обновления Windows > дополнительные параметры**.

Начиная с Windows 10 версии 1703, использование параметров для управления поведением паузы обеспечивает более согласованное взаимодействие, в частности:

- Все активные уведомления о перезапуске очищаются или закрываются
- Отменяются все отложенные перезагрузки
- Отменяются все отложенные и готовые к установке обновления
- Любая установка обновления, выполняемая при активации приостановки, будет пытаться выполнить откат.

Настройка получения Windows Insider Preview сборок устройствами

Начиная с Windows 10 версии 1709 можно устанавливать политики для управления предварительными сборками и их доставкой:

Параметр **Управление предварительными сборками** позволяет администраторам включать и отключать установку предварительных сборок на устройстве. Можно также остановить предварительные сборки после официального выпуска.

- Групповая политика: **Конфигурация компьютера > Административные шаблоны > Компоненты Windows > Центр обновления Windows > Центр обновления Windows для бизнеса** - *Управление предварительными сборками*
- MDM: **Update/ManagePreviewBuilds**
- Microsoft Configuration Manager: **включение двойного сканирования, управление с помощью политики клиентский компонент Центра обновления Windows для бизнеса**

> **Внимание**
>
> Эта политика заменяет политику "Переключение пользовательских элементов управления сборками для предварительной оценки", которая поддерживается только до Windows 10 версии 1703. Ранняя политика доступна здесь:
>
> - Групповая политика: **Конфигурация компьютера/Административные шаблоны/Компоненты Windows/Сборки для сбора данных и предварительные сборки/Переключение пользовательских элементов управления сборками для предварительной оценки**
> - MDM: **System/AllowBuildPreview**

Параметры политики **Выбора получения обновлений компонентов** позволяют выбирать между предварительными кругами тестирования и откладывать или приостанавливать их доставку.

- групповая политика: **Конфигурация компьютера/Административные шаблоны/Компоненты Windows/ клиентский компонент Центра обновления Windows/ клиентский компонент Центра обновления Windows для бизнеса** - *Выберите, когда используются предварительные сборки и обновления компонентов полученный*
- MDM: **Update/BranchReadinessLevel**

Исключение драйверов из обновлений качества

Начиная с Windows 10 версии 1607, вы можете выборочно отказаться от получения пакетов обновления драйверов в рамках обычного цикла обновления качества. Эта политика не применяется к обновлениям драйверов, предоставляемых операционной системой (которые будут упаковываться в рамках обновления для системы безопасности или критического обновления), а также к обновлениям компонентов, где драйверы могут устанавливаться динамически, чтобы обеспечить завершение процесса обновления компонентов.

Параметры политики для исключения драйверов

Развернуть таблицу

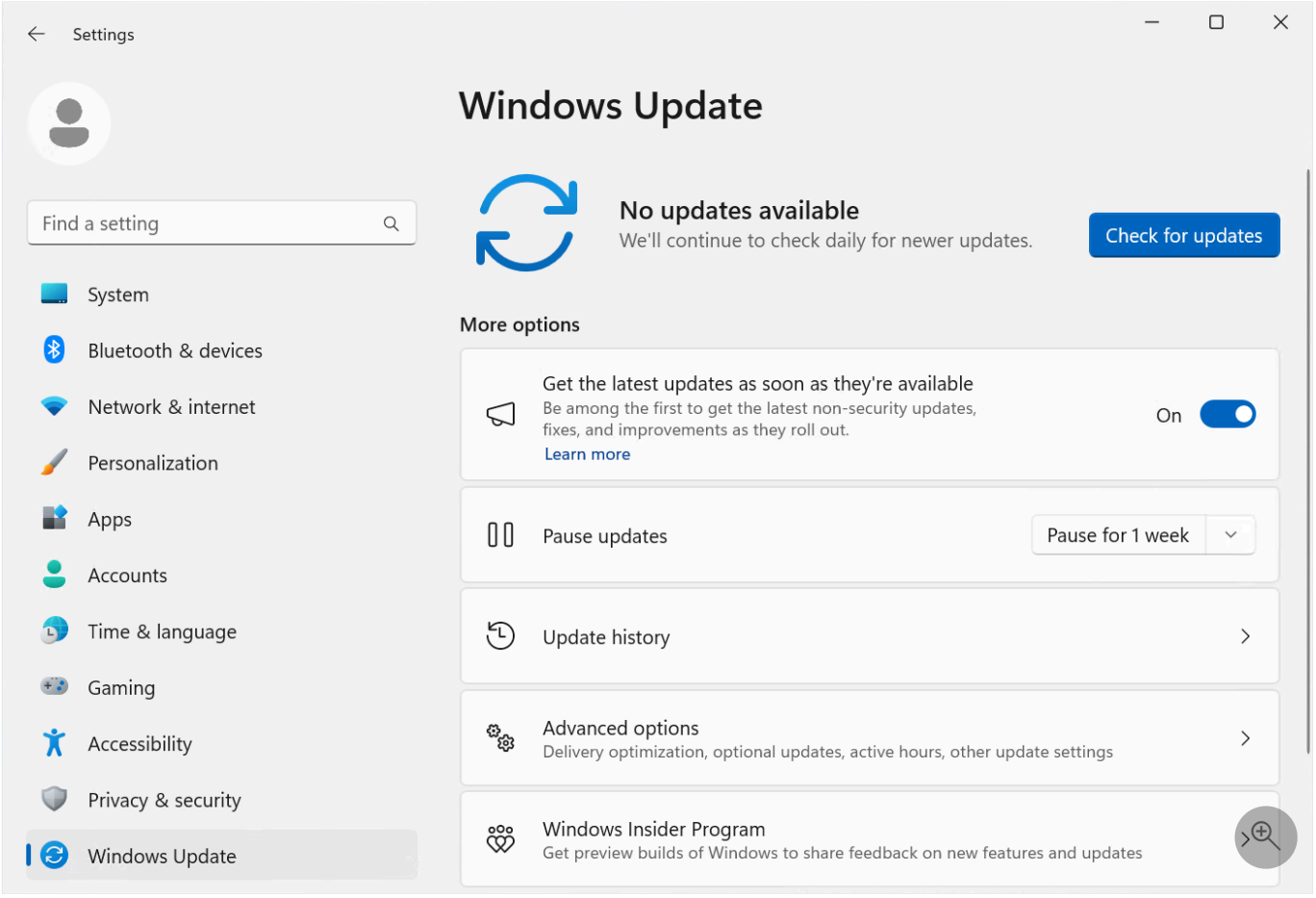
Политика	Устанавливает раздел реестра в HKLM\Software
Объект групповой политики для Windows 10 версии 1607 или более поздней: конфигурация компьютера > Административные шаблоны > Компоненты	\Policies\Microsoft\Windows\WindowsUpdate\ExcludeWUDriversInQualityUpdate

Политика	Устанавливает раздел реестра в HKLM\Software
> Windows клиентский компонент Центра обновления Windows >**Не включать драйверы с Windows Обновления**	
MDM для Windows 10 версии 1607 и более поздних: .. /Vendor/MSFT/Policy/Config/Update/**ExcludeWUDriversInQualityUpdate**	\Microsoft\PolicyManager\default\Update\ExcludeWUDriversInQualityUpdate

Включение необязательных обновлений

Помимо ежемесячного накопительного обновления доступны необязательные обновления для предоставления новых функций и изменений, не относящихся к безопасности. Большинство необязательных обновлений выпускаются в четвертый вторник месяца, известный как необязательные предварительные выпуски, не связанные с безопасностью. Необязательные обновления также могут включать функции, которые постепенно развертываются, известные как управляемые выпуски функций (CFR). Установка необязательных обновлений не включена по умолчанию для устройств, получающих обновления с помощью клиентский компонент Центра обновления Windows клиентских политик. Однако можно включить необязательные обновления для устройств с помощью политики **Включить необязательные обновления** .

Чтобы обеспечить согласованность времени обновления, политика **Включить необязательные обновления** учитывает период отсрочки для обновлений качества. Эта политика позволяет выбрать, должны ли устройства получать cfr в дополнение к дополнительным предварительным выпускам, не обеспечивающим безопасность, или пользователь может принять решение об установке необязательных обновлений. Эта политика может изменить поведение параметра **Получить последние обновления, как только они будут доступны** в **разделе Параметры>Обновление & безопасности**> ***клиентский компонент Центра обновления Windows>Добавить**.



Для политики доступны следующие параметры:

- **Автоматическое получение необязательных обновлений (включая cfr)**:
  - На устройстве автоматически устанавливаются последние необязательные обновления, не связанные с безопасностью, и cfR. Период отсрочки обновления качества применяется к установке этих обновлений.
  - Выбран параметр **Получить последние обновления, как только они будут доступны** , и пользователи не могут изменить параметр.
  - Устройства будут получать cfr на ранних этапах развертывания.

- **Автоматически получать необязательные обновления**:
  - Последние необязательные обновления, не связанные с безопасностью, устанавливаются на устройство автоматически, но cfr — нет. Период отсрочки обновления качества применяется к установке этих обновлений.
  - Параметр **Получить последние обновления, как только они будут доступны** , не выбран и пользователи не могут изменить параметр.

- **Пользователи могут выбрать, какие необязательные обновления следует получать**:
  - Пользователи могут выбрать, какие необязательные обновления следует установить, в **разделе Параметры**>**Обновление & безопасности**>**клиентский компонент Центра обновления Windows**>**Добавить параметры**>**Необязательные обновления**.
    - На устройстве предлагаются необязательные обновления, но для их установки требуется взаимодействие с пользователем, если не включен параметр **Получить последние обновления сразу после их доступности** .
    - CfR предлагаются устройству, но не обязательно на ранних этапах развертывания.
  - Пользователи могут включить параметр **Получать последние обновления, как только они будут доступны** в **разделе Параметры**>**Обновление & безопасности**> ***клиентский компонент Центра обновления Windows**>**Добавить параметры**. Если пользователь включает **получение последних обновлений, как только они будут доступны**, то:
    - Устройство будет получать cfr на ранних этапах развертывания.
    - На устройстве автоматически устанавливаются необязательные обновления.

- **Не настроено** (по умолчанию):
  - Необязательные обновления не устанавливаются на устройстве, и параметр **Получить последние обновления, как только они будут доступны** , отключен.

Политики для включения необязательных обновлений

Развернуть таблицу

Политика	Устанавливает раздел реестра в HKLM\Software
Объект групповой политики применяется к: • Windows 11, версия 22H2 с KB5029351 и более поздние версии • Windows 10 версии 22H2 с KB5032278 или более поздним накопительным обновлением **Расположение объекта групповой политики**: конфигурация > компьютера Административные шаблоны > Компоненты > Windows клиентский компонент Центра обновления Windows > Управление обновлениями, предлагаемыми из клиентский	\Policies\Microsoft\Windows\WindowsUpdate\AllowOptionalContent

Политика	Устанавливает раздел реестра в HKLM\Software
компонент Центра обновления Windows >**Включить необязательные обновления**	
MDM применяется к: • Windows 11, версия 22H2 с KB5029351 и более поздними версиями • Windows 10 версии 22H2 с KB5032278 или более поздним накопительным обновлением **Расположение MDM**: ./Device/Vendor/MSFT/Policy/Config/Update/AllowOptionalContent	\Policies\Microsoft\Windows\WindowsUpdate\AllowOptionalContent

Включение функций, стоящих за временным управлением функциями предприятия

Новые функции и улучшения представлены в ежемесячном накопительном пакете обновления для обеспечения постоянных инноваций для Windows 11. Чтобы дать организациям время для планирования и подготовки, некоторые из этих новых функций временно отключены по умолчанию. Функции, отключенные по умолчанию, перечислены в статье базы знаний ежемесячного накопительного пакета обновления. Как правило, функция по умолчанию отключена, поскольку она существенно влияет либо на работу пользователей, либо на ИТ-администраторов.

Функции, стоящие за временным корпоративным управлением функциями, будут включены в следующем ежегодном обновлении компонентов. Организации могут развертывать обновления компонентов в своем собственном темпе, чтобы отложить эти функции, пока они не будут готовы к ним. Список функций, отключенных по умолчанию, см. в разделе Windows 11 функции временного корпоративного управления.

Параметры политики для включения функций, стоящих за временным корпоративным управлением

Развернуть таблицу

Политика	Устанавливает раздел реестра в HKLM\Software
Объект групповой политики для Windows 11 версии 22H2 с KB5022845 и более поздних версий: конфигурация > компьютера Административные шаблоны > Компоненты > Windows клиентский компонент Центра обновления Windows > Управление взаимодействием > с конечными пользователями. **Включение функций, представленных через обслуживание, которые отключены по умолчанию**	\Policies\Microsoft\Windows\WindowsUpdate\AllowTemporaryEnterpriseFeatureControl
MDM для Windows 11 версии 22H2 с KB5022845 и более поздними версиями: ./Device/Vendor/MSFT/Policy/Config/Update/AllowTemporaryEnterpriseFeatureControl	\Microsoft\PolicyManager\default\Update\AllowTemporaryEnterpriseFeatureControl

Сводка: параметры MDM и групповая политика для Windows 10 версии 1703 и более поздних версий

Ниже приведены краткие справочные таблицы поддерживаемых значений политик для клиентский компонент Центра обновления Windows клиентских политик в Windows 10 версии 1607 и более поздних.

GPO: HKLM\Software\Policies\Microsoft\Windows\WindowsUpdate

Развернуть таблицу

Ключ GPO	Тип ключа	Значение
AllowOptionalContent *добавлен в*: • Windows 11 версии 22H2 с KB5029351 и более поздними версиями • Windows 10 версии 22H2 с KB5032278 или более поздним накопительным обновлением	REG_DWORD	1. Автоматически получать необязательные обновления (включая CFR) 2: Автоматически получать необязательные обновления 3: Пользователи могут выбрать, какие необязательные обновления получать Другое значение или отсутствовать: не получать необязательные обновления
AllowTemporaryEnterpriseFeatureControl *добавлен в Windows 11, версия 22H2*	REG_DWORD	1: разрешено. Включены все функции в последнем ежемесячном накопительном обновлении. Другое значение или отсутствие: функции, отключаемые по умолчанию, останутся отключенными
BranchReadinessLevel	REG_DWORD	2. Системы принимают обновления компонентов для сборки программы предварительной оценки Windows . Быстрый 4: системы принимают обновления компонентов для сборки программы предварительной оценки Windows . Медленный 8: системы принимают обновления компонентов для выпуска сборки программы предварительной оценки Windows Другое значение или отсутствует: Получение всех применимых обновлений
DeferFeatureUpdates	REG_DWORD	1. Отложить обновления компонентов Другое значение или отсутствует: не откладывайте обновления компонентов
DeferFeatureUpdatesPeriodinDays	REG_DWORD	0–365: откладывать обновления компонентов на заданные дни
DeferQualityUpdates	REG_DWORD	1. Отложить обновления качества Другое значение или отсутствует: не откладывайте обновления качества
DeferQualityUpdatesPeriodinDays	REG_DWORD	0-35: откладывать обновления качества на заданные дни
ExcludeWUDriversInQualityUpdate	REG_DWORD	1. Исключите драйверы клиентский компонент Центра обновления Windows Другое значение или отсутствует: предложение

Ключ GPO	Тип ключа	Значение
		клиентский компонент Центра обновления Windows драйверов
PauseFeatureUpdatesStartTime	REG_DWORD	1. Приостановка обновлений компонентов Другое значение или отсутствует: не приостанавливайте обновления компонентов
PauseQualityUpdatesStartTime	REG_DWORD	1. Приостановка обновлений качества Другое значение или отсутствует: не приостанавливайте обновления качества

MDM: HKEY_LOCAL_MACHINE\Software\Microsoft\PolicyManager\default\Update

Развернуть таблицу

Ключ MDM	Тип ключа	Значение
AllowOptionalContent *добавлен в*: • Windows 11 версии 22H2 с KB5029351 и более поздними версиями • Windows 10 версии 22H2 с KB5032278 или более поздним накопительным обновлением	REG_DWORD	1. Автоматически получать необязательные обновления (включая CFR) 2: Автоматически получать необязательные обновления 3: Пользователи могут выбрать, какие необязательные обновления получать Другое значение или отсутствовать: не получать необязательные обновления
AllowTemporaryEnterpriseFeatureControl *добавлен в Windows 11, версия 22H2*	REG_DWORD	1: разрешено. Включены все функции в последнем ежемесячном накопительном обновлении. Другое значение или отсутствие: функции, отключаемые по умолчанию, останутся отключенными
BranchReadinessLevel	REG_DWORD	2. Системы принимают обновления компонентов для сборки программы предварительной оценки Windows . Быстрый 4: системы принимают обновления компонентов для сборки программы предварительной оценки Windows . Медленное 8. Системы принимают обновления компонентов для выпуска windows insider build 32: Системы принимают обновления компонентов из канала общей доступности Примечание. Другое значение или отсутствие: Получение всех применимых обновлений
DeferFeatureUpdatesPeriodinDays	REG_DWORD	0–365: откладывать обновления компонентов на заданные дни
DeferQualityUpdatesPeriodinDays	REG_DWORD	0-35: откладывать обновления качества на заданные дни
ExcludeWUDriversinQualityUpdate	REG_DWORD	1. Исключите драйверы клиентский компонент Центра обновления Windows Другое значение или отсутствует: предложение клиентский компонент Центра обновления Windows драйверов

Ключ MDM	Тип ключа	Значение
PauseFeatureUpdatesStartTime	REG_DWORD	1. Приостановка обновлений компонентов Другое значение или отсутствует: не приостанавливайте обновления компонентов
PauseQualityUpdatesStartTime	REG_DWORD	1. Приостановка обновлений качества Другое значение или отсутствует: не приостанавливайте обновления качества

Обновление устройств до более новых версий Windows

Из-за изменений в политиках клиента клиентский компонент Центра обновления Windows Windows 10 версии 1607 используются другие ключи GPO и MDM, чем доступные в версии 1511. Windows 10, версия 1703 также использует несколько ключей GPO и MDM, которые отличаются от доступных в версии 1607. Однако клиентский компонент Центра обновления Windows клиентских политик устройства под управлением более старых версий по-прежнему будут видеть, что их политики соблюдаются после обновления до более новой версии. Старые ключи политики будут по-прежнему существовать со значениями, перенесенными во время обновления. После обновления до более новой версии будут заполнены только старые ключи, а не ключи новой версии, пока администратор не будет явно определен на устройстве.

Как более ранние версии политик соблюдаются в более новых версиях Windows

Когда устройство под управлением более новой версии видит обновление, доступное на клиентский компонент Центра обновления Windows, устройство сначала оценивает и выполняет ключи политики Windows Обновления для бизнеса для текущей (более новой) версии. Если они отсутствуют, проверяется, задан ли какой-либо из ключей более ранней версии и отложен соответствующим образом. Ключи обновления для более новых версий всегда приоритетнее аналогичных ключей более старых версий.

Сравнение ключей в Windows 10 версии 1607 с Windows 10 версии 1703

Развернуть таблицу

Ключ версии 1607	Ключ версии 1703
PauseFeatureUpdates	PauseFeatureUpdatesStartTime
PauseQualityUpdates	PauseQualityUpdatesStartTime

Last updated on 26.09.2025

Совместное использование политик клиента клиентский компонент Центра обновления Windows и WSUS

Применяется к: ✅ Windows 11, ✅ Windows 10

> **Ищете информацию для потребителей?** См. раздел клиентский компонент Центра обновления Windows: вопросы и ответы.

Политика источника проверки обновлений Windows позволяет выбрать типы обновлений, которые следует получать из WSUS или клиентский компонент Центра обновления Windows клиентских политик.

Мы добавили исходную политику сканирования, начиная с обновления предварительной версии 1 сентября 2021 г. по KB5005101 (сборки ОС 19041.1202, 19042.1202 и 19043.1202). Она применяется к Windows 10 версии 2004 и выше и Windows 11. Эта политика изменяет способ, который устройства определяют, следует ли проверять локальный сервер WSUS или клиентский компонент Центра обновления Windows службу.

> ⓘ **Внимание**
>
> - Если вы используете Configuration Manager и имеете совместно управляемые устройства, дополнительные сведения о настройке клиентов см. в статье **Интеграция с политиками клиентов клиентский компонент Центра обновления Windows**.
> - Политика **Запретить политикам отсрочки обновлений вызывать проверки клиентский компонент Центра обновления Windows**, также известной как двойное сканирование, больше не поддерживается на Windows 11 и на Windows 10 заменяется новой исходной политикой проверки Windows и не рекомендуется использовать. Если вы настроите оба варианта в Windows 10, вы не будете получать обновления из клиентский компонент Центра обновления Windows.

Сведения о политике источника сканирования

Политика указания источника сканирования позволяет указать, получает ли устройство следующие типы обновлений Windows в виде WSUS **или** из клиентский компонент

Центра обновления Windows:

- Обновления компонентов
- Исправления Windows
- Обновления драйверов и встроенного ПО
- Обновления для других продуктов Майкрософт

Мы рекомендуем использовать эту политику при переходе с полностью локальной управляемой среды на облачную. Независимо от того, перемещаете ли вы в облако только драйверы или обновления качества, а затем перемещаете другие рабочие нагрузки, пошаговый подход может облегчить переход.

Поведение сканирования по умолчанию

Чтобы лучше понять исходную политику сканирования, ознакомьтесь со следующим поведением проверки по умолчанию и способами ее изменения:

- Если политики не настроены: все обновления поступают из клиентский компонент Центра обновления Windows.
- Если настроена только политика сервера WSUS, выполните следующие действия.
  - На Windows 10: все обновления поступают из WSUS.
  - В Windows 11. Все обновления по-прежнему поступают из WSUS, если не настроена указанная исходная политика сканирования.
- Если вы настроили сервер WSUS и политики отсрочки для Windows 10: все обновления будут поступать из клиентский компонент Центра обновления Windows, если вы не указали исходную политику сканирования или не отключили двойное сканирование.
- Если настроить сервер WSUS и политику источника сканирования: все обновления будут поступать из источника, выбранного в политике источника сканирования.

> **Совет**
>
> Единственными двумя релевантными политиками, из которых поступают обновления, являются укажите исходную политику сканирования и указывает, настроили ли вы сервер WSUS. Это должно упростить параметры конфигурации.

> **Примечание.**

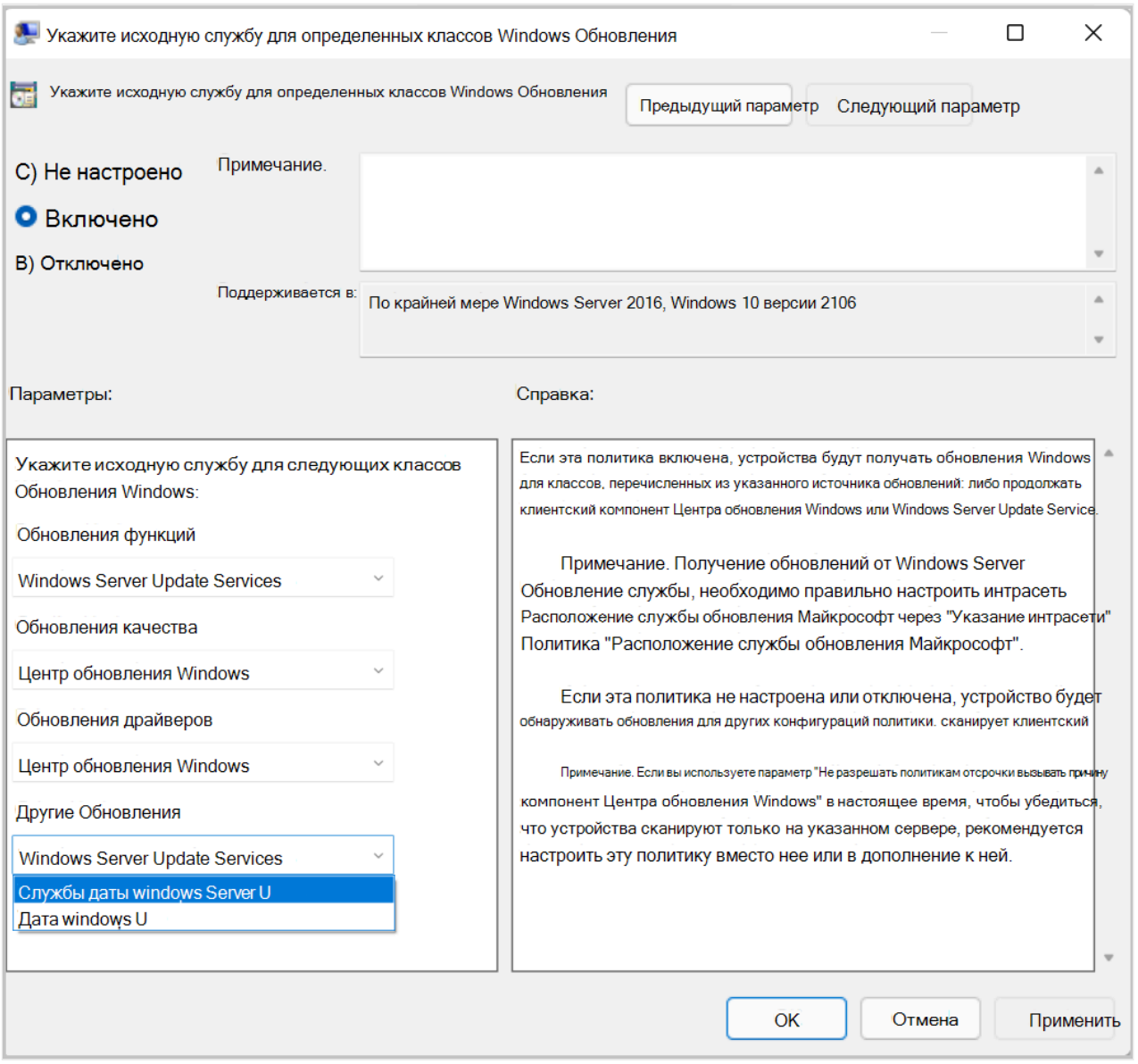
Если у вас есть устройства, настроенные для WSUS, и не настроена политика проверки исходного кода на наличие обновлений компонентов, поступающих из центра обновления Windows, или вы не задаете политики предложения с помощью клиентский компонент Центра обновления Windows клиентских политик, пользователи, выбрав "Проверить обновления в сети" на странице "Параметры", могут увидеть необязательное обновление до Windows 11. Рекомендуется настроить политику источника сканирования или политику предложения, чтобы предотвратить это.

Настройка источников сканирования

Политику можно настроить с помощью следующих двух методов:

1. групповая политика. Укажите исходную службу для определенных классов Windows Обновления

    - Путь: Конфигурация компьютера\Административные шаблоны\Компоненты Windows\клиентский компонент Центра обновления Windows\Управление обновлениями, предлагаемыми из службы обновления Windows Server\



2. Политики поставщика служб конфигурации (CSP):
   SetPolicyDrivenUpdateSourceДля<типа> обновления:

> ⓘ **Примечание.**
>
> - Все эти политики **следует настроить,** если вы используете поставщики облачных служб.
> - Редактирование реестра для изменения поведения политик обновления не рекомендуется. Используйте групповая политика или политику поставщика служб конфигурации (CSP) вместо прямой записи в реестр. Однако если вы решили изменить реестр, убедитесь, что вы также настроили `UseUpdateClassPolicySource` раздел реестра, иначе источник сканирования не будет изменен.
> - Если вы также используете политику **Указание параметров для установки дополнительных компонентов и восстановления компонентов,** чтобы

включить содержимое для FoD и языковых пакетов, см. **статью Как сделать функции по запросу и языковые пакеты доступными при использовании WSUS или Configuration Manager** для проверки конфигурации политики.

- Update/SetPolicyDrivenUpdateSourceForDriverUpdates
- Update/SetPolicyDrivenUpdateSourceForFeatureUpdates
- Update/SetPolicyDrivenUpdateSourceForOtherUpdates
- Update/SetPolicyDrivenUpdateSourceForQualityUpdates

Last updated on 16.05.2025

Соблюдение сроков соответствия требованиям для обновлений

Применяется к: ✅ Windows 11, ✅ Windows 10

Развертывание обновлений компонентов или исправлений для многих организаций является лишь частью уравнения для управления экосистемой устройств. Следующей важной частью является возможность обеспечения соответствия обновлений. клиентский компонент Центра обновления Windows клиентские политики предоставляют элементы управления для управления крайними сроками, когда устройства должны переходить на более новые версии. В этой статье содержатся сведения о том, как обеспечить соблюдение крайних сроков соответствия для клиентов, использующих политики клиентский компонент Центра обновления Windows клиентов.

Политики для крайних сроков соответствия

Политики для Windows 11 версии 22H2 и более поздних версий

Политики для клиентов под управлением Windows 11 версии 22H2 и более поздних

В Windows 11 версии 22H2 и более поздних доступны следующие политики для управления крайними сроками соответствия для обновлений:

Развернуть таблицу

Политика	Описание
Указание крайнего срока автоматического обновления и перезапуска для обновления качества	Эта политика позволяет указать количество дней до автоматической установки обновлений качества на устройствах и льготный период, по истечении которого необходимые перезапуски происходят автоматически. Эта политика включает возможность отказаться от автоматических перезапусков до окончания льготного периода.
Указание крайнего срока автоматического обновления и перезапуска для обновления компонентов	Эта политика позволяет указать количество дней до автоматической установки обновлений компонентов на устройствах и льготный период, по истечении которого автоматически происходит необходимый перезапуск. Эта политика включает возможность отказаться от автоматических перезапусков до окончания льготного периода.

В MDM эти политики доступны в виде отдельных параметров:

- Update/ConfigureDeadlineForFeatureUpdates
- Update/ConfigureDeadlineForQualityUpdates
- Update/ConfigureDeadlineGracePeriod (для обновлений качества)
- Update/ConfigureDeadlineGracePeriodForFeatureUpdates
- Update/ConfigureDeadlineNoAutoRebootForQualityUpdates
- Update/ConfigureDeadlineNoAutoRebootForFeatureUpdates

Если **задан крайний срок для автоматических обновлений и перезапусков** для обновлений качества или компонентов:

Расчет крайнего срока для обновлений качества и компонентов основан на том времени, когда проверка обновлений клиента первоначально обнаружила обновление. Ранее крайний срок основывался на дате выпуска обновления для исправлений и дате ожидания перезагрузки для обновлений компонентов. Изменение для расчета крайнего срока было внесено для повышения предсказуемости перезапуска.

Льготный период для обновлений качества и компонентов начинает обратный отсчет с момента ожидания перезапуска после завершения установки. Этот льготный период особенно полезен для пользователей, возвращающихся из отпуска или времени, что предотвращает немедленную принудительную перезагрузку по возвращении.

Действующий *крайний срок* — это то, что является более поздним временем обнаружения сканирования и указанным крайним сроком или временем обнаружения сканирования плюс льготный период. Как только установка будет завершена и устройство достигнет ожидающей перезагрузки, пользователи смогут запланировать перезапуски до истечения срока действия, а Windows по-прежнему может автоматически перезапускаться в нерабочее время, если пользователи не планируют перезапуски. После достижения действующего крайнего срока устройство пытается перезапустить независимо от времени активности.

> ⓘ **Примечание.**
>
> - При использовании этих политик **пользовательские параметры уведомлений** также используются на клиентах под управлением Windows 11 версии 22H2 и более поздних.
> - При **использовании указания крайнего срока для автоматических обновлений и перезапусков** для обновлений качества или обновлений

компонентов обновления обновления будут скачивание и установка обновлений сразу после их предложения.

- При **использовании параметра Укажите крайний срок для автоматических обновлений и перезапусков** для обновлений качества или обновлений компонентов параметры скачивания, установки и перезагрузки, вытекающие из **параметра Настройка автоматического Обновления**, игнорируются.
  - Начиная с обновления от 10 декабря 2024 г. для клиентов Windows 11 версии 22H2 и более поздних версий **настройка автоматического Обновления** соблюдается до наступления крайнего срока и игнорируется после истечения крайнего срока. Например, если настроить **автоматическую Обновления** для планирования установки обновлений на 3:00, вы также настроили коммерческий крайний срок, то скачивание и установка происходит в запланированное время из **раздела Настройка автоматического Обновления**, если срок не истек.

Пользовательский интерфейс для уведомлений о перезапуске с крайними сроками соответствия

Эти политики крайних сроков также предлагают возможность отказаться от автоматического перезапуска до достижения крайнего срока путем предоставления "задействованного процесса перезапуска" до истечения крайнего срока. На этом этапе устройство автоматически планирует перезагрузку независимо от времени активности.

Эти уведомления отображаются пользователем в зависимости от выбранного параметра и версии операционной системы, работающей на устройстве. Как правило, уведомления пользователей становятся более заметными по мере приближения крайнего срока. Описанный интерфейс используется по умолчанию и предполагает наличие достаточного времени для уведомлений до наступления действующего крайнего срока . Описание не учитывает изменения в политике **отображения параметров уведомлений об обновлениях** (Update/NoUpdateNotificationsDuringActiveHours) или других параметров, которые значительно изменили бы взаимодействие.

Windows 11 версии 23H2 и более поздних

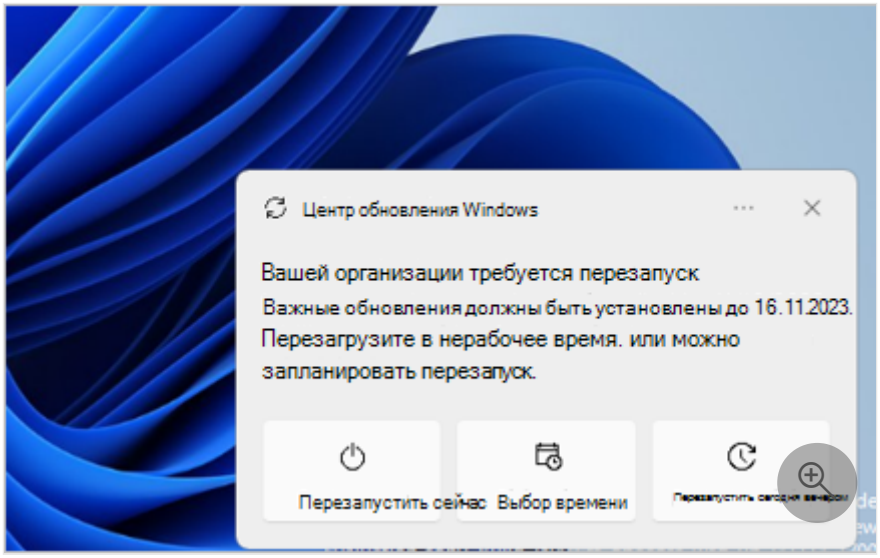
В Windows 11 версии 23H2 и более поздних версий пользователь видит следующие уведомления в зависимости от параметров, выбранных пользователем и ИТ-

администратором:

Если **заданы крайние сроки автоматического обновления и перезапуска** :

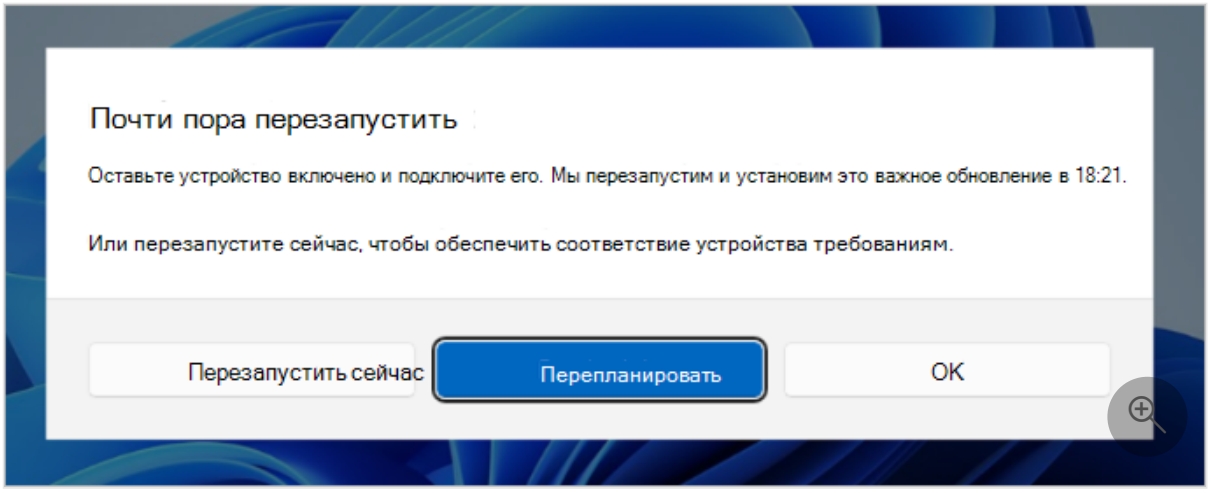
Пока перезагрузка ожидается, до наступления крайнего срока пользователи получают всплывающее уведомление в углу экрана. Уведомление включает дату крайнего срока и параметры перезапуска сейчас, выбора времени для перезапуска или перезапуска сегодня вечером после окончания активных часов.

- Если пользователь задал параметр**Параметры**>**клиентский компонент Центра обновления Windows**>**Добавить параметры**>**Уведомлять меня о необходимости перезагрузки для завершения обновления** до **Включено**, он сразу же получает всплывающее уведомление, когда устройство переходит в состояние ожидания перезагрузки для обновлений. Автоматические перезапуски обновлений блокируются в течение 24 часов после первоначального уведомления, чтобы предоставить этим пользователям время на подготовку.
- Если пользователь установил параметр **Уведомлять меня о необходимости перезагрузки для завершения обновления** до **выкл.** (по умолчанию), он получает всплывающее уведомление о том, что перезагрузка требуется через 24 часа после того, как устройство перейдет в состояние ожидания перезагрузки для обновлений.

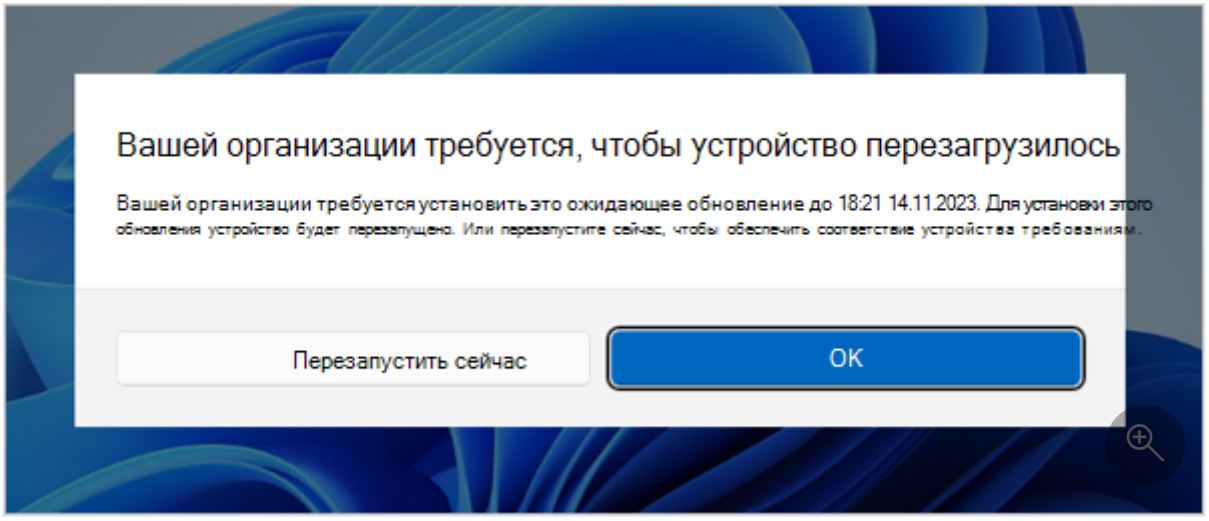


В зависимости от параметров, которые настраивают как пользователи, так и администраторы, всплывающие уведомления могут иногда появляться до наступления крайнего срока, чтобы напомнить пользователю об обновлении. В течение этого времени, если это разрешено, автоматические перезапуски могут быть запланированы после активных часов.

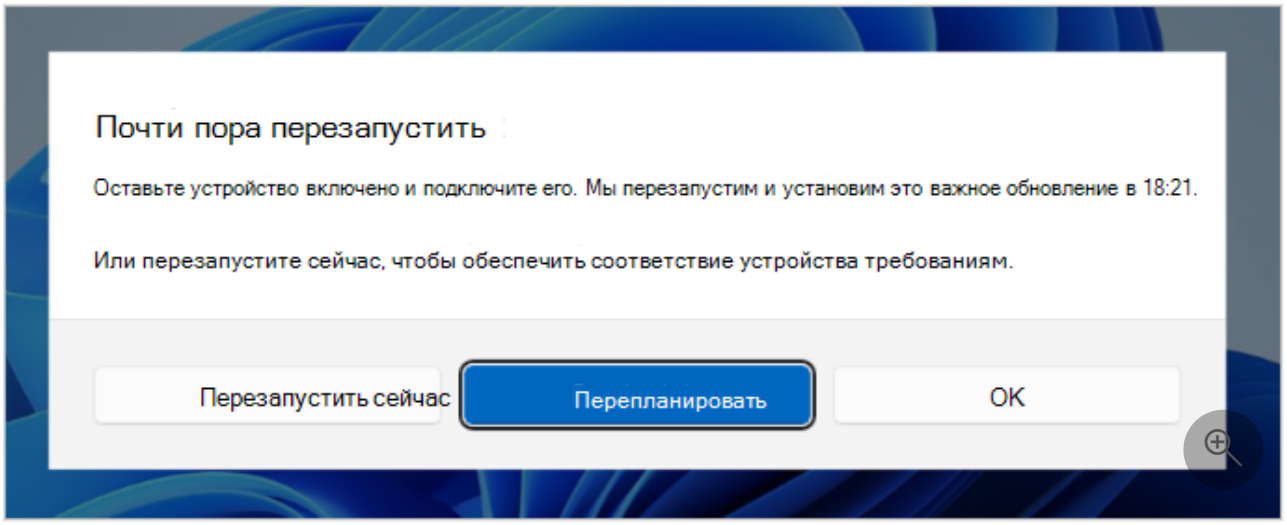
- Если запланирован автоматический перезапуск или пользователь запланировали перезапуск, а пользователь вошел в систему в это время, он получает уведомление за 15 минут до запланированного времени.



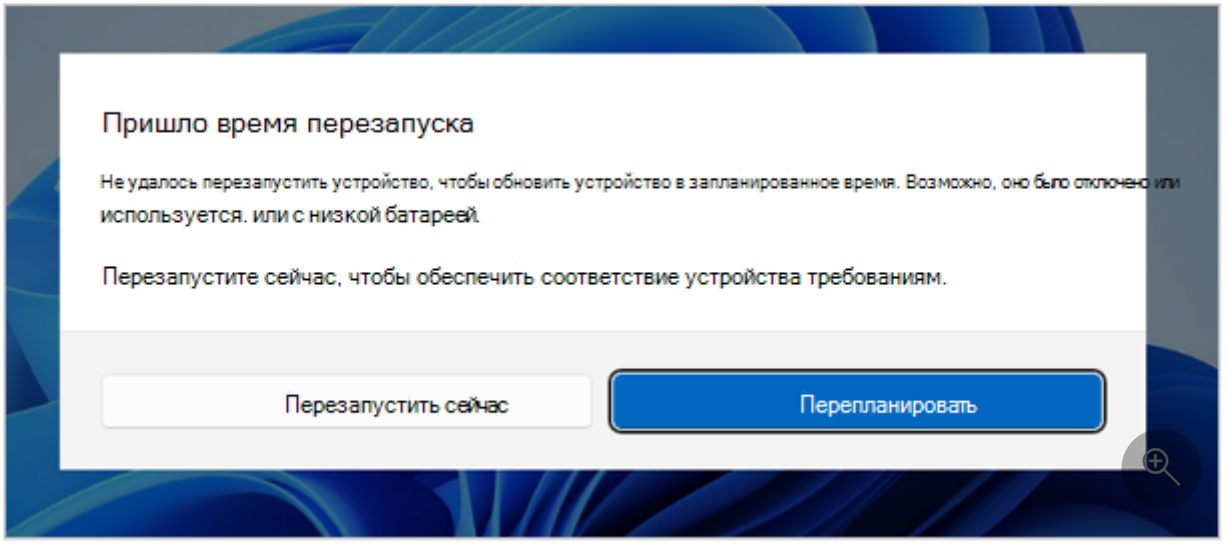
Когда устройство приближается к крайнему сроку, в середине экрана отображается уведомление, содержащее время крайнего срока и параметры для перезапуска или подтверждения уведомления.



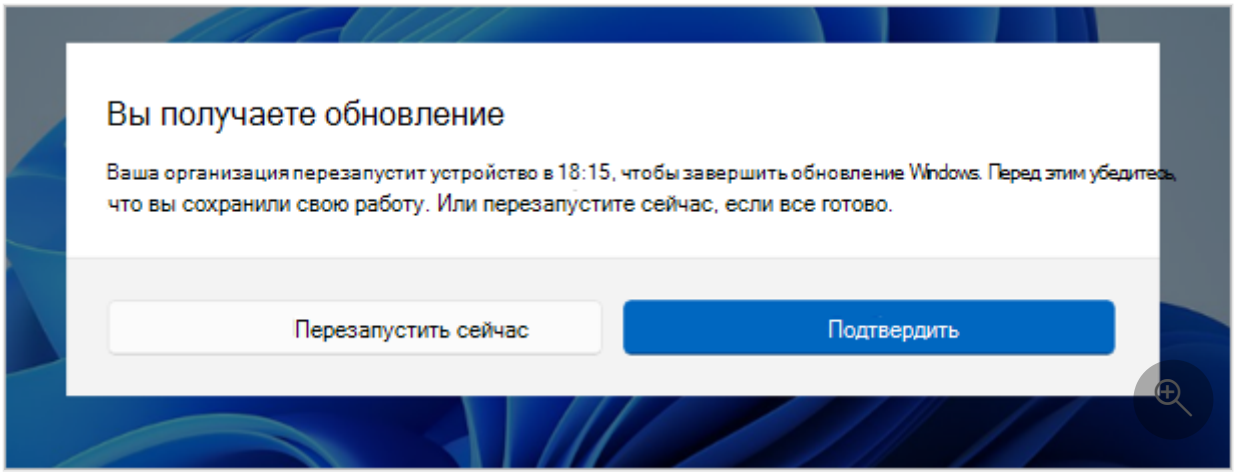
За 15 минут до наступления крайнего срока в середине экрана отображается уведомление, уведомляющее пользователя о том, что произойдет перезагрузка. Пользователи могут подтвердить перезапуск, перепланировать или выбрать перезапуск сейчас.



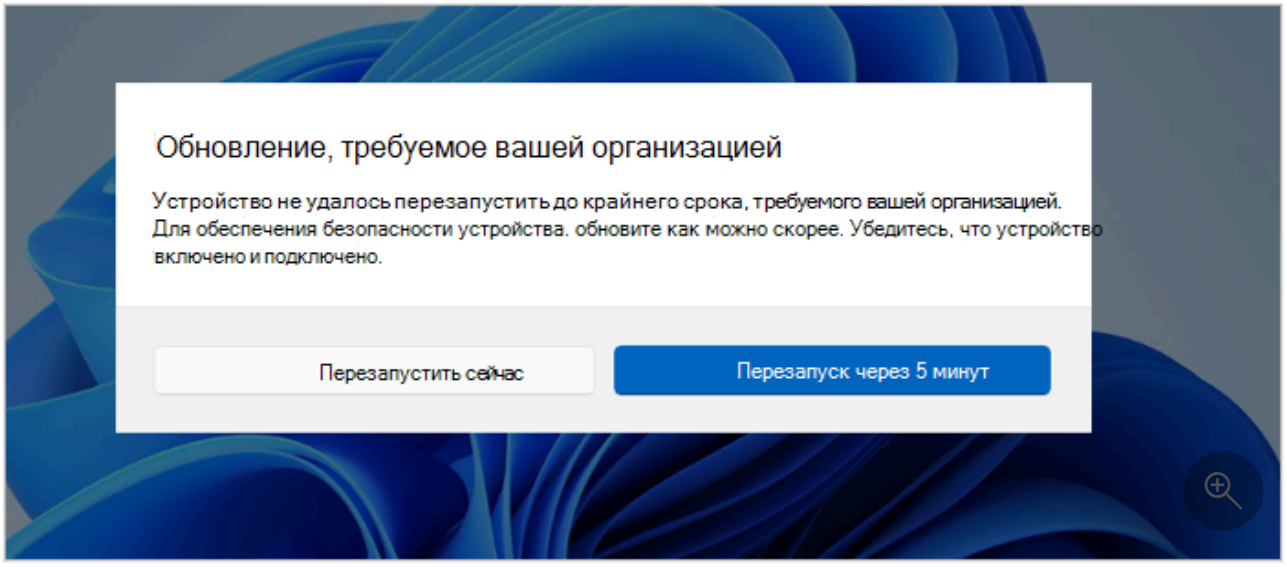
В случаях, когда запланированная пользователем перезагрузка завершается сбоем, но есть еще больше времени до достижения крайнего срока, пользователь получает уведомление о перезапуске сейчас или о переносе перезапуска.



В случаях, когда крайний срок истек, пользователь получает уведомление о необходимости перезапуска. Единственным вариантом, который может выбрать пользователь, является перезапуск или подтверждение. У пользователя есть 15 минут, чтобы выбрать перезапуск, прежде чем устройство будет принудительно перезапущено.



В случаях, когда крайний срок истек и перезагрузка завершилась сбоем, пользователь получает уведомление о необходимости перезапуска. Если устройство подключено, оно будет пытаться перезапускаться каждые 5 минут, пока устройство не будет успешно перезапущено. У пользователя есть 5 минут на перезапуск, прежде чем устройство будет вынуждено перезапустить.



Last updated on 19.03.2025

Интеграция политик клиентский компонент Центра обновления Windows клиентов с решениями управления

Применяется к: ✅ Windows 11, ✅ Windows 10

> **Ищете информацию для потребителей?** См. раздел клиентский компонент Центра обновления Windows: вопросы и ответы.

Развертывания клиентский компонент Центра обновления Windows клиентских политик можно интегрировать с существующими средствами управления, такими как Windows Server Update Services (WSUS) и Microsoft Configuration Manager.

> **Совет**
>
> Эта функция ранее называлась *клиентский компонент Центра обновления Windows для бизнеса*.

Интеграция политик клиента клиентский компонент Центра обновления Windows с Windows Server Update Services

Для Windows 10 версии 1607 и более поздних устройств можно настроить получение обновлений как от клиентский компонент Центра обновления Windows (или Центра обновления Майкрософт), так и от Windows Server Update Services (WSUS). При использовании политик клиентов WSUS и клиентский компонент Центра обновления Windows:

- Устройства получают содержимое Windows от корпорации Майкрософт и откладывают эти обновления в соответствии с клиентский компонент Центра обновления Windows клиентскими политиками.
- Все остальное содержимое, синхронизированное из WSUS, будет непосредственно применено к устройству; то есть обновления для продуктов, отличных от Windows, не будут соответствовать политикам отсрочки.

Пример конфигурации No 1. Отсрочка обновлений клиентский компонент Центра обновления Windows с

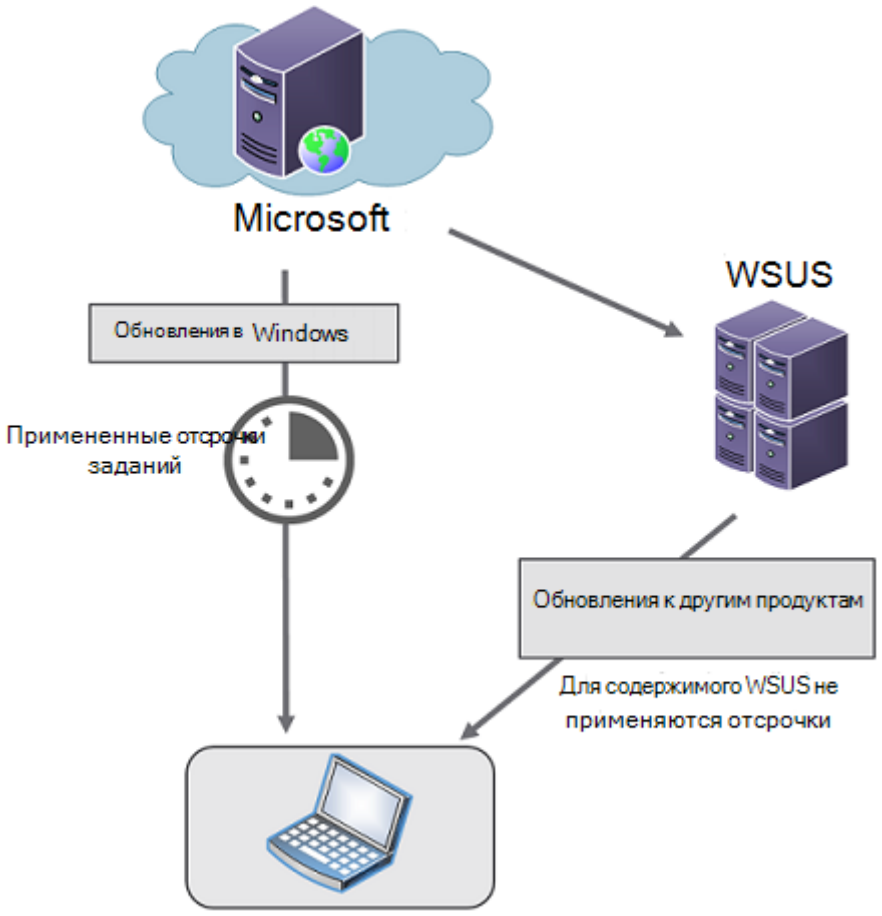
другим содержимым обновлений, размещенным в WSUS

Конфигурация:

- Устройство настроено для отсрочки обновлений качества Windows с помощью политик клиента клиентский компонент Центра обновления Windows
- Устройство также настроено так, что им управляют службы WSUS
- Устройство не настроено для включения Центра обновления Майкрософт (**Update/AllowMUUpdateService** = не включено)
- Администратор отказался включить обновления Office и других продуктов в WSUS
- Администратор также поставил сторонние драйверы в WSUS

Развернуть таблицу

Содержимое	Источник метаданных	Источник полезных данных	Отложено?
Обновления в Windows	Центр обновления Windows	Центр обновления Windows	Да
Обновления Office и других продуктов	WSUS	WSUS	Нет
Сторонние драйверы	WSUS	WSUS	Нет



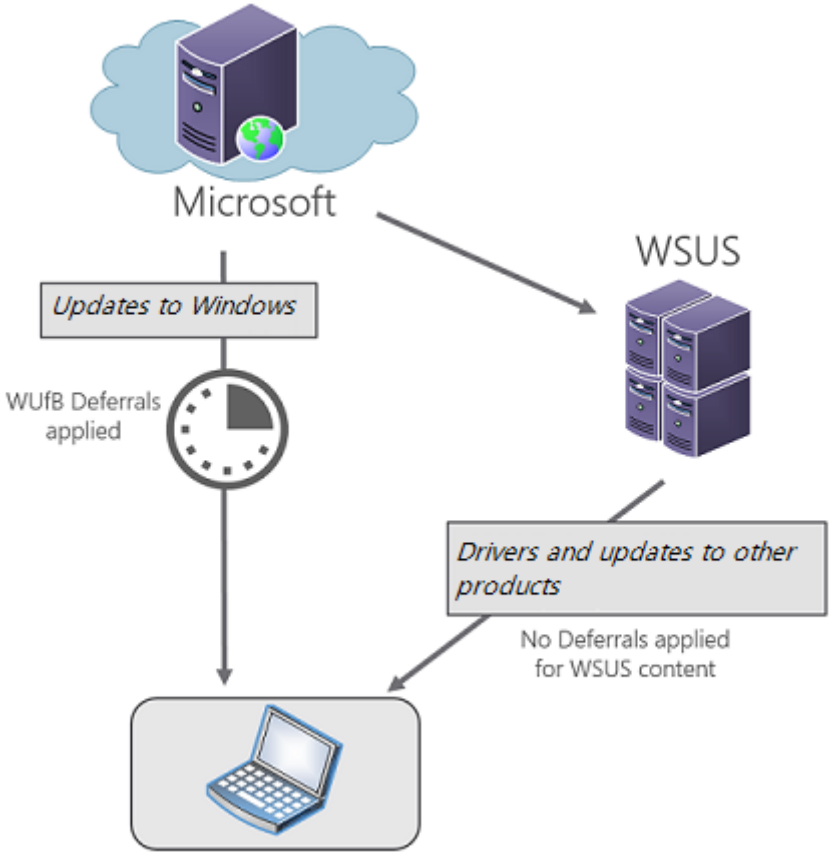
Пример конфигурации No 2. Исключение драйверов из обновлений качества Windows с помощью клиентский компонент Центра обновления Windows клиентских политик

Конфигурация:

- Устройство настроено для отсрочки обновлений качества Windows и исключения драйверов из клиентский компонент Центра обновления Windows обновлений качества (**ExcludeWUDriversInQualityUpdate** = enabled)
- Устройство также настроено так, что им управляют службы WSUS
- Администратор решил разместить драйверы Центра обновления Windows в WSUS

Развернуть таблицу

Содержимое	Источник метаданных	Источник полезных данных	Отложено?
Обновления для Windows (исключая драйверы)	Центр обновления Windows	Центр обновления Windows	Да
Обновления Office и других продуктов	WSUS	WSUS	Нет
Драйверы	WSUS	WSUS	Нет



Пример конфигурации 3. Устройство, настроенное для получения обновлений Майкрософт

Конфигурация:

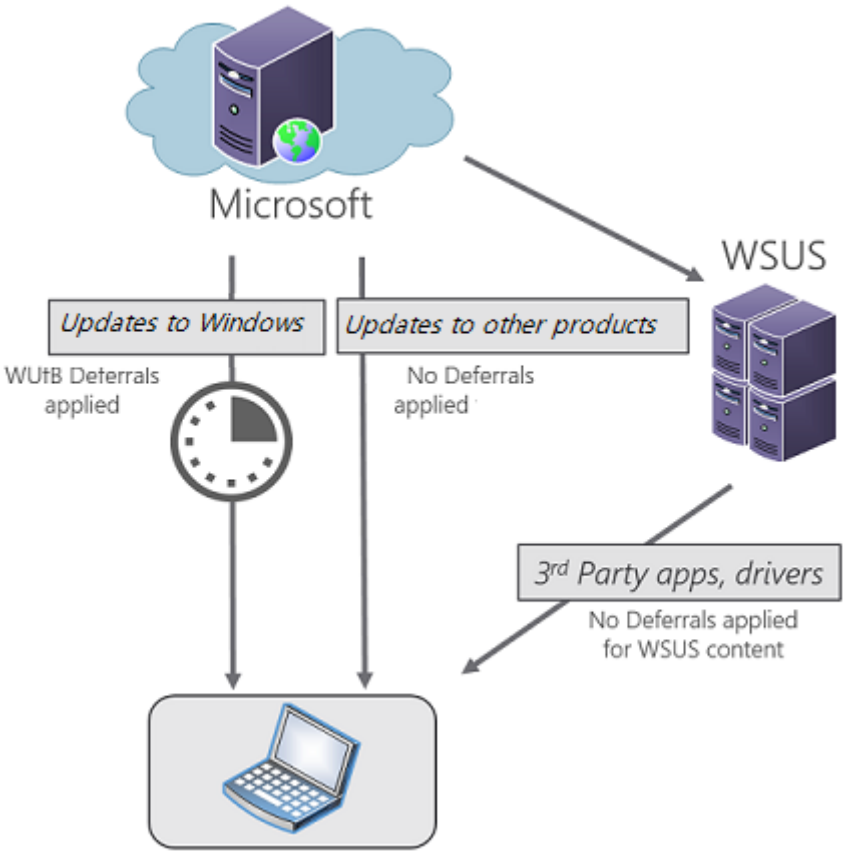
- Устройство настроено для отсрочки обновлений качества с помощью клиентский компонент Центра обновления Windows клиентских политик и управления с помощью WSUS
- Устройство настроено **для получения обновлений для других продуктов Майкрософт** , а также обновлений для Windows (**Update/AllowMUUpdateService** = enabled)
  - Список других продуктов Майкрософт, которые могут быть обновлены, см. в разделе Обновление других продуктов Майкрософт.
- Администратор также разместила на сервере WSUS содержимое обновлений Центра обновления Майкрософт, сторонних и локально опубликованных обновлений.

В этом примере поведение отсрочки обновлений Office и других продуктов, отличных от Windows, немного отличается от режима, если службы WSUS не включены.

- При выключенных службах WSUS обновления откладывались бы так же, как и любые обновления для Windows.
- Однако если также настроены службы WSUS, эти обновления создаются из корпорации Майкрософт, но политики отсрочки не применяются.

Развернуть таблицу

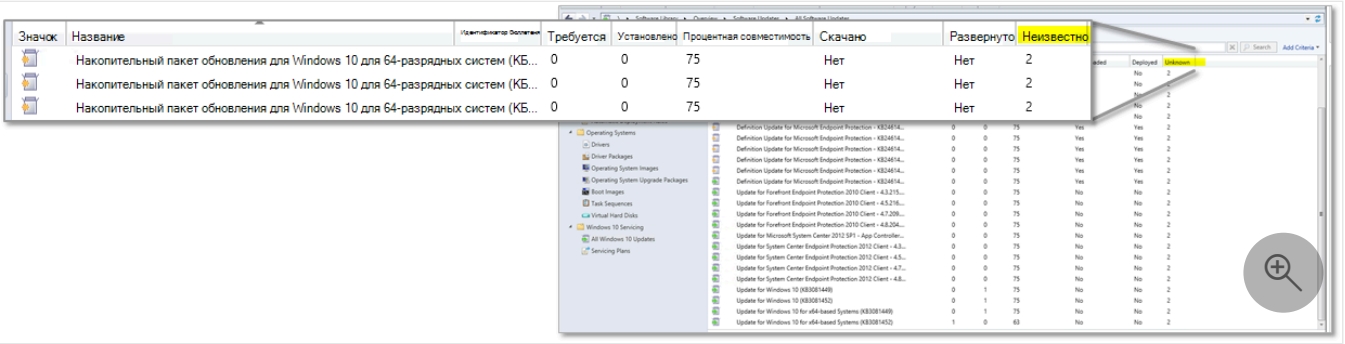
Содержимое	Источник метаданных	Источник полезных данных	Отложено?
Обновления для Windows (исключая драйверы)	Центр обновления Майкрософт	Центр обновления Майкрософт	Да
Обновления Office и других продуктов	Центр обновления Майкрософт	Центр обновления Майкрософт	Нет
Драйверы, сторонние приложения	WSUS	WSUS	Нет



> ⓘ **Примечание.**
>
> Так как администратор включил **Update/AllowMUUpdateService**, размещение содержимого в WSUS не требовалось для конкретного устройства, поскольку оно всегда будет получать содержимое Центра обновления Майкрософт от Майкрософт, если оно настроено таким образом.

Интеграция политик клиента клиентский компонент Центра обновления Windows с Microsoft Configuration Manager

Для Windows 10 версии 1607 организации, которые уже управляют своими системами с помощью решения Configuration Manager, также могут настроить свои устройства для клиентский компонент Центра обновления Windows клиентских политик (то есть задавать политики отсрочки на этих устройствах). Такие устройства отображаются в консоли Configuration Manager, однако они отображаются с состоянием обнаружения **Unknown**.



Дополнительные сведения см. в статье Интеграция с клиентский компонент Центра обновления Windows клиентскими политиками.

Last updated on 01.04.2025

Пошаговое руководство. Настройка клиентских политик клиентский компонент Центра обновления Windows с помощью групповая политика

Применяется к: ✅ Windows 11, ✅ Windows 10, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

> **Ищете информацию для потребителей?** См. раздел клиентский компонент Центра обновления Windows: вопросы и ответы.

Обзор

Вы можете использовать групповая политика с помощью консоли управления групповая политика (GPMC) для управления работой клиентский компонент Центра обновления Windows клиентских политик. Прежде чем вносить изменения в клиентский компонент Центра обновления Windows клиентские политики, следует рассмотреть и разработать стратегию развертывания обновлений. Дополнительные сведения см. в статье Подготовка стратегии обслуживания для обновлений клиента Windows .

ИТ-администратор может настроить политики клиента клиентский компонент Центра обновления Windows с помощью групповая политика или настроить их локально (для каждого устройства). Все соответствующие политики находятся по пути **Конфигурация компьютера** > **Административные шаблоны** > **Компоненты** > **Windows клиентский компонент Центра обновления Windows**.

> **Совет**
>
> Эта функция ранее называлась *клиентский компонент Центра обновления Windows для бизнеса*.

Чтобы управлять обновлениями с помощью клиентский компонент Центра обновления Windows клиентских политик, как описано в этой статье, следует подготовиться к следующим действиям, если вы еще этого не сделали:

- Создайте группы безопасности Active Directory, которые соответствуют кругам развертывания, используемым для поэтапного развертывания обновлений.
- Разрешить доступ к службе клиентский компонент Центра обновления Windows.

- Скачайте и установите шаблоны ADMX, соответствующие вашей версии Windows 10. Дополнительные сведения см. в разделах Создание центрального хранилища и управление им для административных шаблонов групповая политика в Windows и Пошаговое руководство. Управление Windows 10 с помощью административных шаблонов.

Настройка политик клиента клиентский компонент Центра обновления Windows

В этом примере для управления обновлениями используется одна группа безопасности. Обычно рекомендуется использовать по крайней мере три круга (ранние тестировщики для предварительных сборок, широкое развертывание для выпусков, критически важные устройства для зрелых выпусков).

Выполните следующие действия на устройстве со средствами удаленного администрирования сервера или на контроллере домена.

Настройка круга

1. Запустите консоль управления групповая политика (gpmc.msc).
2. Разверните **Домены ><*леса ваш домен*>.
3. Щелкните правой кнопкой мыши <*домен*> и выберите **Создать объект групповой политики в этом домене и свяжите его здесь**.
4. В диалоговом окне **Новый объект групповой политикивведите клиентский компонент Центра обновления Windows политики клиента — Группа 1** в качестве имени нового объекта групповая политика.
5. Щелкните правой кнопкой мыши объект **"клиентский компонент Центра обновления Windows политики клиента — группа 1"** и выберите **изменить**.
6. В Редактор управления групповая политика перейдите в раздел **Политики > конфигурации > компьютера Административные шаблоны > Компоненты > Windows клиентский компонент Центра обновления Windows**. Теперь вы можете приступить к назначению политик этому кольцу (группе) устройств.

Управление предложениями клиентский компонент Центра обновления Windows

Вы можете управлять применением обновлений, например путем отсрочки установки обновления на устройстве или путем приостановки обновлений на определенный период времени.

Определите, какие обновления вы хотите предложить для устройств

Обновления компонентов и исправлений автоматически предлагаются устройствам, подключенным к клиентский компонент Центра обновления Windows с помощью клиентский компонент Центра обновления Windows клиентских политик. Однако вы можете выбрать, будут ли устройства дополнительно получать другие Обновления Майкрософт или драйверы, применимые к такому устройству.

Чтобы включить Microsoft Обновления, с помощью консоли управления групповая политика перейдите в раздел **Конфигурация > компьютера Административные шаблоны > Компоненты > Windows клиентский компонент Центра обновления Windows > Настройка автоматического Обновления** и выберите пункт **Установите обновления для других продуктов Майкрософт**. Список других продуктов Майкрософт, которые могут быть обновлены, см. в разделе Обновление других продуктов Майкрософт.

Драйверы включаются автоматически, так как они полезны для систем устройств. Рекомендуется разрешить политике драйверов обновлять драйверы на устройствах (по умолчанию), но этот параметр можно отключить, если вы предпочитаете управлять драйверами вручную. Если вы хотите по какой-либо причине отключить обновления драйверов, используйте консоль управления групповая политика, чтобы перейти в раздел **Конфигурация > компьютера Административные шаблоны > Windows Компоненты > клиентский компонент Центра обновления Windows > Не включать драйверы с Обновления Windows** и включить политику.

Мы также рекомендуем разрешить обновления продуктов Майкрософт, как обсуждалось ранее.

Установка, когда устройства получают обновления компонентов и качества

Я хочу получать предварительные версии следующего обновления компонентов

1. Убедитесь, что вы зарегистрированы в программе предварительной оценки Windows для бизнеса. Это бесплатная программа, доступная для коммерческих

клиентов, которая поможет им в проверке обновлений компонентов перед выпуском. Присоединение к программе позволяет получать обновления до их выпуска, а также получать сообщения электронной почты и содержимое, связанное с тем, что будет в ближайших обновлениях.

2. Используйте консоль управления групповая политика, чтобы перейти к разделу **Конфигурация > компьютера Административные шаблоны > Компоненты > Windows клиентский компонент Центра обновления Windows > клиентский компонент Центра обновления Windows для управления бизнесом > Предварительный просмотр сборок** и установка политики в **значение Включить предварительные сборки** для любого из тестовых устройств, которые требуется установить предварительные сборки.

3. Использование консоли управления групповая политика для перехода к разделу **Конфигурация > компьютера Административные шаблоны > Компоненты > Windows клиентский компонент Центра обновления Windows > клиентский компонент Центра обновления Windows для бизнеса > Выберите, когда будут получены предварительные сборки и обновления компонентов**. В области **Параметры** выберите одну из предварительных сборок в раскрывающемся меню. Мы повторно раскомментируем **программу предварительной оценки Windows Slow** для коммерческих клиентов, используя предварительные сборки для проверки.

4. Нажмите **OK**.

Я хочу управлять выпущенными обновлениями компонентов, которые получают мои устройства

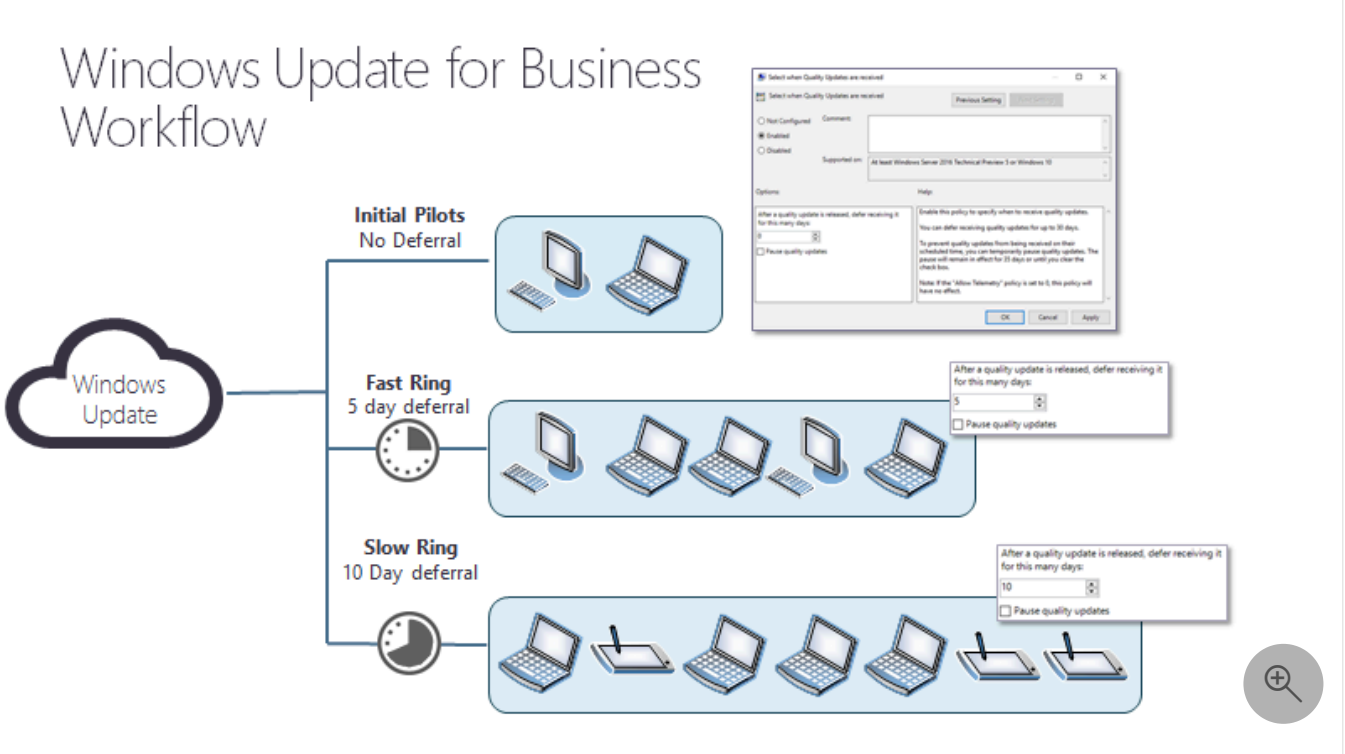
Администратор клиентский компонент Центра обновления Windows может отложить или приостановить обновления. Обновления компонентов можно отложить до 365 дней, а обновления качества — до 30 дней. Отсрочка просто означает, что вы не получите обновление, пока оно не будет выпущено по крайней мере на указанное количество дней отсрочки (дата предложения = дата выпуска + дата отсрочки). Обновления компонентов или исправлений можно приостановить на срок до 35 дней с указанной даты начала.

- Чтобы отложить или приостановить обновление компонентов: **конфигурация > компьютера Административные шаблоны > Компоненты > Windows клиентский компонент Центра обновления Windows > клиентский компонент Центра обновления Windows для бизнеса > Выберите, когда получены предварительные сборки и обновления компонентов**
- Отложить или приостановить обновление качества: **конфигурация > компьютера Административные шаблоны > Компоненты > Windows клиентский компонент**

Центра обновления Windows > клиентский компонент Центра обновления Windows для бизнеса > Выберите, когда получено Обновления качества

Пример

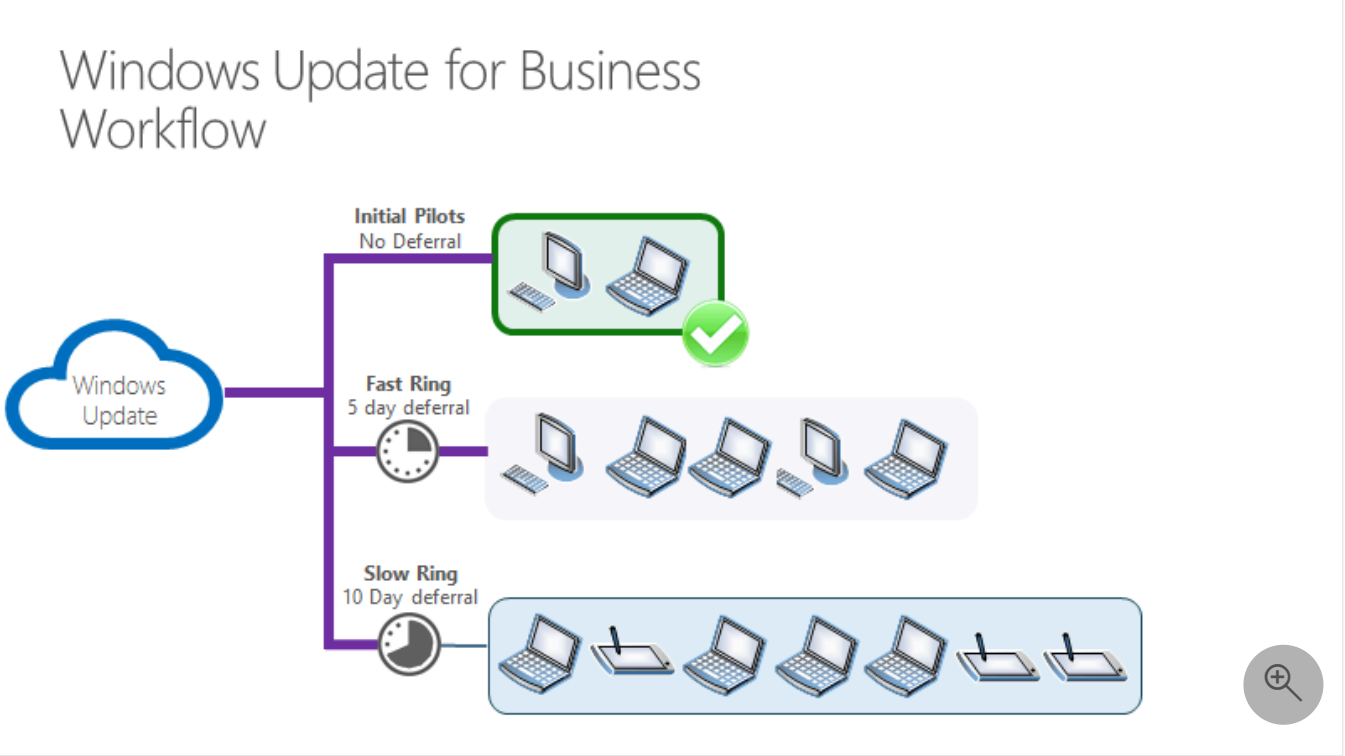
В этом примере есть три круга для обновления качества. Первый круг ("пилотный") имеет период отсрочки в 0 дней. Второе кольцо ("быстрый") имеет отсрочку в пять дней. Третье кольцо ("медленно") имеет отсрочку в 10 дней.



После выпуска обновления качества оно предлагается устройствам в пилотном кольце при следующем сканировании обновлений.

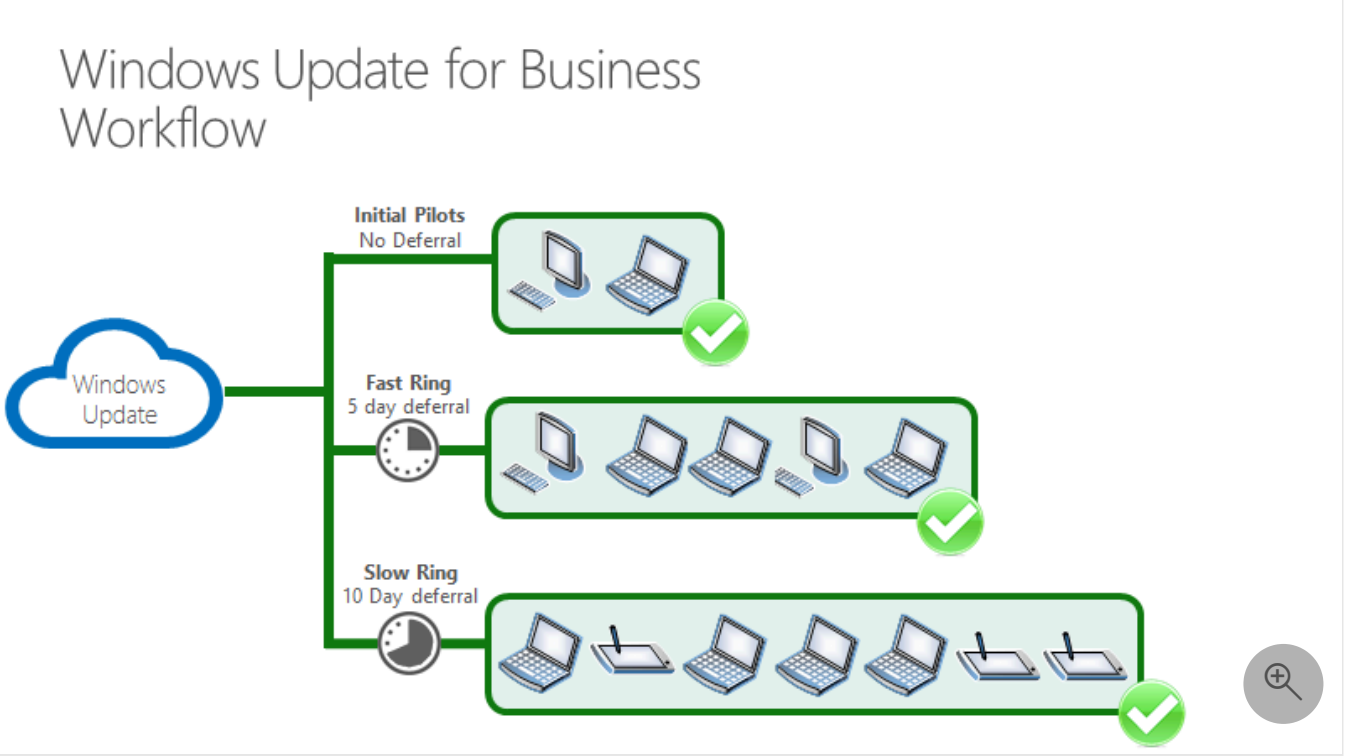
Пять дней спустя

Устройствам в быстром кольце предлагается обновление качества при следующем сканировании обновлений.



Десять дней спустя

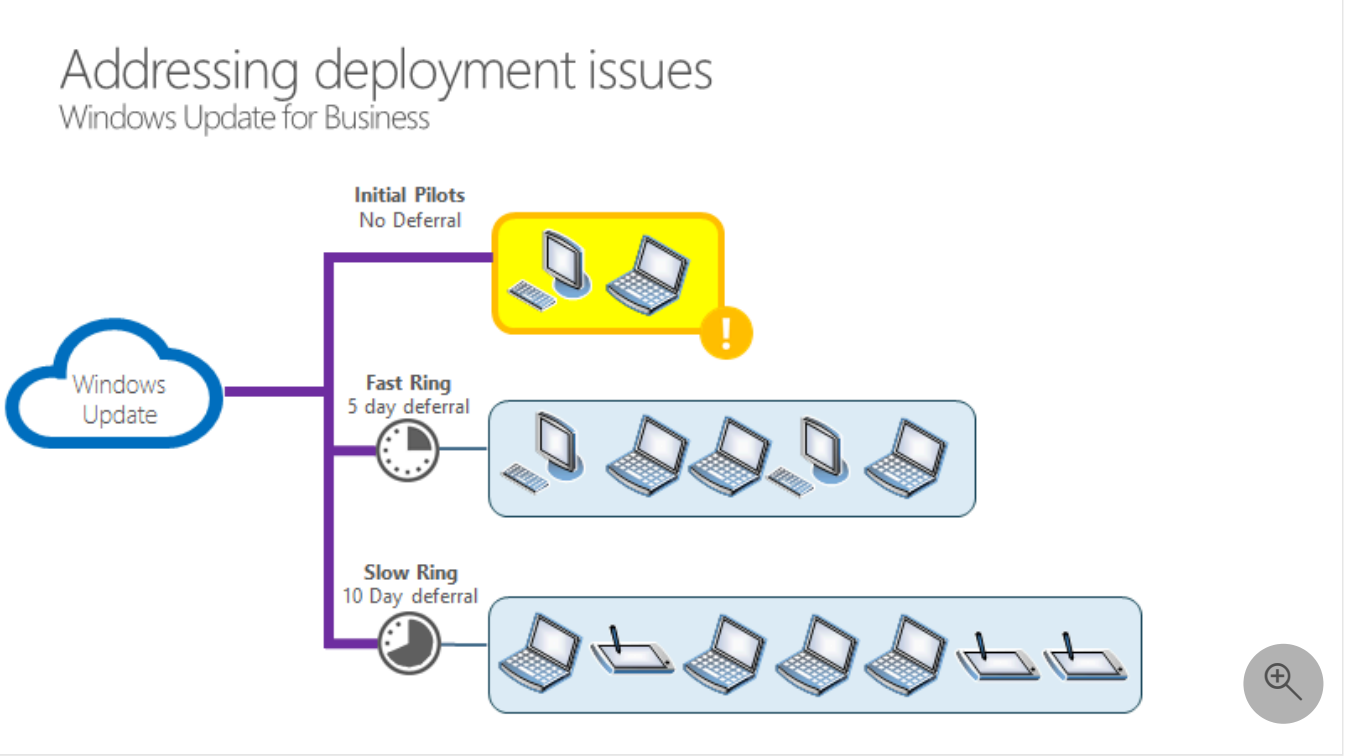
Через десять дней после выпуска обновления качества оно предлагается устройствам в медленном кольце при следующем сканировании обновлений.



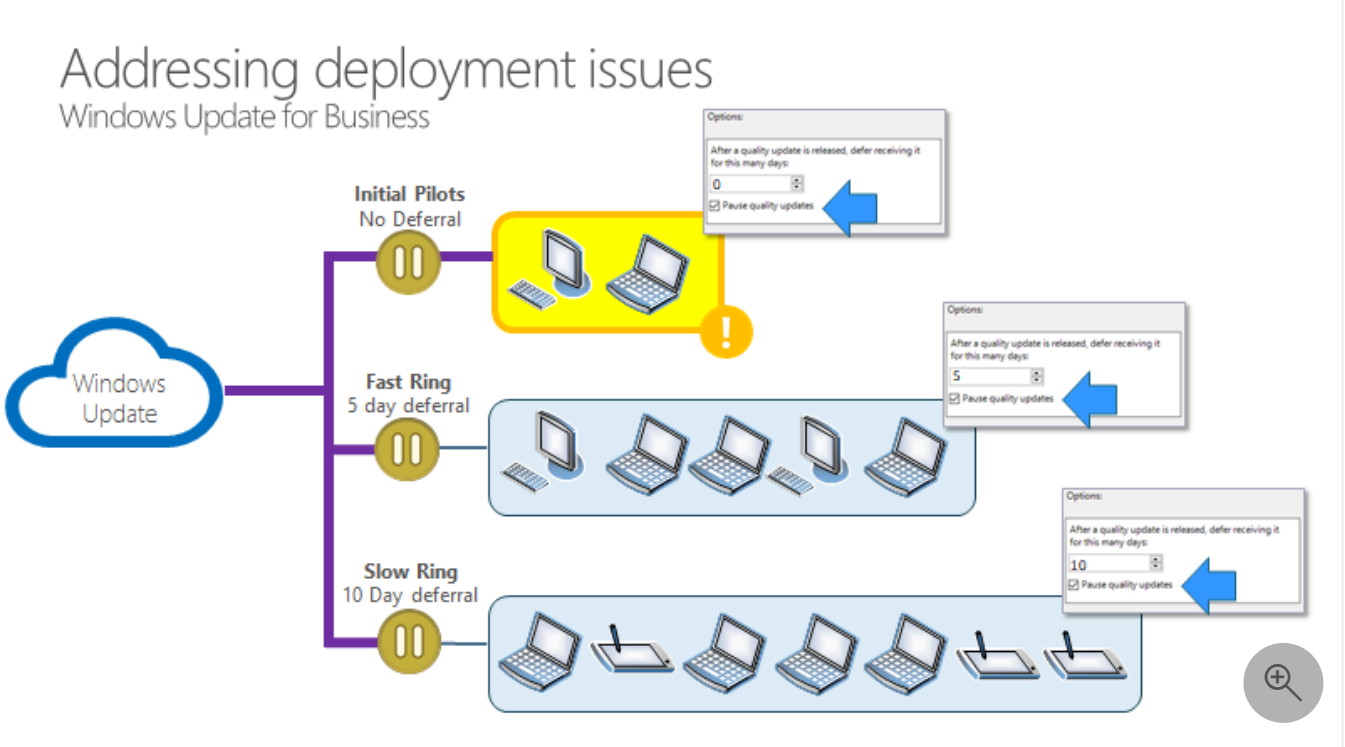
Если проблем не возникнет, всем устройствам, проверяющим наличие обновлений, будет предложено обновление качества в течение 10 дней после выпуска в три волны.

Что делать, если с обновлением возникает проблема?

В этом примере обнаружена некоторая проблема при развертывании обновления в "пилотном" круге.



На этом этапе ИТ-администратор может задать политику для приостановки обновления. В этом примере администратор выбирает поле **Приостановить обновления качества** проверка.



Теперь обновление всех устройств приостановлено в течение 35 дней. Когда пауза будет удалена, им будет предложено *следующее* обновление качества, которое в идеале не

будет иметь той же проблемы. Если проблема по-прежнему возникает, ИТ-администратор может снова приостановить обновления.

Я хочу остаться на определенной версии

Если вам нужно, чтобы устройство оставалось на версии за пределами момента, когда будут истекать отсрочки для следующей версии или если вам нужно пропустить версию, используйте параметр **Выбрать версию целевого обновления компонентов** вместо **параметра Указать, когда получены предварительные сборки и обновления компонентов** для отложений обновлений компонентов. При использовании этой политики укажите версию, которую будут использовать устройства. Если вы не обновите его до того, как устройство достигнет конца обслуживания, устройство будет автоматически обновлено после 60 дней после окончания обслуживания для его выпуска.

При настройке политики целевой версии, если указать версию обновления компонентов, которая старше текущей версии, или задать недопустимое значение, устройство не будет получать обновления компонентов, пока политика не будет обновлена. При указании политики целевой версии отсрочки обновления компонентов не будут действовать.

Управление обновлениями для пользователей

Я хочу управлять загрузкой, установкой и перезапуском устройств после обновлений

Рекомендуется разрешить автоматическое обновление — это поведение по умолчанию. Если политика автоматического обновления не настроена, устройство попытается скачать, установить и перезапустить в лучшее для пользователя время с помощью встроенной логики, такой как интеллектуальные часы активности.

Для более детального управления можно задать максимальный период активности, который пользователь может задать с помощью **административных шаблонов >> Конфигурации > компьютера Компоненты Windows клиентский компонент Центра обновления Windows > Укажите диапазон активных часов для автоматического перезапуска**.

Рекомендуется воздерживаться от настройки политики активных часов, так как она включена по умолчанию, когда автоматическое обновление не отключено, и обеспечивает более удобный интерфейс, когда пользователи могут задавать собственные часы активности. Если вы хотите задать часы активности, используйте **административные шаблоны > конфигурации > компьютера Компоненты > Windows клиентский**

компонент Центра обновления Windows > Отключить автоматическую перезагрузку для обновлений в часы активности.

Для обновления в нерабочее время не нужно задавать дополнительные параметры: просто не отключайте автоматический перезапуск. Для более детального управления рекомендуется использовать автоматические обновления для планирования времени установки, дня или недели. Для этого используйте административные **шаблоны > конфигурации > компьютера Компоненты > Windows клиентский компонент Центра обновления Windows > Настроить автоматическую Обновления**, а затем выберите **Автозагрузка и запланируйте установку**. Этот параметр можно настроить в соответствии с временем установки обновления на устройствах.

При настройке этих политик установка происходит автоматически в указанное время, и устройство перезапустится через 15 минут после завершения установки (если она не была прервана пользователем).

Я хочу обеспечить безопасность устройств и соответствие крайним срокам обновления

Рекомендуется использовать **административные шаблоны > конфигурации > компьютера Компоненты > Windows клиентский компонент Центра обновления Windows > Укажите крайний срок для автоматических обновлений и перезапусков** для обновлений компонентов и исправлений, чтобы обеспечить безопасность устройств на Windows 10 версии 1709 и более поздних. Это позволяет указать количество дней, которые могут пройти после того, как обновление предлагается устройству, прежде чем оно должно быть установлено. Кроме того, можно задать количество дней, которое может пройти после ожидающего перезапуска, прежде чем пользователь будет вынужден перезапустить.

Дополнительные сведения см. в статье Применение крайних сроков соответствия для обновлений.

Параметры конечных пользователей для уведомлений

Относится к:

- Windows 11 версии 23H2 с KB5037771 или более поздней
- Windows 11 версии 22H2 с KB5037771 или более поздней

Пользователи могут настроить параметры для уведомлений об ожидающих перезапусках обновлений в **разделе Параметры>клиентский компонент Центра обновления Windows>Добавить параметры>Уведомлять меня о необходимости перезапуска для**

завершения обновления. Этот параметр контролируется конечным пользователем и не контролируется и не настраивается ИТ-администраторами.

Для параметра **Уведомлять меня о необходимости перезагрузки для завершения обновления** у пользователей есть следующие параметры:

- **Отключено** (по умолчанию): после того как устройство перейдет в состояние ожидания перезагрузки для обновлений, уведомления о перезапуске отключаются в течение 24 часов. В течение первых 24 часов автоматические перезапуски по-прежнему могут происходить в нерабочее время. Как правило, пользователи получают меньше уведомлений о предстоящих перезапусках, пока приближается крайний срок.
  - Если крайний срок установлен на 1 день, пользователи получают уведомление о крайнем сроке и окончательное уведомление о неразглавлении за 15 минут до принудительного перезапуска.

- **Включено**. Пользователи немедленно получают всплывающее уведомление, когда устройство переходит в состояние ожидания перезагрузки для обновлений. Автоматические перезапуски обновлений блокируются в течение 24 часов после первоначального уведомления, чтобы дать этим пользователям время на подготовку к перезапуску. По истечении 24 часов может произойти автоматический перезапуск. Этот параметр рекомендуется для пользователей, которые хотят получать уведомления о предстоящих перезапусках.
  - Если крайний срок установлен на 1 день, возникает начальное уведомление, автоматический перезапуск блокируется в течение 24 часов, а пользователи получают еще одно уведомление до крайнего срока и окончательное уведомление о неразглавлении за 15 минут до принудительного перезапуска.

Если крайний срок установлен в течение 0 дней, независимо от выбранного параметра, единственным уведомлением, которое получают пользователи, является окончательное уведомление о неразглавлении за 15 минут до принудительного перезапуска.

Пользователь предпочитает уведомления, когда используются крайние сроки соответствия . Политика для крайних сроков соответствия требованиям находится в разделе **Конфигурация компьютера**>**Административные шаблоны**>**Компоненты**> Windows **клиентский компонент Центра обновления Windows**>**Назначить крайние сроки для автоматического обновления и перезапуска**.

- В Windows версии 22H2 и более поздних версиях политика **указать крайние сроки для автоматического обновления и перезапуска** разделена на две политики: **укажите крайний срок для автоматического обновления и перезапуска для обновления качества** и **укажите крайний срок для автоматического обновления и перезапуска для обновления компонентов**.

Я хочу управлять уведомлениями, которые видит пользователь

Существуют дополнительные параметры, влияющие на уведомления.

Рекомендуется использовать уведомления по умолчанию, так как они предназначены для предоставления наилучшего взаимодействия с пользователем при настройке настроенных политик соответствия. Если у вас есть дополнительные потребности, которые не удовлетворяются параметрами уведомлений по умолчанию, можно использовать **административные шаблоны** > **конфигурации** > **компьютера Компоненты** > **Windows клиентский компонент Центра обновления Windows** > **Параметры отображения для уведомлений об обновлении** со следующими значениями:

0 (по умолчанию) — используйте клиентский компонент Центра обновления Windows уведомления
по умолчанию **1** — отключить все уведомления, за исключением предупреждений о перезапуске
2 — отключить все уведомления, включая предупреждения о перезапуске.

Вариант **2** создает плохое взаимодействие с личными устройствами; Рекомендуется только для устройств киоска, на которых отключен автоматический перезапуск.

> ⓘ **Примечание.**
>
> Начиная с Windows 11 версии 22H2, в качестве дополнительных параметров для **отображения параметров уведомлений об обновлении** добавлен параметр **Применить только в часы активности**. Если выбран параметр **Применить только в часы активности** , уведомления будут отключены только в часы активности при использовании параметров `1` или `2` . Чтобы обеспечить обновление устройства, уведомление по-прежнему будет отображаться в часы активности, если выбран параметр **Применить только в часы активности** и после достижения крайнего срока при настройке **укажите крайние сроки для автоматического обновления и перезапуска** .

Дополнительные параметры доступны в разделе **Конфигурация** > **компьютера Административные шаблоны** > **Компоненты** > **Windows клиентский компонент Центра обновления Windows** > **Настройка автоматического перезапуска расписания предупреждений о перезапуске для обновлений**. Этот параметр позволяет указать период для уведомлений с напоминанием об автоматическом перезапуске (от 2 до 24 часов; по умолчанию — 4 часа) до обновления и указать период для автоматически перезапущенных уведомлений о неминуемых предупреждениях (по умолчанию — 15–60

минут). Рекомендуется использовать уведомления по умолчанию. Эта политика является устаревшей и неприменима для Windows 11. Устаревшие политики могут быть удалены в будущем выпуске.

Я хочу управлять параметрами обновления, к которым может получить доступ пользователь

Каждое устройство Windows предоставляет пользователям различные элементы управления, которые они могут использовать для управления Обновления Windows. Они могут получить доступ к этим элементам управления с помощью поиска, чтобы найти Обновления Windows или выбрав **Обновления и безопасность** в **разделе Параметры**. Мы предоставляем возможность отключить различные элементы управления, доступные для пользователей.

Пользователи с доступом к параметрам приостановки обновления могут запретить обновление компонентов и исправлений в течение 7 дней. Вы можете запретить пользователям приостановку обновлений на странице параметров клиентский компонент Центра обновления Windows с помощью административных **шаблонов >> конфигурации > компьютера Компоненты Windows клиентский компонент Центра обновления Windows > Удалить доступ к приостановке обновлений**. При отключении этого параметра пользователи увидят **, что некоторые параметры управляются вашей организацией** , а параметры приостановки обновления неактивны.

Если вы используете сервер обновления Windows Server (WSUS), вы можете запретить пользователям проверять клиентский компонент Центра обновления Windows. Для этого используйте административные **шаблоны > конфигурации > компьютера Компоненты > Windows клиентский компонент Центра обновления Windows > Удалить доступ, чтобы использовать все функции клиентский компонент Центра обновления Windows**.

Я хочу включить необязательные обновления

Относится к:

- Windows 11 версии 22H2 с KB5029351 и более поздними версиями
- Windows 10 версии 22H2 с KB5032278 или более поздним накопительным обновлением

Помимо ежемесячного накопительного обновления доступны необязательные обновления для предоставления новых функций и изменений, не относящихся к безопасности. Большинство необязательных обновлений выпускаются в четвертый вторник месяца, известный как необязательные предварительные выпуски, не связанные с безопасностью. Необязательные обновления также могут включать функции, которые

постепенно развертываются, известные как управляемые выпуски функций (CFR). Установка необязательных обновлений не включена по умолчанию для устройств, получающих обновления с помощью клиентский компонент Центра обновления Windows клиентских политик. Однако вы можете включить необязательные обновления для устройств с помощью административных **шаблонов > конфигурации > компьютера Компоненты > Windows клиентский компонент Центра обновления Windows > Управление обновлениями, предлагаемыми из клиентский компонент Центра обновления Windows > Включить необязательные обновления**.

Чтобы обеспечить согласованность времени обновления, политика **Включить необязательные обновления** учитывает период отсрочки для обновлений качества. Эта политика позволяет выбрать, должны ли устройства получать cfr в дополнение к дополнительным предварительным выпускам, не обеспечивающим безопасность, или пользователь может принять решение об установке необязательных обновлений. Эта политика может изменить поведение параметра **Получить последние обновления, как только они будут доступны** в **разделе Параметры**>**Обновление & безопасности**> *__клиентский компонент Центра обновления Windows__>**Добавить**.

Для политики доступны следующие параметры:

- **Автоматическое получение необязательных обновлений (включая cfr)**:
  - На устройстве автоматически устанавливаются последние необязательные обновления, не связанные с безопасностью, и cfR. Период отсрочки обновления качества применяется к установке этих обновлений.
  - Выбран параметр **Получить последние обновления, как только они будут доступны** , и пользователи не могут изменить параметр.
  - Устройства будут получать cfr на ранних этапах развертывания.

- **Автоматически получать необязательные обновления**:
  - Последние необязательные обновления, не связанные с безопасностью, устанавливаются на устройство автоматически, но cfr — нет. Период отсрочки обновления качества применяется к установке этих обновлений.
  - Параметр **Получить последние обновления, как только они будут доступны** , не выбран и пользователи не могут изменить параметр.

- **Пользователи могут выбрать, какие необязательные обновления следует получать**:
  - Пользователи могут выбрать, какие необязательные обновления следует установить, в **разделе Параметры**>**Обновление & безопасности**>**клиентский компонент Центра обновления Windows**>**Добавить параметры**>**Необязательные обновления**.

    - На устройстве предлагаются необязательные обновления, но для их установки требуется взаимодействие с пользователем, если не включен параметр **Получить последние обновления сразу после их доступности** .
    - CfR предлагаются устройству, но не обязательно на ранних этапах развертывания.
  - Пользователи могут включить параметр **Получать последние обновления, как только они будут доступны** в **разделе Параметры**>**Обновление & безопасности**> ***клиентский компонент Центра обновления Windows**>**Добавить параметры**. Если пользователь включает **получение последних обновлений, как только они будут доступны**, то:
    - Устройство будет получать cfr на ранних этапах развертывания.
    - На устройстве автоматически устанавливаются необязательные обновления.

- **Не настроено** (по умолчанию):
  - Необязательные обновления не устанавливаются на устройстве, и параметр **Получить последние обновления, как только они будут доступны** , отключен.

Я хочу включить функции, представленные через обслуживание, которые отключены по умолчанию

(*Начиная с Windows 11 версии 22H2 или более поздней*)

Новые функции и улучшения представлены в ежемесячном накопительном пакете обновления для обеспечения постоянных инноваций для Windows 11. Чтобы дать организациям время для планирования и подготовки, некоторые из этих новых функций временно отключены по умолчанию. Функции, отключенные по умолчанию, перечислены в статье базы знаний ежемесячного накопительного пакета обновления. Как правило, функция по умолчанию отключена, поскольку она существенно влияет либо на работу пользователей, либо на ИТ-администраторов.

Функции, отключенные по умолчанию от обслуживания обновлений, будут включены в следующем ежегодном обновлении компонентов. Организации могут развертывать обновления компонентов в своем собственном темпе, чтобы отложить эти функции, пока они не будут готовы к ним.

Эти функции можно включить с помощью **административных шаблонов > конфигурации > компьютера Компоненты > Windows клиентский компонент Центра обновления Windows > Управление взаимодействием > с конечными пользователями. Включить функции, представленные через обслуживание, которые по умолчанию отключены**. Доступны следующие варианты:

- **Включено**: включены все функции в последнем ежемесячном накопительном обновлении.
  - Если для политики задано значение **Включено**, все функции, которые сейчас отключены, будут включены при следующей перезагрузке устройства.
- **Отключено** — функции, отключаемые по умолчанию, останутся отключенными
- **Не настроено** — функции, отключаемые по умолчанию, останутся отключенными

Last updated on 26.09.2025

Пошаговое руководство. Настройка политик клиентский компонент Центра обновления Windows клиентов с помощью поставщиков облачных служб и MDM

Применяется к: ✅ Windows 11, ✅ Windows 10

> **Ищете информацию для потребителей?** См. раздел клиентский компонент Центра обновления Windows: вопросы и ответы.

Обзор

Политики поставщика служб конфигурации (CSP) можно использовать для управления работой клиентский компонент Центра обновления Windows клиентских политик с помощью средства мобильной Управление устройствами (MDM). Прежде чем вносить изменения в клиентский компонент Центра обновления Windows клиентские политики, следует рассмотреть и разработать стратегию развертывания обновлений.

> **Совет**
>
> Эта функция ранее называлась *клиентский компонент Центра обновления Windows для бизнеса*.

ИТ-администратор может настроить политики клиентов клиентский компонент Центра обновления Windows с помощью Microsoft Intune или средства MDM сторонних специалистов.

Чтобы управлять обновлениями с помощью клиентский компонент Центра обновления Windows клиентских политик, следует подготовиться к следующим действиям, если это еще не сделано:

- Создайте группы безопасности Active Directory, которые соответствуют кругам развертывания, используемым для поэтапного развертывания обновлений. Дополнительные сведения о кругах развертывания в клиенте Windows см. в статье Создание кругов развертывания для обновлений клиента Windows .
- Разрешить доступ к службе клиентский компонент Центра обновления Windows.

Управление предложениями клиентский компонент Центра обновления Windows

Вы можете управлять применением обновлений, например путем отсрочки установки обновления на устройстве или путем приостановки обновлений на определенный период времени.

Определите, какие обновления вы хотите предложить для устройств

Обновления компонентов и исправлений автоматически предлагаются устройствам, подключенным к клиентский компонент Центра обновления Windows с помощью клиентский компонент Центра обновления Windows клиентских политик. Однако вы можете выбрать, будут ли устройства дополнительно получать другие Обновления Майкрософт или драйверы, применимые к такому устройству.

Чтобы включить Microsoft Обновления, используйте Update/AllowMUUpdateService.

Драйверы включаются автоматически, так как они полезны для систем устройств. Рекомендуется разрешить политике драйверов обновлять драйверы на устройствах (по умолчанию), но этот параметр можно отключить, если вы предпочитаете управлять драйверами вручную. Если вы хотите по какой-либо причине отключить обновления драйверов, используйте Update/ExcludeWUDriversInQualityUpdate.

Мы также рекомендуем разрешить обновления продуктов Майкрософт, как обсуждалось ранее.

Установка, когда устройства получают обновления компонентов и качества

Я хочу получить предварительные версии следующего обновления компонентов

1. Убедитесь, что вы зарегистрированы в программе предварительной оценки Windows для бизнеса. Программа предварительной оценки Windows — это бесплатная программа, доступная для коммерческих клиентов, которая поможет им в проверке обновлений компонентов перед выпуском. Присоединение к программе позволяет получать обновления до их выпуска, а также получать сообщения электронной почты и содержимое, связанное с тем, что ожидается в следующих обновлениях.

2. Для любого из тестовых устройств, которые требуется установить предварительные сборки, используйте Update/ManagePreviewBuilds. Установите параметр **Включить предварительные сборки**.

3. Используйте Update/BranchReadinessLevel и выберите одну из предварительных сборок. Программа предварительной оценки Windows Slow — это рекомендуемый канал для коммерческих клиентов, которые используют предварительные сборки для проверки.

4. Кроме того, вы можете отложить предварительные обновления компонентов так же, как и выпущенные обновления, установив период отсрочки до 14 дней с помощью update/DeferFeatureUpdatesPeriodInDays. Если вы тестируете с помощью медленных сборок программы предварительной оценки Windows, мы рекомендуем получать предварительные обновления в ИТ-отдел на 0-й день выпуска обновления, а затем иметь отсрочку на 7–10 дней перед развертыванием для группы тестировщиков. Это расписание гарантирует, что при обнаружении проблемы можно приостановить развертывание предварительной версии обновления до того, как оно достигнет тестов.

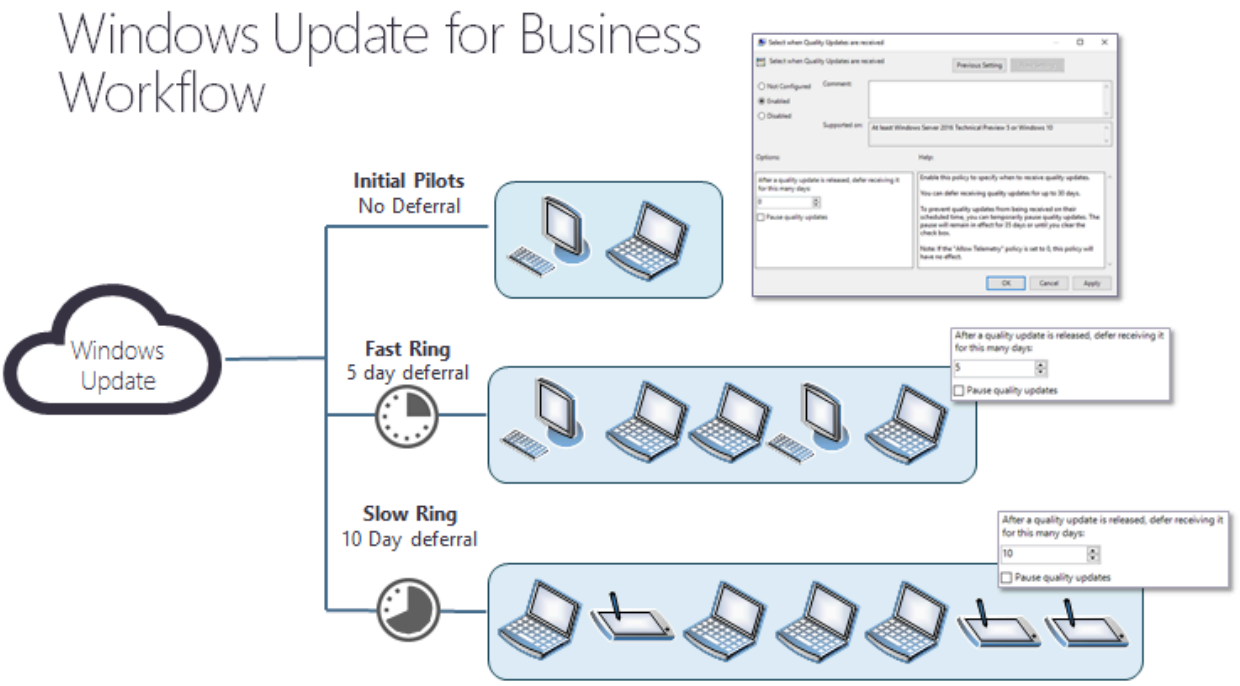
Я хочу управлять выпущенными обновлениями компонентов, которые получают мои устройства

Администратор клиентский компонент Центра обновления Windows может отложить или приостановить обновления. Обновления компонентов можно отложить до 365 дней, а обновления качества — до 30 дней. Отсрочка просто означает, что вы не получите обновление, пока оно не будет выпущено по крайней мере на указанное количество дней отсрочки (дата предложения = дата выпуска + дата отсрочки). Обновления компонентов или исправлений можно приостановить на срок до 35 дней с указанной даты начала.

- Чтобы отложить обновление компонентов: Update/DeferFeatureUpdatesPeriodInDays
- Приостановка обновления компонентов: Update/PauseFeatureUpdatesStartTime
- Чтобы отложить обновление качества: Update/DeferQualityUpdatesPeriodInDays
- Приостановка обновления качества: Update/PauseQualityUpdatesStartTime

Пример

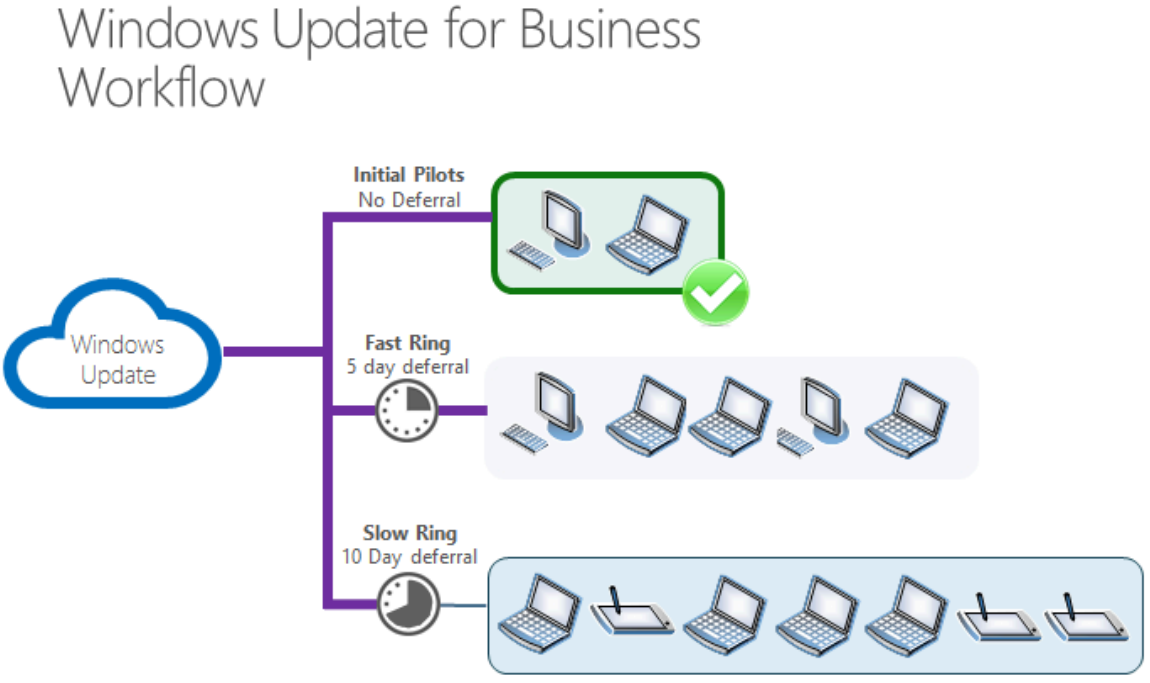
В этом примере есть три круга для обновления качества. Первый круг ("пилотный") имеет период отсрочки в 0 дней. Второе кольцо ("быстрый") имеет отсрочку в пять дней. Третье кольцо ("медленно") имеет отсрочку в десять дней.



После выпуска обновления качества оно предлагается устройствам в пилотном кольце при следующем сканировании обновлений.

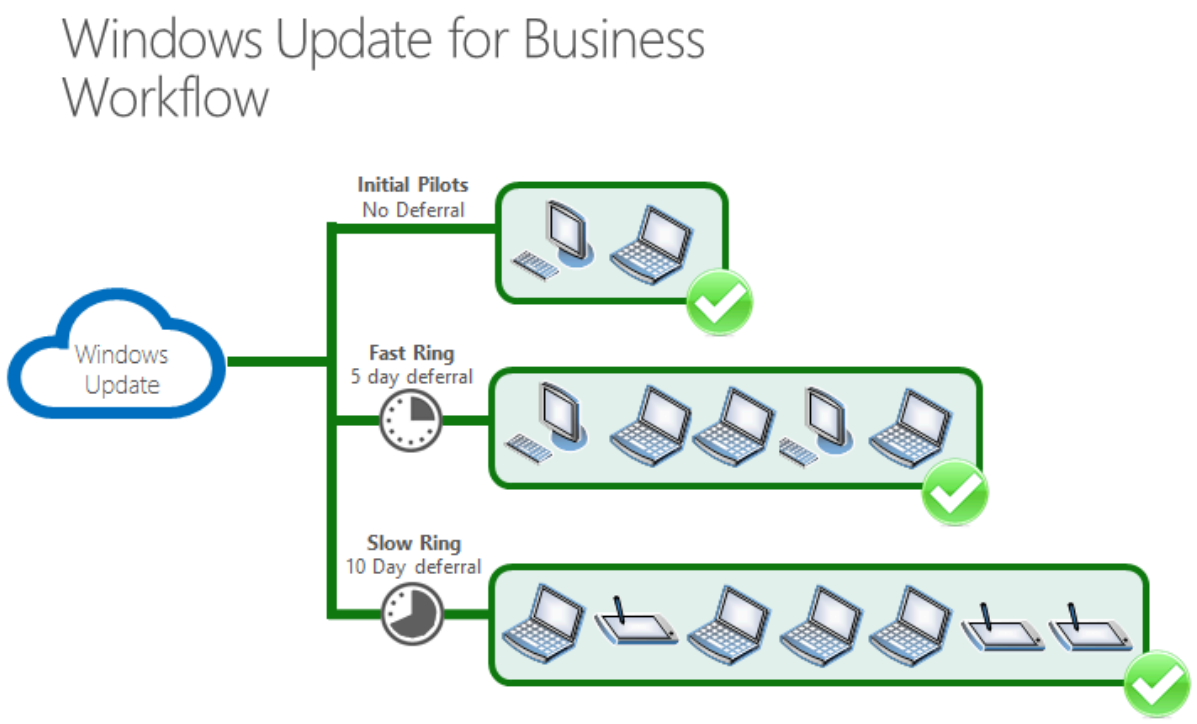
Пять дней спустя

Устройствам в быстром кольце предлагается обновление качества при следующем сканировании обновлений.



Десять дней спустя

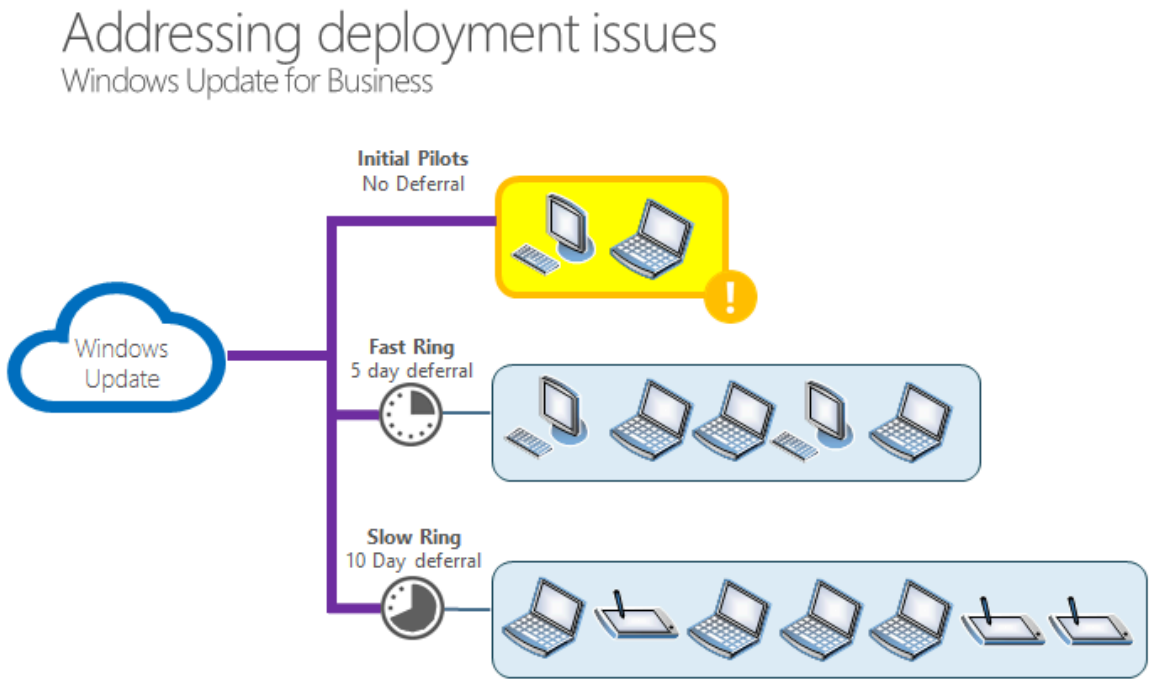
Через десять дней после выпуска обновления качества оно предлагается устройствам в медленном кольце при следующем сканировании обновлений.



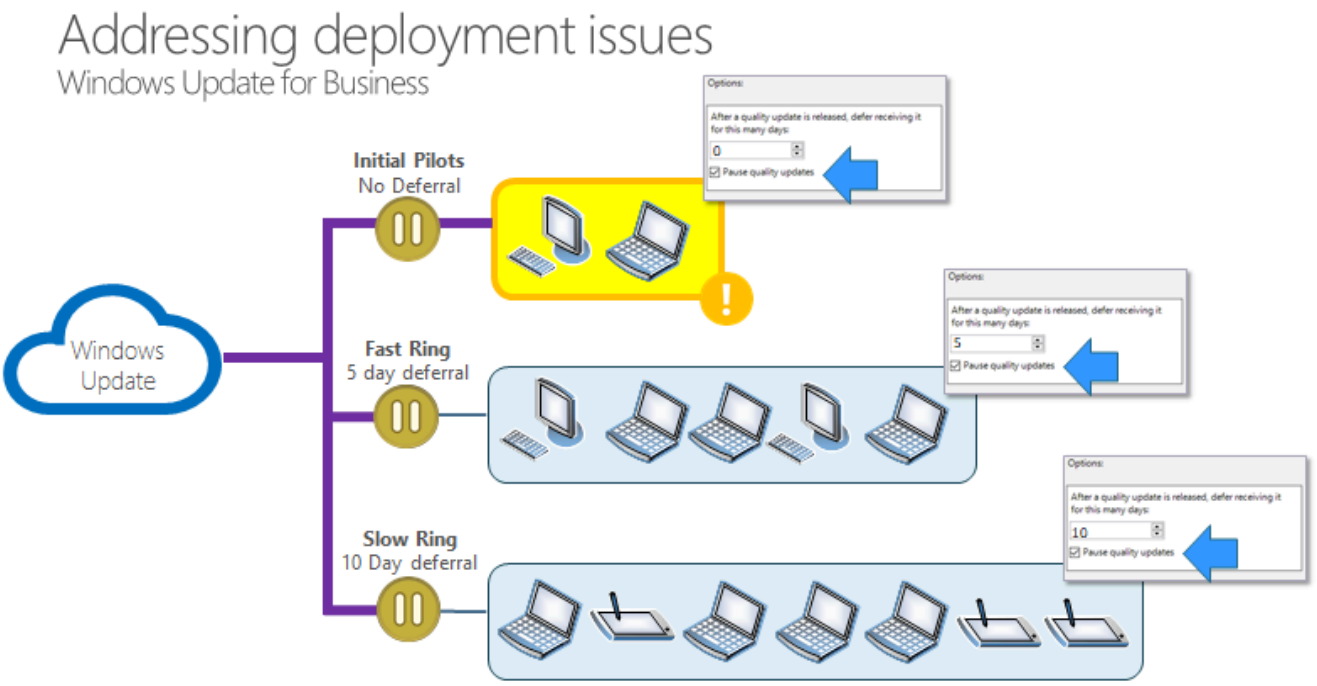
Если проблем не возникает, всем устройствам, проверяющим наличие обновлений, предлагается обновление качества в течение десяти дней после выпуска в три волны.

Что делать, если с обновлением возникает проблема?

В этом примере обнаружена некоторая проблема при развертывании обновления в "пилотном" круге.



На этом этапе ИТ-администратор может задать политику для приостановки обновления. В этом примере администратор выбирает поле **Приостановить обновления качества** проверка.



Теперь обновление всех устройств приостановлено в течение 35 дней. Когда пауза будет удалена, им будет предложено *следующее* обновление качества, которое в идеале не будет иметь той же проблемы. Если проблема по-прежнему возникает, ИТ-администратор может снова приостановить обновления.

Я хочу остаться на определенной версии

Если вам нужно, чтобы устройство оставалось на версии за пределами того момента, когда будут продолжаться отсрочки для следующей версии или если вам нужно пропустить версию (например, обновление осенью выпуска до падающего выпуска), используйте Update/TargetReleaseVersion (или Развертывание Обновления предварительной версии компонента в Intune) вместо отсрочки обновления компонентов. При использовании этой политики укажите версию, к которой требуется переместить устройства или остаться в ней (например, "1909"). Сведения о версии можно найти на странице сведений о выпуске Windows 10.

Управление обновлениями для пользователей

Я хочу управлять загрузкой, установкой и перезапуском устройств после обновлений

Рекомендуется разрешить автоматическое обновление, что является поведением по умолчанию. Если политика автоматического обновления не настроена, устройство пытается скачать, установить и перезапустить в лучшее для пользователя время с помощью встроенной логики, например интеллектуальных часов активности.

Для более детального управления можно задать максимальный период активности, который пользователь может задать с помощью update/ActiveHoursMaxRange. Вы также можете задать определенное время начала и окончания для активной работы с помощью Update/ActiveHoursEnd и Update/ActiveHoursStart.

Рекомендуется воздерживаться от настройки политики активных часов, так как она включена по умолчанию, когда автоматическое обновление не отключено, и обеспечивает более удобный интерфейс, когда пользователи могут задавать собственные часы активности.

Чтобы выполнить обновление в нерабочее время, используйте команду Update/AllowAutoUpdate с параметром 2 (который является параметром по умолчанию). Для более детального управления рекомендуется использовать автоматические обновления для планирования времени установки, дня или недели. Чтобы использовать расписание, используйте вариант 3, а затем задайте следующие политики, соответствующие вашему плану:

- Update/ScheduledInstallDay
- Update/ScheduledInstallEveryWeek
- Update/ScheduledInstallFirstWeek
- Update/ScheduledInstallFourthWeek
- Update/ScheduledInstallSecondWeek
- Update/ScheduledInstallThirdWeek
- Update/ScheduledInstallTime

При настройке этих политик установка происходит автоматически в указанное время, и устройство перезапустится через 15 минут после завершения установки (если она не была прервана пользователем).

Если вы не хотите разрешать автоматическое обновление до крайнего срока, установите для параметра Update/AllowAutoUpdate значение Параметр 5, который отключает автоматическое обновление.

Я хочу обеспечить безопасность устройств и соответствие крайним срокам обновления

Рекомендуется установить определенные крайние сроки для обновлений компонентов и качества, чтобы обеспечить безопасность устройств в Windows 10 версии 1709 и более поздних. Крайние сроки работают, позволяя указать количество дней, которые могут пройти после того, как обновление предлагается устройству до его установки. Кроме того, можно задать количество дней, которое может пройти после ожидающего перезапуска, прежде чем пользователь будет вынужден перезапустить. Дополнительные сведения об этих параметрах см. в разделе Применение крайних сроков соответствия для обновлений. Следующие параметры применяют крайние сроки соответствия для обновлений:

Для Windows 10 версии 22H2:

- Update/ConfigureDeadlineForFeatureUpdates
- Update/ConfigureDeadlineForQualityUpdates
- Update/ConfigureDeadlineGracePeriod
- Update/ConfigureDeadlineGracePeriodForFeatureUpdates
- Обновление и настройкаDeadlineNoAutoReboot

Для Windows 11 версии 22H2 и более поздних:

- Update/ConfigureDeadlineForFeatureUpdates
- Update/ConfigureDeadlineForQualityUpdates
- Update/ConfigureDeadlineGracePeriod (для обновлений качества)
- Update/ConfigureDeadlineGracePeriodForFeatureUpdates
- Update/ConfigureDeadlineNoAutoRebootForQualityUpdates
- Update/ConfigureDeadlineNoAutoRebootForFeatureUpdates

> ⓘ **Примечание.**
>
> - При использовании этих политик **пользовательские параметры уведомлений** также используются на клиентах под управлением Windows 11 версии 22H2 и более поздних.
> - При **использовании параметра Укажите крайние сроки для автоматических обновлений и перезапусков** для обновлений качества или компонентов обновления обновления будут загружаться и устанавливаться сразу после их предложения.
> - При **использовании указания крайних сроков для автоматических обновлений и перезапусков** для обновлений качества или обновлений компонентов параметры скачивания, установки и перезагрузки, вытекающие из **параметра Настройка автоматического Обновления**, игнорируются.

- Начиная с обновления от 10 декабря 2024 г. для клиентов Windows 11 версии 22H2 и более поздних версий настройка автоматического Обновления соблюдается до наступления крайнего срока и игнорируется после истечения крайнего срока.

Параметры конечных пользователей для уведомлений

Относится к:

- Windows 11 версии 23H2 с KB5037771 или более поздней
- Windows 11 версии 22H2 с KB5037771 или более поздней

Пользователи могут настроить параметры для уведомлений об ожидающих перезапусках обновлений в **разделе Параметры**>**клиентский компонент Центра обновления Windows**>**Добавить параметры**>**Уведомлять меня о необходимости перезапуска для завершения обновления**. Этот параметр контролируется конечным пользователем и не контролируется и не настраивается ИТ-администраторами.

Для параметра **Уведомлять меня о необходимости перезагрузки для завершения обновления** у пользователей есть следующие параметры:

- **Отключено** (по умолчанию): после того как устройство перейдет в состояние ожидания перезагрузки для обновлений, уведомления о перезапуске отключаются в течение 24 часов. В течение первых 24 часов автоматические перезапуски по-прежнему могут происходить в нерабочее время. Как правило, пользователи получают меньше уведомлений о предстоящих перезапусках, пока приближается крайний срок.
  - Если крайний срок установлен на 1 день, пользователи получают уведомление о крайнем сроке и окончательное уведомление о неразглавлении за 15 минут до принудительного перезапуска.

- **Включено**. Пользователи немедленно получают всплывающее уведомление, когда устройство переходит в состояние ожидания перезагрузки для обновлений. Автоматические перезапуски обновлений блокируются в течение 24 часов после первоначального уведомления, чтобы дать этим пользователям время на подготовку к перезапуску. По истечении 24 часов может произойти автоматический перезапуск. Этот параметр рекомендуется для пользователей, которые хотят получать уведомления о предстоящих перезапусках.
  - Если крайний срок установлен на 1 день, возникает начальное уведомление, автоматический перезапуск блокируется в течение 24 часов, а пользователи

получают еще одно уведомление до крайнего срока и окончательное уведомление о неразглавлении за 15 минут до принудительного перезапуска.

Если крайний срок установлен в течение 0 дней, независимо от выбранного параметра, единственным уведомлением, которое получают пользователи, является окончательное уведомление о неразглавлении за 15 минут до принудительного перезапуска.

Предпочтения пользователей для уведомлений применяются, если используются следующие политики для крайних сроков соответствия :

Для Windows 10 версии 22H2:

- Update/ConfigureDeadlineForFeatureUpdates
- Update/ConfigureDeadlineForQualityUpdates
- Update/ConfigureDeadlineGracePeriod
- Update/ConfigureDeadlineGracePeriodForFeatureUpdates
- Обновление и настройкаDeadlineNoAutoReboot

Для Windows 11 версии 22H2 и более поздних:

- Update/ConfigureDeadlineForFeatureUpdates
- Update/ConfigureDeadlineForQualityUpdates
- Update/ConfigureDeadlineGracePeriod (для обновлений качества)
- Update/ConfigureDeadlineGracePeriodForFeatureUpdates
- Update/ConfigureDeadlineNoAutoRebootForQualityUpdates
- Update/ConfigureDeadlineNoAutoRebootForFeatureUpdates

Я хочу управлять уведомлениями, которые видит пользователь

Существуют дополнительные параметры, влияющие на уведомления.

Рекомендуется использовать уведомления по умолчанию, так как они предназначены для предоставления наилучшего взаимодействия с пользователем при настройке заданных политик соответствия. Если у вас есть дополнительные потребности, которые не удовлетворяются параметрами уведомлений по умолчанию, можно использовать политику Update/NoUpdateNotificationsDuringActiveHours со следующими значениями:

0 (по умолчанию) — используйте уведомления по умолчанию клиентский компонент Центра обновления Windows
1 . Отключение всех уведомлений, за исключением предупреждений о перезапуске
2 . Отключение всех уведомлений, включая предупреждения о перезапуске

> ⓘ **Примечание.**
>
> Вариант **2** создает плохое взаимодействие с личными устройствами; Рекомендуется только для устройств киоска, на которых отключен автоматический перезапуск.

Дополнительные параметры доступны в разделе Update/ScheduleRestartWarning. Эта политика является устаревшей и неприменима для Windows 11. Устаревшие политики могут быть удалены в будущем выпуске. Этот параметр позволяет указать период для уведомлений с напоминанием об автоматическом перезапуске (от 2 до 24 часов; по умолчанию — 4 часа) до обновления. Вы также можете указать период для автоматического перезапуска оповещений о неминуемом предупреждении с помощью команды Update/ScheduleImminentRestartWarning (по умолчанию — 15–60 минут). Рекомендуется использовать уведомления по умолчанию. Эта политика является устаревшей и неприменима для Windows 11. Устаревшие политики могут быть удалены в будущем выпуске.

Я хочу управлять параметрами обновления, к которым может получить доступ пользователь

Каждое устройство Windows предоставляет пользователям различные элементы управления, которые они могут использовать для управления Обновления Windows. Они могут получить доступ к этим элементам управления с помощью поиска, чтобы найти Обновления Windows или выбрав **Обновления и безопасность** в **разделе Параметры**. Мы предоставляем возможность отключить различные элементы управления, доступные для пользователей.

Пользователи с доступом к параметрам приостановки обновления могут запретить обновление компонентов и исправлений в течение 7 дней. Вы можете запретить пользователям приостановку обновлений на странице параметров клиентский компонент Центра обновления Windows с помощью Update/SetDisablePauseUXAccess. При отключении этого параметра пользователи увидят **, что некоторые параметры управляются вашей организацией** , а параметры приостановки обновления неактивны.

Если вы используете сервер обновления Windows Server (WSUS), вы можете запретить пользователям проверять клиентский компонент Центра обновления Windows. Для этого используйте Update/SetDisableUXWUAccess.

Я хочу включить функции, представленные через обслуживание, которые отключены по умолчанию

(*Начиная с Windows 11 версии 22H2 или более поздней*)

Новые функции и улучшения представлены в ежемесячном накопительном пакете обновления для обеспечения постоянных инноваций для Windows 11. Чтобы дать организациям время для планирования и подготовки, некоторые из этих новых функций временно отключены по умолчанию. Функции, отключенные по умолчанию, перечислены в статье базы знаний ежемесячного накопительного пакета обновления. Как правило, функция по умолчанию отключена, поскольку она существенно влияет либо на работу пользователей, либо на ИТ-администраторов.

Функции, отключенные по умолчанию от обслуживания обновлений, будут включены в следующем ежегодном обновлении компонентов. Организации могут развертывать обновления компонентов в своем собственном темпе, чтобы отложить эти функции, пока они не будут готовы к ним.

Эти функции можно включить с помощью AllowTemporaryEnterpriseFeatureControl. Доступны следующие варианты:

- **0** (по умолчанию): запрещено. Функции, отключаемые по умолчанию, останутся отключенными
- **1**: разрешено. Включены все функции в последнем ежемесячном накопительном обновлении.
  - Если для политики задано значение **1**, все функции, которые сейчас отключены, будут включены при следующей перезагрузке устройства.

Я хочу включить необязательные обновления

Относится к:

- Windows 11 версии 22H2 с KB5029351 и более поздними версиями
- Windows 10 версии 22H2 с KB5032278 или более поздним накопительным обновлением

Помимо ежемесячного накопительного обновления доступны необязательные обновления для предоставления новых функций и изменений, не относящихся к безопасности. Большинство необязательных обновлений выпускаются в четвертый вторник месяца, известный как необязательные предварительные выпуски, не связанные с безопасностью. Необязательные обновления также могут включать функции, которые постепенно развертываются, известные как управляемые выпуски функций (CFR). Установка необязательных обновлений не включена по умолчанию для устройств, получающих обновления с помощью клиентский компонент Центра обновления Windows клиентских политик. Однако можно включить необязательные обновления для устройств

с помощью AllowOptionalContent. Дополнительные сведения о необязательном содержимом см. в разделе Включение необязательных обновлений.

Last updated on 18.03.2025

Активация подписки Windows

Применяется к: ✅ Windows 11, ✅ Windows 10

Функция активации подписки позволяет переходить от выпуска Windows Pro к выпуску Enterprise или с Windows Pro для образовательных учреждений. Эту функцию можно использовать с подпиской на лицензии Windows Корпоративная E3 или E5.

> **Совет**
>
> Windows Pro для образовательных учреждений аналогит Windows Pro, а Windows для образовательных учреждений — Windows Enterprise. Другими словами, Windows для образовательных учреждений — это шаг от Windows Pro для образовательных учреждений, аналогично тому, как Windows Корпоративная — это шаг от Windows Pro.

Функция активации подписки устраняет необходимость вручную развертывать образы выпусков Enterprise или Education на каждом целевом устройстве, а затем позже:

- Создание локальных служб управления ключами, таких как KMS или активация на основе MAK.
- Ввод универсальных ключей корпоративной лицензии (GVLK).
- Перезагрузка клиентских устройств.

Дополнительные сведения о развертывании корпоративных лицензий см. в разделе Развертывание лицензий Windows Enterprise.

Активация подписки для Enterprise

Windows Корпоративная E3 и E5 доступна в виде веб-службы по подписке. Windows Enterprise можно развернуть в организации без ключей и перезагрузок.

- Устройства с текущей лицензией на выпуск Windows Pro можно легко обновить до Windows Enterprise.
- Лицензии программного обеспечения Windows Enterprise на основе ключа продукта можно перенести в подписки Windows Enterprise.

Организации с соглашением Enterprise также могут воспользоваться этой службой, используя традиционные устройства, присоединенные к Active Directory. В этом сценарии пользователь Active Directory, выполняющий вход на своем устройстве, должен быть синхронизирован с Microsoft Entra ID с помощью Microsoft Entra Connect Sync.

> ⓘ **Примечание.**
>
> Активация подписки доступна для соответствующих устройств под управлением поддерживаемых в настоящее время версий Windows. Активацию подписки нельзя использовать для обновления до более новой версии Windows.

Добавление политики условного доступа

Организациям, которые используют функцию активации подписки, чтобы пользователи могли "переходить" из одной версии Windows в другую и использовать политики условного доступа для управления доступом, должны исключить одно из следующих облачных приложений из своих политик условного доступа с помощью **выбора исключенных облачных приложений**:

- API-интерфейсы службы Универсального магазина и веб-приложение, AppID 45a330b1-b1ec-4cc1-9161-9f03992aa49f.
- Магазин Windows для бизнеса, AppID 45a330b1-b1ec-4cc1-9161-9f03992aa49f.

  > ⓘ **Примечание.**
  >
  > Microsoft Store для бизнеса и Microsoft Store для образования стираются. Дополнительные сведения см. в разделе Microsoft Store для бизнеса и 31 марта 2023 г.

Хотя идентификатор приложения одинаков в обоих экземплярах, имя облачного приложения зависит от клиента.

Дополнительные сведения о настройке исключений в политиках условного доступа см. в разделе Исключения приложений.

Если устройство находится в автономном режиме в течение длительного периода времени, оно может не активироваться автоматически, если это исключение условного доступа отсутствует. Установка этого исключения условного доступа гарантирует, что активация подписки продолжит работать без проблем.

Начиная с Windows 11 версии 23H2 с KB5034848 или более поздней, пользователи получают запрос на проверку подлинности с всплывающее уведомление, когда активация подписки требуется повторно активировать. Всплывающее уведомление отобразит следующее сообщение:

> **Для учетной записи требуется проверка подлинности**
>
> **Войдите в рабочую или учебную учетную запись, чтобы проверить свои данные.**

Кроме того, в области **Активация** может появиться следующее сообщение:

> **Войдите в рабочую или учебную учетную запись, чтобы проверить свои данные.**

Запрос на проверку подлинности обычно возникает, когда устройство находится в автономном режиме в течение длительного периода времени. Это изменение устраняет необходимость в исключении в политике условного доступа для Windows 11 версии 23H2 с KB5034848 или более поздней. Политику условного доступа по-прежнему можно использовать с Windows 11 версии 23H2 с KB5034848 или более поздней, если запрос на проверку подлинности пользователя через всплывающее уведомление не требуется.

Активация подписки для образовательных учреждений

Активация подписки для образовательных учреждений работает так же, как и выпуск Enterprise. Тем не менее, чтобы использовать активацию подписки для образовательных учреждений, устройство должно иметь Windows Pro для образовательных учреждений и активный план подписки с лицензией Enterprise. Дополнительные сведения см. в разделе требований .

Наследование активаций

Унаследованная активация позволяет виртуальным машинам Windows наследовать состояние активации от узла клиента Windows. Когда пользователь с назначенной лицензией Windows E3/E5 или A3/A5 создает новую виртуальную машину Windows с помощью узла Windows, виртуальная машина наследует состояние активации от хост-компьютера. Это не зависит от того, входит ли пользователь с локальной учетной записью или использует учетную запись Microsoft Entra на виртуальной машине.

Для поддержки унаследованной активации главный компьютер и виртуальная машина должны работать под управлением поддерживаемой в настоящее время версии Windows. Платформа гипервизора также должна быть Windows Hyper-V.

Требования

Требования к Windows Enterprise

Для клиентов Майкрософт с Соглашениями Enterprise (EA) или Соглашениями о продуктах Майкрософт & службами (MPSA) должны соблюдаться следующие требования:

- Поддерживаемая версия выпуска Windows Pro или Enterprise, установленная на обновляемых устройствах.
- Microsoft Entra доступны для управления удостоверениями.
- Устройства должны быть Microsoft Entra присоединены или Microsoft Entra гибридное присоединение. Присоединенные к рабочей группе или Microsoft Entra зарегистрированные устройства не поддерживаются.

Для клиентов Майкрософт, у которых нет лицензий EA или MPSA, windows Enterprise E3/E5 или A3/A5 можно получить через поставщика облачных решений (CSP). При использовании CSP для управления лицензиями требования к управлению удостоверениями и устройствам одинаковы. Дополнительные сведения о получении Windows Enterprise E3 через CSP см. в статье Windows Корпоративная E3 в CSP.

> ⓘ **Примечание.**
>
> Эти требования не применяются к общей активации клиента Windows в Azure. Для активации Azure требуется только подключение к Azure KMS. Azure KMS поддерживает виртуальные машины, присоединенные к рабочей группе, гибридные и Microsoft Entra. В большинстве сценариев активация виртуальных машин Azure выполняется автоматически. Дополнительные сведения см. в статье **Общие сведения о конечных точках Azure KMS для активации продуктов Windows на виртуальных машинах Azure**.

> ⓘ **Внимание**
>
> С 1 октября 2022 г. активация подписки доступна для *коммерческих* клиентов и клиентов *GCC* . В настоящее время он недоступен для клиентов GCC High или DoD. Дополнительные сведения см. в разделе **Включение активации подписки с помощью существующего ea**.

Требования к Windows для образовательных учреждений

- Поддерживаемая версия Windows Pro для образовательных учреждений, установленная на обновляемых устройствах.

- Устройство с цифровой лицензией Windows Pro для образовательных учреждений. Эти сведения можно подтвердить на панели **Активация**приложения **"Параметры"** в разделе **Параметры > Активация системы>**.
- Клиент для образовательных учреждений должен иметь активную подписку на Microsoft 365 с лицензией Windows Корпоративная или Windows Корпоративная или Подписка для образовательных учреждений.
- Устройства должны быть Microsoft Entra присоединены или Microsoft Entra гибридное присоединение. Присоединенные к рабочей группе или Microsoft Entra зарегистрированные устройства не поддерживаются.

> **Внимание**
>
> Если Windows Pro преобразуется в Windows Pro для образовательных учреждений, активация подписки не работает. Чтобы активация подписки работала, необходимо переимыслить устройство в Windows Pro для образовательных учреждений. Кроме того, можно переименовать имя устройства непосредственно в Windows для образовательных учреждений.

Преимущества

С выпусками Windows Корпоративная или Windows для образовательных учреждений организация может воспользоваться преимуществами безопасности и контроля корпоративного уровня. Ранее только организации с соглашением о корпоративном лицензировании Майкрософт могли развертывать выпуски для образовательных учреждений или корпоративных выпусков для своих пользователей. Так как Windows Корпоративная E3/E5 или A3/A5 доступна в виде веб-службы, она доступна в некоторых каналах, что позволяет всем организациям воспользоваться преимуществами функций Windows корпоративного уровня.

Чтобы сравнить выпуски Windows и просмотреть цены, ознакомьтесь со следующими сайтами:

- Сравнение выпусков Windows
- Цены на Enterprise Mobility + Security.

Преимущества перехода на Windows в качестве веб-службы:

- Лицензии для Windows Корпоративная и для образовательных учреждений проверяются на основе Microsoft Entra учетных данных. Существует систематический способ назначения лицензий конечным пользователям и группам в организации.

- При входе пользователя запускается автоматическое обновление выпуска без необходимости перезагрузки.
- Поддержка мобильных рабочих ролей и активации "Принеси свое устройство" (BYOD) или "Выберите свое устройство" (CYOD). Эта поддержка поддерживает переход от локальных ключей KMS и MAK.
- Поддержка соответствия требованиям через назначение лицензии.
- Лицензии можно динамически обновлять для разных пользователей, что позволяет оптимизировать инвестиции в лицензирование с учетом меняющихся потребностей.

Принцип работы

Устройство Microsoft Entra присоединено, например из области Доступ к рабочей или учебной области в приложении **Параметры**, которую можно найти в разделе **Параметры**>**Учетные**> записи**Доступ к рабочей или учебной работе.**

Windows Корпоративная назначается пользователю, например через Центр администрирования Microsoft 365. Когда лицензированный пользователь входит на устройство, которое соответствует требованиям, используя свои учетные данные Microsoft Entra, Windows выполняет переход с pro edition на enterprise или с Pro для образовательных учреждений на образовательный. После активизации выпуска функции enterprise/education будут разблокированы. Когда срок действия подписки пользователя истек или передается другому пользователю, устройство плавно переходит к Выпуску Windows Pro или Windows Pro для образовательных учреждений по истечении срока действия текущей подписки.

> ⓘ **Примечание.**
>
> - Устройства под управлением поддерживаемой версии Windows Pro могут получить канал общей доступности Windows Enterprise на пяти устройствах для каждого пользователя, на который распространяется лицензия. Это ограничение также применяется при переходе из Windows Pro для образовательных учреждений в Windows для образовательных учреждений. Это преимущество не включает долгосрочный канал обслуживания.
> - Устройство Windows Pro выполняется до выпуска Windows Enterprise только в том случае, если лицензия **Windows Enterprise** назначена из Центр администрирования Microsoft 365.

- На устройстве Windows Pro для образовательных учреждений только до выпуска Windows для образовательных учреждений лицензия **Windows Корпоративная** назначается из Центр администрирования Microsoft 365.

Сценарии

Сценарий 1

Используется поддерживаемая версия Windows. Приобретена подписка на Windows Корпоративная E3 или E5, либо есть существующая подписка E3 или E5, но Windows Корпоративная еще не развернута.

Все устройства Windows Pro шаг до Windows Enterprise. Когда пользователь с поддержкой активации подписки входит в систему, устройства, уже работающие под управлением Windows Enterprise, переходят из выпуска ENTERPRISE, активированного KMS или MAK, на выпуск Enterprise, активированный подпиской.

Сценарий 2

Microsoft Entra используются устройства, присоединенные к Active Directory, под управлением поддерживаемой версии Windows. Microsoft Entra синхронизация настроена. Действия, описанные в разделе Развертывание лицензий Windows Enterprise, выполняются, чтобы получить номер SKU в размере 0 долл. США и новую лицензию Windows Корпоративная E3 или E5 в Microsoft Entra ID. Затем лицензия назначается всем пользователям Microsoft Entra, которые могут быть синхронизированными учетными записями Active Directory. При входе этого пользователя устройство автоматически выполняет переход с Windows Pro на Windows Корпоративная или с Windows Pro для образовательных учреждений на Windows Для образовательных учреждений.

Более ранние версии Windows

Если устройства работают под управлением Windows 7 или Windows 8.1, требуются дополнительные действия. Подход к очистке и загрузке по-прежнему работает, но его может быть проще обновить с Windows 7 Pro непосредственно до поддерживаемого в настоящее время Windows 10 Корпоративная выпуска. Этот путь поддерживается и завершает перемещение за один шаг. Однако версии Windows, более новые, чем Windows 10, не поддерживают обновление с Windows 7 или Windows 8.1. Для версий Windows, более новых, чем Windows 10, сначала потребуется обновление до Windows 10,

а затем обновление до версии Windows Корпоративная, чем Windows 10. В этом сценарии очистка и загрузка могут быть более практичными.

Лицензии

Следующие политики применяются к приобретению и продлению лицензий на устройствах.

- Обновленные устройства пытаются продлить лицензии примерно каждые 30 дней. Для успешного приобретения или продления лицензии они должны быть подключены к Интернету.
- Если устройство отключено от Интернета, до истечения срока действия текущей подписки Windows меняется на Pro или Pro для образовательных учреждений. Как только устройство снова будет подключено к Интернету, лицензия автоматически продлевается.
- Для каждой пользовательской лицензии можно обновить до пяти устройств. Если пользовательская лицензия используется для шестого устройства, компьютер, на котором пользователь не вошел в систему в течение длительного времени, возвращается на Pro или Pro Education.
- Если устройство соответствует требованиям и лицензированный пользователь входит в систему на этом устройстве, оно обновляется.

Лицензии можно перераспределить от одного пользователя к другому, что позволяет оптимизировать инвестиции в лицензирование с учетом меняющихся потребностей.

При использовании Microsoft Entra подписки лицензирование на основе групп является предпочтительным способом назначения лицензий enterprise E3 и E5 пользователям. Дополнительные сведения см. в статье Основы группового лицензирования в Microsoft Entra ID.

Существующие развертывания Windows 10 Корпоративная

В поддерживаемых в настоящее время версиях Windows активация подписки автоматически извлекает встроенный ключ активации Windows и активирует базовую лицензию Pro. Затем лицензия перейдит к enterprise с помощью активации подписки. Это поведение автоматически переносит устройства из KMS или MAK, активированных Enterprise, в подписку Enterprise.

Активация подписки не устраняет необходимость активации базовой ОС. Это требование по-прежнему существует для запуска подлинной установки Windows.

> ⊗ **Внимание**
>
> Активация Windows, внедренная в встроенное ПО, выполняется автоматически только во время установки Windows при первом включении (OOBE).

Если компьютер никогда не активировался с помощью ключа Pro, используйте следующий скрипт из консоли PowerShell с повышенными привилегиями:

PowerShell

```
$(Get-WmiObject SoftwareLicensingService).OA3xOriginalProductKey | foreach{ if ( $null -ne $_ ) { Write-Host "Installing"$_;changepk.exe /Productkey $_ } else { Write-Host "No key present" } }
```

Получение лицензии на Microsoft Entra ID

Если в организации есть Соглашение Enterprise (EA) или Software Assurance (SA):

- Организации с традиционным EA должны заказать номер SKU в размере 0 долл. США, обработать электронные письма, отправленные администратору лицензий компании, и назначить лицензии с помощью Microsoft Entra ID. В идеале лицензии назначаются группам с помощью функции Microsoft Entra ID P1 или P2 для назначения групп. Дополнительные сведения см. в разделе Включение активации подписки с помощью существующего ea.
- Администратор лицензий может назначать лицензии Microsoft Entra пользователям с тем же процессом, который используется для Приложения Microsoft 365.
- Новые клиенты с Windows Корпоративная и EA/SA могут приобрести и подписку SA, и связанную с ней облачную подписку за 0 долл. США.

Если у организации есть Соглашение о продуктах майкрософт & услуг (MPSA):

- Новые клиенты автоматически отправляются по электронной почте сведения о службе. Следуйте инструкциям и инструкциям, приведенным в сообщении электронной почты.
- Существующие клиенты MPSA получают сообщения электронной почты об активации службы, которые позволяют администратору клиента назначать пользователей службе.
- Новые клиенты MPSA, приобретающие подписку на программное обеспечение Windows Enterprise E3 и E5, могут использовать как традиционный метод активации

подписок на основе ключей, так и новые.

Развертывание лицензий

Дополнительные сведения см. в разделе Развертывание лицензий Windows Enterprise.

Доступ к виртуальным рабочим столам (VDA)

Подписки на Windows Корпоративная также доступны для виртуализированных клиентов. Корпоративные E3 и E5 доступны для доступа к виртуальному рабочему столу (VDA) в Microsoft Azure или в другом квалифицированном мультитенантном hoster (QMTH).

Виртуальные машины должны быть настроены для включения подписок Windows Enterprise для VDA. Поддерживаются клиенты, присоединенные к Active Directory и Microsoft Entra. См. Включение VDA для активации подписки.

Связанное содержимое

- Развертывание лицензий Windows Enterprise.
- Спланируйте реализацию гибридного соединения Microsoft Entra.
- Сравнение выпусков Windows.
- Windows для бизнеса.

Last updated on 14.05.2025

Windows Корпоративная E3 в CSP

Применяется к: ✅ Windows 11, ✅ Windows 10

Windows Enterprise E3 в CSP предоставляет по подписке эксклюзивные функции, зарезервированные для выпусков Windows Enterprise. Это предложение доступно через поставщик облачных решений (CSP) в Центре партнеров в качестве веб-службы. Windows Enterprise E3 в CSP предоставляет гибкую подписку на пользователя для небольших и средних организаций (от одного до сотен пользователей). Чтобы воспользоваться этим предложением, необходимо выполнить следующие предварительные требования:

- Текущая поддерживаемая версия Windows, установленная и активируемая, на обновляемых устройствах.
- Microsoft Entra доступны для управления удостоверениями.

Переход с Windows Pro на Windows Корпоративная выполняется проще, чем когда-либо прежде, без ключей и перезагрузки. После ввода пользователем учетных данных Microsoft Entra, связанных с лицензией Windows Enterprise E3, операционная система переходит с Windows Pro на Windows Корпоративная, и все соответствующие функции Enterprise будут разблокированы. Когда срок действия лицензии на подписку истекает или передается другому пользователю, устройство Enterprise легко переходит к Windows Pro.

Ранее только организации с соглашением о корпоративном лицензировании Майкрософт могли развертывать Windows Корпоративная для своих пользователей. Теперь с Windows Корпоративная E3 в CSP малые и средние организации могут с легкостью воспользоваться преимуществами корпоративных выпусков.

При покупке Windows Enterprise E3 через партнера включаются следующие преимущества:

- **Выпуск Windows Enterprise**. Устройства под управлением Windows Pro могут получить Windows Enterprise Current Branch (CB) или Current Branch for Business (CBB). Это преимущество не включает Long Term Service Branch (LTSB).
- **Поддержка любого количества пользователей, от одного до нескольких сотен**. Хотя программа Windows Корпоративная E3 в CSP не имеет ограничений на количество лицензий, которые может иметь организация, эта программа предназначена для небольших и средних организаций.
- **Развертывание до пяти устройств**. Для каждого пользователя, на который распространяется лицензия, выпуск Windows Enterprise можно развернуть на пяти устройствах.
- **Откат до Windows Pro в любое время**. Когда срок действия подписки пользователя истекает или передается другому пользователю, устройство Windows Enterprise

плавно переходит к выпуску Windows Pro (по истечении льготного периода до 90 дней).
- **Помесячная оплата за каждого пользователя**. Эта модель делает Windows Корпоративная E3 доступной для организаций.
- **Возможность перераспределения лицензий между пользователями**. Лицензии можно быстро и легко перераспределить от одного пользователя к другому, что позволяет оптимизировать инвестиции в лицензирование с учетом меняющихся потребностей.

Как программа Windows Enterprise E3 в CSP сравнивается с соглашениями о корпоративном лицензировании Майкрософт и Software Assurance?

- Программы корпоративного лицензирования Microsoft являются более объемными и предоставляют доступ к лицензированию всех продуктов корпорации Майкрософт.

- Программа Software Assurance обеспечивает организациям преимущества, которые можно разделить на следующие категории:

  - **Развертывание и управление**. К этим преимуществам относятся службы планирования:
    - Оптимизация рабочего стола Майкрософт (MDOP).
    - Права доступа к виртуальному рабочему столу Windows.
    - Права на использование в роуминге Windows.
    - Другие преимущества.

  - **Обучение**. К этой категории относятся ваучеры на обучение, электронное обучение через Интернет и программа использования ПО на домашних компьютерах.

  - **Поддержка**. К этим преимуществам относятся:
    - Поддержка решения проблем 24x7.
    - Возможности резервного копирования для аварийного восстановления.
    - глобальный монитор служб System Center.
    - Пассивный вторичный экземпляр SQL Server.

  - **Специализация**. Эти преимущества включают в себя повышение доступности лицензирования, что позволяет переносить программное обеспечение из более ранней версии в выпуск более высокого уровня. Он также распределяет платежи лицензий и Software Assurance на три равные ежегодные суммы.

    Кроме того, в Windows Корпоративная E3 в CSP партнер может управлять лицензиями для организации. С помощью Software Assurance организация должна управлять собственными лицензиями.

Таким образом, программа Windows Корпоративная E3 в CSP — это предложение обновления, которое предоставляет организациям малого и среднего размера более простой и гибкий доступ к преимуществам выпуска Windows Enterprise. Программы корпоративного лицензирования Майкрософт и Software Assurance, с другой стороны, более широки в область и предоставляют преимущества помимо доступа к выпуску Windows Enterprise.

Сравнение выпусков Windows Pro и Enterprise

Выпуск Windows Enterprise имеет множество функций, недоступных в Windows Pro. В таблице 1 перечислены некоторые функции Windows Корпоративная, не доступные в Windows Pro. Многие из этих компонентов связаны с безопасностью, тогда как другие обеспечивают управление устройствами на более детальном уровне.

Таблица 1. Функции Windows Enterprise не найдены в Windows Pro

Развернуть таблицу

Функция	Описание
Credential Guard	Credential Guard использует безопасность на основе виртуализации для защиты секретов безопасности, чтобы доступ к ним могли получить только привилегированные системные программы. Примерами секретов безопасности, которые можно защитить, являются хэши паролей NTLM и билеты на предоставление билетов Kerberos. Эта защита помогает предотвратить атаки pass-the-Hash или Pass-the-Ticket. К возможностям Credential Guard относятся: • **Безопасность на уровне оборудования** . Credential Guard использует функции безопасности аппаратной платформы (такие как безопасная загрузка и виртуализация) для защиты производных учетных данных домена и других секретов. • **Безопасность на основе виртуализации** . Службы Windows, которые получают доступ к производным учетным данным домена и другим секретам, выполняются в виртуализированной защищенной среде, которая изолирована. • **Улучшенная защита от постоянных угроз** . Credential Guard работает с другими технологиями (например, Device Guard), чтобы обеспечить дополнительную защиту от атак, независимо от того, насколько они постоянны. • **Улучшенная управляемость**— Credential Guard можно управлять с помощью групповая политика, инструментария управления Windows (WMI) или Windows PowerShell.

Функция	Описание
	Подробнее об этом: Защита извлеченных учетных данных домена с помощью Credential Guard. *Требуется Credential Guard* *UEFI 2.3.1 или более поздней версии с доверенной загрузкой* *Необходимо включить расширения виртуализации, такие как Intel VT-x, AMD-V и SLAT.* *x64 версия Windows* *IOMMU, например Intel VT-d, AMD-Vi* *Блокировка BIOS* • *TPM 2.0 рекомендуется для аттестации работоспособности устройства (использует программное обеспечение, если TPM 2.0 отсутствует)*
Управление AppLocker	Эта функция помогает ИТ-специалистам определять, какие приложения и файлы пользователи могут запускать на устройстве. К таким приложениям и файлам относятся исполняемые файлы, сценарии, файлы установщика Windows, библиотеки DLL, упакованные приложения и установщики упакованных приложений. Подробнее об этом: AppLocker.
Виртуализация приложений (App-V)	Эта функция делает приложения доступными для конечных пользователей без установки приложений непосредственно на устройствах пользователей. App-V превращает приложения в централизованно управляемые службы, которые никогда не устанавливаются и не конфликтуют с другими приложениями. Эта также гарантирует актуальность приложений, т. е. наличие в них последних обновлений безопасности. Дополнительные сведения см. в статье Начало работы с клиентом App-V для Windows.
Виртуализация взаимодействия с пользователем (UE-V)	С помощью этой функции настраиваемые пользователем параметры Windows и приложений можно записывать и хранить в централизованно управляемом сетевом файловом ресурсе. Когда пользователи входят в систему, их персонализированные параметры применяются к рабочему сеансу независимо от того, в какие сеансы инфраструктуры виртуальных рабочих столов (VDI) устройства или виртуального рабочего стола они входят. UE-V предоставляет следующие функции: • указывать, какие приложения и параметры Windows синхронизируются между устройствами пользователя; • доставлять параметры в любое время, где бы на территории организации не работал пользователь; • Создание пользовательских шаблонов для бизнес-приложений

Функция	Описание
	• Восстановление параметров после замены или обновления оборудования или после повторного создания образа виртуальной машины в исходное состояние Дополнительные сведения см. в статье Общие сведения о виртуализации взаимодействия с пользователем (UE-V).
Управляемое взаимодействие с пользователем	Эта функция помогает настроить и заблокировать пользовательский интерфейс устройства Windows, чтобы ограничить его определенной задачей. Например, устройство можно настроить для управляемого сценария, например киоска или устройства класса. После выхода пользователя из системы интерфейс автоматически будет сброшен. Доступ к таким службам, как Магазин Windows, также может быть ограничен. Для Windows 10 можно также управлять параметрами макета "Пуск", например: • удалить команды «Завершение работы», «Перезагрузка», «Сон», «Гибернация» во избежание доступа к ним; • удалить команду «Выход» (плитку «Пользователь») из меню «Пуск»; • удалить список часто используемых программ из меню «Пуск»; • удалить список всех программ из меню «Пуск»; • запретить пользователям настраивать начальный экран; • принудительно запускать меню «Пуск» во весь экран или в размере меню; • запретить изменение параметров панели задач и меню «Пуск».

Развертывание лицензий Windows Enterprise E3

См. статью Развертывание лицензий Windows Enterprise.

Развертывание компонентов Windows Enterprise

Теперь, когда выпуск Windows Корпоративная работает на устройствах, как используются функции и возможности выпуска Enterprise? Какие следующие шаги необходимо предпринять для каждого из компонентов, перечисленных в таблице 1?

В следующих разделах приведены высокоуровневые задачи, которые необходимо выполнить в среде, чтобы помочь пользователям воспользоваться преимуществами возможностей выпуска Windows Enterprise.

Credential Guard

> ⓘ **Примечание.**

Требуется UEFI 2.3.1 или более поздней версии с доверенной загрузкой; Необходимо включить расширения виртуализации, такие как Intel VT-x, AMD-V и SLAT; x64 версия Windows; IOMMU, например Intel VT-d, AMD-Vi; Блокировка BIOS; TPM 2.0 рекомендуется для аттестации работоспособности устройства (будет использовать программное обеспечение, если TPM 2.0 отсутствует).

Credential Guard можно реализовать на устройствах Windows Enterprise, включив Credential Guard на этих устройствах. Credential Guard использует функции безопасности на основе виртуализации Windows (Hyper-V), которые должны быть включены на каждом устройстве, прежде чем Credential Guard можно будет включить. Credential Guard можно включить с помощью одного из следующих методов:

- **Автоматически**. Credential Guard можно включить для одного или нескольких устройств с помощью групповая политика. Параметры групповой политики автоматически добавляют функции безопасности на основе виртуализации и настраивают параметры реестра Credential Guard на управляемых устройствах.
- **Вручную**. Credential Guard можно включить вручную, выполнив одно из следующих действий:
  - Добавьте функции безопасности на основе виртуализации в разделе «Программы и компоненты» или с помощью системы обслуживания образов развертывания и управления ими (DISM).
  - Настройте параметры реестра Credential Guard с помощью редактора реестра или средства проверки готовности оборудования для Device Guard и Credential Guard.

    Эти действия вручную можно автоматизировать с помощью средства управления, например Microsoft Configuration Manager.

Подробнее об использовании Credential Guard см. в следующих материалах:

- Обзор Credential Guard
- Вопросы безопасности для изготовителей оригинального оборудования
- Средство проверки готовности оборудования для Device Guard и Credential Guard

Управление AppLocker

AppLocker в Windows Enterprise можно управлять с помощью групповая политика. групповая политика требуется наличие AD DS и присоединение устройств Windows Enterprise к домену AD DS. Правила AppLocker можно создать с помощью групповая политика. Затем правила AppLocker можно настроить на соответствующие устройства.

Подробнее об управлении AppLocker с помощью групповой политики см. в руководстве по развертыванию AppLocker.

App-V

Для поддержки клиентов App-V требуется серверная инфраструктура App-V. Основные необходимые компоненты App-V:

- **Сервер App-V**. Сервер App-V обеспечивает управление App-V, публикацию виртуализированных приложений, потоковую передачу приложений и функции отчетности. Все эти службы можно запустить на одном сервере или по отдельности на нескольких серверах. Например, может существовать несколько серверов потоковой передачи. Клиенты App-V связываются с серверами App-V, чтобы определить, какие приложения опубликованы для пользователя или для устройства, а затем запустить виртуализированное приложение с сервера.

- **Секвенсор App-V**. Секвенсор App-V — это типовое клиентское устройство, которые используется для упаковки (записи) приложений и подготовке их к размещению на сервере App-V. Приложения устанавливаются в последовательность App-V, а программное обеспечение последовательности App-V определяет файлы и параметры реестра, которые были изменены во время установки приложения. Затем секвенсор записывает эти параметры, чтобы создать виртуализированное приложение.

- **Клиент App-V**. Клиент App-V должен быть включен на любом клиентском устройстве Windows Enterprise E3, которое должно запускать приложения с сервера App-V.

Подробнее о реализации сервера App-V, секвенсора App-V и клиента App-V см. в следующих материалах:

- Начало работы с клиентом App-V для Windows
- Развертывание сервера App-V
- Развертывание секвенсора App-V и настройка клиента

UE-V

Для UE-V требуются серверные и клиентские компоненты, которые необходимо скачать, активировать и установить. К этим компонентам относятся:

- **Служба UE-V**. Служба UE-V (когда она включена на устройствах) отслеживает зарегистрированные приложения и Windows на предмет изменения параметров, а затем синхронизирует эти параметры между устройствами.

- **Пакеты параметров**. В параметрах пакетов, создаваемых службой UE-V, хранятся параметры приложений и параметры Windows. Параметры пакетов формируются, сохраняются локально и копируются в место хранения параметров.

- **Место хранения параметров**. Это расположение является стандартным сетевым ресурсом, к которому пользователи могут получить доступ. Служба UE-V проверяет это расположение и создает скрытную системную папку, в которой хранятся и из которой извлекаются параметры пользователей.

- **Шаблоны расположения параметров**. Шаблоны расположения параметров — это XML-файлы, которые UE-V использует для мониторинга параметров классических приложений и параметров рабочего стола Windows и их синхронизации между компьютерами пользователей. По умолчанию в состав UE-V входит несколько шаблонов расположения параметров. Пользовательские шаблоны расположения параметров также можно создавать, изменять или проверять с помощью генератора шаблонов UE-V. Шаблоны расположения параметров не требуются для приложений Windows.

- **Список универсальных приложений для Windows**. UE-V определяет, для каких Windows-приложений необходимо синхронизировать параметры, по управляемому списку приложений. По умолчанию в этот список входит большинство Windows-приложений.

Подробнее о развертывании UE-V см. в следующих материалах:

- Обзор виртуализации взаимодействия с пользователем (UE-V)
- Начало работы с UE-V
- Подготовка к развертыванию UE-V

Управляемое взаимодействие с пользователем

Функция управляемого взаимодействия с пользователем — это набор функций выпуска Windows Enterprise и соответствующих параметров, которые можно использовать для управления взаимодействием с пользователем. В таблице 2 описаны параметры управляемого взаимодействия с пользователем (по категориям), доступные только в выпуске Windows Enterprise. Способы управления, используемые для настройки каждого компонента, зависят от компонента. Некоторые функции настраиваются с помощью групповой политики, тогда как другие — с помощью Windows PowerShell, системы обслуживания образов развертывания и управления ими (DISM) или других средств командной строки. Для групповая политика параметров требуется AD DS с устройствами Windows Enterprise, присоединенными к домену AD DS.

Таблица 2. Компоненты управляемого взаимодействия с пользователем

Развернуть таблицу

Компонент	Описание
Настройка макета начального экрана	Настраиваемый макет начального экрана можно развернуть для пользователей в домене. Повторно создавать образ не требуется, а чтобы обновить макет начального экрана, достаточно перезаписать XML-файл, содержащий макет. XML-файл позволяет настраивать макеты начального запуска для разных отделов или организаций с минимальными затратами на управление. Подробнее об этом компоненте см. в статье Настройка меню Пуск, начального экрана и панели задач Windows 10 с помощью групповой политики.
Загрузка без фирменного стиля	Элементы Windows, которые появляются при запуске или возобновлении работы Windows, можно подавлять. Экран сбоя, когда Windows обнаруживает ошибку, из-за которой не удается восстановиться, также можно подавить. Подробнее об этом компоненте см. в статье Загрузка без фирменного стиля.
Пользовательский вход	Функция пользовательского входа может использоваться для подавления элементов пользовательского интерфейса Windows, относящихся к экрану приветствия и экрану завершения работы. Например, можно отключить все элементы пользовательского интерфейса экрана приветствия и предоставить настраиваемый пользовательский интерфейс входа. Экран Сопоставителя заблокированного завершения работы (BSDR) также можно отключить, и приложения могут быть автоматически завершены, пока ОС ожидает закрытия приложений перед завершением работы. Подробнее об этом компоненте см. в статье Настраиваемый вход в систему.
Средство запуска оболочки	Предоставляет ограниченный доступ для запуска только классического приложения для Windows через средство запуска оболочки для замены оболочки. Подробнее об этом компоненте см. в статье Средство запуска оболочки.
Фильтр клавиатуры	Фильтр клавиатуры можно использовать для подавления нежелательных нажатий клавиш или сочетаний клавиш. Обычно пользователи могут использовать определенные сочетания клавиш Windows, например CTRL+ALT+DELETE или CTRL+SHIFT+TAB, для управления устройством путем блокировки экрана или закрытия запущенного приложения через диспетчер задач. Эти действия с клавиатуры не являются желательными на устройствах, предназначенных для определенной цели. Подробнее об этом компоненте см. в статье Фильтр клавиатуры.
Объединенный фильтр записи	Единый фильтр записи (UWF) можно использовать на устройстве для защиты физических носителей, включая большинство стандартных типов записываемых хранилищ, поддерживаемых Windows, например:

Компонент	Описание
	• Физические жесткие диски • Твердотельные накопители • Внутренние USB-устройства • Внешние устройства SATA . UWF также можно использовать для отображения в ОПЕРАЦИОННОй системе носителя только для чтения в виде записываемого тома. Подробнее об этом компоненте см. в статье Объединенный фильтр записи.

Связанные статьи

- Активация подписки Windows Enterprise.
- Спланируйте реализацию гибридного соединения Microsoft Entra.
- Сравнение выпусков Windows .
- Windows для бизнеса .

Last updated on 14.05.2025

Настройка VDA для активации подписки Windows

Относится к:

- Windows 10
- Windows 11

В этом документе описывается настройка виртуальных машин для включения активации подписки Windows в сценарии доступа к виртуальному рабочему столу Windows (VDA). Windows VDA — это устройство или пользовательский механизм лицензирования для управления доступом к виртуальным рабочим столам.

Инструкции по развертыванию предоставляются для следующих сценариев.

1. Виртуальные машины, присоединенные к Active Directory
2. виртуальные машины, присоединенные к Microsoft Entra
3. Виртуальные машины Azure Gallery

Требования

- На виртуальных машинах должна быть установлена поддерживаемая версия выпуска Windows Pro.
- Виртуальные машины должны быть присоединены к Active Directory или Microsoft Entra ID.
- Виртуальные машины должны размещаться в квалифицированном мультитенантном hoster (QMTH).

Активация

Сценарий 1

- Виртуальная машина работает под управлением поддерживаемой версии Windows.
- Виртуальная машина размещается в Azure, авторизованном аутсорсере или другом квалифицированном мультитенантном hoster (QMTH).

  Когда пользователь с правами VDA входит в виртуальную машину, используя свои Microsoft Entra учетные данные, виртуальная машина автоматически активируется до уровня Enterprise. Активация Windows Pro не требуется. Эта функция устраняет

необходимость обслуживания KMS или MAK в соответствующей облачной инфраструктуре.

Сценарий 2

- Узел Hyper-V и виртуальная машина работают под управлением поддерживаемой версии Windows.

  Наследуемая активация включена. Все виртуальные машины, созданные пользователем с лицензией Windows E3 или E5, автоматически активируются независимо от того, входит ли пользователь с локальной учетной записью или с помощью учетной записи Microsoft Entra.

Сценарий 3

- Хостер не является авторизованным партнером QMTH.

  В этом сценарии базовая лицензия Windows Pro должна быть активирована перед использованием активации подписки Windows Enterprise. Активация выполняется с помощью универсального ключа корпоративной лицензии (GVLK) и сервера активации KMS с корпоративной лицензией, предоставляемого хостером. Кроме того, можно использовать сервер активации KMS. Активация KMS предоставляется для виртуальных машин Azure. Дополнительные сведения см. в статье Устранение неполадок с активацией виртуальной машины Windows Azure.

Примеры проблем активации см. в разделе Устранение проблем при взаимодействии с пользователем.

Виртуальные машины, присоединенные к Active Directory

1. Используйте следующие инструкции для подготовки виртуальной Машины для Azure: Подготовьте виртуальный жесткий диск Windows или VHDX, чтобы загрузить Azure

2. (Необязательно) Чтобы отключить проверку подлинности на уровне сети, введите следующую команду в командной строке с повышенными привилегиями:

   Командная строка Windows

   ```
   REG.exe ADD "HKLM\SYSTEM\CurrentControlSet\Control\Terminal
   Server\WinStations\RDP-Tcp" /v UserAuthentication /t REG_DWORD /d 0 /f
   ```

3. В командной строке с повышенными привилегиями введите **sysdm.cpl**.

4. На вкладке Удаленно выберите **Разрешить удаленные подключения к этому компьютеру** , а затем выберите **Выбрать пользователей**.

5. Нажмите **кнопку Добавить**, введите **прошедшие проверку подлинности пользователи**, а затем три раза нажмите **кнопку ОК** .

6. Следуйте инструкциям по использованию средства sysprep в разделе Шаги для подготовки виртуального жесткого диска, а затем снова запустите виртуальную машину.

7. Если необходимо активировать Windows Pro, как описано в сценарии 3, выполните следующие действия, чтобы использовать конфигурацию Windows Designer и внедрить ключ активации. В противном случае перейдите к шагу 8.

   a. Установите конструктор конфигураций Windows.

   b. Откройте Designer конфигурации Windows и выберите **Подготовить службы классических приложений**.

   c. В разделе **Имя** введите **Desktop AD Enrollment Pro GVLK**, нажмите кнопку **Готово**, а затем на странице **Настройка устройства** введите имя устройства.

   > ⓘ **Примечание.**
   >
   > Вы можете использовать другое имя проекта, но это имя также используется с dism.exe на следующем шаге.

   d. В **разделе Введите ключ продукта** введите ключ Pro GVLK: `W269N-WFGWX-YVC9B-4J6C9-T83GX`.

   e. На странице Настройка сети выберите **отключение**.

   f. На странице управления учетными записями выберите **Регистрация в Active Directory**, а затем введите данные учетной записи.

   > ⓘ **Примечание.**
   >
   > Этот шаг отличается для виртуальных машин, присоединенных к Microsoft Entra.

g. На странице "Добавить приложения", при необходимости, добавьте приложения. Этот шаг является необязательным.

h. На странице Добавить сертификаты, при необходимости, добавьте сертификаты. Этот шаг является необязательным.

i. На странице Готово выберите **Создать**.

j. В проводнике откройте VHD, чтобы подключить образ диска. Определите букву диска для подключенного образа.

k. Введите следующую команду в командной строке с повышенными привилегиями. Замените букву `G` буквой диска подключенного образа и введите имя проекта, которое вы использовали, если оно отличается от предложенного:

Командная строка Windows

```
Dism.exe /Image=G:\ /Add-ProvisioningPackage /PackagePath: "Desktop AD Enrollment Pro GVLK.ppkg"
```

l. Щелкните правой кнопкой мыши подключенный образ в проводнике и выберите **Извлечь**.

8. См. инструкции в статье Отправка и создание виртуальной машины из обобщенного виртуального жесткого диска , чтобы войти в Azure, получить сведения об учетной записи хранения, отправить виртуальный жесткий диск и создать управляемый образ.

виртуальные машины, присоединенные к Microsoft Entra

> ⓘ **Внимание**
>
> Microsoft Entra пакеты подготовки имеют ограничение в 180 дней на массовое использование маркеров. Через 180 дней необходимо обновить пакет подготовки и повторно внедрить его в образ. Существующие виртуальные машины, которые Microsoft Entra присоединены и развернуты, не потребуется повторно создавать.

Для виртуальных машин, присоединенных к Microsoft Entra, следуйте тем же инструкциям, что и для виртуальных машин, присоединенных к Active Directory, со следующими исключениями:

- Во время установки с помощью Designer конфигурации Windows в поле **Имя** введите имя проекта, указывающее, что он не подходит для виртуальных машин, присоединенных к Active Directory, таких как **GVLK для групповой регистрации рабочих столов Pro**.
- Во время установки с конфигурацией Windows Designer на странице Управление учетными записями вместо регистрации в Active Directory выберите **Регистрация в Microsoft Entra ID**, **выберите Получить массовый маркер**, войдите и добавьте массовый маркер, используя учетные данные вашей организации.
- При вводе PackagePath используйте ранее введенное имя проекта. Например, **Desktop Bulk Enrollment Token Pro GVLK.ppkg**
- При попытке получить доступ к виртуальной машине с помощью удаленного рабочего стола необходимо создать пользовательский файл параметров RDP, как описано ниже в разделе Создание настраиваемых параметров RDP для Azure.

Виртуальные машины Azure Gallery

1. (Необязательно) Чтобы отключить проверку подлинности на уровне сети, введите следующую команду в командной строке с повышенными привилегиями:

   Командная строка Windows

   ```
   REG.exe ADD "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" /v UserAuthentication /t REG_DWORD /d 0 /f
   ```

2. В командной строке с повышенными привилегиями введите `sysdm.cpl`.
3. На вкладке Удаленно выберите **Разрешить удаленные подключения к этому компьютеру** , а затем выберите **Выбрать пользователей**.
4. Нажмите **кнопку Добавить**, введите **прошедшие проверку подлинности пользователи**, а затем три раза нажмите **кнопку OK** .
5. Установите конструктор конфигураций Windows.
6. Откройте Designer конфигурации Windows и выберите **Подготовить службы классических приложений**.
7. Если необходимо активировать Windows Pro, как описано в сценарии 3, выполните следующие действия. В противном случае перейдите к шагу 8.

a. В разделе **Имя** введите **GVLK токена массовой регистрации рабочего стола**, нажмите кнопку **Готово**, а затем на странице **Настройка устройства** введите имя устройства.

b. В **разделе Введите ключ продукта** введите ключ Pro GVLK: `W269N-WFGWX-YVC9B-4J6C9-T83GX`.

8. В разделе **Имя** введите **Массовая регистрация на рабочем столе**, нажмите кнопку **Готово**, а затем на странице **Настройка устройства** введите имя устройства.

9. На странице Настройка сети выберите **отключение**.

10. На странице Управление учетными записями выберите **Регистрация в Microsoft Entra ID**, выберите **Получить массовый маркер**, войдите в систему и добавьте массовый маркер, используя учетные данные организации.

11. На странице "Добавить приложения", при необходимости, добавьте приложения. Этот шаг является необязательным.

12. На странице Добавить сертификаты, при необходимости, добавьте сертификаты. Этот шаг является необязательным.

13. На странице Готово выберите **Создать**.

14. Скопируйте PPKG-файл на удаленную виртуальную машину. Откройте пакет подготовки, чтобы установить его. Этот процесс перезапустит систему.

> ⓘ **Примечание.**
>
> При попытке получить доступ к виртуальной машине с помощью удаленного рабочего стола необходимо **создать пользовательский файл параметров RDP**.

Создание настраиваемых параметров протокола удаленного рабочего стола для Azure

1. Откройте подключение к удаленному рабочему столу и введите IP-адрес или DNS-имя удаленного узла.

2. Выберите **Показать параметры**, а затем в разделе Параметры подключения выберите **Сохранить как**. Сохраните RDP-файл в расположении, где он будет использоваться.

3. Закройте окно подключения к удаленному рабочему столу и откройте Блокнот.

4. Откройте RDP-файл в Блокноте, чтобы изменить его.

5. Введите или замените строку, которая указывает уровень проверки подлинности с помощью следующих двух строк текста:

   ```text
   enablecredsspsupport:i:0
   authentication level:i:2
   ```

   Значения `enablecredsspsupport` и `authentication level` должны отображаться в файле только один раз.

6. Сохраните изменения, а затем используйте этот пользовательский RDP-файл с учетными данными Microsoft Entra для подключения к виртуальной машине Azure.

Связанные статьи

Активация подписки Windows

Рекомендуемые параметры для рабочих столов VDI

Технический документ о лицензировании рабочего стола Windows для сред VDI

Last updated on 14.05.2025

Развертывание лицензий Windows Корпоративная

Применяется к: ✅ Windows 11, ✅ Windows 10

В этой статье описывается развертывание лицензий Windows Корпоративная E3 или E5 с активацией подписки или Enterprise E3 в CSP и Microsoft Entra ID.

Для этих функций активации требуется поддерживаемая и лицензированная версия Windows Pro:

- Активация подписки с помощью соглашения Enterprise (EA) или соглашения о продуктах Майкрософт & служб (MPSA).
- Корпоративный E3 в CSP.
- Для автоматической активации, отличной от KMS, также требуется устройство с встроенным ключом активации встроенного ПО.
- Для активации подписки *требуется* лицензирование Enterprise per user. Это не работает с лицензированием *для каждого устройства* .

Включение активации подписки с помощью существующего ea

Клиенты EA с существующим клиентом Microsoft 365 могут выполнить следующие действия, чтобы включить лицензии на подписку Windows в существующем клиенте:

1. Обратитесь к торговому посреднику, чтобы разместить заказ на один номер SKU в размере 0 долл. США на пользователя. По состоянию на 1 октября 2022 г. доступно три номера SKU в зависимости от текущей лицензии windows Enterprise SA:

Развернуть таблицу

SKU	Описание
AAA-51069	`Win OLS Activation User Alng Sub Add-on E3`
AAA-51068	`Win OLS Activation User Sub Add-on E5`
VRM-00001	`Win OLS Activation User GCC Sub Per User`

> **Примечание.**

С 1 октября 2022 г. активация подписки доступна для *коммерческих* клиентов и клиентов *GCC* . В настоящее время он недоступен для клиентов GCC High или DoD.

2. После размещения заказа администратор OLS по соглашению получит электронное письмо с активацией службы, в котором указано, что лицензии на подписку подготовлены в клиенте.

3. Лицензии на подписку теперь можно назначать пользователям.

Чтобы обновить контактные данные и повторно отправить сообщение электронной почты для активации, выполните следующую процедуру:

1. Войдите в центра поддержки корпоративных лицензий Майкрософт.

2. Выберите **Подписки**.

3. Выберите **Список соглашений о веб-службах**.

4. Введите номер соглашения и нажмите кнопку **Поиск**.

5. Выберите **имя службы**.

6. В разделе **Контакт по подписке** выберите имя, указанное в разделе **Фамилия**.

7. Обновите контактные данные, а затем выберите **Обновить контактные данные**. Это действие активирует новое сообщение электронной почты.

Подготовка к развертыванию: просмотр требований

- На устройствах должна быть установлена поддерживаемая версия Windows Pro.
- Microsoft Entra присоединено или гибридный домен, присоединенный с помощью Microsoft Entra Connect. Клиенты, объединенные в федерацию с Microsoft Entra ID, также имеют право.

Дополнительные сведения см. в разделе Проверка требований к устройствам далее в этой статье.

Синхронизация Active Directory с Microsoft Entra ID

Если есть домен локальная служба Active Directory Доменные службы (AD DS), удостоверения в локальном домене AD DS необходимо синхронизировать с Microsoft

Entra ID. Эта синхронизация необходима для того, чтобы у пользователей было *одно удостоверение*, которое они могут использовать для доступа к локальным приложениям и облачным службам, которые используют Microsoft Entra ID. Примером облачной службы является Windows Корпоративная E3 или E5.

Дополнительные сведения об интеграции локальных доменов AD DS с Microsoft Entra ID см. в следующих ресурсах:

- Настройка гибридного присоединения Microsoft Entra
- Что такое гибридное удостоверение с Microsoft Entra ID?
- схема установки Microsoft Entra Connect и Microsoft Entra Connect Health

Назначение лицензий пользователям

После заказа подписки Windows отправляется сообщение электронной почты с рекомендациями по использованию Windows в качестве веб-службы. Для назначения лицензии доступны следующие методы:

- Если доступна необходимая Microsoft Entra подписка, лицензирование на основе групп является предпочтительным способом назначения пользователям лицензий Enterprise E3 или E5.
- Лицензии можно назначить вручную, войдя в Центр администрирования Microsoft 365.
- Лицензии можно назначить, отправив электронную таблицу.
- Лицензии можно назначить с помощью PowerShell.

Обзор процесса обновления

Теперь, когда подписка установлена и лицензии назначены пользователям, устройства под управлением поддерживаемых версий Windows Pro можно обновить до выпуска Enterprise.

> **Совет**
>
> В этом пошаговом руководстве по обновлению предполагается, что Autopilot не используется. Сведения об использовании Autopilot при присоединении к Microsoft Entra ID см. в статье **Присоединение к Microsoft Entra, управляемое пользователем: развертывание устройства**.

Шаг 1. Присоединение устройств Windows Pro к Microsoft Entra ID

При первом запуске устройства Windows Pro может присоединиться к Microsoft Entra ID во время установки. Существующие устройства также могут присоединяться к Microsoft Entra ID.

Присоединение устройства к Microsoft Entra ID во время запуска при первом запуске устройства

1. Включите устройство в первый раз, чтобы инициировать установку Windows и интерфейс запуска (OOBE).

2. На экране **Является ли это подходящей страной или регионом?** выберите нужную страну или регион, а затем нажмите кнопку **Да** .

3. На экране **Является ли это правильной раскладкой клавиатуры или методом ввода?** выберите нужные методы ввода и клавиатуры, а затем нажмите кнопку **Да** .

4. На экране **Хотите добавить вторую раскладку клавиатуры?** при необходимости добавьте дополнительные методы ввода или клавиатуры, выбрав **Добавить макет**. В противном случае нажмите кнопку **Пропустить** .

5. Если сетевое подключение не обнаружено, появится экран **Подключение к сети** . Подключитесь к беспроводной или проводной сети с доступом к Интернету, а затем нажмите кнопку **Далее** .

6. На этом этапе могут быть установлены обновления для программы установки Windows. Если обновления установлены, устройство перезагружается, чтобы завершить установку обновлений.

7. В Windows 11 Pro выпусках появится экран **Присвоение имени устройства**. Присвойте устройству имя и нажмите кнопку **Далее** . После присвоения имени устройство может перезагрузиться.

8. В Windows 11 Pro выпусках **появится экран Как вы хотите настроить это устройство?** Выберите **Настроить для работы или учебы** , а затем нажмите кнопку **Далее** .

9. На экране **Давайте настроим параметры для вашей работы или учебного заведения** :

    a. В текстовом **someone@example.com** поле **в разделе Вход введите** имя пользователя для учетной записи пользователя Microsoft Entra, а затем нажмите

кнопку **Далее**. Имя пользователя имеет формат электронной почты user@domain.com.

b. В текстовом поле **Пароль** в **разделе Ввод пароля** введите пароль для учетной записи пользователя Microsoft Entra, а затем нажмите кнопку **Войти**.

10. Устройство выполняет оставшуюся часть установки Windows, включая настройку параметров организации.

11. На экране **Выбор параметров конфиденциальности для устройства** настройте параметры конфиденциальности при необходимости, нажав кнопку **Далее** , чтобы перейти между параметрами. После завершения нажмите кнопку **Принять** .

12. В зависимости от устройства и конфигурации параметров организации могут появиться дополнительные экраны. Например, может появиться экран **Windows Hello**.

После завершения программы установки Windows пользователь автоматически войдет в систему, а устройство Microsoft Entra присоединено к подписке организации.

Присоединение устройства к Microsoft Entra ID, когда устройство уже настроено с Windows

> ⓘ **Внимание**
>
> Убедитесь, что вход пользователя не является учетной записью **BUILTIN или администратора** . Этот пользователь не может использовать действие для `+ Connect` присоединения к рабочей или учебной учетной записи.

Откройте**рабочую или учебную область Доступ кучетным**> записям в приложении **"Параметры"**, щелкнув следующую ссылку:

Доступ на рабочем месте или в учебном учреждении

или

1. Щелкните правой кнопкой мыши меню **Пуск** и выберите **Выполнить**.

2. В окне **Выполнить** рядом с **полем Открыть:**введите:

```
Консоль
ms-settings:workplace
```

и нажмите **кнопку ОК**.

или

1. Щелкните правой кнопкой мыши меню **Пуск** и выберите **Параметры**.
2. В приложении **Параметры** выберите **Учетные записи** в области слева.
3. В области **Учетные записи** выберите **Доступ к рабочей или учебной работе**.

После открытия рабочей **или учебной области Доступ к учетным > записям** :

1. На панели **Учетные > записи Доступ к рабочим или учебным заведениям** рядом с **пунктом Добавить рабочую или учебную учетную запись** нажмите кнопку **Подключиться** .
2. В открывавшемся окне **учетной записи Майкрософт** :
   a. На странице **Настройка рабочей или учебной учетной записи** в разделе **Альтернативные действия выберитеПрисоединить это устройство к Microsoft Entra ID**.
   b. В **текстовом поле Email или телефоне** на странице **Входа введите** имя пользователя для учетной записи Microsoft Entra, а затем нажмите кнопку **Далее**. Имя пользователя имеет формат электронной почты user@domain.com.
   c. В текстовом поле **Пароль** на странице **Ввод пароля** введите пароль для учетной записи пользователя Microsoft Entra, а затем нажмите кнопку **Войти**.
   d. Когда **откроется окно Убедитесь, что это ваша организация** , подтвердите правильность сведений и нажмите кнопку **Присоединиться** .
   e. Устройство присоединяется к Microsoft Entra ID подписке организации. После завершения отобразится страница **Все задано!** Нажмите кнопку **Готово** , чтобы завершить процесс.

Устройство теперь Microsoft Entra присоединено к подписке организации.

Шаг 2. Активация выпуска Pro

Windows Pro необходимо активировать на устройстве. Однако если устройство работает под управлением поддерживаемой в настоящее время версии Windows, большинство современных устройств автоматически активирует выпуск Windows Pro с помощью встроенного ключа активации.

Шаг 3. Вход с помощью учетной записи Microsoft Entra

После присоединения устройства к Microsoft Entra ID и завершения установки или запуска запуска Windows пользователь входит в систему со своей учетной записью Microsoft Entra. После входа пользователя с помощью учетной записи Microsoft Entra лицензия Windows Корпоративная E3 или E5, связанная с пользователем, включает возможности выпуска Windows Enterprise на устройстве.

Шаг 4. Проверка того, что Windows 10 Корпоративная активирована

Чтобы проверить подписку на Windows Корпоративная E3 или E5, выполните следующие действия.

Откройте панель **Активация** в приложении **"Параметры"** , выбрав следующую ссылку:

Активация

или

1. Щелкните правой кнопкой мыши меню **Пуск** и выберите **Выполнить**.
2. В окне **Выполнить** рядом с **полем Открыть:**введите:

   Консоль

   ```
   ms-settings:activation
   ```

   и нажмите **кнопку OK**.

или

1. Щелкните правой кнопкой мыши меню **Пуск** и выберите **Параметры**.
2. В приложении **Параметры** выберите **Система** на панели слева.
3. На панели **Система** выберите **Активация**.

После открытия области **Активация системы**>:

1. В области **Активация системы** > разверните узел **Состояние активации** и **Подписка**, чтобы просмотреть полные сведения о состоянии и состоянии активации:

   a. В разделе **Состояние активации** убедитесь, что Windows активирована. Должно отобразиться сообщение:

`Windows is activated with a digital license`

b. В разделе **Подписка** убедитесь, что Windows 11 Корпоративная подписка активна. Должно отобразиться сообщение:

`Windows 11 Enterprise subscription is active`

> ⓘ **Примечание.**
>
> Если подписка Windows Корпоративная еще не применена, панель **Подписка** не отображается.

Устройство работает, когда активна и подписка, и активация. Если возникли проблемы с лицензией Windows Корпоративная E3 или E5 или активацией лицензии, на панели **Активация** отображается соответствующее сообщение об ошибке или состояние. Эти сведения можно использовать для диагностики процесса лицензирования и активации.

Убедитесь, что выпуск Enterprise включен с помощью slmgr

Slmgr также можно использовать для проверки сведений об активации:

1. Откройте командную строку.
2. Чтобы получить основные сведения о лицензировании, выполните следующую команду в командной строке:

   Командная строка Windows

   ```
   slmgr /dli
   ```

   Откроется окно со следующими выходными данными:

   Консоль

   ```
   Name: Windows(R), Professional edition
   Description: Windows(R) Operating System, RETAIL channel
   Partial Product Key: 3V66T
   License Status: Licensed
   ```

Чтобы получить подробные сведения о лицензировании, выполните следующую команду:

Командная строка Windows

```
slmgr /dlv
```

Дополнительные сведения о **Slmgr** см . bSlmgr.vbs параметрах для получения сведений об активации корпоративных лицензий.

Устранение проблем в процессе обновления

В некоторых случаях у пользователей могут возникнуть проблемы с активацией подписки Windows Корпоративная E3 или E5. Ниже перечислены наиболее распространенные проблемы, с которыми могут столкнуться пользователи.

- Подписка на Windows Корпоративная E3 или E5 истекла, была удалена или не применена.
- Windows Pro так и не была активирована.

При возникновении проблем с активацией подписки на Windows Корпоративная E3 или E5 в области **активации** могут возникать следующие ошибки:

- **Windows Pro не активирована**

  Если Windows Pro не активирована на устройстве, в области **Активация** отображается следующее сообщение:

  `Windows is not activated`

  Кроме того, может отображаться следующее сообщение:

  `We can't activate Windows on this device right now. You can try activating again later or go to the Store to buy genuine Windows. Error code: 0xC004F034.`

  Ниже приведены примеры, в которых может возникнуть эта проблема.
  - На устройстве нет встроенного ключа активации.
  - Начальный выпуск Windows не был Windows Pro. Например, начальный выпуск Windows был Windows Home.

  В таких случаях ключ Windows Pro может потребоваться ввести вручную.

- **Подписка Windows Корпоративная не активна**

  Если устройство с подпиской Windows Корпоративная истекло или удалено, в области **Активация** для **параметра Подписка** отображается следующее сообщение:

  `Windows Enterprise subscription isn't valid.`

> ⓘ **Примечание.**
>
> Если подписка Windows Корпоративная никогда не применялась, панель **Подписка** не отображается.

Проверка соответствия устройств требованиям

Если на устройстве возникают проблемы с активацией лицензий Windows Корпоративная E3 или E5, убедитесь, что оно соответствует всем требованиям:

- На устройствах должна быть установлена поддерживаемая в настоящее время версия Windows Pro. Версии Windows Pro, которые поддерживают эту функцию, не поддерживают.
- Устройства должны быть присоединены к Microsoft Entra ID или присоединены к гибридному домену с помощью Microsoft Entra Connect. Клиенты, объединенные в федерацию с Microsoft Entra ID, также имеют право.
- Для автоматической активации Windows Pro на устройстве должен быть внедрен ключ активации встроенного ПО.

Используйте следующие руководства, чтобы проверить каждое из этих требований:

- **Определите, поддерживается ли в настоящее время версия Windows**.

  Чтобы определить, поддерживается ли в настоящее время версия Windows, выполните следующие действия:

  1. Открытие командной строки
  2. В окне командной строки введите:

Командная строка Windows
`winver.exe`

  3. Откроется окно **Сведения о Windows** , в котором отображаются версия ОС и сведения о сборке Windows.
  4. Сравните сведения из окна **"Сведения о Windows** " с жизненным циклом поддержки Windows:
     - Windows 11 сведения о выпуске.
     - Windows 10 сведения о выпуске.

- **Определите, Microsoft Entra ли устройство присоединено**.

  Чтобы определить, присоединено ли устройство Microsoft Entra:

  1. Откройте командную строку.
  2. В окне командной строки введите:

     Командная строка Windows

     ```
     dsregcmd.exe /status
     ```

  3. Просмотрите выходные данные. В первом разделе **Состояние устройства** убедитесь, что значение **AzureAdJoined** равно **ДА**. Если значение равно **ДА**, устройство присоединяется к Microsoft Entra ID.

     Консоль

     ```
     +----------------------------------------------------------------------+
     | Device State                                                         |
     +----------------------------------------------------------------------+

             AzureAdJoined : YES
          EnterpriseJoined : NO
              DomainJoined : NO
           Virtual Desktop : NOT SET
                Device Name : Demo-PC
     ```

- **Определите, есть ли на устройствах встроенный ключ активации встроенного ПО**.

  Чтобы определить, имеет ли устройство встроенный ключ активации встроенного ПО:

  1. Откройте командную строку Windows PowerShell с повышенными привилегиями.
  2. В командной строке с повышенными привилегиями Windows PowerShell введите:

     PowerShell

     ```
     (Get-CimInstance -query 'select * from
     SoftwareLicensingService').OA3xOriginalProductKey
     ```

  3. Если на устройстве есть встроенный ключ активации встроенного ПО, ключ отображается в выходных данных. Если выходные данные пусты, устройство не имеет встроенного ключа активации. Большинство современных oem-

устройств, предназначенных для запуска поддерживаемых в настоящее время версий Windows, имеют встроенный ключ встроенного ПО.

- **Убедитесь, что пользователю Microsoft Entra назначена лицензия**.

  Дополнительные сведения см. в разделе Назначение лицензий пользователям.

Рекомендуемые методики

Добавление политики условного доступа

Если устройство находится в автономном режиме в течение длительного периода времени, активация подписки может не активироваться автоматически на устройстве. Чтобы устранить эту проблему, используйте политики условного доступа для управления доступом, исключив одно из следующих облачных приложений из своих политик условного доступа с помощью **выбора исключенных облачных приложений**:

- API-интерфейсы службы Универсального магазина и веб-приложение, AppID 45a330b1-b1ec-4cc1-9161-9f03992aa49f.
- Магазин Windows для бизнеса, AppID 45a330b1-b1ec-4cc1-9161-9f03992aa49f.

  > ⓘ **Примечание.**
  >
  > Microsoft Store для бизнеса и Microsoft Store для образования стираются. Дополнительные сведения см. в разделе **Microsoft Store для бизнеса и 31 марта 2023 г**.

Хотя идентификатор приложения одинаков в обоих экземплярах, имя облачного приложения зависит от клиента.

Дополнительные сведения о настройке исключений в политиках условного доступа см. в разделе Исключения приложений.

Установка этой политики условного доступа гарантирует, что активация подписки продолжит работать без проблем.

Начиная с Windows 11 версии 23H2 с KB5034848 или более поздней, пользователи получают запрос на проверку подлинности с всплывающее уведомление, когда активация подписки требуется повторно активировать. Всплывающее уведомление отобразит следующее сообщение:

> **Для учетной записи требуется проверка подлинности**
>
> **Войдите в рабочую или учебную учетную запись, чтобы проверить свои данные.**

Кроме того, в области **Активация** может появиться следующее сообщение:

> **Войдите в рабочую или учебную учетную запись, чтобы проверить свои данные.**

Запрос на проверку подлинности обычно возникает, когда устройство находится в автономном режиме в течение длительного периода времени. Это изменение устраняет необходимость в исключении в политике условного доступа для Windows 11 версии 23H2 с KB5034848 или более поздней. Политику условного доступа по-прежнему можно использовать с Windows 11 версии 23H2 с KB5034848 или более поздней, если запрос на проверку подлинности пользователя через всплывающее уведомление не требуется.

Убедитесь, что клиентский компонент Центра обновления Windows не заблокирован

Если устройство не может подключиться к клиентский компонент Центра обновления Windows, оно может потерять состояние активации или заблокировать обновление до Windows Корпоративная. Убедитесь, что клиентский компонент Центра обновления Windows не заблокированы на устройстве:

- С помощью `gpedit.msc` редактора групповой политики в домене убедитесь, что следующий параметр групповой политики имеет значение **Отключено** или **Не настроено**:

  Конфигурация> компьютера**Административные шаблоны**>**Компоненты**> Windows> клиентский компонент Центра обновления Windows **Управление обновлениями, предлагаемыми службой**> Обновления Windows Server**Не подключайтесь к расположениям клиентский компонент Центра обновления Windows в Интернете**

  Если для этой политики **задано значение Включено**, ее необходимо изменить на **Отключено** или **Не настроено**.

- В следующем разделе реестра:

  `HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate`

  проверка, если значение `DoNotConnectToWindowsUpdateInternetLocations` существует. Если значение существует, убедитесь, что оно имеет REG_DWORD значение `0`. Если

вместо этого задано `1`значение , его необходимо изменить на `0`. Значение можно изменить, выполнив следующую команду из командной строки с повышенными привилегиями:

Командная строка Windows

```
reg.exe add HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate /v
DoNotConnectToWindowsUpdateInternetLocations /t REG_DWORD /d 1 /f
```

> ⓘ **Примечание.**
>
> Убедитесь, что сначала проверка групповую политику **Не подключаться к клиентский компонент Центра обновления Windows расположениям в Интернете**. Если политика **включена**, то этот раздел реестра в конечном итоге будет сброшен обратно `1` в значение даже после того, как он будет установлен вручную `0` через `reg.exe`. Если для политики **Не подключаться к расположениям в Интернете клиентский компонент Центра обновления Windowsзначение Отключено** или **Не настроено**, значение реестра останется равным `0`.

Задержка активации корпоративной лицензии Windows

Активация лицензии Enterprise в Windows может быть отложена. Эта задержка выполняется по умолчанию. Windows использует встроенный кэш при определении допустимости обновления. Это поведение включает обработку ответов, указывающих, что устройство не подходит для обновления. После приобретения, соответствующего требованиям, может потребоваться до четырех дней, прежде чем будет включена возможность обновления и истекает срок действия кэша.

Доступ к виртуальным рабочим столам (VDA)

Подписки на Windows Корпоративная также доступны для виртуализированных клиентов. Корпоративные E3 и E5 доступны для доступа к виртуальному рабочему столу (VDA) в Azure или на другом квалифицированном мультитенантном узле.

Виртуальные машины должны быть настроены для включения подписок Windows Enterprise для VDA. Поддерживаются клиенты, присоединенные к Active Directory и Microsoft Entra. Дополнительные сведения см. в разделе Включение VDA для активации подписки Enterprise.

Связанное содержимое

- Активация подписки Windows.
- Регистрация устройств с Windows в MDM.

Last updated on 14.05.2025

Активация корпоративных лицензий для Windows

Применяется к: ✅ Windows 11, ✅ Windows 10, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

> **Совет**
>
> Ищете сведения о корпоративном лицензировании?
>
> - Скачайте справочное руководство по корпоративному лицензированию Майкрософт.
>
> Ищете сведения об активации розничной торговли?
>
> - Активируйте Windows.
> - Активация продукта для Windows.

Это руководство предназначено для организаций, которые планируют использовать активацию корпоративных лицензий для развертывания и активации Windows.

Активация корпоративных лицензий представляет собой процесс, который заказчики корпоративных лицензий Microsoft используют для автоматизации и администрирования активации операционных систем Windows, Microsoft Office и других продуктов Microsoft в крупных организациях. Корпоративное лицензирование доступно для клиентов, приобретающих программное обеспечение в различных корпоративных программах (например , Open и Select), а также участникам программ, таких как Программа партнеров Майкрософт и Visual Studio Codespace.

Активация корпоративных лицензий — это решение, которое автоматизирует и управляет активацией продукта на компьютерах под управлением Windows, лицензированных по программе корпоративного лицензирования. Активация корпоративных лицензий также используется с другим программным обеспечением Майкрософт (прежде всего пакетами Office), которое продается по соглашениям корпоративного лицензирования и поддерживает активацию корпоративных лицензий.

В этом руководстве содержатся сведения и пошаговые инструкции по выбору метода активации корпоративных лицензий, подходящего для среды, а затем для успешной настройки этого решения. В этом руководстве описываются функции активации корпоративных лицензий и средства для управления активацией корпоративных лицензий.

Для успешного планирования и реализации стратегии активации корпоративных лицензий необходимы следующие элементы:

- ознакомиться и понять процесс активации продукта;
- просмотреть и проанализировать доступные типы или модели активации;
- рассмотреть возможность подключения активируемых клиентов;
- выбрать метод или методы, используемые для каждого типа клиента;
- Определите типы и количество необходимых ключей продукта.
- Определите потребности в мониторинге и отчетности в организации.
- установить и настроить средства, необходимые для поддержки выбранных методов;

Помните, что метод активации не изменяет ответственность организации перед требованиями к лицензированию. Убедитесь, что все программное обеспечение, используемое в организации, должным образом лицензируется и активируется в соответствии с условиями лицензионных соглашений.

Связанное содержимое

- Планирование активации корпоративных лицензий.
- Активируйте с помощью службы управления ключами.
- Активируйте с помощью активации на основе Active Directory.
- Активация клиентов под управлением Windows.
- Мониторинг активации.
- Используйте средство управления активацией корпоративных лицензий.
- Приложение. Сведения, отправляемые в корпорацию Майкрософт во время активации.

Last updated on 14.05.2025

Планирование активации корпоративных лицензий

Применяется к: ✅ Windows 11, ✅ Windows 10, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

> **Совет**
>
> Ищете сведения об активации розничной торговли?
>
> - **Активируйте Windows**.
> - **Активация продукта для Windows**.

Активация продукта — это процесс проверки программного обеспечения у производителя после его установки на определенном компьютере. Активация подтверждает, что продукт является подлинным, а не мошеннической копией. Активация также подтверждает, что ключ продукта или серийный номер действительны и не скомпрометирован или отозван. Активация также устанавливает связь между ключом продукта и конкретной установкой.

Во время активации анализируются сведения о конкретной установке. Для активации через Интернет эти сведения отправляются на сервер корпорации Майкрософт. Эта информация может включать версию программного обеспечения, ключ продукта, IP-адрес компьютера и сведения об устройстве. Методы активации, используемые корпорацией Майкрософт, предназначены для защиты конфиденциальности пользователей и не могут использоваться для отслеживания компьютера или пользователя. Собранные данные подтверждают, что ПО является законно лицензированной копией, и используются для статистического анализа. Корпорация Майкрософт не использует эти сведения для идентификации или связи с пользователем или организацией.

> **Примечание.**
>
> IP-адрес используется только для проверки расположения запроса, так как некоторые выпуски Windows (например, "Начальные" выпуски) можно активировать только на определенных географических целевых рынках.

Каналы распространения и активация

Обычно ПО Майкрософт распространяется по трем основным каналам: в розницу, через изготовителей оборудования (OEM) и в рамках соглашений корпоративного лицензирования. Для каждого канала доступны свои методы активации. Поскольку организации могут приобретать ПО по нескольким каналам одновременно (например, покупать одни продукты в розницу, а другие — по программе корпоративного лицензирования), большинство организаций предпочитают использовать сочетание нескольких методов активации.

Розничная активация

Для розничной активации каждая приобретенная копия поставляется с одним уникальным ключом продукта, который часто называют ключом розничной торговли. Пользователь вводит этот ключ во время установки продукта. Компьютер использует розничный ключ для выполнения активации после окончания установки. В большинстве случаев активация осуществляется через Интернет, но возможна также активация по телефону.

Существуют и другие сценарии распространения. Карточки с ключами продукта доступны для активации предустановленных или скачанных продуктов. Такие программы, как программа обновления Windows Anytime Upgrade и Get Genuine, позволяют пользователям приобретать легальные ключи отдельно от ПО. Эти электронные ключи могут поставляются с носителем, содержащим программное обеспечение, они могут быть отправлены как программное обеспечение, или они могут быть предоставлены на печатном карта или электронной копии. Активация продуктов с этими ключами в любом формате осуществляется одинаково.

Изготовители оборудования

Большинство изготовителей оборудования (OEM) продают системы, включающие стандартную сборку операционной системы Windows. Поставщик оборудования активирует Windows, связывая операционную систему с встроенным ПО или BIOS компьютера. Эта активация происходит до отправки компьютера клиенту, и никаких дополнительных действий не требуется.

Активация OEM действительна при условии, что клиент использует образ системы, предоставленный изготовителем оборудования. Активация OEM доступна только для компьютеров, которые приобретаются через OEM-каналы и содержат предустановленную операционную систему Windows.

Корпоративное лицензирование

Для корпоративного лицензирования предлагаются индивидуальные программы, соответствующие размеру и покупательским предпочтениям организации. Чтобы стать клиентом корпоративного лицензирования, организация должна настроить соглашение о корпоративном лицензировании с корпорацией Майкрософт. Существует распространенное недоразумение при получении лицензий на новый компьютер с помощью корпоративного лицензирования. Есть два законных способа приобрести полную клиентскую лицензию Windows для нового компьютера.

- Предустановка лицензии изготовителем оборудования.
- Покупка коробочного продукта в розницу.

Лицензии, предоставляемые по программам корпоративного лицензирования, например по соглашениям Open License, Select License и Enterprise, включают только обновления для клиентских версий ОС Windows. Прежде чем можно будет воспользоваться правами на обновление, полученными в рамках корпоративного лицензирования, для каждого компьютера под управлением поддерживаемых версий Windows потребуется существующая розничная или oem-версия операционной системы.

Корпоративное лицензирование также доступно через определенные подписки или программы членства, такие как Microsoft Partner Network и Visual Studio Codespace. Эти корпоративные лицензии могут содержать определенные ограничения или другие изменения общих условий, применимых к корпоративному лицензированию.

> ⓘ **Примечание.**
>
> Некоторые выпуски операционной системы, например Windows Корпоративная, и некоторые выпуски программного обеспечения доступны только в рамках соглашений о корпоративном лицензировании или подписок.

Модели активации

Пользователи и ИТ-отделы в основном не могут выбирать, каким образом активировать продукты, приобретенные по розничным или OEM-каналам. Oem выполняет активацию на фабрике, и пользователю или ИТ-отделу не нужно предпринимать никаких действий по активации.

При использовании розничного продукта средство управления активацией корпоративных лицензий (VAMT), который рассматривается далее в этом руководстве, помогает отслеживать ключи и управлять ими. Для каждой активации розничной торговли можно выбрать следующие варианты:

- Активация через Интернет.
- Активация по телефону.
- Активация прокси-сервера VAMT.

Активация по телефону в основном используется в ситуациях, когда компьютер изолирован от всех сетей. Активация прокси-сервера VAMT с ключами розничной торговли иногда используется, когда ИТ-отдел хочет централизовать активацию розничной торговли. VAMT также можно использовать, если компьютер с розничной версией операционной системы изолирован от Интернета, но подключен к локальной сети. Однако для продуктов с корпоративной лицензией необходимо определить оптимальный метод или сочетание методов для использования в среде. Для поддерживаемых в настоящее время версий Windows Pro и Enterprise можно выбрать одну из следующих трех моделей:

- Несколько ключей активации (MAK).
- KMS.
- Активация на основе Active Directory.

> ⓘ **Примечание.**
>
> Активация на основе маркеров для Windows Enterprise (включая LTSC) и Windows Server доступна в определенных ситуациях, когда утвержденные клиенты полагаются на инфраструктуру открытых ключей в изолированной среде с высоким уровнем безопасности. За дополнительными сведениями обратитесь к группе по учетным записям Майкрософт или представителю службы.

Ключ многократной активации

Ключ множественной активации (MAK) обычно используется в небольших или средних организациях, имеющих соглашение о корпоративном лицензировании, но не отвечающих требованиям по эксплуатации KMS. Mak также можно использовать, если предпочтителен более простой подход. MAK также позволяет постоянно активировать:

- Компьютеры, изолированные от KMS.
- Компьютеры, входящие в изолированную сеть, в которых недостаточно компьютеров для использования KMS.

Чтобы использовать ключ MAK, он должен быть установлен на активируемых компьютерах. Ключ MAK используется для однократной активации при помощи размещенных в Интернете служб активации Майкрософт, по телефону или путем прокси-активации с помощью VAMT.

В упрощенном представлении ключ MAK аналогичен розничному ключу, за исключением того, что MAK можно применять для активации нескольких компьютеров. Каждый ключ MAK можно использовать строго определенное число раз. VAMT помогает отслеживать количество выполненных активаций с помощью каждого ключа и количество оставшихся активаций.

Организации могут загрузить ключи MAK и KMS с веб-сайта Microsoft Volume Licensing Service Center. Каждый MAK имеет предустановленное число активаций, которое основано на проценте от количества лицензий, приобретенных организацией. Однако количество доступных активаций можно увеличить с помощью MAK, вызвав корпорацию Майкрософт.

Служба управления ключами

С помощью службы управления ключами (KMS) ИТ-специалисты могут проводить активации в локальной сети, так что отдельным компьютерам больше не нужно будет подключаться к серверам Майкрософт для активации продуктов. KMS — это упрощенная служба, которая не требует выделенной системы и может быть легко размещена в системе, предоставляющей другие службы.

Корпоративные выпуски поддерживаемых в настоящее время версий Windows и Windows Server автоматически подключаются к системе, где размещается KMS для запроса активации. Никаких действий от пользователя не требуется.

Для KMS требуется минимальное количество компьютеров(физических или виртуальных машин) в сетевой среде. Организация должна иметь по крайней мере пять компьютеров для активации поддерживаемых в настоящее время версий Windows Server и не менее 25 компьютеров для активации клиентских компьютеров под управлением поддерживаемых версий клиента Windows. Эти минимальные количества называются *порогами активации*.

Планирование использования KMS включает выбор оптимального расположения узла KMS и количества узлов KMS. Один узел KMS может обрабатывать большое количество активаций, но организации часто развертывают два узла KMS для обеспечения доступности. KMS можно разместить на клиентском компьютере или на сервере. Настройка KMS рассматривается далее в этом руководстве.

Активация с помощью Active Directory

Активация на основе Active Directory аналогична активации с помощью KMS, но активированный компьютер не должен поддерживать периодическое подключение к узлу KMS. Вместо этого присоединенный к домену компьютер под управлением поддерживаемых в настоящее время версий Windows или Windows Server запрашивает

инструкции ADDS для объекта активации корпоративных лицензий, хранящегося в домене. Операционная система проверяет цифровые подписи, содержащиеся в объекте активации, а затем активирует устройство.

Активация с помощью Active Directory позволяет организациям активировать компьютеры через подключение к собственному домену. Многие компании имеют компьютеры в удаленных расположениях или филиалах, где нецелесообразно подключаться к KMS или не достигает порогового значения активации KMS. Вместо использования MAK активация на основе Active Directory позволяет активировать компьютеры под управлением поддерживаемых в настоящее время версий Windows и Windows Server при условии, что компьютеры могут связаться с доменом компании. Активация на основе Active Directory предлагает преимущество расширения служб активации корпоративных лицензий везде, где уже есть домен.

Сеть и подключения

Современная корпоративная сеть характеризуется множеством нюансов и взаимосвязей. В этом разделе рассматривается оценка сети организации и доступных подключений, чтобы определить, как происходит активация корпоративных лицензий.

Основная сеть

Основная сеть организации — это часть сети, которая обеспечивает стабильное, высокоскоростное и надежное подключение к серверам инфраструктуры. Во многих случаях основная сеть также подключена к Интернету. Однако подключение к Интернету не является обязательным условием для использования активации на основе KMS или Active Directory после того, как сервер KMS или ADDS будет настроен и активен. Основная сеть организации, скорее всего, состоит из нескольких сегментов сети. Во многих организациях основная сеть составляет большую часть бизнес-сети.

В основной сети рекомендуется централизованное решение KMS. Также можно использовать активацию на основе Active Directory, но во многих организациях KMS может по-прежнему требоваться для компьютеров, которые не присоединены к домену. Некоторые администраторы предпочитают использовать оба решения, чтобы получить максимальную гибкость, другие же выбирают только решение на основе KMS для упрощения работы. Активация на основе Active Directory в качестве единственного решения работает, если все клиенты в организации работают под управлением поддерживаемых в настоящее время версий Windows.

Типичная основная сеть, включающая узел KMS, показана на рис. 1.

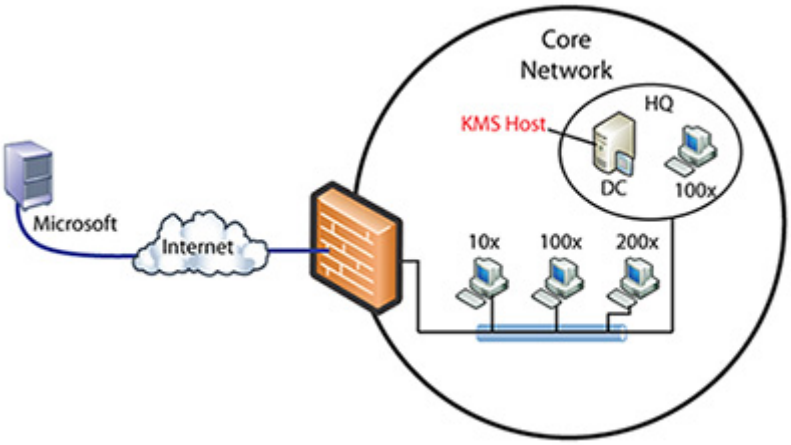


Рисунок 1. Типичная основная сеть

Изолированные сети

В крупной сети некоторые сегменты могут быть изолированы либо по соображениям безопасности, либо из-за географических проблем или проблем с подключением.

Изоляция из соображений безопасности

Сегмент сети, изолированный от основной сети брандмауэром или отключенный от других сетей, иногда называется *зоной с высоким уровнем безопасности*. Оптимальный способ активации компьютеров в изолированной сети зависит от политик безопасности, действующих в организации.

Если изолированная сеть может:

- Доступ к основной сети с помощью исходящих запросов через TCP-порт 1688
- Разрешено принимать удаленные вызовы процедур (RPC)

активацию можно выполнить с помощью KMS в основной сети, избегая необходимости достижения дополнительных пороговых значений активации.

Если изолированная сеть полностью участвует в корпоративном лесу и может устанавливать типичные подключения к контроллерам домена, например:

- Использование протокола LDAP для запросов
- Использование службы доменных имен (DNS) для разрешения имен

тогда этот сценарий является хорошей возможностью использовать активацию на основе Active Directory для поддерживаемых в настоящее время версий Windows и Windows Server.

Если изолированная сеть не может взаимодействовать с сервером KMS основной сети и не может использовать активацию на основе Active Directory, узел KMS можно настроить в изолированной сети. Такая конфигурация показана на рис. 2. Однако если изолированная сеть содержит только несколько компьютеров, порог активации KMS не достигнет. В этом случае для активации можно использовать ключи MAK.

Если сеть полностью изолирована, рекомендуется использовать активацию, не зависят от MAK, возможно, с помощью телефона, но также возможна активация прокси-сервера VAMT. Пакеты MAK также можно использовать для активации новых компьютеров во время установки, прежде чем они будут помещены в изолированную сеть.

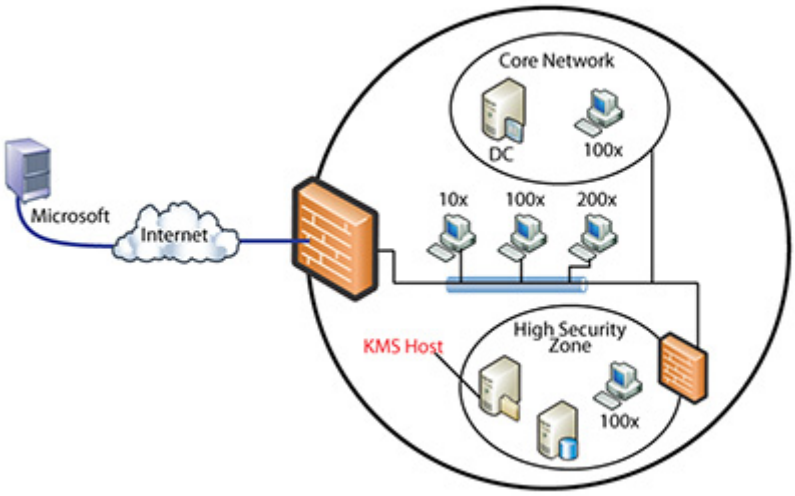


Рисунок 2. Новый узел KMS в изолированной сети

Филиалы и удаленные сети

От добычи полезных ископаемых до судов в море, организации часто имеют несколько компьютеров, которые не легко подключиться к основной сети или Интернету. В филиалах некоторых организаций имеются крупные и тесно связанные друг с другом сетевые сегменты, однако их подключение к остальным корпоративным подразделениям осуществляется по медленным или ненадежным каналам глобальной сети. В таких ситуациях существует несколько вариантов.

- **Активация с помощью Active Directory**. На любом сайте, где клиентские компьютеры работают под управлением поддерживаемых версий Windows, активация на основе Active Directory поддерживается, и ее можно активировать, присоединившись к домену.
- **Локальный KMS-сервер**. Если на объекте насчитывается не менее 25 клиентских компьютеров, можно провести активацию с помощью локального KMS-сервера.
- **Удаленный (основной) KMS-сервер**. Если удаленный сайт имеет подключение к существующему KMS, возможно, через виртуальную частную сеть (VPN) к основной

сети, этот KMS можно использовать. Использование существующего KMS означает, что порог активации должен быть достигнут только на этом сервере.

- **Активация с помощью MAK**. Если на узле мало компьютеров и у него нет связи с существующим узлом KMS, оптимальным вариантом является активация с помощью MAK.

Неподключенные компьютеры

Некоторые пользователи могут находиться в удаленных расположениях или перемещаться во многие расположения. Это типичный сценарий для мобильных клиентов, например компьютеров торговых представителей или других пользователей, работающих удаленно, но не в филиалах. Данный сценарий также применим к удаленным филиалам, не имеющим подключения к основной сети. Этот филиал можно считать "изолированной сетью", где количество компьютеров составляет один. Отключенные компьютеры могут использовать активацию на основе Active Directory, KMS или MAK в зависимости от частоты подключения компьютеров к основной сети.

Активацию на основе Active Directory можно использовать на компьютерах, если они соответствуют следующим условиям:

- Компьютер присоединен к домену.
- На компьютере установлена поддерживаемая в настоящее время версия Windows или Windows Server.
- Компьютер подключается к домену не реже одного раза в 180 дней напрямую или через VPN.

В противном случае для компьютеров, которые редко или никогда не подключаются к сети, следует использовать независимую активацию MAK через телефон или Через Интернет.

Лаборатории тестирования и разработки

В лабораторных средах часто присутствует большое количество виртуальных компьютеров, причем конфигурация физических компьютеров и виртуальных компьютеров часто меняется. Поэтому сначала определите, требуется ли активация компьютеров в лабораториях тестирования и разработки. Поддерживаемые в настоящее время выпуски Windows, включающие корпоративное лицензирование, работают в обычном режиме, даже если они не могут активироваться немедленно.

Если тестовые или разрабатываемые копии операционной системы находятся в рамках лицензионного соглашения, компьютеры лаборатории, возможно, не нужно

активировать, если они часто перестраиваются. Если компьютеры лаборатории необходимо активировать, обработайте лабораторию как изолированную сеть и используйте методы, описанные выше в этом руководстве. В лабораториях с высокой текучестью компьютеров и несколькими клиентами KMS необходимо отслеживать количество активаций KMS. Время кэширования KMS запросов активации, возможно, потребуется изменить. По умолчанию используется значение 30 дней.

Сопоставление сети с методами активации

Оценив сетевое подключение и количество компьютеров на каждом сайте, можно определить сведения, необходимые для определения наиболее подходящих методов активации. Эти сведения можно заполнить в таблице 1, чтобы помочь принять это решение.

Таблица 1. Критерии для методов активации

Развернуть таблицу

Критерий	Метод активации
Количество присоединенных к домену компьютеров, которые будут подключаться к контроллеру домена по крайней мере каждые 180 дней. Компьютеры могут быть мобильными, полуизолированными либо располагаться в филиале или основной сети.	Активация с помощью Active Directory
Количество компьютеров в основной сети, которые будут подключаться по крайней мере каждые 180 дней напрямую или через VPN. В основной сети должен быть достигнут порог активации через KMS.	KMS (централизованная)
Количество компьютеров, которые не подключаются к сети по крайней мере раз в 180 дней, или если ни один из сетей не соответствует порогу активации.	MAK
Количество компьютеров в полуизолированных сетях, имеющих подключение к KMS в основной сети.	KMS (централизованная)
Количество компьютеров в изолированных сетях, где достигнуто пороговое значение активации KMS.	KMS (локальная)
Количество компьютеров в изолированных сетях, на которых не достигнуто пороговое значение активации KMS.	MAK
Количество компьютеров в лабораториях тестирования и разработки, которые не будут активированы.	Нет

Критерий	Метод активации
Количество компьютеров без корпоративной лицензии для розничной торговли.	Розничная (через Интернет или по телефону)
Количество компьютеров без корпоративной лицензии OEM.	OEM (на заводе)
Общее количество активаций компьютера. Этот итог должен соответствовать общему количеству лицензированных компьютеров в организации.	

Выбор и приобретение ключей

Когда известно, какие ключи необходимы, ключи должны быть получены. В целом получить ключи многократной установки можно двумя способами.

- Перейдите в раздел **Ключи продуктов** веб-сайта Microsoft Volume Licensing Service Center для следующих соглашений: Open, Open Value, Select, Enterprise и Services Provider License.
- Обратитесь в Центр активации Майкрософт.

Ключи узла KMS

Для узла KMS требуется ключ, который активирует (проверяет подлинность) узла KMS в Майкрософт. Этот ключ называется *ключом узла KMS*, но формально он называется *ключом корпоративной лицензии (CSVLK) для конкретного клиента Майкрософт* . В некоторых документах и справочниках по Интернету используется термин ключ KMS, но CSVLK является правильным названием для текущей документации и средств управления.

Узел KMS под управлением поддерживаемой в настоящее время версии Windows Server может активировать как windows Server, так и клиентские операционные системы Windows. Ключ узла KMS также необходим для создания объектов активации в ADDS, как описано далее в этом руководстве. Ключ узла KMS необходим для всех настроенных KMS. Кроме того, необходимо определить, будет ли использоваться активация на основе Active Directory.

Универсальные ключи корпоративного лицензирования

Если компьютеры активируются с помощью KMS или активации на основе Active Directory при использовании пользовательского установочного носителя или образа для установки Windows, установите универсальный ключ корпоративной лицензии (GVLK) при создании

пользовательского установочного носителя или образа. GVLK должен соответствовать устанавливаемой версии Windows.

Установочный носитель из выпусков операционной системы Windows microsoft for Enterprise может уже содержать GVLK. Один ключ GVLK доступен для каждого типа установки. GVLK активирует программное обеспечение не на серверах активации Майкрософт, а для объекта активации на основе KMS или Active Directory. Иными словами, GVLK не работает, если не найден допустимый ключ узла KMS. GVLK — это единственные ключи продуктов, которые не нужно хранить в конфиденциальном режиме.

Как правило, GVLK не требуется вводить вручную, если компьютер:

- Активируется с помощью ключа MAK или розничной торговли.
- Преобразование в активацию KMS или активацию на основе Active Directory.

Если необходимо найти GVLK для определенного клиентского выпуска, см. статью Активация клиентов и ключи продуктов служб управления ключами (KMS).

Ключи многократной активации

Также требуются ключи MAK с соответствующим количеством доступных активаций. Количество использования MAK можно увидеть на веб-сайте Центра обслуживания корпоративного лицензирования или в VAMT.

Выбор узла KMS

Для KMS не требуется выделенный сервер. Его можно разместить совместно с другими службами, такими как контроллеры домена ADDS и контроллеры домена только для чтения.

Узлы KMS могут работать на физических компьютерах или виртуальных машинах с любой поддерживаемой операционной системой Windows. Узел KMS под управлением поддерживаемых в настоящее время версий Windows Server может активировать любой клиент Или серверную операционную систему Windows, поддерживающую активацию корпоративных лицензий. Узел KMS под управлением поддерживаемой версии клиента Windows может активировать только компьютеры с поддерживаемой версией клиента Windows.

Один узел KMS поддерживает неограниченное число клиентов KMS, но Майкрософт рекомендует развертывать минимум два узла KMS для обеспечения отказоустойчивости. Однако, поскольку все больше клиентов активируются с помощью активации на основе

Active Directory, KMS и избыточность KMS могут не потребоваться. Большинство организаций могут использовать всего два узла KMS для всей инфраструктуры.

Активация с помощью KMS показана на рис. 3 и происходит следующим образом.

1. Администратор настраивает узел KMS и устанавливает ключ узла KMS с использованием консоли VAMT.
2. Майкрософт проверяет ключ узла KMS, и узел начинает ожидать запросы.
3. Узел KMS обновляет записи ресурса в DNS, чтобы дать клиентам возможность найти узел KMS. Добавление записей DNS вручную требуется, если среда не поддерживает протокол динамического обновления DNS.
4. Клиент с установленным ключом GVLK использует DNS, чтобы обнаружить узел KMS.
5. Клиент отправляет один пакет узлу KMS.
6. Узел KMS записывает сведения о клиенте, отправившем запрос (с использованием идентификатора клиента). Идентификаторы клиентов используются для подсчета количества клиентов и определения случаев, когда один и тот же компьютер запрашивает активацию повторно. Идентификатор клиента применяется только для определения того, достигнуты ли пороги активации. Идентификаторы не хранятся постоянно и не передаются в корпорацию Майкрософт. В случае перезапуска KMS сбор идентификаторов клиентов начинается снова.
7. Если ключ узла KMS соответствует продуктам в GVLK, узел KMS отправляет один пакет обратно клиенту. Этот пакет содержит количество компьютеров, запрашивающих активацию с этого узла KMS.
8. Если данное количество превышает порог активации для активируемого продукта, то клиент активируется. Если порог активации не достигнут, клиент пытается повторить попытку.

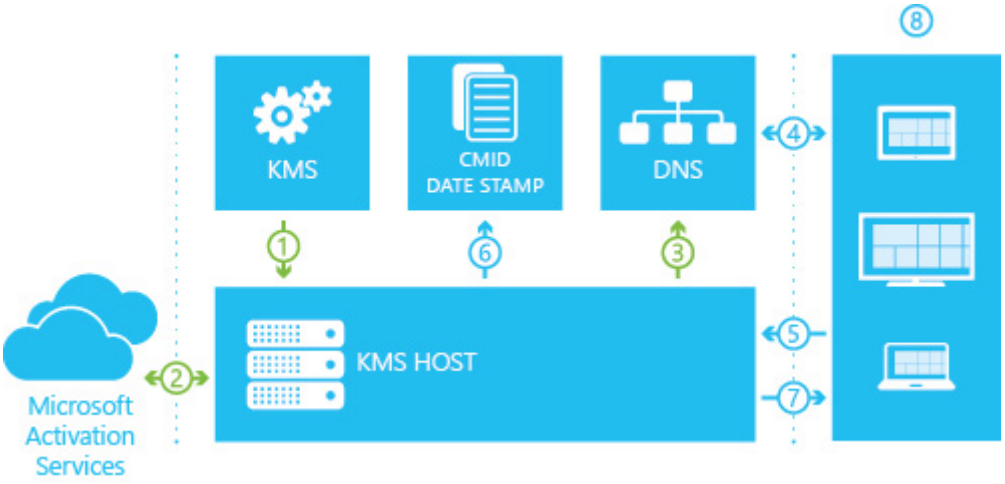


Рисунок 3. Процесс активации с помощью KMS

Связанное содержимое

- Активация корпоративных лицензий для Windows.

Last updated on 14.05.2025

Активация с помощью службы управления ключами

Применяется к: ✅ Windows 11, ✅ Windows 10, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

> **Совет**
>
> Сведения об активации розничной торговли см. в следующих статьях:
>
> - Активация Windows
> - Активация продукта для Windows

Активацию корпоративных лицензий можно выполнить с помощью службы управления ключами (KMS). KMS можно разместить как в клиентской версии Windows, так и в Windows Server.

Служба управления ключами в клиентской версии Windows

Установка ключа узла KMS на компьютере под управлением клиентской версии Windows позволяет использовать следующие сценарии для этого узла KMS:

- Активация других компьютеров под управлением той же клиентской версии Windows.
- Активация других компьютеров под управлением более ранних клиентских версий Windows.

Клиенты находят сервер KMS с помощью записей ресурсов в DNS, поэтому требуется определенная конфигурация DNS. Этот сценарий может быть полезным, если организация использует активацию корпоративных лицензий для клиентов и активацию на основе MAK для меньшего числа серверов.

Чтобы включить функции KMS, на узле KMS устанавливается ключ KMS. Затем узел активируется через Интернет или по телефону с помощью служб активации Майкрософт.

Настройка KMS в клиентской версии Windows

KMS можно активировать в клиентских версиях Windows с помощью `slmgr.vbs`. Чтобы активировать KMS в клиентской версии Windows, выполните следующие действия.

1. Откройте окно командной строки с повышенными привилегиями.
2. В окне командной строки с повышенными привилегиями выполните следующую команду, чтобы установить ключ KMS:

   Командная строка Windows

   ```
   cscript.exe slmgr.vbs /ipk <KMS_Key>
   ```

3. После установки ключа KMS его необходимо активировать одним из следующих методов:

   - Чтобы активировать в сети, в окне командной строки с повышенными привилегиями выполните следующую команду:

   Командная строка Windows

   ```
   cscript.exe slmgr.vbs /ato
   ```

   - Чтобы активировать по телефону, выполните следующие действия.

     a. В окне командной строки с повышенными привилегиями выполните следующую команду:

     Командная строка Windows

     ```
     cscript.exe slmgr.vbs /dti
     ```

     Эта команда должна отобразить идентификатор установки.

     b. Позвоните по телефонным номерам службы поддержки корпоративного лицензионного ключа Майкрософт. Следуйте голосовой подсказке и при появлении запроса введите идентификатор установки, полученный на предыдущем шаге.

     c. Продолжайте следовать голосовой подсказке. При появлении запроса запишите 48-значный идентификатор подтверждения для активации ОС, указанный в запросах.

     d. В окне командной строки с повышенными привилегиями выполните следующую команду:

     Командная строка Windows

     ```
     cscript.exe slmgr.vbs /atp <confirmation_ID_from_previous_step>
     ```

Служба управления ключами в Windows Server

Установка ключа узла KMS на компьютер под управлением Windows Server позволяет активировать компьютеры под управлением той же или более ранней версии Windows Server. Кроме того, он также позволяет активировать клиентские версии Windows.

> ⓘ **Внимание**
>
> Ключ KMS клиента не может быть установлен в KMS в Windows Server.

Настройка KMS в Windows Server

1. Войдите на сервер Windows Server с учетной записью с учетными данными локального администратора.
2. Откройте **Диспетчер сервера**.
3. В меню **Управление** в **диспетчере сервера** выберите **Добавить роли и компоненты**. Откроется окно **Мастер добавления ролей и компонентов** .
4. В **мастере добавления ролей и компонентов** выполните следующие действия.
   a. На странице **Перед началом работы** нажмите кнопку **Далее >** .
   b. На странице **Выбор типа**/ установки**выберитеУстановка на основе ролей или компонентов**, а затем нажмите кнопку **Далее>**.
   c. На странице **Выбор сервера**/ назначения убедитесь, что выбран параметр **Выбрать сервер из пула серверов**. В разделе **Пул серверов** выберите сервер, на котором нужно установить KMS, а затем нажмите кнопку **Далее >** .
   d. На странице **Выбор ролей/сервера** в разделе **Роли** выберите **Службы активации корпоративных** лицензий и нажмите кнопку **Далее >** .
   e. В появившемся окне **Добавление компонентов, необходимых для служб активации корпоративных лицензий** ? нажмите кнопку **Добавить компоненты** , а затем нажмите кнопку **Далее >** .
   f. На**странице**Выбор компонентов**/ нажмите кнопку **Далее>**.
   g. На странице **Службы активации корпоративных лицензий** нажмите кнопку **Далее >** .

h. На странице **Подтверждение выбора установки/подтверждение нажмите** кнопку **Установить** .

i. Установка может занять несколько минут. После завершения установки роли нажмите кнопку **Закрыть** .

5. Перейдите в **меню**> "Пуск" **Администрирование Windows** и выберите **Средства активации корпоративных лицензий**. Откроется окно **Средства активации корпоративных** лицензий.

6. В окне **Средства активации корпоративных лицензий** :

a. На странице**Введениев средства**/ активации корпоративных лицензий нажмите кнопку **Далее>**.

b. На странице **Выбор типа активации метода/активации** корпоративных лицензий выберите параметр **Служба управления ключами (KMS)** и укажите компьютер, который выступает в качестве узла KMS. Этот компьютер может быть сервером, на котором была установлена роль KMS, или другим сервером или клиентским компьютером. После указания сервера или компьютера нажмите кнопку **Далее >** .

c. На странице Управление**ключом продукта** узла /**KMS**введите ключ узла KMS в текстовом поле **Установка ключа узла KMS** и нажмите кнопку **Зафиксировать**.

d. Если будет предложено подтвердить замену существующего ключа, выберите **Да**.

e. После установки ключа продукта на странице **Установка ключа продукта Успешное/управление ключами** продукта убедитесь, что выбран параметр **Активировать продукт** , а затем нажмите кнопку **Далее >** , чтобы начать процесс активации.

f. На странице **Активация/управления ключами продукта** убедитесь, что текущий продукт отображается в меню **Выбор продукта** , а затем выберите нужный метод активации. Доступные методы:

- **Активный в сети** . Если выбран этот параметр, нажмите кнопку **Зафиксировать** , чтобы завершить активацию продукта в сети.

- **Активен по телефону** . Если выбран этот параметр:

i. Выберите нужное расположение в раскрывающемся меню **Выберите расположение** и нажмите кнопку **Далее >** .

ii. На странице **Активация по телефону/управление ключами продукта** следуйте инструкциям, чтобы активировать продукт по телефону.

iii. После завершения нажмите кнопку **Зафиксировать** .

g. На странице **Активация успешное/управление ключами продукта** просмотрите параметры конфигурации:

- Если параметры конфигурации выполняются должным образом, нажмите кнопку **Закрыть** .
- Если требуется изменить конфигурацию, выполните следующие действия:

  i. Нажмите кнопку **Далее >** .

  ii. На странице **Настройка параметров службы управления ключами или управления ключами продукта** внесите необходимые изменения в конфигурацию и нажмите кнопку **Фиксация** .

  iii. На**странице Конфигурация выполнена**/ успешно, нажмите кнопку **Закрыть**.

После настройки узла KMS он начинает прослушивать запросы на активацию. Однако клиенты не активируются успешно до тех пор, пока не будет достигнуто пороговое значение активации.

Проверка конфигурации службы управления ключами

Активацию корпоративных служб KMS можно проверить с сервера узла KMS или с клиентского компьютера. Для активации корпоративных служб KMS требуется минимальное пороговое значение в 25 компьютеров перед обработкой запросов активации. Описанный здесь процесс проверки увеличивает число активаций каждый раз, когда клиентский компьютер обращается к узлу KMS. Если порог активации не достигнут, проверка создает сообщение об ошибке вместо сообщения подтверждения.

> ⓘ **Примечание.**
>
> Если активация на основе Active Directory была настроена перед настройкой активации KMS, необходимо использовать клиентский компьютер, который не пытается активировать себя с помощью активации на основе Active Directory.

Например, клиентский компьютер, который является компьютером рабочей группы, который не присоединен к домену.

Для проверки действия активации корпоративной лицензии KMS выполните следующие действия.

1. Откройте журнал событий на узле KMS и убедитесь, что он опубликован в DNS.
2. На клиентском компьютере откройте окно командной строки с повышенными привилегиями и выполните команду:

   Командная строка Windows

   ```
   cscript.exe slmgr.vbs /ato
   ```

   Команда `/ato` вызывает попытку активации операционной системы с помощью ключа, установленного в операционной системе. Ответ должен отображать состояние лицензии и подробные сведения о версии Windows.
3. На клиентском компьютере или узле KMS откройте окно командной строки с повышенными привилегиями и выполните команду.

   Командная строка Windows

   ```
   cscript.exe slmgr.vbs /dlv
   ```

   Команда `/dlv` отображает подробные сведения о лицензировании. В ответ должно появиться сообщение о недостаточно большом значении счетчика активации KMS. Этот тест подтверждает правильность работы KMS, даже если клиент не активирован.

Дополнительные сведения об использовании и синтаксисе скрипта `slmgr.vbs` см. в разделе ПараметрыSlmgr.vbs.

ⓘ Внимание

Для успешной активации клиентам требуется подключение RPC через TCP/IP к узлу KMS. Дополнительные сведения см. в статье **Планирование активации служб управления ключами (KMS): требования к сети** и **ошибки удаленного вызова процедур (RPC).**

Связанное содержимое

- Планирование активации служб управления ключами (KMS).

Last updated on 14.05.2025

Активация с помощью Active Directory

Применяется к: ✅ Windows 11, ✅ Windows 10, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Microsoft Office

> **Совет**
>
> Ищете сведения об активации розничной торговли?
>
> - Активируйте Windows.
> - Активация продукта для Windows.

Активация на основе Active Directory реализуется как служба ролей, которая использует доменные службы Active Directory (ADDS) для хранения объектов активации. Активация на основе Active Directory требует обновления схемы леса в `adprep.exe` поддерживаемой ОС сервера. После обновления схемы старые контроллеры домена по-прежнему могут активировать клиенты.

Все присоединенные к домену компьютеры с поддерживаемой ОС с универсальным ключом корпоративной лицензии (GVLK) активируются автоматически и прозрачно. Присоединенные к домену компьютеры остаются активированными до тех пор, пока они остаются членами домена и поддерживают периодический контакт с контроллером домена. Активация выполняется после запуска службы лицензирования. При запуске этой службы компьютер автоматически обращается к ADD, получает объект активации и активируется без вмешательства пользователя.

Чтобы разрешить компьютерам с GVLK активировать себя, используйте консоль средства активации корпоративных лицензий или средство управления активацией корпоративных лицензий (VAMT) в более ранних версиях Windows Server, чтобы создать объект в лесу ADDS. Объект активации создается путем отправки ключа узла службы управления ключами (KMS) в Корпорацию Майкрософт, как показано на рис. 10.

Процесс заключается в следующем.

1. Выполните *одну из* следующих задач:

   - Установите роль сервера служб активации корпоративных лицензий на контроллере домена, а затем добавьте ключ узла KMS с помощью мастера средств активации корпоративных лицензий.

   - Расширьте уровень схемы домена до Windows Server 2012 R2 или более поздней версии, а затем добавьте ключ узла KMS с помощью VAMT.

2. Майкрософт проверяет ключ узла KMS, и создается объект активации.

3. Клиентские компьютеры активируются, получая объект активации от контроллера домена во время запуска.

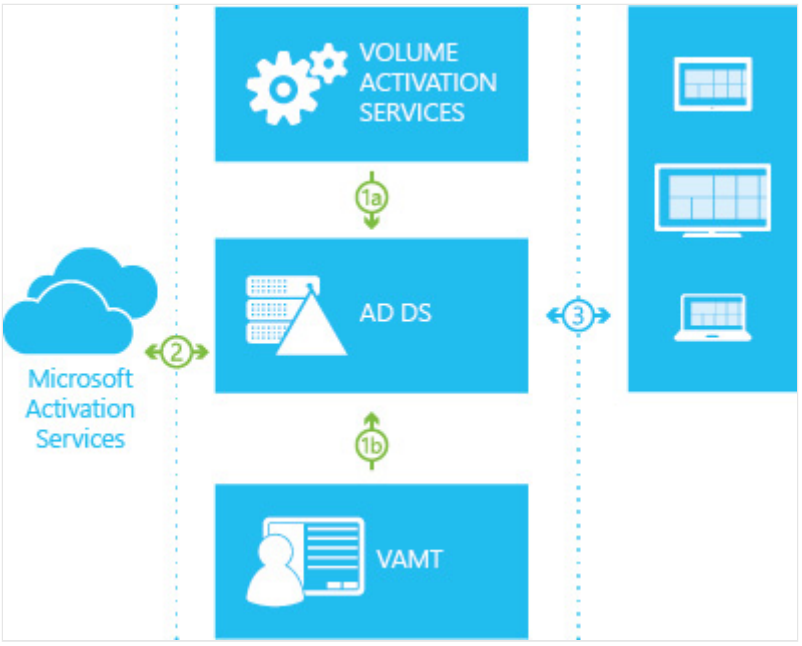


Рисунок 10. Процесс активации с помощью Active Directory

Для сред, в которых все компьютеры присоединены к домену и работают под управлением поддерживаемой версии ОС, активация на основе Active Directory является лучшим вариантом для активации клиентских компьютеров и серверов. Активация на основе Active Directory может разрешить удаление всех узлов KMS из среды. Если среда содержит один из следующих элементов:

- Более ранние версии операционных систем и приложений с корпоративной лицензией
- Компьютеры рабочей группы за пределами домена

узел KMS по-прежнему необходим для поддержания состояния активации.

Клиенты, активированные с помощью активации на основе Active Directory, поддерживают состояние активации в течение 180 дней с момента последнего контакта с доменом. Они периодически пытаются повторно активировать до этого и в конце 180-дневного периода. По умолчанию попытки повторной активации выполняются каждые 7 дней.

При возникновении события повторной активации клиент запрашивает объект активации ADDS. Клиентские компьютеры проверяют объект активации и сравнивают его с локальной версией, определяемой ключом GVLK. Если объект и GVLK совпадают, происходит повторная активация. Если не удается получить объект ADDS, клиентские компьютеры используют активацию KMS. Если компьютер удален из домена и компьютер

или служба Защиты программного обеспечения перезапущены, Windows изменит состояние на **Не активировано** , и компьютер пытается активировать с помощью KMS.

Пошаговая настройка: активация с помощью Active Directory

> ⓘ **Примечание.**
>
> Администратор, выполнив следующие действия, должен быть членом локальной группы **администраторов** на всех компьютерах, упомянутых в этих шагах. Кроме того, они также должны быть членом группы **администраторов предприятия** , так как настройка активации на основе Active Directory изменяет параметры на уровне леса.

Чтобы настроить активацию на основе Active Directory в поддерживаемой версии Windows Server, выполните следующие действия.

1. Используйте учетную запись с учетными данными **администратора домена** и **администратора предприятия** для входа в контроллер домена.
2. Запустите **диспетчер сервера**.
3. Добавьте роль **Служб активации корпоративных лицензий** , как показано на рис. 11.

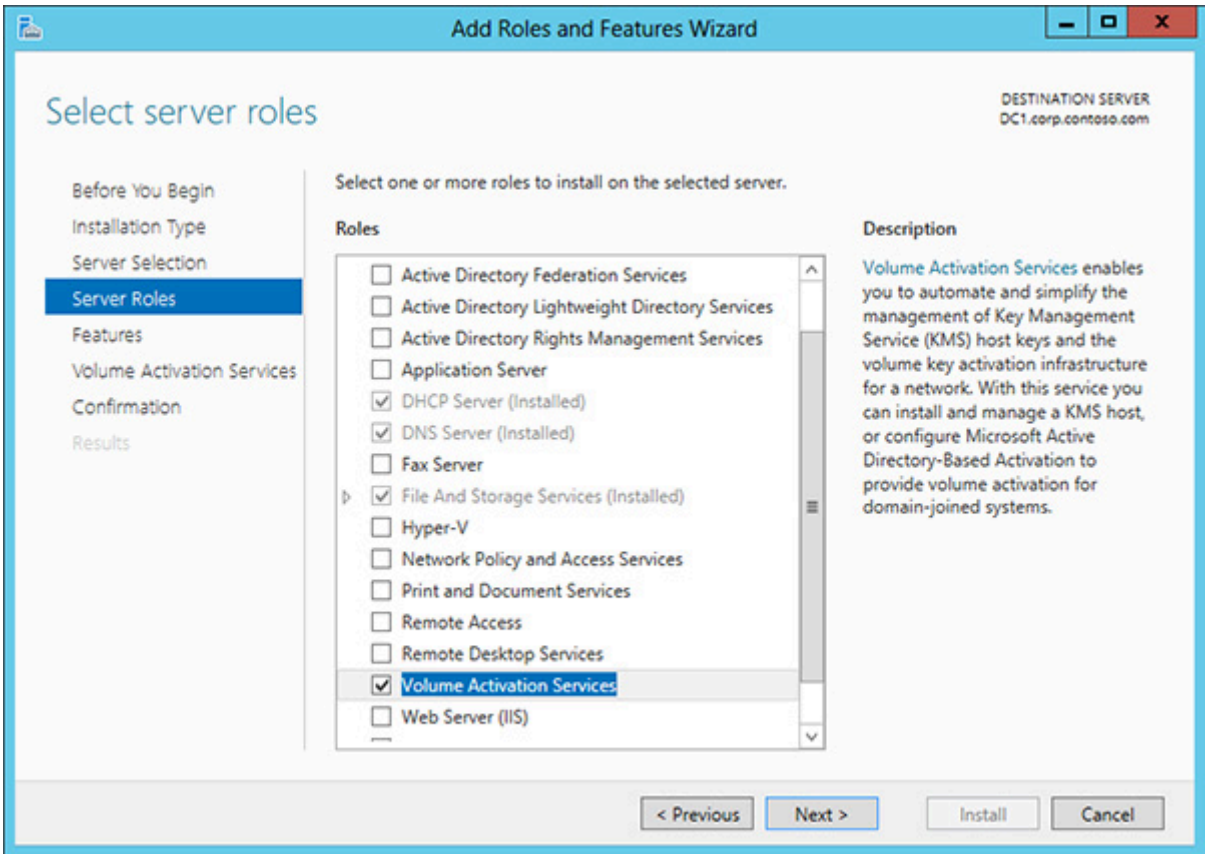


Рисунок 11. Добавление роли "Службы активации корпоративных лицензий"

4. Выберите **Средства активации корпоративных лицензий**, как показано на рис. 12.

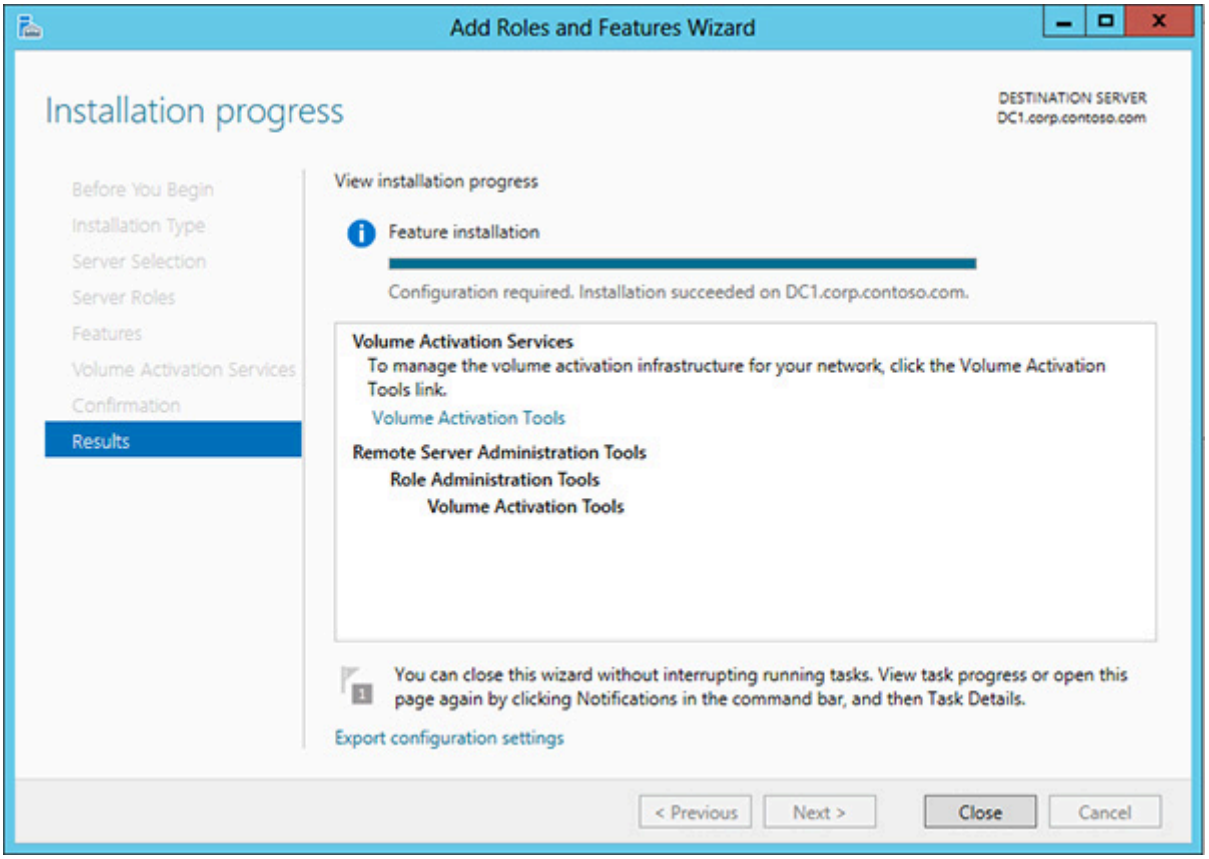


Рисунок 12. Запуск средств активации корпоративных лицензий

5. Выберите параметр **Активная активация Directory-Based** , как показано на рис. 13.

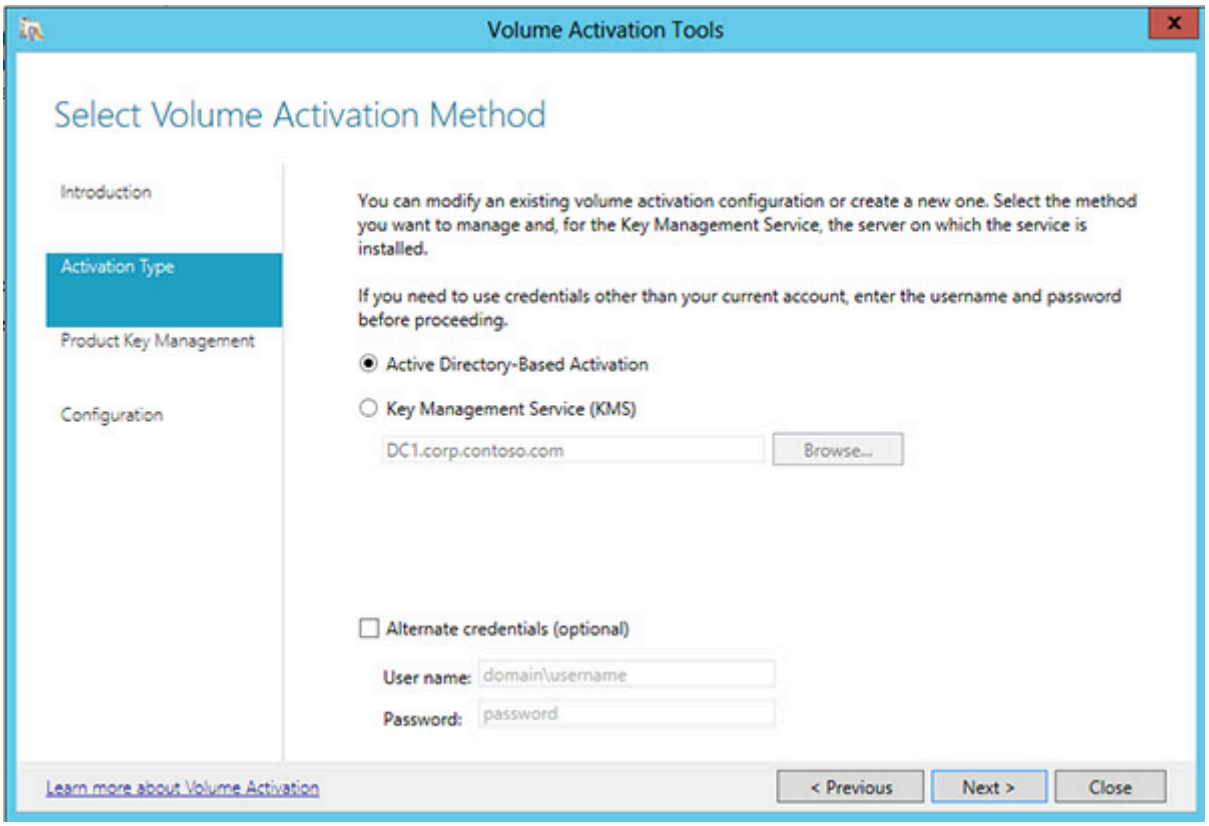


Рисунок 13. Выбор варианта "Активация с помощью Active Directory"

6. Введите ключ узла KMS организации и при необходимости укажите отображаемое имя, как показано на рис. 14.

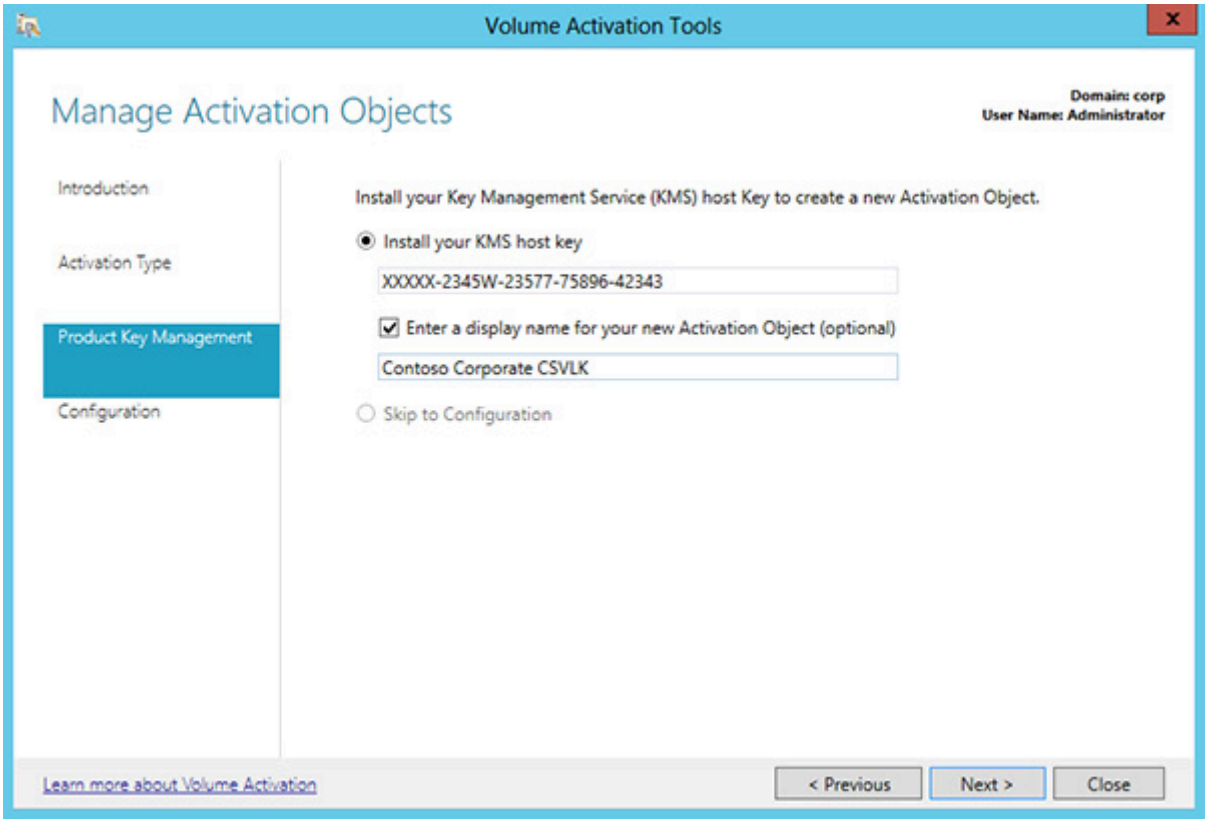


Рисунок 14. Ввод ключа узла KMS организации

7. Активируйте ключ узла KMS организации по телефону или через Интернет, как показано на рис. 15.

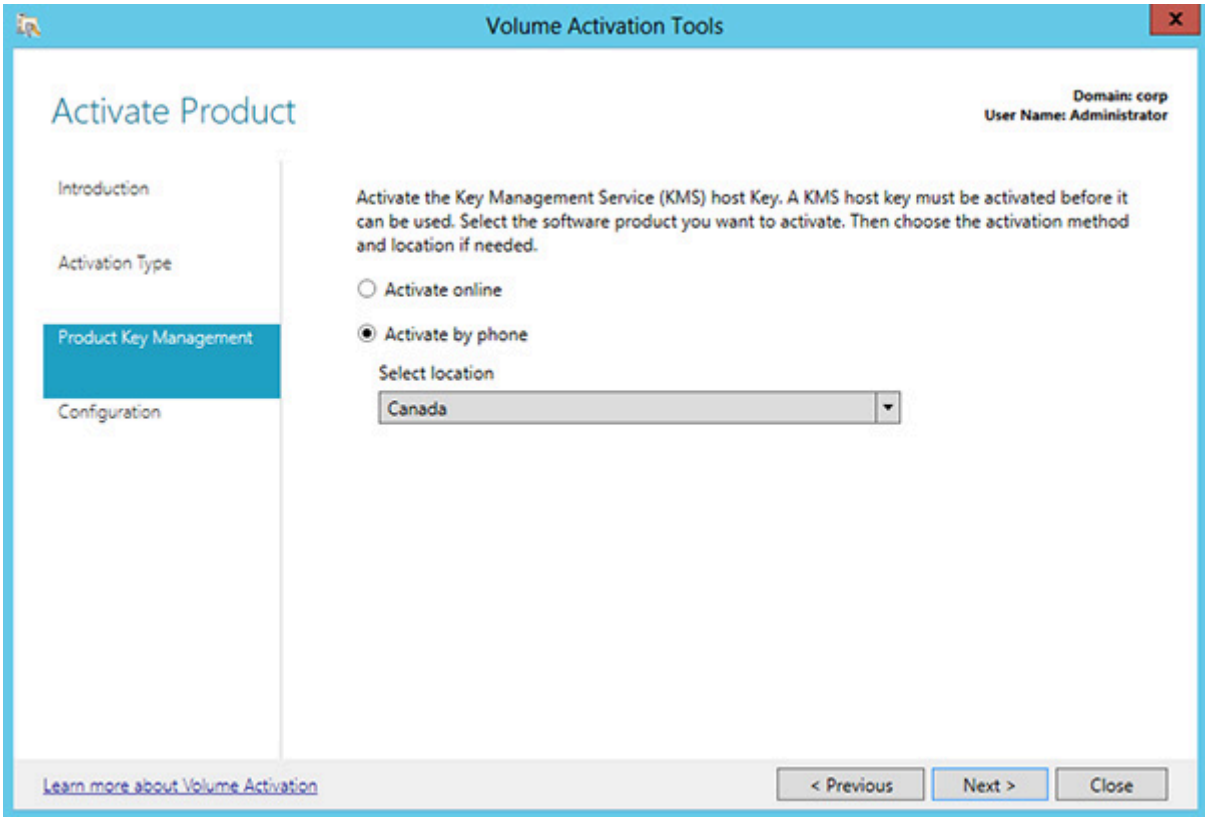


Рисунок 15. Выбор способа активации продукта

> ⓘ **Примечание.**
>
> Чтобы активировать ключ узла KMS или ключ корпоративной лицензии клиента (CSVLK) для Microsoft Office, на сервере, на котором установлена роль сервера активации корпоративных лицензий, необходимо установить пакет корпоративных лицензий Office для конкретной версии.
>
> - Пакет Office 2016 VL.
> - Пакет Office 2019 VL.
> - Пакет Office LTSC 2021 VL.
>
> Дополнительные сведения см. в статье Активация корпоративных лицензируемых версий Office с помощью Active Directory.

8. После активации ключа нажмите **кнопку Зафиксировать**, а затем нажмите **кнопку Закрыть**.

Проверка конфигурации активации с помощью Active Directory

Чтобы проверить конфигурацию активации на основе Active Directory, выполните следующие действия.

1. После настройки активации на основе Active Directory запустите компьютер под управлением выпуска Windows, настроенного по корпоративному лицензированию.
2. Если на компьютере ранее был настроен ключ MAK, замените ключ MAK на GVLK. `slmgr.vbs /ipk` Выполните команду и укажите GVLK в качестве нового ключа продукта.
3. Если компьютер не присоединен к домену организации, присоедини его к домену.
4. Выполните вход на компьютер.
5. Откройте проводник Windows, щелкните правой кнопкой мыши **Компьютер** и выберите **Пункт Свойства**.
6. Прокрутите вниз до раздела **активации Windows** и убедитесь, что этот клиент активирован.

> ⓘ **Примечание.**
>
> При использовании как KMS, так и активации на основе Active Directory может быть трудно определить, был ли клиент активирован с помощью KMS или активации на основе Active Directory. Во время теста рассмотрите возможность отключения KMS или убедитесь, что используется клиентский компьютер, еще не активированный KMS. Команда `slmgr.vbs /dlv` также указывает, использовался ли KMS.
>
> Для управления отдельными активациями или применения нескольких (массовых) активаций используйте VAMT.

Связанное содержимое

- Активация корпоративных лицензий для Windows.

Last updated on 14.05.2025

Активация клиентов под управлением Windows

Применяется к: ✅ Windows 11, ✅ Windows 10, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

> **Совет**
>
> Ищете сведения об активации розничной торговли?
>
> - Активируйте Windows.
> - Активация продукта для Windows.

После настройки службы управления ключами (KMS) или активации на основе Active Directory в сети активировать клиент под управлением Windows будет легко. Если на компьютере настроен универсальный ключ корпоративной лицензии (GVLK), ИТ-службе или пользователю не нужно предпринимать никаких действий. Все будет работать без каких-либо настроек.

Образы и установочный носитель для корпоративного выпуска уже должны быть настроены с помощью ключа GVLK. При запуске клиентского компьютера служба лицензирования проверяет текущее состояние лицензирования компьютера.

Если требуется активация или повторная активация, выполняется следующая последовательность действий.

1. Если компьютер является членом домена, он запрашивает у контроллера домена объект активации корпоративных лицензий. Если настроена активация с помощью Active Directory, контроллер домена возвращает объект. Если объект соответствует следующим требованиям:

    - Соответствует выпуску установленного программного обеспечения
    - Имеет соответствующий GVLK

затем компьютер активируется (или активируется повторно). Компьютер не требуется снова активировать в течение 180 дней, хотя операционная система пытается повторно активировать с более короткими регулярными интервалами.

1. Если компьютер не является членом домена или объект активации корпоративных лицензий недоступен, компьютер отправляет ЗАПРОС DNS, чтобы попытаться найти сервер KMS. Если можно связаться с сервером KMS, активация происходит, если KMS имеет ключ, соответствующий GVLK компьютера.

2. Компьютер пытается активировать на серверах Майкрософт, если он настроен с помощью MAK.

Если клиент не может успешно активировать себя, он периодически пытается повторить попытку. Частота повторных попыток зависит от текущего состояния лицензирования и от того, был ли клиентский компьютер успешно активирован в прошлом. Например, если клиентский компьютер ранее использовал активацию на основе Active Directory для активации, он периодически пытается связаться с контроллером домена при каждой перезагрузке.

Принципы работы службы управления ключами

KMS использует топологию клиент-сервер. Клиентские компьютеры KMS могут находить главные компьютеры KMS при помощи DNS или статической конфигурации. Клиенты KMS связываются с узлом KMS, используя удаленные вызовы процедур (RPC) по TCP/IP.

Порог активаций с использованием службы управления ключами

Физические компьютеры и виртуальные машины можно активировать, связавшись с узлом KMS. Чтобы получить право на активацию KMS, должно быть минимальное количество соответствующих компьютеров. Это минимальное значение называется пороговым значением активации. Клиенты KMS будут активированы только после выполнения этого порогового значения. Каждый узел KMS подсчитывает количество компьютеров, запрашивающих активацию до тех пор, пока не будет достигнуто пороговое значение.

В ответ на каждый действительный запрос активации от клиента KMS узел KMS сообщает число компьютеров, которые уже обратились к нему за активацией. Клиентские компьютеры, получающие число ниже порогового значения активации, не активируются. Например, если первые два компьютера, которые обращаются к узлу KMS, работают под управлением поддерживаемой в настоящее время версии клиента Windows, первый получает количество активаций 1, а второй — число активаций 2. Если следующий компьютер является виртуальной машиной под управлением поддерживаемой в настоящее время версии клиента Windows, она получает количество активаций 3 и т. д. Ни один из этих компьютеров не активируется, так как должно быть достигнуто число активаций, равных 25 или более.

Когда клиенты KMS ожидают достижения KMS порогового значения активации, они подключаются к узлу KMS каждые два часа, чтобы получить текущее количество

активаций. Они активируются при достижении порогового значения.

В нашем примере, если следующий компьютер, который обращается к узлу KMS, работает под управлением поддерживаемой в настоящее время версии Windows Server, он получает количество активаций, равное 4, так как количество активаций является накопительным. Если компьютер под управлением поддерживаемой в настоящее время версии Windows Server получает число активаций, равное 5 или более, он активируется. Если компьютер под управлением поддерживаемой в настоящее время версии клиента Windows получает число активаций 25 или более, он активируется.

Кэш счетчика активаций

Для отслеживания порога активации узел KMS ведет учет клиентов KMS, запрашивающих активацию. Узел KMS присваивает каждому клиенту KMS идентификатор и сохраняет его в таблице. По умолчанию каждый запрос на активацию хранится в таблице до 30 дней. Когда клиент возобновляет активацию, кэшированный идентификатор клиента удаляется из таблицы, создается новая запись, и 30-дневный период начинается снова. Если клиентский компьютер KMS не продлевает активацию в течение 30 дней, узел KMS удаляет соответствующий идентификатор клиента из таблицы и уменьшает количество активаций на один.

Однако узел KMS только дважды кэширует число идентификаторов клиентов, которые требуются для достижения порога активации. Таким образом, в таблице хранятся только 50 последних идентификаторов клиентов, и идентификатор клиента может быть удален раньше, чем через 30 дней.

Тип клиентского компьютера, который пытается активировать, задает общий размер кэша. Например, если узел KMS получает запросы на активацию только от серверов, кэш содержит только 10 идентификаторов клиентов, что в два раза превышает требуемое пороговое значение 5. Однако если клиентский компьютер под управлением клиента Windows обращается к узлу KMS, KMS увеличивает размер кэша до 50, чтобы обеспечить более высокое пороговое значение. KMS никогда не уменьшает размер кэша.

Подключение службы управления ключами

Для активации с помощью KMS требуется подключение TCP/IP. По умолчанию узлы и клиенты KMS используют DNS для публикации и поиска KMS. Можно использовать параметры по умолчанию, которые не требуют практически никаких административных действий. Однако узлы KMS и клиентские компьютеры можно настроить вручную на основе конфигурации сети и требований безопасности.

Продление активации с помощью службы управления ключами

Активации с помощью KMS действуют в течение 180 дней (*срок действия активации*). Чтобы оставаться активированными, клиентские компьютеры KMS должны продлевать активацию, подключаясь к узлу KMS не реже одного раза в 180 дней. По умолчанию клиентские компьютеры KMS пытаются возобновлять активацию каждые семь дней. Если активировать лицензию с помощью KMS не удается, клиентский компьютер повторяет попытки каждые два часа. После возобновления активации клиентского компьютера интервал действия активации начинается снова.

Публикация службы управления ключами

KMS использует записи расположения службы (SRV) в DNS для хранения расположений узлов KMS и связи с ними. Узлы KMS используют протокол динамических обновлений DNS (если он доступен) для публикации записей SRV службы KMS. Если динамическое обновление недоступно или узел KMS не имеет прав на публикацию записей ресурсов, необходимо выполнить одно из следующих действий:

- Записи DNS должны быть опубликованы вручную.
- Клиентские компьютеры должны быть настроены для подключения к определенным узлам KMS.

Обнаружение клиентом службы управления ключами

По умолчанию клиентские компьютеры KMS запрашивают информацию о KMS в DNS. Когда клиентский компьютер KMS впервые запрашивает информацию о KMS, он выбирает узел KMS случайным образом из списка записей расположения службы (SRV), возвращаемого DNS. Адрес DNS-сервера, содержащего записи ресурсов службы (SRV), можно указать в качестве суффикса на клиентских компьютерах KMS. Эта функция позволяет одному DNS-серверу объявлять записи ресурсов службы (SRV) для KMS и клиентские компьютеры KMS с другими основными DNS-серверами, чтобы найти их.

Можно добавить параметры приоритета и веса в значение реестра DnsDomainPublishList для KMS. Установка групп приоритетов узлов KMS и взвешивания в каждой группе позволяет указать, какой узел KMS следует попробовать клиентским компьютерам в первую очередь, и балансирует трафик между несколькими узлами KMS. Все поддерживаемые в настоящее время версии Windows и Windows Server предоставляют эти параметры приоритета и веса.

Если узел KMS, выбираемый клиентским компьютером, не отвечает, клиентский компьютер KMS удаляет этот узел KMS из списка ресурсов службы (SRV) и случайным образом выбирает другой узел KMS из списка. Когда узел KMS отвечает, клиентский компьютер KMS кэширует его имя и использует его для последующих попыток активации и продления. Если кэшированный узел KMS не отвечает на последующее продление, клиентский компьютер KMS обнаруживает новый узел KMS, запрашивая DNS для записей ресурсов службы KMS (SRV).

По умолчанию клиентские компьютеры подключаются к узлу KMS для активации с помощью анонимных RPC через TCP-порт 1688, хотя порт по умолчанию можно изменить. После того как клиентский компьютер устанавливает сеанс TCP с узлом KMS, клиентский компьютер отправляет один пакет запроса. Узел KMS в ответ передает значение счетчика активаций. Если счетчик соответствует порогу активации или превышает его, клиентский компьютер активируется, а сеанс закрывается. Клиентский компьютер KMS использует ту же процедуру для запросов продления. При этом в каждом направлении передается 250 байтов.

Конфигурация DNS-сервера

Для функции автоматической публикации KMS по умолчанию требуются запись расположения службы (SRV) и поддержка протокола динамических обновлений DNS. Поведение клиентского компьютера KMS по умолчанию и публикация записей ресурсов службы KMS (SRV) поддерживаются в следующих средах:

- DNS-сервер под управлением программного обеспечения Майкрософт.
- DNS-сервер, поддерживающий записи ресурсов служб (SRV) (по запросу примечаний [RFC] 2782) и динамические обновления (согласно IETF RFC 2136).

Например, Berkeley Internet Domain Name версий 8.x и 9.x поддерживает записи SRV и динамическое обновление. Узел KMS необходимо настроить таким образом, чтобы у него были учетные данные для создания и обновления следующих записей ресурсов на DNS-серверах: службы (SRV), узла IPv4 (A) и узла IPv6 (AAAA). Либо записи необходимо создать вручную. Чтобы предоставить узлу KMS необходимые учетные данные, рекомендуется создать группу безопасности в AD DS, а затем добавить все узлы KMS в эту группу. На DNS-сервере под управлением программного обеспечения Майкрософт убедитесь, что этой группе безопасности предоставлен полный контроль над записью _VLMCS._TCP. Это требование должно выполняться в каждом домене DNS, который содержит записи ресурсов службы KMS (SRV).

Активация первого узла службы управления ключами

Узлы KMS в сети должны установить ключ KMS и затем активироваться в Майкрософт. Установка ключа KMS включает службу KMS на узле KMS. После установки ключа KMS завершите активацию узла KMS по телефону или через Интернет. После этой начальной активации узел KMS не передает никаких сведений корпорации Майкрософт. Ключи KMS устанавливаются только на узлах KMS и никогда на отдельных клиентских компьютерах KMS.

Активация последующих узлов службы управления ключами

Каждый ключ KMS можно установить максимум на шести узлах KMS. Эти узлы могут быть физическими компьютерами или виртуальными машинами. После активации узла KMS один и тот же узел можно повторно активировать до девяти раз с одним и тем же ключом. Если организации требуется более шести узлов KMS, можно запросить дополнительные активации для ключа KMS организации, вызвав Центр активации корпоративного лицензирования Майкрософт для запроса исключения.

Принципы работы ключа многократной активации (MAK)

MAK используется для однократной активации с размещенными службами активации Майкрософт. Каждый MAK имеет предопределенное число разрешенных активаций. Это число основано на соглашениях о корпоративном лицензировании и может не соответствовать точному количеству лицензий организации. Каждая активация, использующая MAK с размещенной службой активации Майкрософт, учитывается при определении предела активаций.

Компьютеры можно активировать с помощью MAK двумя способами:

- **Независимая активация MAK**. Каждый компьютер независимо от других подключается к серверам Майкрософт и активируется через Интернет или по телефону. Независимая активация MAK лучше всего подходит для компьютеров в организации, которые не поддерживают подключение к корпоративной сети. Схема независимой активации MAK показана на рисунке 16.

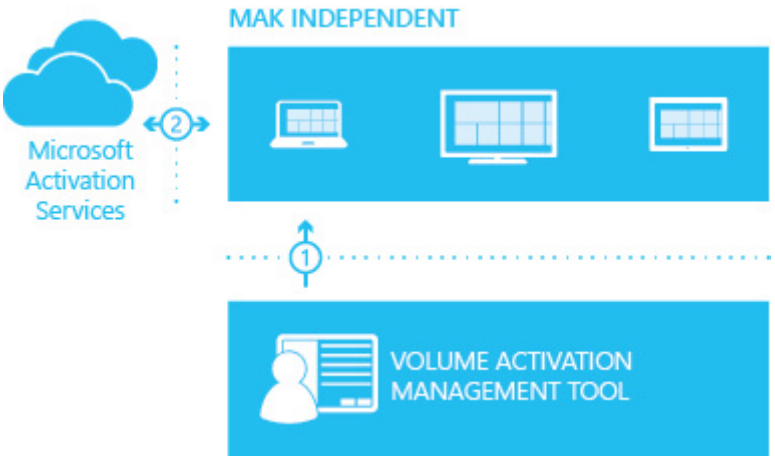


Рисунок 16. Независимая активация MAK

- **Прокси-активация MAK**. В этом случае выполняется централизованный запрос активации от нескольких компьютеров посредством одного подключения к серверам Майкрософт. Активацию прокси-сервера MAK можно настроить с помощью VAMT. Прокси-активация MAK подходит для сред, в которых из соображений безопасности ограничен прямой доступ к Интернету или корпоративной сети. Он также подходит для лабораторий разработки и тестирования, в которые не хватает этого подключения. Прокси-активация MAK с помощью VAMT показана на рисунке 17.

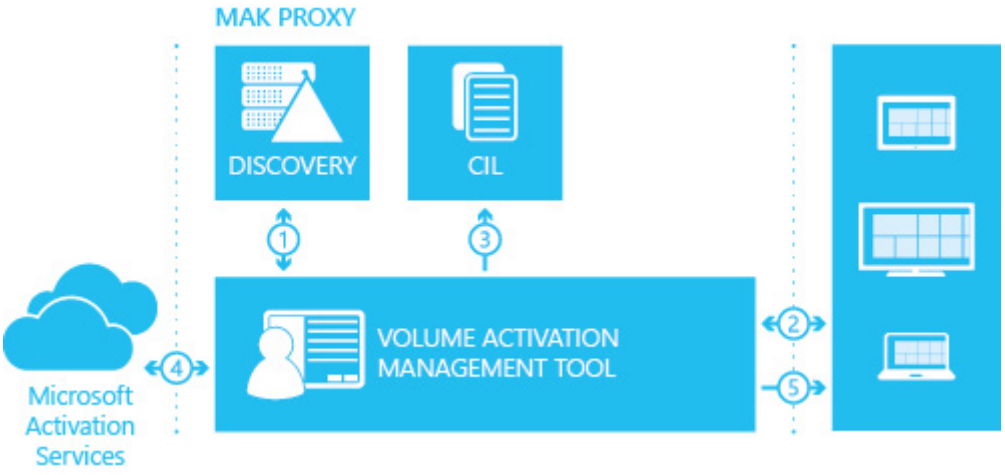


Рисунок 17. Прокси-активация MAK с помощью VAMT

MAK рекомендуется для:

- Компьютеры, которые редко или никогда не подключаются к корпоративной сети.
- Среды, в которых количество компьютеров, требующих активации, не соответствует пороговому значению активации KMS.

MAK можно использовать для отдельных компьютеров или с образом, который можно дублировать или установить с помощью решений развертывания Майкрософт. MAK также можно использовать на компьютере, на который изначально была настроена

активация KMS. Переключение с KMS на MAK полезно для перемещения компьютера из основной сети в отключенную среду.

Архитектура и активация ключа множественной активации (MAK)

При независимой активации MAK ключ продукта MAK устанавливается на клиентском компьютере. Ключ предписывает компьютеру выполнить самостоятельную активацию на серверах Майкрософт через Интернет.

В активации прокси-сервера MAK VAMT:

- Устанавливает ключ продукта MAK на клиентском компьютере.
- Получает идентификатор установки с целевого компьютера.
- Отправляет идентификатор установки в корпорацию Майкрософт от имени клиента.
- Получает идентификатор подтверждения.

Затем средство активирует клиентский компьютер, установив код подтверждения.

Активация от имени обычного пользователя

Для поддерживаемых в настоящее время версий Windows для активации не требуются права администратора. Однако учетная запись администратора по-прежнему требуется для других задач активации или лицензий, таких как "перезахоружить".

Связанное содержимое

- Активация корпоративных лицензий для Windows.

Last updated on 14.05.2025

Мониторинг активации

Применяется к: ✅ Windows 11, ✅ Windows 10, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

> **Совет**
>
> Ищете сведения об активации розничной торговли?
>
> - Активируйте Windows.
> - Активация продукта для Windows.

Успешное выполнение процесса активации компьютера под управлением Windows можно отслеживать несколькими способами. Вот наиболее популярные методы:

- Использование веб-сайта Microsoft Volume Licensing Service Center для отслеживания использования ключей MAK.
- `Slmgr /dlv` Использование команды на клиентском компьютере или на узле KMS. Полный список параметров см. вSlmgr.vbs параметрах для получения сведений об активации корпоративных лицензий.
- Использование инструментария управления Windows (WMI) для просмотра состояния лицензирования. WMI делает состояние лицензирования доступным для сторонних или пользовательских средств, которые могут получить доступ к WMI. Windows PowerShell также можно использовать для доступа к сведениям WMI.
- Большинство действий и событий лицензирования записываются в журнал событий (например, события журнала приложений 12288-12290).
- Microsoft System Center Operations Manager и пакет управления KMS могут предоставлять анализ и сведения пользователям System Center Operations Manager.
- Сведения о процедурах устранения неполадок с ключом множественной активации (MAK) или службой управления ключами (KMS) см. в статье Устранение ошибок активации .
- Средство управления активацией корпоративных лицензий (VAMT) предоставляет единый сайт, с которого можно управлять активациями корпоративных лицензий и отслеживать их. Дополнительные сведения см. в статье Введение в VAMT.

Связанное содержимое

Активация корпоративных лицензий для Windows.

Last updated on 14.05.2025

Использование средства управления активацией корпоративных лицензий

Применяется к: ✅ Windows 11, ✅ Windows 10, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

> **Совет**
>
> Ищете сведения об активации розничной торговли?
>
> - **Активируйте Windows**.
> - **Активация продукта для Windows**.

Средство управления активацией корпоративных лицензий (VAMT) имеет ряд полезных функций, включая возможность выполнения прокси-активации VAMT, а также отслеживания и контроля нескольких типов ключей продуктов.

Процесс активации томов, розничных и нескольких ключей активации (MAK) для Windows, Office и некоторых других продуктов Майкрософт можно автоматизировать и централизованно управлять с помощью VAMT. VAMT может управлять активацией корпоративных лицензий с помощью MAK или службы управления ключами (KMS). Это стандартная оснастка консоли управления Майкрософт.

Для поддерживаемых в настоящее время версий Windows Server VAMT можно установить непосредственно из диспетчер сервера, выбрав роль Службы активации корпоративных лицензий или средства администрирования удаленного сервера, средства администрирования ролей и средства активации корпоративных лицензий.

Для поддерживаемых в настоящее время версий клиента Windows VAMT можно установить в составе комплекта средств оценки и развертывания Windows (Windows ADK). Windows ADK можно скачать бесплатно. Дополнительные сведения, включая ссылки на скачивание Windows ADK, см . в статье Скачивание и установка Windows ADK.

Активация с помощью VAMT

VAMT можно использовать для завершения процесса активации в продуктах с помощью ключей MAK и розничной торговли. Компьютеры можно активировать как по отдельности, так и в группах. VAMT включает два сценария активации.

- **Активация через Интернет**. Активация через Интернет позволяет активировать через Интернет любые продукты, установленные с mak, KMS-узлом или ключами

розничных продуктов. В сети можно активировать один или несколько подключенных компьютеров. Этот процесс требует, чтобы каждый продукт сообщал сведения об активации напрямую корпорации Майкрософт.

- **Прокси-активация**. Этот метод активации включает активацию корпоративных лицензий для продуктов, установленных на клиентских компьютерах без доступа к Интернету. Главный компьютер VAMT распространяет MAK, ключ узла KMS или розничный ключ продукта на один или несколько клиентских продуктов и регистрирует код установки с каждого клиентского продукта. Узел VAMT отправляет идентификатор установки в Майкрософт от имени клиентских продуктов и получает соответствующие коды подтверждения. После этого узел VAMT устанавливает коды подтверждения на клиентских продуктах, завершая их активацию.

  При использовании этого метода доступ к Интернету требуется только на хост-компьютере VAMT. Активация прокси-сервера с помощью VAMT полезна для изолированных сегментов сети и в случаях, когда организация имеет сочетание активаций на основе розничной торговли, MAK и KMS.

Отслеживание продуктов и компьютеров

VAMT предоставляет обзор состояния активации и лицензирования компьютеров в сети организации, как показано на рис. 18. Для упреждающего управления лицензированием также доступно несколько предварительно созданных отчетов.

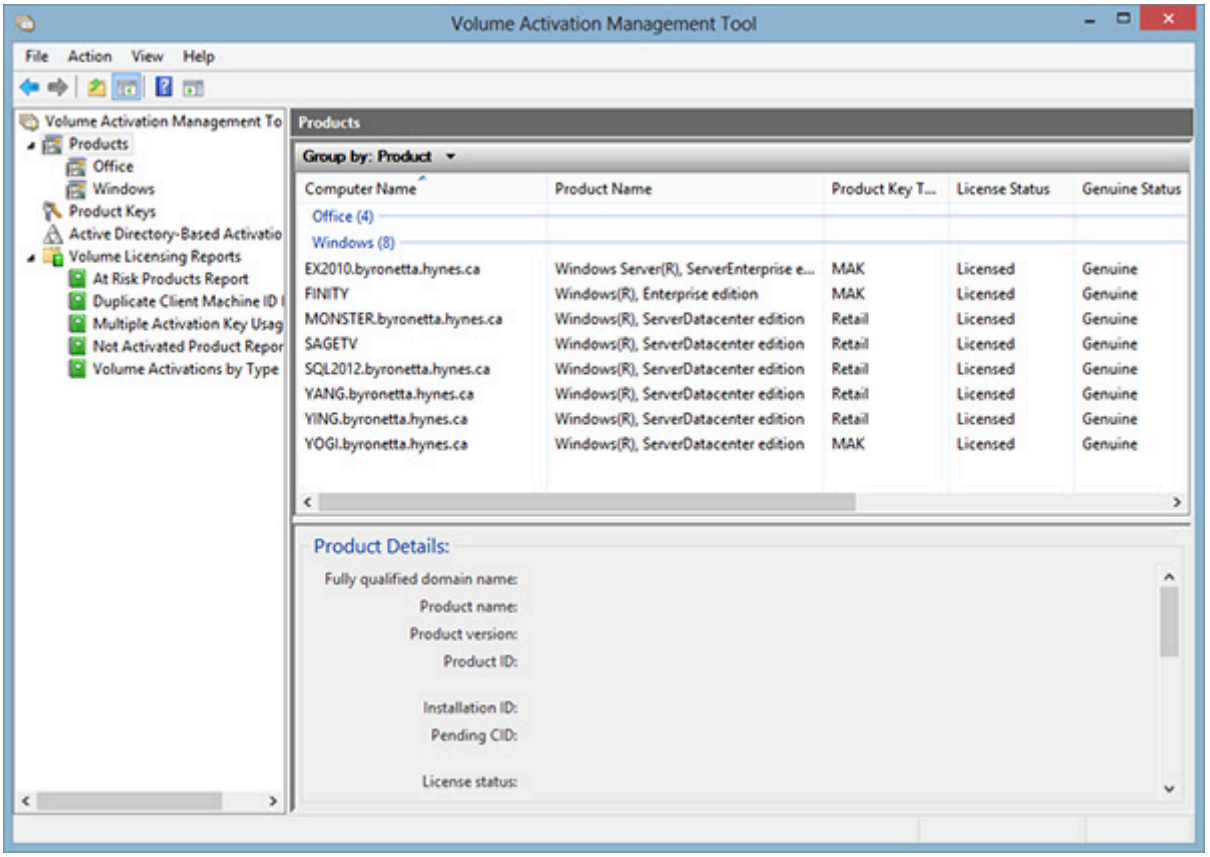


Рис. 18. VAMT с отображением состояния лицензирования нескольких компьютеров

Отслеживание использования ключей

VAMT упрощает отслеживание различных ключей, выданных организации. Каждый ключ можно ввести в VAMT, а затем VAMT может использовать эти ключи для активации клиентов через Интернет или прокси-сервера. Средство также может описать, к какому типу ключа он относится и к какой группе продуктов он принадлежит. VAMT представляет собой наиболее удобный способ быстро определить количество оставшихся активаций MAK. На рисунке 19 показан пример типов ключей и использования.

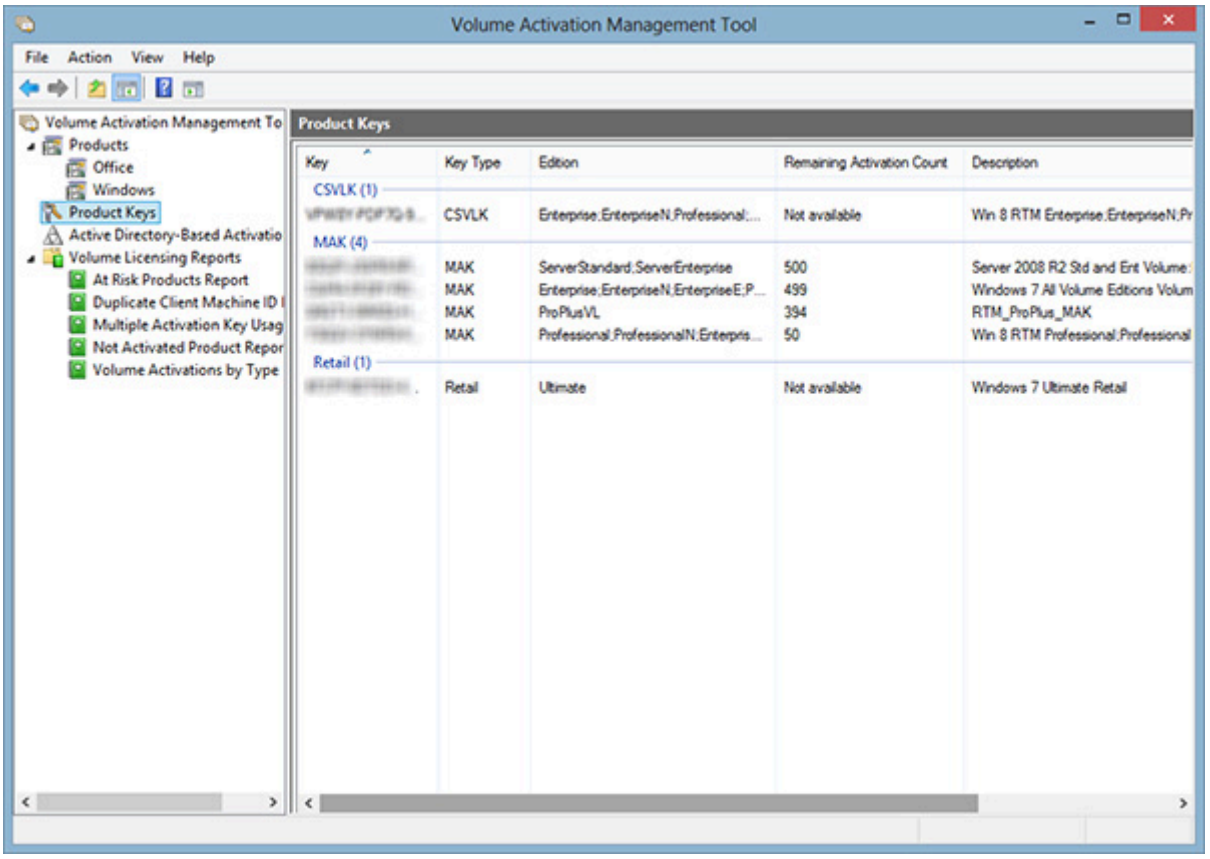


Рис. 19. VAMT с отображением типов ключей и использования

Другие возможности

VAMT хранит данные в базе данных Microsoft SQL Server для обеспечения производительности и устойчивости, а также предоставляет единый графический пользовательский интерфейс для управления активациями и выполнения прочих сопутствующих задач, например следующих.

- **Добавление и удаление компьютеров**. VAMT можно использовать для обнаружения компьютеров в локальной среде. VAMT обнаруживает компьютеры, запрашивая AD

DS, рабочие группы, имена или IP-адреса отдельных компьютеров либо с помощью общего запроса LDAP.

- **Обнаружение продуктов**. VAMT можно использовать для обнаружения Windows, Windows Server, Office и выбора других продуктов, установленных на клиентских компьютерах.

- **Управление данными активации**. VAMT хранит данные активации в базе данных SQL Server. Средство может экспортировать эти данные в формате XML на другие узлы VAMT или в архив.

Дополнительные сведения см. в следующих разделах:

- Обзор средство управления активацией корпоративных лицензий (VAMT).

Связанное содержимое

- Активация корпоративных лицензий для Windows.

Last updated on 14.05.2025

Приложение. Сведения, отправляемые в Майкрософт в процессе активации

Статья • 02.04.2024 •

Применяется к: ✅ Windows 11, ✅ Windows 10, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

> **Совет**
>
> Ищете сведения об активации розничной торговли?
>
> - Активируйте Windows.
> - Активация продукта для Windows.

При активации компьютера под управлением поддерживаемой в настоящее время версии Windows в корпорацию Майкрософт отправляются следующие сведения:

- Код продукта Майкрософт (пятизначный код, определяющий активируемый продукт Windows).
- Идентификатор канала или код сайта, определяющий способ первоначального получения продукта Windows. Например, идентификатор канала или код сайта определяет, был ли продукт:
  - Первоначально приобретено в розничном магазине.
  - Получается в качестве копии оценки.
  - Получается с помощью программы корпоративного лицензирования.
  - Предустановлено производителем компьютера.
- Дата установки и успешность установки.
- Сведения, которые помогают подтвердить, что ключ продукта Windows не изменен.
- Компьютерный мейк и модель.
- Сведения о версии операционной системы и программного обеспечения.
- Параметры региона и языка.
- Уникальный номер, называемый *глобально уникальным идентификатором* (GUID), который назначается компьютеру.

- Ключ продукта (хэш) и идентификатор продукта.
- Имя BIOS, номер редакции и дата редакции.
- Серийный номер тома (хэш) жесткого диска.
- Результат проверка активации.

  Этот результат включает коды ошибок и следующие сведения о любых эксплойтах активации и связанных с ними вредоносных или несанкционированных программ, которые были найдены или отключены:

  - Идентификатор эксплойтов активации.
  - Текущее состояние эксплойтов активации, например очистка или карантин.
  - Идентификация производителя компьютера.
  - Имя файла и хэш эксплойта активации в дополнение к хэшу связанных компонентов программного обеспечения, которые могут указывать на наличие эксплойта активации.
- Имя и хэш содержимого файла инструкций по запуску компьютера.
- Если лицензия Windows используется на основе подписки, сведения о том, как работает подписка.

Standard сведения о компьютере также отправляются, но IP-адрес компьютера хранится только временно.

Использование сведений

Корпорация Майкрософт использует эти сведения для подтверждения правильно лицензированной копии программного обеспечения. Корпорация Майкрософт не использует эти сведения для связи с отдельными потребителями.

Дополнительные сведения см. в заявлении о конфиденциальности Майкрософт.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Технический справочник по средству управления активациями корпоративных лицензий (VAMT)

Средство управления активацией корпоративных лицензий (VAMT) обеспечивает автоматизацию и централизованное управление процессом активации розничной торговли для Windows, Office и выбора других продуктов Майкрософт. VAMT может управлять активацией корпоративных лицензий с помощью нескольких ключей активации (MAK) или службы управления ключами Windows (KMS). VAMT — это стандартная оснастка консоли управления (MMC). VAMT можно установить на любом компьютере с поддерживаемой версией ОС Windows.

> **Внимание**
>
> VAMT предназначена для управления активацией корпоративных лицензий для всех поддерживаемых в настоящее время версий Windows, Windows Server и Office.

VAMT доступен только в пакете EN-US (x86).

Дальнейшие действия

Введение в VAMT

Last updated on 14.05.2025

Введение в VAMT

Средство управления активацией корпоративных лицензий (VAMT) позволяет сетевым администраторам и другим ИТ-специалистам автоматизировать и централизованно управлять Windows, Office, а также выбирать другие процессы активации корпоративных и розничных продуктов Майкрософт. VAMT может управлять активацией корпоративных лицензий с помощью нескольких ключей активации (MAK) или службы управления ключами Windows (KMS). VAMT — это стандартная оснастка консоли управления Майкрософт (MMC), которую можно установить на любом компьютере с поддерживаемой версией ОС Windows.

> ⓘ **Примечание.**
>
> VAMT можно установить на физических или виртуальных экземплярах и управлять ими. VAMT не может определить, являются ли удаленные продукты виртуальными. Пока продукты могут отвечать на вызовы инструментария управления Windows (WMI), они будут обнаруживаться и активироваться.

Управление активацией MAK и розничной лицензией

Для активации Windows, Windows Server или Office на отдельном компьютере или группе компьютеров можно использовать mak или ключ продукта розничной торговли. VAMT включает два разных сценария активации:

- **Активация через Интернет**. Многие организации поддерживают единый системный образ Windows или пакет установки Office для развертывания в организации. Иногда также требуется использовать ключи розничных продуктов в особых ситуациях. Активация через Интернет позволяет активировать через Интернет любые продукты, установленные с помощью MAK, узла KMS или ключей розничных продуктов на одном или нескольких подключенных компьютерах в сети. Для этого необходимо, чтобы каждый продукт передавал сведения об активации непосредственно в Майкрософт.

- **Активация прокси-сервера**. Этот метод активации позволяет выполнять активацию корпоративных лицензий для продуктов, установленных на клиентских компьютерах без доступа к Интернету. Главный компьютер VAMT распределяет ключ MAK, ключ узла KMS (CSVLK) или ключ продукта розничной торговли в один или несколько клиентских продуктов и собирает идентификатор установки (IID) из каждого клиентского продукта. Узел VAMT отправляет идентификаторы IID в корпорацию

Майкрософт от имени клиентских продуктов и получает соответствующие идентификаторы подтверждения (CID). Затем узел VAMT устанавливает CID в клиентских продуктах для завершения активации. При использовании этого метода доступ к Интернету требуется только на хост-компьютере VAMT. Вы также можете активировать продукты, установленные на компьютерах в рабочей группе, изолированной от любой более крупной сети, установив второй экземпляр VAMT на компьютере в рабочей группе. Затем используйте съемный носитель для передачи данных активации между этим новым экземпляром VAMT и подключенным к Интернету узлом VAMT.

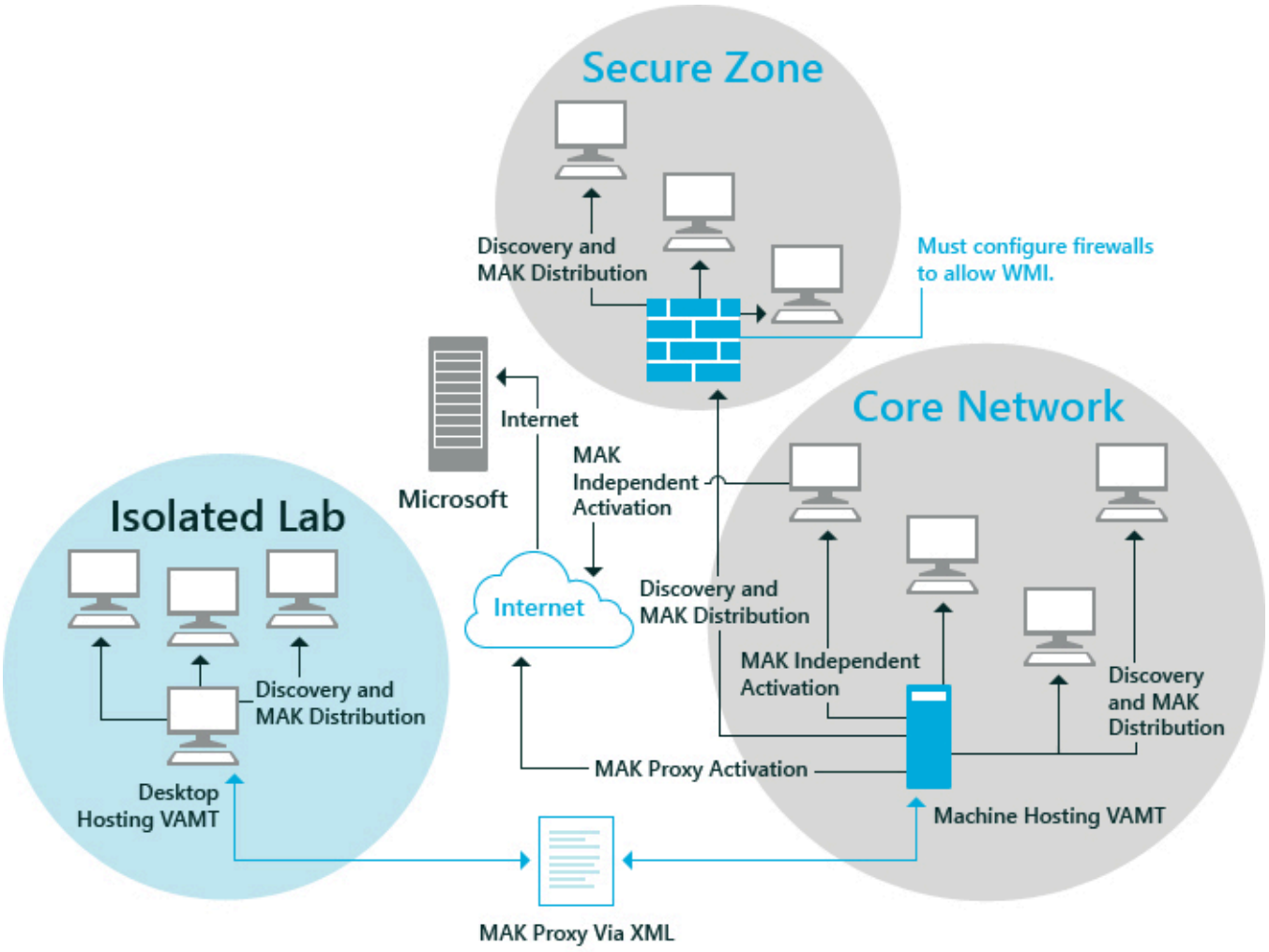
Управление активацией KMS

В дополнение к активации MAK или розничной активации можно использовать VAMT для активации корпоративных лицензий с помощью KMS. VAMT может устанавливать и активировать ключи GVLK (клиент KMS) на клиентских продуктах. GVLK — это ключи продуктов по умолчанию, используемые выпусками Windows, Windows Server и Office с корпоративными лицензиями.

VAMT обрабатывает ключ продукта узла KMS (CSVLK) так же, как ключ продукта розничного типа. Интерфейс ввода ключа продукта и управления активацией идентичен для обоих типов ключей продукта.

Корпоративная среда

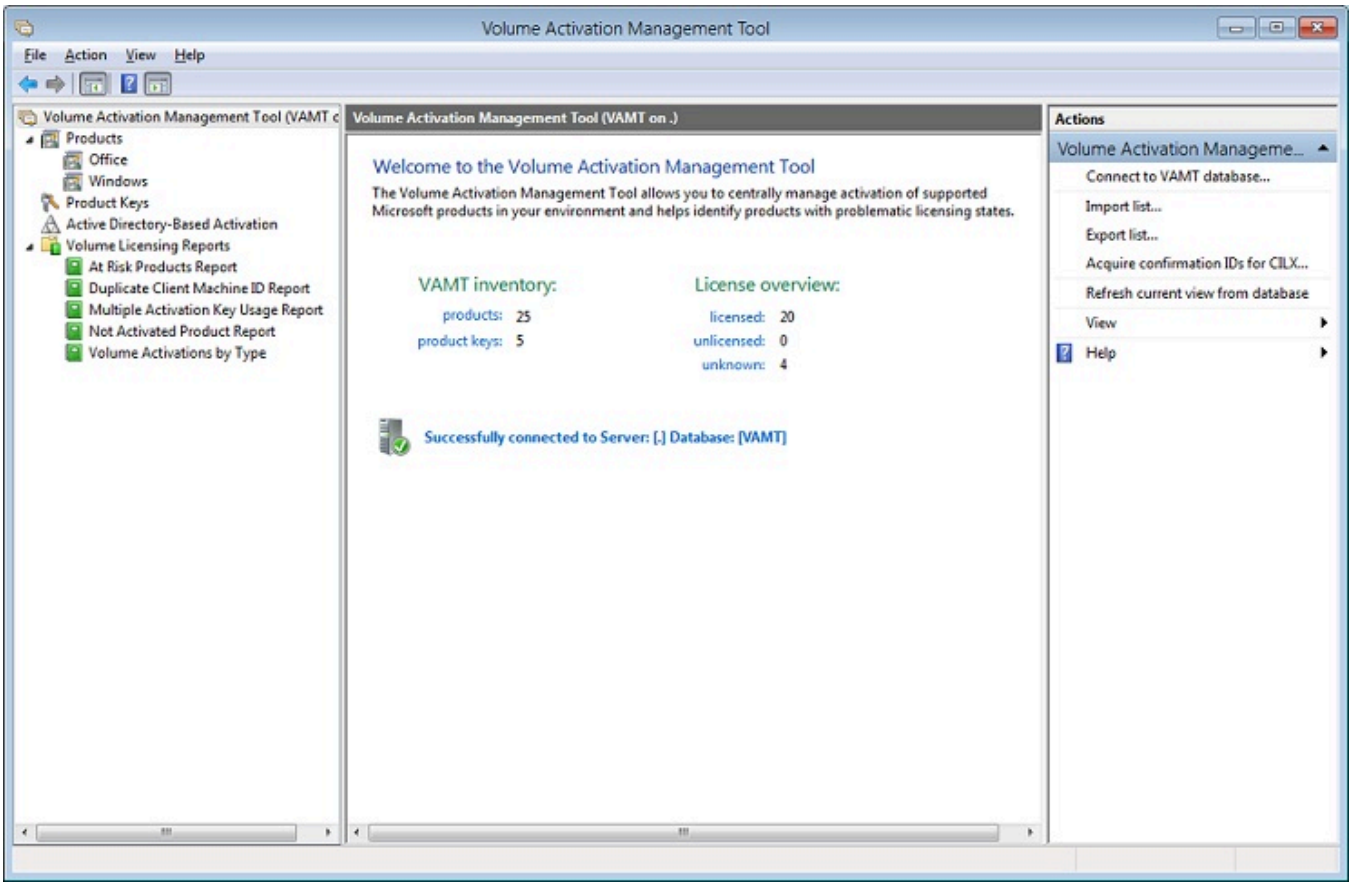
VAMT обычно реализуется в корпоративных средах. На следующем снимку экрана показаны три распространенные среды: базовая сеть, безопасная зона и изолированная лаборатория.



- В основной сетевой среде все компьютеры находятся в общей сети, управляемой доменными службами Active Directory (AD DS).
- Безопасная зона представляет сетевые компьютеры с более высоким уровнем безопасности, которые имеют дополнительную защиту брандмауэра.
- Изолированная лабораторная среда — это рабочая группа, которая физически отделена от основной сети, а ее компьютеры не имеют доступа к Интернету. Политика безопасности сети гласит, что никакие сведения, которые могли бы идентифицировать конкретный компьютер или пользователя, не могут быть переданы из изолированной лаборатории.

Пользовательский интерфейс VAMT

На следующем снимку экрана показан графический пользовательский интерфейс VAMT:



VAMT предоставляет единый графический пользовательский интерфейс для управления активациями и выполнения других задач, связанных с активацией, таких как:

- **Добавление и удаление компьютеров**. Вы можете использовать VAMT для обнаружения компьютеров в локальной среде. VAMT может обнаруживать компьютеры, запрашивая AD DS, рабочие группы, имя отдельного компьютера или IP-адрес или общий запрос LDAP.

- **Обнаружение продуктов**. Вы можете использовать VAMT для обнаружения Windows, Windows Server, Office и выбора других продуктов, установленных на клиентских компьютерах.

- **Мониторинг состояния активации**. Вы можете собирать сведения об активации каждого продукта, включая последние пять символов используемого ключа продукта, текущее состояние лицензии (например, Лицензировано, Grace, Нелицензировано) и сведения о выпуске продукта.

- **Управление ключами продукта**. Вы можете хранить несколько ключей продуктов и использовать VAMT для установки этих ключей в удаленные клиентские продукты. Вы также можете определить количество оставшихся активаций для mak.

- **Управление данными активации**. VAMT хранит данные активации в базе данных SQL. VAMT может экспортировать эти данные в другие узлы VAMT или в архив в формате XML.

Дальнейшие действия

Требования VAMT

Last updated on 14.05.2025

Общие сведения об активации активной Directory-Based

Активная активация Directory-Based (ADBA) позволяет предприятиям активировать компьютеры через подключение к их домену. Многие компании имеют компьютеры в расположениях, где используются продукты, зарегистрированные в компании. Ранее эти компьютеры должны были использовать ключ розничной торговли или ключ многократной активации (MAK) или физически подключаться к сети, чтобы активировать свои продукты с помощью служб управления ключами (KMS). ADBA предоставляет способ активации этих продуктов, если компьютеры могут присоединиться к домену компании. Когда пользователь присоединяет свой компьютер к домену, объект ADBA автоматически активирует Windows, установленную на его компьютере, при условии, что на компьютере установлен общий ключ корпоративной лицензии (GVLK). Ни один физический компьютер не требуется выступать в качестве объекта активации, так как он распределен по всему домену. ADBA имеет следующие преимущества

- Нет дополнительных устройств, необходимых для обслуживания (узел KMS)
- Не требуется RPC, использует LDAP
- Работает с RODC

Примечание. Активация ADBA работает только в одном лесу, даже если настроено отношение доверия. Для каждого леса требуется собственный объект ADBA. KMS может работать в нескольких лесах, если запись DNS SRV создается вручную в DNS каждого леса, при условии, что создается двухсторонняя связь доверия.

Сценарии ADBA

ADBA можно использовать, если требуется активировать только присоединенные к домену устройства.

Если у вас есть сервер, на котором размещена служба KMS, может потребоваться повторно активировать лицензии, если сервер заменен новым узлом. При использовании ADBA повторно активировать лицензии не требуется.

ADBA также упрощает балансировку нагрузки при наличии нескольких серверов KMS, так как клиент может подключаться к любому контроллеру домена. ADBA проще, чем использовать службу DNS для балансировки нагрузки путем настройки значений приоритета и веса.

Для некоторых решений VDI также требуется, чтобы новые клиенты активировались во время создания перед их добавлением в пул. В этом сценарии VDI ADBA может устранить потенциальные проблемы VDI, которые могут возникнуть из-за сбоя KMS.

Методы ADBA

VAMT позволяет ИТ-специалистам управлять объектом ADBA и активировать его. Активацию можно выполнить с помощью следующих методов:

- Активация по сети. Чтобы активировать лес ADBA в сети, пользователь выбирает функцию **Online activate forest** , выбирает ключ узла KMS (CSVLK) для использования и присваивает объекту ADBA имя.
- Активация прокси-сервера. Для активации прокси-сервера пользователь сначала выбирает функцию **леса активации прокси-сервера** , выбирает ключ узла KMS (CSVLK), присваивает объекту ADBA имя и предоставляет имя файла для сохранения CILx-файла, содержащего идентификатор установки. Затем пользователь переносит этот файл на компьютер с VAMT с подключением к Интернету, а затем выбирает функцию **Получение идентификаторов подтверждения для CILX** на целевой странице VAMT и предоставляет исходный CILx-файл. Когда VAMT загрузит идентификаторы подтверждения в исходный CILx-файл, пользователь возвращает этот файл обратно в исходный экземпляр VAMT, где пользователь завершает процесс активации прокси-сервера, выбрав функцию **Применить идентификатор подтверждения к домену Active Directory** .

Связанные статьи

- Активация леса Active Directory в Интернете
- Активация леса Active Directory с помощью прокси-сервера

Last updated on 10.06.2025

Требования VAMT

В этой статье содержатся сведения о ключе продукта и требованиях к системе для VAMT.

Требования к ключу продукта

Средство управления активацией корпоративных лицензий (VAMT) можно использовать для активации с помощью любого из следующих типов ключей продукта.

Развернуть таблицу

Тип ключа продукта	Где получить
• Ключ множественной активации (MAK) • Ключ узла службы управления ключами (KMS) (CSVLK) • Ключи установки клиента KMS (GVLK)	Ключи корпоративного лицензирования можно получить только по подписанному контракту от корпорации Майкрософт. Дополнительные сведения см. на портале корпоративного лицензирования Майкрософт.
Ключи розничных продуктов	Получено во время покупки продукта.

Системные требования

В следующей таблице перечислены требования к системе для главного компьютера VAMT.

Развернуть таблицу

Элемент	Минимальные требования к системе
Компьютер и процессор	Процессор x86 или x64 с тактовой частотой 1 ГГц
Память	1 ГБ ОЗУ для x86 или 2 ГБ ОЗУ для 64-разрядных процессоров
Жёсткий диск	16 ГБ свободного места на жестком диске для x86 или 20 ГБ для x64
Внешний диск	Съемный носитель (необязательно)
Display	Монитор с разрешением 1024 x 768 или выше
Network	Подключение к удаленным компьютерам через инструментарий управления Windows (TCP/IP) и веб-службу активации Майкрософт в

Элемент	Минимальные требования к системе
	Интернете через HTTPS
Операционная система	Поддерживаемые в настоящее время версии клиента Windows и Windows Server.
Дополнительные требования	• Подключение к базе данных SQL Server. Дополнительные сведения см. в разделе Установка VAMT. • PowerShell, который входит во все поддерживаемые в настоящее время версии Windows.

Связанное содержимое

Установка VAMT

Настройка клиентских компьютеров

Last updated on 14.05.2025

Установка VAMT

Применяется к: ✅ Windows 11, ✅ Windows 10, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

В этой статье описывается установка средство управления активацией корпоративных лицензий (VAMT). VAMT устанавливается в составе пакета средств оценки и развертывания Windows (ADK) для Windows.

> ⓘ **Внимание**
>
> VAMT требуются права локального администратора на всех управляемых компьютерах, чтобы депонировать идентификаторы подтверждения (CID), получить состояние лицензии клиентских продуктов и установить ключи продуктов. Если VAMT используется для управления продуктами и ключами продуктов на локальном хост-компьютере, но права администратора недоступны, запустите VAMT с повышенными привилегиями. Для достижения наилучших результатов при активации на основе Active Directory рекомендуется запускать VAMT при входе в систему от имени администратора домена.

> ⓘ **Примечание.**
>
> Оснастка VAMT консоли управления (MMC) поставляется в виде пакета x86.

Требования

- Windows Server с возможностями рабочего стола, с доступом к Интернету (для консоли VAMT main) и всеми обновлениями.
- Последняя версия Windows ADK.
- Любая поддерживаемая версия SQL Server Express. Рекомендуется использовать последнюю версию.
- Кроме того, любой **поддерживаемый полный** экземпляр SQL.

Установка SQL Server Express или использование любого полного экземпляра SQL

1. Скачайте и откройте пакет SQL Server Express.

2. В поле **Выберите тип установки:** выберите **Базовый**.

3. На экране **Условия лицензии сервера Microsoft SQL Server** примите условия лицензии, нажав кнопку **Принять**.

4. На экране **Укажите SQL Server расположение установки** в разделе **РАСПОЛОЖЕНИЕ УСТАНОВКИ *:**укажите расположение установки или используйте путь по умолчанию, а затем нажмите кнопку **Установить**.

5. После завершения установки на странице **Установка успешно завершена!** в разделе **ИМЯ ЭКЗЕМПЛЯРа** запишите имя экземпляра для установки. Имя экземпляра используется далее в разделе Настройка VAMT для подключения к SQL Server Express или полной SQL Server.

6. После того как имя экземпляра будет отмечено, нажмите кнопку **Закрыть** , а затем нажмите кнопку **Да** , чтобы подтвердить выход из установщика.

Установка VAMT с помощью ADK

1. Скачайте последнюю версию Windows ADK.

   Если более ранняя версия уже установлена, рекомендуется сначала удалить старую версию ADK перед установкой последней версии. Существующие данные VAMT хранятся в базе данных VAMT.

2. Откройте установщик ADK, скачанный на предыдущем шаге. Откроется окно **Комплект средств оценки и развертывания Windows** .

3. В окне **Комплект средств оценки и развертывания Windows** :

   a. На странице **Указание расположения** в разделе **Путь установки введите** расположение установки или используйте путь по умолчанию. Рекомендуется установить по пути по умолчанию. После этого нажмите кнопку **Далее** .

   b. На странице **Конфиденциальность комплектов windows** выберите параметр конфиденциальности, а затем нажмите кнопку **Далее** .

   c. На странице **Лицензионное соглашение** примите условия лицензии, нажав кнопку **Принять** .

   d. На странице **Выберите компоненты, которые требуется установить**, выберите **средство управления активацией корпоративных лицензий (VAMT).** При необходимости выберите дополнительные компоненты для установки. После этого нажмите кнопку **Установить** .

e. После завершения установки **отобразится страница Добро пожаловать в комплект средств оценки и развертывания Windows** ! Нажмите кнопку **Закрыть** .

Настройка VAMT для подключения к SQL Server Express или полному SQL Server

1. В меню Пуск в разделе **Комплекты Windows** выберите **Volume Active Management Tool 3.1**. Откроется окно **Параметры подключения к базе данных** .

2. В окне **Параметры подключения к базе данных** :

   a. Рядом с **полем Server:**введите имя экземпляра сервера, как определено в разделе Установка SQL Server Express или использование любого полного экземпляра SQL. Если SQL является удаленным, обязательно используйте полное доменное имя.

   b. Рядом с **полем База данных:** добавьте имя базы данных.

   c. После ввода имени сервера базы данных и базы данных нажмите кнопку **Подключиться** .

   d. Нажмите кнопку **Да** , чтобы создать базу данных.

Удаление VAMT

Чтобы удалить VAMT, выполните приведенные далее действия.

1. Щелкните правой кнопкой мыши меню "Пуск" и выберите **Параметры**.

2. Выберите **Приложения** в области слева.

3. В области справа в разделе **Приложения** выберите **Установленные приложения**.

   Кроме того, щелкните следующую ссылку, чтобы автоматически открыть приложение **"Параметры"** на странице **Установленные приложения** :

   Установленные приложения

4. Прокрутите список установленных приложений и найдите **Комплект средств для оценки и развертывания Windows**.

5. Щелкните три точки **...** рядом с элементом **Комплект средств оценки и развертывания Windows,** а затем нажмите **кнопку Изменить**. Откроется окно **Комплект средств оценки и развертывания Windows** .

6. В окне **Комплект средств оценки и развертывания Windows** :

   a. На странице **Обслуживание компонентов комплекта средств оценки и развертывания Windows** выберите **Изменить**, а затем нажмите кнопку **Далее** .

   b. На странице **Выберите функции, которые нужно изменить**, снимите флажок **средство управления активацией корпоративных лицензий (VAMT)** и нажмите кнопку **Изменить**.

   c. После завершения удаления **отобразится страница Изменение.** Нажмите кнопку **Закрыть** .

Last updated on 14.05.2025

Настройка клиентских компьютеров

Чтобы обеспечить правильную работу средство управления активацией корпоративных лицензий (VAMT), на всех клиентских компьютерах требуются определенные изменения конфигурации:

- В брандмауэре клиентского компьютера необходимо задать исключение.
- Раздел реестра должен быть создан и правильно задан для компьютеров в рабочей группе; В противном случае контроль учетных записей Windows® (UAC) не разрешает удаленные административные операции.

Организации, в которых VAMT будет широко использоваться, могут извлечь выгоду из внесения этих изменений в образ master для Windows.

> ⓘ **Внимание**
>
> Эта процедура применяется только к клиентам под управлением Windows Vista или более поздней версии. Сведения о клиентах под управлением Windows XP с пакетом обновления 1 (SP1) см. в статье Подключение через брандмауэр Windows.

Настройка брандмауэра Windows для разрешения доступа VAMT

Включите VAMT для доступа к клиентским компьютерам с помощью панель управления **брандмауэра Windows**:

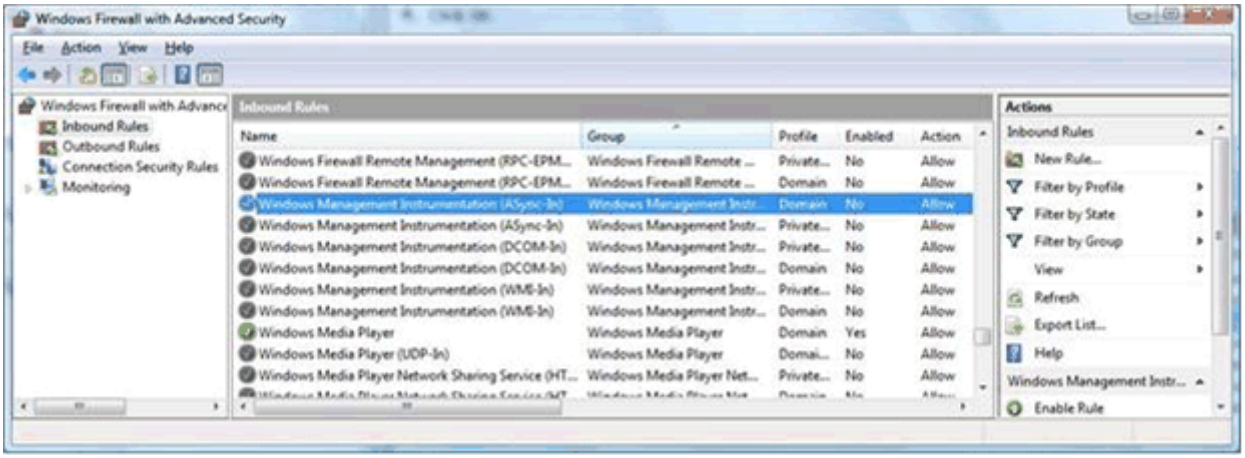
1. Откройте панель управления и дважды щелкните **Система и безопасность**.
2. Выберите **Брандмауэр Windows**.
3. Выберите **Разрешить программу или компонент через брандмауэр Windows**.
4. Выберите параметр **Изменить параметры** .
5. Установите флажок **Инструментарий управления Windows (WMI).**
6. Нажмите **OK**.

> ⚠ **Предупреждение**
>
> По умолчанию исключения брандмауэра Windows применяются только к трафику, исходя из локальной подсети. Чтобы развернуть исключение для нескольких

подсетей, необходимо изменить параметры исключения в брандмауэре Windows в режиме повышенной безопасности, как описано ниже.

Настройка брандмауэра Windows для разрешения доступа VAMT в нескольких подсетях

Включите VAMT для доступа к клиентским компьютерам в нескольких подсетях с помощью **брандмауэра Windows в режиме повышенной безопасности** панель управления:



1. Откройте панель управления и дважды щелкните **Администрирование**.
2. Выберите **Брандмауэр Windows в режиме повышенной безопасности**.
3. Внесите изменения для каждого из следующих трех элементов WMI для соответствующего сетевого профиля (домен, общедоступный, частный):
    - Инструментирование управления Windows (асинхронное)
    - Инструментирование управления Windows (DCOM-in)
    - Инструментарий управления Windows (WMI-in)
4. В диалоговом окне **Брандмауэр Windows в режиме повышенной безопасности** выберите **Правила для входящего трафика** на панели слева.
5. Щелкните правой кнопкой мыши нужное правило и выберите **Свойства** , чтобы открыть диалоговое окно **Свойства** .
    - На вкладке **Общие** установите флажок **Разрешить подключение** .

- На вкладке **Область** измените параметр Удаленный IP-адрес с "Локальная подсеть" (по умолчанию), чтобы разрешить конкретный доступ.
- На вкладке **Дополнительно** проверьте выбор всех профилей, применимых к сети (домен, частный или общедоступный).

В некоторых сценариях через аппаратный брандмауэр разрешен только ограниченный набор портов TCP/IP. Администраторы должны убедиться, что WMI (который использует RPC через TCP/IP) разрешен через эти типы брандмауэров. По умолчанию порт WMI является динамически выделенным случайным портом выше 1024. В следующей статье майкрософт описывается, как администраторы могут ограничить диапазон динамически выделенных портов. Ограничение диапазона динамически выделенных портов полезно, если, например, аппаратный брандмауэр разрешает трафик только в определенном диапазоне портов.

Дополнительные сведения см. в разделе Настройка динамического выделения портов RPC для работы с брандмауэрами.

Создание значения реестра для VAMT для доступа к компьютеру, присоединенном к рабочей группе

> ⚠ **Предупреждение**
>
> В этом разделе содержатся сведения об изменении реестра. Перед изменением реестра обязательно создайте резервную копию. Кроме того, убедитесь, что вы знаете, как восстановить реестр в случае возникновения проблемы. Дополнительные сведения о резервном копировании, восстановлении и изменении реестра см. в разделе **Сведения о реестре Windows для опытных пользователей**.

На клиентском компьютере создайте следующий раздел реестра с помощью regedit.exe.

1. Перейдите к `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system`
2. Введите следующие данные:
   - **Имя значения: LocalAccountTokenFilterPolicy**
   - **Тип: DWORD**
   - **Данные значения: 1**

> ⓘ **Примечание.**

Чтобы обнаружить управляемые VAMT компьютеры Windows в рабочих группах, необходимо включить обнаружение сети на каждом клиенте.

Варианты развертывания

Существует несколько вариантов настройки исключения брандмауэра WMI для компьютеров:

- **Образ.** Добавьте конфигурации в образ Windows master, развернутый для всех клиентов.
- **Групповая политика.** Если клиенты являются частью домена, все клиенты можно настроить с помощью групповая политика. Параметр групповая политика для исключения брандмауэра WMI находится в GPMC. MSC at: **Конфигурация**> компьютера**Параметры**>**Windows Параметры**> безопасности**Брандмауэр Windows в режиме повышенной безопасности**>**Брандмауэр Windows с расширенными правилами для**>**входящих подключений**.
- **Сценарий.** Выполнение скрипта с помощью Microsoft Configuration Manager или стороннего средства удаленного выполнения скриптов.
- **Вручную.** Настройте исключение брандмауэра WMI отдельно на каждом клиенте.

Приведенные выше конфигурации открывают дополнительный порт через брандмауэр Windows на целевых компьютерах и должны выполняться на компьютерах, защищенных сетевым брандмауэром. Чтобы разрешить VAMT запрашивать актуальное состояние лицензирования, необходимо сохранить исключение WMI. Мы рекомендуем администраторам обращаться к своим политикам безопасности сети и принимать четкие решения при создании исключения WMI.

Связанные статьи

Требования VAMT

Установка VAMT

Last updated on 14.05.2025

Добавление и удаление компьютеров

Вы можете добавить компьютеры, на которых установлены любые поддерживаемые продукты Windows или Office, в базу данных средство управления активацией корпоративных лицензий (VAMT) с помощью функции **Обнаружение продуктов**. Вы можете искать компьютеры в домене Active Directory, по имени отдельного компьютера или IP-адресу, в рабочей группе или по общему запросу LDAP. Вы можете удалить компьютеры из базы данных VAMT с помощью функции **Delete** . После добавления компьютеров можно добавить продукты, установленные на компьютерах, запустив функцию **Обновить состояние лицензии** .

Перед добавлением компьютеров убедитесь, что на всех целевых компьютерах было включено исключение брандмауэра инструментария управления Windows (WMI), необходимое для VAMT. Дополнительные сведения см. в разделе Настройка клиентских компьютеров.

Добавление компьютеров в базу данных VAMT

1. Откройте VAMT.
2. Выберите **Обнаружение продуктов** в меню **Действия** в области справа, чтобы открыть диалоговое окно **Обнаружение продуктов** .
3. В диалоговом окне **Обнаружение продуктов** выберите **Поиск компьютеров в Active Directory** , чтобы отобразить параметры поиска, а затем выберите нужный параметр поиска. Вы можете искать компьютеры в домене Active Directory, по имени отдельного компьютера или IP-адресу, в рабочей группе или по общему запросу LDAP.

    - Чтобы найти компьютеры в домене Active Directory, выберите **Поиск компьютеров в Active Directory**, а затем в разделе **Критерии фильтра домена** в списке доменных имен выберите имя домена, который требуется выполнить поиск. Вы можете еще больше сузить поиск, введя имя в поле **Фильтр по имени компьютера** , чтобы найти конкретный компьютер в домене. Этот фильтр поддерживает подстановочный знак звездочки (*). Например, при вводе "a*" будут отображаться только имена компьютеров, начинающиеся с буквы "a".
    - Чтобы выполнить поиск по имени отдельного компьютера или IP-адресу, выберите **Вручную ввести имя или IP-адрес**, а затем введите полное имя или IP-адрес в текстовом поле **Один или несколько имен компьютеров или IP-**

адресов, разделенных запятыми . Разделите несколько записей с помощью запятой. VAMT поддерживает адресацию IPv4 и IPV6.

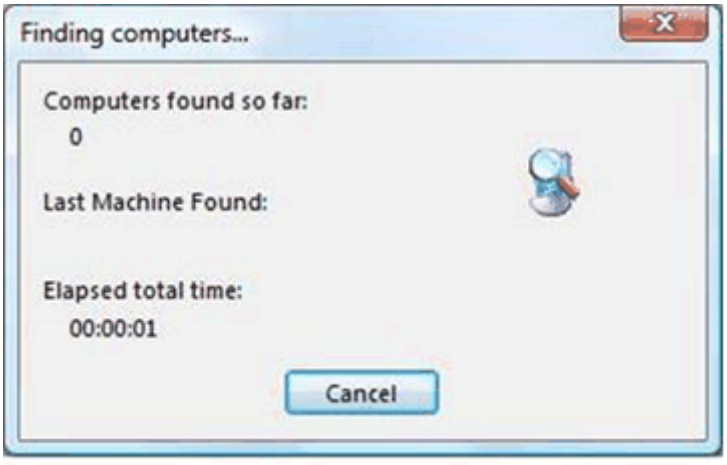
- Чтобы найти компьютеры в рабочей группе, выберите **Поиск компьютеров в рабочей группе**, а затем в разделе **Условия фильтра рабочей группы** в списке имен рабочих групп выберите имя рабочей группы, которую требуется выполнить поиск. Вы можете еще больше сузить поиск, введя имя в поле **Фильтр по имени компьютера** , чтобы найти конкретный компьютер в рабочей группе. Этот фильтр поддерживает подстановочный знак звездочки (*). Например, при вводе "a*" будут отображаться только имена компьютеров, начинающиеся с буквы "a".

- Чтобы выполнить поиск компьютеров с помощью общего запроса LDAP, выберите **Поиск с запросом LDAP** и введите запрос в текстовое поле. VAMT проверит только синтаксис запроса LDAP, но в противном случае выполнит запрос без дополнительных проверок.

4. Выберите **Поиск**.

5. VAMT выполняет поиск указанных компьютеров и добавляет их в базу данных VAMT. Во время поиска VAMT отображает сообщение **Поиск компьютеров** , показанное ниже.

   Чтобы отменить поиск, нажмите **кнопку Отмена**. После завершения поиска имена вновь обнаруженных компьютеров отображаются в представлении списка продуктов в центральной области.



> **ⓘ Внимание**
>
> На этом шаге в базу данных VAMT добавляются только компьютеры, а не продукты, установленные на компьютерах. Чтобы добавить продукты,

необходимо запустить функцию **Обновить состояние лицензии** .

Добавление продуктов в VAMT

1. В списке **Продукты** выберите компьютеры, для которых необходимо добавить сведения о продукте в базу данных VAMT.

2. Можно воспользоваться функцией **Filter**, чтобы сузить область поиска компьютеров. Для этого нажмите **Filter** на панели справа, чтобы открыть диалоговое окно **Filter Products**.

3. В диалоговом окне **Filter Products** можно отфильтровать список по имени компьютера, названию продукта, типу ключа продукта, состоянию лицензии или любому сочетанию этих параметров.

    - Чтобы отфильтровать список по имени компьютера, введите нужное имя в поле **Computer Name**.

    - Чтобы отфильтровать список по названию продукта, типу ключа продукта или состоянию лицензии, выберите список, который вы хотите использовать для фильтра, и выберите параметр . При необходимости выберите **очистить все фильтры** , чтобы создать новый фильтр.

4. Выберите **Фильтр**. VAMT отображает отфильтрованный список на центральной панели.

5. В правой части области **Действия** выберите **Обновить состояние лицензии** , а затем выберите параметр учетных данных. Выберите **Альтернативные учетные данные** , только если вы обновляете продукты, для которых требуются учетные данные администратора, отличные от тех, которые использовались для входа на компьютер. Если вы предоставляете альтернативные учетные данные, в диалоговом окне **Безопасность Windows** введите соответствующее имя пользователя и пароль и нажмите кнопку **OK**.

6. VAMT отображает диалоговое окно **Сбор сведений о продукте** , в котором собирается состояние лицензирования всех поддерживаемых продуктов на выбранных компьютерах. По завершении процесса обновленное состояние лицензирования каждого продукта появится в представлении списка продуктов в центральной области.

> ⓘ **Примечание.**

Если на компьютере установлено несколько поддерживаемых продуктов, VAMT добавляет запись для каждого продукта. Запись отображается под соответствующим заголовком продукта.

Удаление компьютеров из базы данных VAMT

Вы можете удалить компьютер, щелкнув его в представлении списка продуктов, а затем щелкнув **Удалить** в меню **Выбранный элемент** в правой области. В появившемся диалоговом окне **Подтверждение удаления выбранных продуктов** выберите **Да** , чтобы удалить компьютер. Если на компьютере указано несколько продуктов, необходимо удалить каждый продукт, чтобы полностью удалить компьютер из базы данных VAMT.

Связанные статьи

Обновление состояния продукта

Удаление продуктов

Last updated on 14.05.2025

Обновление состояния продукта

После добавления компьютеров в базу данных средство управления активацией корпоративных лицензий (VAMT) необходимо использовать функцию **Обновить состояние лицензии** для добавления продуктов, установленных на компьютерах. Обновление **состояния лицензии** также можно использовать в любое время для получения актуального состояния лицензии для любых продуктов в базе данных VAMT. Чтобы получить состояние лицензии, VAMT должна иметь административные разрешения на всех выбранных компьютерах, а инструментарий управления Windows (WMI) должен быть доступен через брандмауэр Windows. Кроме того, для компьютеров рабочей группы необходимо создать раздел реестра, чтобы включить удаленные административные действия в разделе Контроль учетных записей пользователей (UAC). Дополнительные сведения см. в разделе Настройка клиентских компьютеров.

> ⓘ **Примечание.**
>
> Для запроса состояния лицензии требуется допустимое имя компьютера для каждой запрашиваемой системы. Если база данных VAMT содержит компьютеры, добавленные без личных сведений, имена компьютеров будут недоступны для этих компьютеров, а состояние этих компьютеров не будет обновлено.

Обновление состояния лицензии продукта

1. Откройте VAMT.
2. В списке **Продукты** выберите один или несколько продуктов, состояние которых необходимо обновить.
3. В правой части области **Действия** выберите **Обновить состояние лицензии** , а затем выберите параметр учетных данных. Выберите **Альтернативные учетные данные** только при обновлении продуктов, для которых требуются учетные данные администратора, отличные от тех, которые используются для входа на компьютер.
4. Если укажите альтернативные учетные данные, в диалоговом окне **Безопасность Windows** введите соответствующее имя пользователя и пароль и нажмите кнопку **ОК**.

   VAMT отображает диалоговое окно **Сбор сведений о продукте** при сборе состояния всех выбранных продуктов. По завершении процесса в представлении списка продуктов в центральной области появится обновленное состояние лицензирования каждого продукта.

> **Примечание.**
>
> Если обнаруженный ранее продукт Microsoft Office удаляется с удаленного компьютера, обновление его состояния лицензирования приводит к удалению записи из представления списка продуктов **Office** , что приводит к уменьшению общего количества обнаруженных продуктов. Однако установка Windows на том же компьютере не удаляется и всегда отображается в представлении списка продуктов **Windows** .

Связанное содержимое

Добавление и удаление компьютеров

Удаление продуктов

Last updated on 14.05.2025

Удаление продуктов

Чтобы удалить один или несколько продуктов из средство управления активацией корпоративных лицензий (VAMT), их можно удалить из представления списка продуктов в центральной области.

Удаление одного или нескольких продуктов

1. Выберите узел продукта в левой области.
2. Можно воспользоваться функцией **Filter**, чтобы сузить область поиска компьютеров. Для этого нажмите **Filter** на панели справа, чтобы открыть диалоговое окно **Filter Products**.
3. В диалоговом окне **Filter Products** можно отфильтровать список по имени компьютера, названию продукта, типу ключа продукта, состоянию лицензии или любому сочетанию этих параметров.
    - Чтобы отфильтровать список по имени компьютера, введите нужное имя в поле **Computer Name**.
    - Чтобы отфильтровать список по названию продукта, типу ключа продукта или состоянию лицензии, выберите список, который вы хотите использовать для фильтра, и выберите параметр . При необходимости выберите **очистить все фильтры** , чтобы создать новый фильтр.
4. Выберите **Фильтр**. VAMT отображает отфильтрованный список на центральной панели.
5. Выберите продукты, которые нужно удалить.
6. Выберите **Удалить** в меню **Выбранные элементы** на панели справа.
7. В диалоговом окне **Подтверждение удаления выбранных продуктов** нажмите **кнопку OK**.

Связанные статьи

Добавление и удаление компьютеров

Обновление состояния продукта

Last updated on 14.05.2025

Добавление и удаление ключа продукта

Прежде чем использовать ключ продукта с ключом многократной активации (MAK), ключом розничной торговли или ключом узла KMS (CSVLK), необходимо сначала добавить его в базу данных средство управления активацией корпоративных лицензий (VAMT).

Добавление ключа продукта

1. Откройте VAMT.
2. В левой боковой области щелкните правой кнопкой мыши узел **Ключи продуктов** , чтобы открыть меню **Действия** .
3. Выберите **Добавить ключи продукта** , чтобы открыть диалоговое окно **Добавление ключей продукта** .
4. В диалоговом окне **Добавление ключей продуктов** выберите один из следующих методов, чтобы добавить ключи продукта:
    - Чтобы добавить ключи продукта вручную, выберите **Ввести ключи продукта, разделенные разрывами строк**, введите один или несколько ключей продукта, разделенных разрывами строк, и нажмите **кнопку Добавить ключи**.
    - Чтобы импортировать CSV-файл со списком ключей продукта, выберите **Выберите файл ключа продукта для импорта**, перейдите в расположение файла, нажмите **кнопку Открыть** , чтобы импортировать файл, а затем выберите **Добавить ключи**.

> ⓘ **Примечание.**
>
> Если вы активируете большое количество продуктов с помощью MAK, обновите число активаций MAK, чтобы обеспечить поддержку необходимого количества активаций. В списке ключей продуктов в центральной области выберите MAK и щелкните **Обновить данные ключа продукта в Интернете** на правой панели, чтобы связаться с Корпорацией Майкрософт и получить количество оставшихся активаций для MAK. Для этого шага требуется доступ к Интернету. Вы можете получить только оставшееся число активаций для MAK.

Удаление ключа продукта

- Чтобы удалить ключ продукта из списка, выберите ключ в списке и нажмите кнопку **Удалить** в меню **Выбранные элементы** на панели справа. Выберите **Да** , чтобы подтвердить удаление ключа продукта. Удаление ключа продукта из базы данных VAMT не повлияет на состояние активации любых продуктов или компьютеров в сети.

Связанные статьи

Установка ключа продукта

Установка ключа клиента KMS

Last updated on 14.05.2025

Установка ключа продукта

С помощью средства управления активацией корпоративных лицензий (VAMT) можно установить розничный ключ, ключ многократной активации (MAK) и ключ сервера службы управления ключами (CSVLK).

Установка ключа продукта

1. Откройте VAMT.
2. В области слева выберите продукт, на который нужно установить ключи.
3. Можно воспользоваться функцией **Filter**, чтобы сузить область поиска компьютеров. Для этого нажмите **Filter** на панели справа, чтобы открыть диалоговое окно **Filter Products**.
4. В диалоговом окне **Filter Products** можно отфильтровать список по имени компьютера, названию продукта, типу ключа продукта, состоянию лицензии или любому сочетанию этих параметров.
    - Чтобы отфильтровать список по имени компьютера, введите нужное имя в поле **Computer Name**.
    - Чтобы отфильтровать список по названию продукта, типу ключа продукта или состоянию лицензии, выберите список, который вы хотите использовать для фильтра, и выберите параметр . При необходимости выберите **очистить все фильтры** , чтобы создать новый фильтр.
5. Выберите **Фильтр**.
6. В представлении списка продуктов на центральной панели отсортируйте список (при необходимости) и выберите продукты для установки ключей. Можно выбрать несколько продуктов с помощью клавиши **CTRL** или **SHIFT**.
7. Выберите **Установить ключ продукта** в меню **Выбранные элементы** в области справа, чтобы открыть диалоговое окно **Установка ключа продукта** .
8. В диалоговом окне **Select Product Key** отображаются ключи, которые доступны для установки. В разделе **Recommended MAKs** VAMT может отображать один или несколько рекомендуемых ключей MAK в зависимости от выбранных продуктов. Можно выбрать рекомендуемый ключ продукта или ключ продукта из списка **All Product Keys**. Используйте полосу прокрутки, чтобы просмотреть описания каждого ключа в разделе **Description**. Выбрав ключ продукта, который требуется установить, выберите **Установить ключ**. Одновременно можно установить только один ключ.

9. VAMT отображает диалоговое окно **Installing product key** во время попытки установить ключ продукта для выбранных продуктов. По окончании этого процесса его состояние отобразится в столбце **Action Status** диалогового окна. Нажмите **кнопку Закрыть** , чтобы закрыть диалоговое окно. Вы также можете выбрать флажок **Автоматически закрывать по завершении** проверка при появлении диалогового окна.

   Это же состояние отображается в столбце **Status of Last Action** в представлении списка продуктов на центральной панели.

   > ⓘ **Примечание.**
   >
   > Установка ключа продукта завершится ошибкой, если VAMT найдет несоответствующие типы или выпуски ключей. VAMT отобразит состояние сбоя и продолжит установку со следующего продукта в списке. Дополнительные сведения о выборе правильного ключа MAK или ключа узла KMS (CSVLK) см. **Выбор правильного ключа многократной установки для Windows**.

Связанные статьи

Добавление и удаление ключа продукта

Установка ключа клиента KMS

Last updated on 14.05.2025

Установка ключа клиента KMS

С помощью средства управления активацией корпоративных лицензий (VAMT) можно установить универсальный ключ многократной установки (GVLK) или ключ продукта клиента KMS. Например, если вы преобразуете продукт, активированный MAK, в активацию KMS.

> ⓘ **Примечание.**
>
> По умолчанию в выпусках Windows Vista, Windows® 7, Windows 8, Windows 10, Windows Server 2008, Windows Server 2008 R2, Windows Server® 2012 и Microsoft® Office 2010 с корпоративными лицензиями для активации используется KMS. Ключи GVLK уже установлены в выпусках этих продуктов с корпоративными лицензиями.

Установка ключа клиента KMS

1. Откройте VAMT.
2. В левой области выберите **Продукты** , чтобы открыть представление списка продуктов в центральной области.
3. В представлении списка продуктов в центральной области выберите продукты для установки ключей GVLK. Можно воспользоваться функцией **Filter**, чтобы сузить область поиска компьютеров. Для этого нажмите **Filter** на панели справа, чтобы открыть диалоговое окно **Filter Products**.
4. В диалоговом окне **Filter Products** можно отфильтровать список по имени компьютера, названию продукта, типу ключа продукта, состоянию лицензии или любому сочетанию этих параметров.
    - Чтобы отфильтровать список по имени компьютера, введите нужное имя в поле **Computer Name**.
    - Чтобы отфильтровать список по названию продукта, типу ключа продукта или состоянию лицензии, выберите список, который вы хотите использовать для фильтра, и выберите параметр . При необходимости выберите **очистить все фильтры** , чтобы создать новый фильтр.
5. Выберите **Фильтр**. VAMT отображает отфильтрованный список на центральной панели.

6. Выберите **Установить ключ продукта** в меню **Выбранные элементы** в области справа, чтобы открыть диалоговое окно **Установка ключа продукта** .

7. В диалоговом окне **Install Product Key** отображаются ключи, доступные для установки.

8. Выберите параметр **Автоматически выбирать ключ клиента AD или KMS** , а затем выберите **Установить ключ**.

   VAMT отображает диалоговое окно **Installing product key** во время попытки установить ключ продукта для выбранных продуктов. По окончании этого процесса его состояние отобразится в столбце **Action Status** диалогового окна. Нажмите **кнопку Закрыть** , чтобы закрыть диалоговое окно. Вы также можете выбрать флажок **Автоматически закрывать по завершении** проверка при появлении диалогового окна.

   Это же состояние отображается в столбце **Status of Last Action** в представлении списка продуктов на центральной панели.

Связанные статьи

Запуск активации KMS

Добавление и удаление ключа продукта

Установка ключа продукта

Last updated on 14.05.2025

Запуск активации через Интернет

Вы можете использовать средство управления активацией корпоративных лицензий (VAMT), чтобы включить активацию клиентских продуктов через Интернет. Вы можете установить клиентские продукты с любым ключом продукта, который подходит для активации через Интернет: ключом многократной активации (MAK), розничным ключом и ключом узла служб управления ключами Windows (KMS).

Требования

Перед запуском активации через Интернет убедитесь, что сеть и установка VAMT соответствуют следующим требованиям:

- VAMT устанавливается на центральном компьютере, который имеет сетевой доступ ко всем клиентским компьютерам.
- Как узел VAMT, так и клиентский компьютеры имеют доступ к Интернету.
- Продукты, которые требуется активировать, добавляются в VAMT.
- VAMT имеет административные разрешения на всех компьютерах, которые вы планируете активировать, и доступ к инструментарию управления Windows (WMI) можно получить через брандмауэр Windows. Дополнительные сведения см. в разделе Настройка клиентских компьютеров.

Ключи продуктов, установленные в клиентских продуктах, должны иметь достаточное количество оставшихся активаций. Если вы активируете ключ MAK, вы можете получить оставшееся количество активаций для этого ключа, выбрав MAK в списке ключей продукта в центральной области, а затем щелкнув **Обновить данные ключа продукта** в интернете в правой области. Это действие извлекает количество оставшихся активаций для MAK от корпорации Майкрософт. На этом шаге требуется доступ к Интернету, а оставшееся количество активаций можно получить только для MAK.

Запуск активации через Интернет

1. Откройте VAMT.
2. При необходимости в представлении списка продуктов в центральной области отсортируйте список. Можно воспользоваться функцией **Filter**, чтобы сузить область поиска компьютеров. Для этого нажмите **Filter** на панели справа, чтобы открыть диалоговое окно **Filter Products**.

3. В диалоговом окне **Filter Products** можно отфильтровать список по имени компьютера, названию продукта, типу ключа продукта, состоянию лицензии или любому сочетанию этих параметров.

    - Чтобы отфильтровать список по имени компьютера, введите нужное имя в поле **Computer Name**.

    - Чтобы отфильтровать список по названию продукта, типу ключа продукта или состоянию лицензии, выберите список, который вы хотите использовать для фильтра, и выберите параметр . При необходимости выберите **очистить все фильтры** , чтобы создать новый фильтр.

4. Выберите **Фильтр**. VAMT отображает отфильтрованный список на центральной панели.

5. Выберите продукты, которые нужно активировать. Можно выбрать несколько продуктов с помощью клавиши **CTRL** или **SHIFT**.

6. Выберите **Активировать** в меню **Выбранные элементы** на правой панели **Действия** , а затем наведите указатель на **пункт Активировать**. Если панель **Действия** не отображается, нажмите кнопку Показать или скрыть область действий, расположенную на панели инструментов справа от кнопки Справка.

7. Наведите указатель мыши на **пункт Активация в сети**, а затем выберите соответствующий параметр учетных данных. Если выбрать параметр **Альтернативные учетные данные** , вам будет предложено ввести альтернативное имя пользователя и пароль.

8. VAMT отображает диалоговое окно **Активация продуктов** , пока не завершит запрошенное действие. После завершения активации состояние отображается в столбце **Состояние действия** диалогового окна. Нажмите **кнопку Закрыть** , чтобы закрыть диалоговое окно. Вы также можете выбрать флажок **Автоматически закрывать по завершении** проверка при появлении диалогового окна.

    То же состояние отображается в столбце **Состояние последнего действия** в представлении списка продуктов в центральной области.

    > ⓘ **Примечание.**
    >
    > Активация через Интернет не позволяет сохранить идентификаторы подтверждения (CID). В результате вы не сможете выполнить локальную повторную активацию.

Примечание.

Вы можете использовать активацию через Интернет для выбора продуктов с разными типами ключей и одновременной активации продуктов.

Связанные статьи

Запуск активации прокси-сервера

Запуск активации KMS

Запуск локальной повторной активации

Last updated on 14.05.2025

Запуск активации прокси-сервера

Статья • 26.07.2024

Вы можете использовать средство управления активацией корпоративных лицензий (VAMT) для запуска активации клиентских компьютеров, у которых нет доступа к Интернету. Клиентские продукты можно установить с любым типом ключа продукта, который подходит для активации прокси-сервера: ключом множественной активации (MAK), ключом узла KMS (CSVLK) или ключом розничной торговли.

В типичном сценарии активации прокси-сервера главный компьютер VAMT распространяет MAK на один или несколько клиентских компьютеров и собирает идентификатор установки (IID) с каждого компьютера. Главный компьютер VAMT отправляет идентификаторы IID в корпорацию Майкрософт от имени клиентских компьютеров и получает соответствующие идентификаторы подтверждения (CID). Затем главный компьютер VAMT устанавливает CID на клиентском компьютере для завершения активации. При использовании этого метода активации доступ к Интернету требуется только на хост-компьютере VAMT.

> ⓘ **Примечание**
>
> Для рабочих групп, которые полностью изолированы от любой более крупной сети, по-прежнему можно запустить MAK, ключ узла KMS (CSVLK) или активацию прокси-сервера розничной торговли. Для этого необходимо установить второй экземпляр VAMT на компьютере в изолированной группе и использовать съемный носитель для передачи данных активации между этим компьютером и другим главным компьютером VAMT с доступом к Интернету. Дополнительные сведения об этом сценарии см. в разделе **Сценарий 2. Активация прокси-сервера**. Аналогичным образом прокси-сервер может активировать ключ узла KMS (CSVLK), расположенный в изолированной сети. Вы также можете активировать ключ узла KMS (CSVLK) в основной сети, если не хотите, чтобы главный компьютер KMS подключались к Корпорации Майкрософт через Интернет.

Требования

Перед активацией прокси-сервера убедитесь, что сеть и установка VAMT соответствуют следующим требованиям:

- На компьютере с доступом к Интернету установлен экземпляр VAMT. Если вы выполняете активацию прокси-сервера для изолированной рабочей группы, вам также потребуется установить VAMT на одном из компьютеров в рабочей группе.
- Продукты для активации добавлены в VAMT и устанавливаются с ключом розничного продукта, ключом узла KMS (CSVLK) или MAK. Если продукты не были установлены с соответствующим ключом продукта, см. инструкции по установке ключа продукта в разделе Добавление и удаление ключа продукта .
- VAMT имеет административные разрешения на все продукты для активации, а инструментарий управления Windows (WMI) доступен через брандмауэр Windows.
- Для компьютеров рабочей группы необходимо создать раздел реестра, чтобы включить удаленные административные действия в разделе Контроль учетных записей пользователей (UAC). Дополнительные сведения см. в разделе Настройка клиентских компьютеров.

  Ключи продуктов, установленные в клиентских продуктах, должны иметь достаточное количество оставшихся активаций. Если вы активируете ключ MAK, вы можете получить оставшееся количество активаций для этого ключа, выбрав MAK в списке ключей продукта в центральной области, а затем щелкнув **Обновить данные ключа продукта** в интернете в правой области. Это действие извлекает количество оставшихся активаций для MAK от корпорации Майкрософт. На этом шаге требуется доступ к Интернету, а оставшееся количество активаций можно получить только для MAK.

Запуск активации прокси-сервера

1. Откройте VAMT.
2. При необходимости установите ключи продукта. Дополнительные сведения см. в следующих разделах:
   - Установите ключ продукта для установки ключа retail, MAK или ключа узла KMS (CSVLK).
   - Установите ключ клиента KMS , чтобы установить ключи GVLK (клиент KMS).
3. В списке **Продукты** в центральной области выберите отдельные продукты для активации. Функцию **Фильтр** можно использовать для сужения поиска

продуктов, щелкнув **Фильтр** в области справа, чтобы открыть диалоговое окно **Фильтрация продуктов** .

4. В диалоговом окне **Filter Products** можно отфильтровать список по имени компьютера, названию продукта, типу ключа продукта, состоянию лицензии или любому сочетанию этих параметров.

    - Чтобы отфильтровать список по имени компьютера, введите нужное имя в поле **Computer Name**.
    - Чтобы отфильтровать список по названию продукта, типу ключа продукта или состоянию лицензии, выберите список, который вы хотите использовать для фильтра, и выберите параметр . При необходимости выберите **очистить все фильтры** , чтобы создать новый фильтр.

5. Выберите **Фильтр**. VAMT отображает отфильтрованный список на центральной панели.

6. В области справа выберите **Активировать** , а затем выберите **Активация прокси-сервера** , чтобы открыть диалоговое окно **Активация прокси-сервера** .

7. В диалоговом окне **Активация прокси-сервера** выберите **Применить идентификатор подтверждения, применить к выбранным компьютерам и активировать**.

8. Если вы активируете продукты, для которых требуются учетные данные администратора, отличные от используемых в настоящее время, установите флажок **Использовать альтернативные учетные данные** .

9. Нажмите **ОК**.

10. VAMT отображает диалоговое окно **Активация продуктов** , пока не завершит запрошенное действие. Если вы выбрали параметр **Альтернативные учетные данные** , вам будет предложено ввести учетные данные.

    > ⓘ **Примечание**

    Активацию прокси-сервера можно использовать для выбора продуктов с разными типами ключей и одновременной активации продуктов.

Связанные статьи

Запуск активации через Интернет

Запуск активации KMS

Запуск локальной повторной активации

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Запуск активации KMS

Средство управления активацией корпоративных лицензий (VAMT) можно использовать для активации корпоративных лицензий с помощью службы управления ключами (KMS). VAMT можно использовать для активации универсальных ключей корпоративного лицензирования или ключей клиента KMS на продуктах, доступных для VAMT. GVLK — это ключи продуктов по умолчанию, используемые выпусками windows Vista, Windows 7, Windows 8, Windows 10, Windows Server 2008, Windows Server 2008 R2, Windows Server® 2012 и Microsoft Office 2010. Пакеты GVLK уже установлены в выпусках этих продуктов с корпоративными лицензиями.

Требования

Перед настройкой активации KMS убедитесь, что сеть и установка VAMT соответствуют следующим требованиям:

- Узел KMS настроен и включен.
- Клиенты KMS могут получить доступ к узлу KMS.
- VAMT устанавливается на центральном компьютере с сетевым доступом ко всем клиентским компьютерам.
- Продукты для активации были добавлены в VAMT. Дополнительные сведения о добавлении ключей продукта см. в статье Установка ключа клиента KMS.
- VAMT имеет административные разрешения на всех компьютерах, которые нужно активировать, и инструментарий управления Windows (WMI) доступен через брандмауэр Windows. Дополнительные сведения см. в разделе Настройка клиентских компьютеров.

Настройка устройств для активации KMS

1. Откройте VAMT.
2. При необходимости настройте параметры активации KMS. Если вам не нужно настраивать параметры, перейдите к шагу 6 в этой процедуре. В противном случае перейдите к шагу 2.
3. Чтобы настроить параметры, в строке меню выберите **Вид**, а затем выберите **Параметры**, чтобы открыть диалоговое окно **Параметры средство управления активацией корпоративных лицензий**.

4. В разделе **Выбор узла служб управления ключами** выберите один из следующих параметров:

    - **Автоматические поиски узла KMS с помощью DNS (по умолчанию).** При выборе этого параметра VAMT сначала очищает все ранее настроенные узлы KMS на целевом компьютере и указывает компьютеру запрашивать службу доменных имен (DNS) для поиска узла KMS и попытки активации.

    - **Найдите узел KMS с помощью DNS в этом домене для поддерживаемых продуктов**. Введите доменное имя. При выборе этого параметра VAMT сначала очищает все ранее настроенные узлы KMS на целевом компьютере и указывает компьютеру запрашивать DNS в указанном домене, чтобы найти узел KMS и попытаться активировать.

    - **Используйте определенный узел KMS**. Введите имя узла KMS и порт узла KMS. Для сред, которые не используют DNS для идентификации узла KMS, VAMT задает указанное имя узла KMS и порт узла KMS на целевом компьютере, а затем указывает компьютеру попытаться выполнить активацию с определенным узлом KMS.

5. Нажмите **кнопку Применить**, а затем нажмите **кнопку OK**, чтобы закрыть диалоговое окно **Параметры средство управления активацией корпоративных лицензий**.

6. Выберите продукты для активации, выбрав отдельные продукты в представлении списка продуктов в центральной области. Можно воспользоваться функцией **Filter**, чтобы сузить область поиска компьютеров. Для этого нажмите **Filter** на панели справа, чтобы открыть диалоговое окно **Filter Products**. В диалоговом окне **Filter Products** можно отфильтровать список по имени компьютера, названию продукта, типу ключа продукта, состоянию лицензии или любому сочетанию этих параметров.

    - Чтобы отфильтровать список по имени компьютера, введите нужное имя в поле **Computer Name**.

    - Чтобы отфильтровать список по названию продукта, типу ключа продукта или состоянию лицензии, выберите список, который вы хотите использовать для фильтра, и выберите параметр . При необходимости выберите **очистить все фильтры** , чтобы создать новый фильтр.

7. Выберите **Фильтр**. VAMT отображает отфильтрованный список на центральной панели.

8. В правой области выберите **Активировать** в меню **Выбранные элементы** , а затем выберите **Активация тома**.

9. Выберите параметр учетных данных. Выберите **Альтернативные учетные данные** , только если вы активируете продукты, для которых требуются учетные данные администратора, отличные от используемых в настоящее время.

10. Если вы предоставляете альтернативные учетные данные, введите соответствующее имя пользователя и пароль и нажмите кнопку **OK**. VAMT отображает диалоговое окно **Активация корпоративных лицензий** , пока не завершит запрошенное действие. По завершении процесса в представлении списка продуктов в центральной области появится обновленное состояние активации каждого продукта.

Связанные статьи

Запуск активации через Интернет

Запуск активации прокси-сервера

Запуск локальной повторной активации

Last updated on 14.05.2025

Запуск локальной повторной активации

Если вы переустановили Windows® или Microsoft® Office 2010 на компьютере, который был первоначально активирован с помощью прокси-активации (MAK, retail или CSLVK (узел KMS)) и не вносил существенных изменений в оборудование, используйте эту локальную процедуру повторной активации для повторной активации программы на этом компьютере. Локальная повторная активация зависит от данных, созданных во время начальной активации прокси-сервера и сохраненных в базе данных средство управления активацией корпоративных лицензий (VAMT). База данных содержит идентификатор установки (IID) и идентификатор подтверждения (ожидающий CID). Локальная повторная активация использует эти данные для повторного применения CID и повторной активации этих продуктов. Повторное применение того же CID позволяет сохранить оставшиеся активации ключа.

> ⓘ **Примечание.**
>
> Во время начальной активации прокси-сервера CID привязывается к цифровому отпечатку пальца, который вычисляется на основе значений, присвоенных нескольким различным аппаратным компонентам компьютера. Если на компьютере произошли значительные изменения оборудования, этот отпечаток больше не будет соответствовать CID. В этом случае необходимо получить новый идентификатор CID для компьютера от корпорации Майкрософт.

Запуск локальной повторной активации

1. Откройте VAMT. Убедитесь, что вы подключены к нужной базе данных.
2. В левой области выберите продукт, который требуется повторно активировать, чтобы отобразить список продуктов.
3. В представлении списка продуктов в центральной области выберите нужные продукты для повторной активации. Чтобы отсортировать список по имени компьютера, щелкните заголовок **Имя компьютера** . Функцию **Фильтр** также можно использовать для сужения поиска компьютеров, щелкнув **Фильтр** в правой области, чтобы открыть диалоговое окно **Фильтр продуктов** .
4. В диалоговом окне **Filter Products** можно отфильтровать список по имени компьютера, названию продукта, типу ключа продукта, состоянию лицензии или любому сочетанию этих параметров.

- Чтобы отфильтровать список по имени компьютера, введите нужное имя в поле **Computer Name**.
- Чтобы отфильтровать список по названию продукта, типу ключа продукта или состоянию лицензии, выберите список, который вы хотите использовать для фильтра, и выберите параметр . При необходимости выберите **очистить все фильтры** , чтобы создать новый фильтр.

5. Выберите **Фильтр**. VAMT отображает отфильтрованный список на центральной панели.
6. В области справа выберите **Активировать**, а затем — **Применить идентификатор подтверждения**.
7. Выберите параметр учетных данных. Выберите **Альтернативные учетные данные** , только если вы повторно активируете продукты, для которых требуются учетные данные администратора, отличные от используемых в настоящее время.
8. Если вы предоставляете альтернативные учетные данные, в диалоговом окне **Безопасность Windows** введите соответствующее имя пользователя и пароль и нажмите **кнопку OK**.

   VAMT отображает диалоговое окно **Применить идентификатор подтверждения** .
9. Если вы используете ключ продукта, отличный от ключа продукта, используемого для начальной активации, необходимо завершить новую активацию, чтобы получить новый идентификатор CID.
10. Если вы активируете продукт, которому требуются учетные данные администратора, отличные от используемых в настоящее время, установите флажок **Использовать альтернативные учетные данные** проверка.
11. Нажмите **OK**.

Связанная статья

Запуск активации через Интернет

Запуск активации прокси-сервера

Запуск активации KMS

Last updated on 14.05.2025

Активация леса Active Directory в сети

Вы можете использовать функцию активации средство управления активацией корпоративных лицензий (VAMT) Active Directory-Based (ADBA), чтобы активировать лес Active Directory (AD) через Интернет. ADBA позволяет определенным продуктам наследовать активацию от домена.

> ⓘ **Внимание**
>
> ADBA применяется только к общим ключам корпоративного лицензирования (GVLK) и ключам узла KMS (CSVLK). Чтобы использовать ADBA, в лесу AD необходимо установить один или несколько ключей узла KMS (CSVLK), а клиентские ключи (GVLK) — в клиентских продуктах.

Требования

Перед активацией по сети убедитесь, что сеть и установка VAMT соответствуют следующим требованиям:

- VAMT устанавливается на главный компьютер с доступом к Интернету.
- VAMT имеет административные разрешения для домена Active Directory.
- Ключ узла KMS (CSVLK), который вы планируете использовать, добавляется в VAMT в узле **Ключи продуктов** .

Выполнение активации леса Active Directory в сети

1. Откройте VAMT.
2. В левой области выберите узел **Активная активация Directory-Based** .
3. В правой области **Действия** выберите **Online активировать лес** , чтобы открыть диалоговое окно **Установка ключа продукта** .
4. В диалоговом окне **Установка ключа продукта** выберите ключ узла KMS (CSVLK), который нужно применить к лесу AD.
5. При необходимости введите новое имя объекта активации Active Directory-Based.

   > ⓘ **Внимание**

Если вы хотите переименовать объект ADBA, это необходимо сделать сейчас. После нажатия кнопки **Установить ключ** имя изменить нельзя.

6. Выберите **Установить ключ**.
7. VAMT отображает диалоговое окно **Активация Active Directory** , пока не завершит запрошенное действие.

Активированный объект и дата его создания отображаются в узле **Активная активация Directory-Based** в центральной области.

Связанные статьи

- Сценарий 1. Активация по сети
- Добавление и удаление компьютеров

Last updated on 14.05.2025

Активация с помощью прокси-сервера леса Active Directory

Функцию активации active Directory-Based (ADBA) средство управления активацией корпоративных лицензий (VAMT) можно использовать для активации леса Active Directory (AD) для изолированной рабочей группы без доступа к Интернету. ADBA позволяет определенным продуктам томов наследовать активацию от домена.

> **ⓘ Внимание**
>
> ADBA применяется только к *общим ключам корпоративного лицензирования (GVLK)* и *ключу узла KMS (CSVLK)*. Чтобы использовать ADBA, в лесу AD необходимо установить один или несколько ключей узла KMS (CSVLK), а клиентские ключи (GVLK) — в клиентских продуктах.

В типичном сценарии активации прокси-сервера главный компьютер VAMT распространяет ключ продукта на один или несколько клиентских компьютеров и собирает идентификатор установки (IID) с каждого компьютера. Главный компьютер VAMT отправляет идентификаторы IID в корпорацию Майкрософт от имени клиентских компьютеров и получает соответствующие идентификаторы подтверждения (CID). Затем главный компьютер VAMT устанавливает CID на клиентском компьютере для завершения активации. При использовании этого метода активации доступ к Интернету должен иметь только главный компьютер VAMT.

> **ⓘ Примечание.**
>
> Для рабочих групп, изолированных от любой более крупной сети, по-прежнему можно выполнить активацию леса AD. Для этого необходимо установить второй экземпляр VAMT на компьютере в изолированной группе и использовать съемный носитель для передачи данных активации между этим компьютером и другим главным компьютером VAMT с доступом к Интернету. Вы также можете активировать ключ узла KMS (CSVLK) в основной сети, если не хотите, чтобы главный компьютер подключалась к Корпорации Майкрософт через Интернет.

Требования

Перед активацией прокси-сервера убедитесь, что сеть и установка VAMT соответствуют следующим требованиям:

- На компьютере с доступом к Интернету установлен экземпляр VAMT. Если вы выполняете активацию прокси-сервера для изолированной рабочей группы, необходимо также установить VAMT на одном из компьютеров в рабочей группе.
- VAMT имеет административные разрешения для домена Active Directory.

Активация прокси-сервера леса Active Directory

1. Откройте VAMT.
2. В левой области выберите узел **Активная активация Directory-Based** .
3. В правой области **Действия** выберите **Прокси-сервер активировать лес** , чтобы открыть диалоговое окно **Установка ключа продукта** .
4. В диалоговом окне **Установка ключа продукта** выберите ключ узла KMS (CSVLK), который требуется активировать.
5. Если вы хотите переименовать объект ADBA, введите новое имя объекта активации Active Directory-Based. Если вы хотите переименовать объект ADBA, это необходимо сделать сейчас. После нажатия кнопки **Установить ключ** имя изменить нельзя.
6. Введите имя файла, в котором требуется сохранить идентификатор автономной установки, или перейдите к расположению файла и нажмите кнопку **Открыть**. Если вы активируете лес AD в изолированной рабочей группе, сохраните `.cilx` файл на съемных носителях.
7. Выберите **Установить ключ**. VAMT отображает диалоговое окно **Активация Active Directory** , пока не завершит запрошенное действие. Активированный объект и дата его создания отображаются в узле **Активная активация Directory-Based** в центральной области.
8. Вставьте съемный носитель в узел VAMT с доступом к Интернету. Убедитесь, что вы находитесь на корневом узле и что **представление средство управления активацией корпоративных лицензий** отображается в центральной области.
9. В правой области **Действия** выберите **Получение идентификаторов подтверждения для CILX** , чтобы открыть диалоговое окно **Получение идентификаторов подтверждения для файла** .
10. В диалоговом окне **Получение идентификаторов подтверждения для файла** перейдите к расположению `.cilx` файла, экспортированного с изолированного главного компьютера рабочей группы. Выберите файл и нажмите кнопку **Открыть**. VAMT отображает сообщение **идентификаторов подтверждения приобретения** , когда оно связывается с корпорацией Майкрософт и получает идентификаторы CID.

11. Когда процесс сбора CID завершится, VAMT отображает **средство управления активацией корпоративных лицензий** сообщение, в котором показано, сколько идентификаторов подтверждения успешно получено, а также имя файла, в котором были сохранены идентификаторы. Нажмите **кнопку OK** , чтобы закрыть сообщение.
12. Удалите запоминающее устройство, содержащее `.cilx` файл, с подключенного к Интернету главного компьютера VAMT и вставьте его в главный компьютер VAMT в изолированной рабочей группе.
13. Откройте VAMT и выберите узел **Активация активной Directory-Based** на левой панели.
14. В правой области **Действия** выберите **Применить идентификатор подтверждения к домену Active Directory**, перейдите к файлу `.cilx` и нажмите кнопку **Открыть**.

VAMT отображает диалоговое окно **Активация Active Directory** , пока не завершит запрошенное действие. Активированный объект и дата его создания отображаются в узле **Активная активация Directory-Based** в центральной области.

Связанные статьи

Добавление и удаление компьютеров

Last updated on 14.05.2025

Импорт и экспорт данных средство управления активацией корпоративных лицензий

С помощью средство управления активацией корпоративных лицензий (VAMT) можно импортировать данные активации продукта из файла сведений о компьютерах (`.cilx` или `.cil`) в SQL Server. Также используйте VAMT для экспорта данных активации продукта в `.cilx` файл. Файл `.cilx` — это XML-файл, в котором хранятся данные об активации компьютера и продукта.

Данные можно импортировать или экспортировать в следующих сценариях:

- Импорт и слияние данных из предыдущих версий VAMT.
- Экспорт данных для активации прокси-сервера.

> ⚠ **Предупреждение**
>
> Редактирование `.cilx` файла с помощью приложения, отличного от VAMT, может привести к повреждению `.cilx` файла. Этот метод не поддерживается.

Импорт данных VAMT

Чтобы импортировать данные в VAMT, используйте следующий процесс:

1. Откройте VAMT.
2. В правой области **Действия** выберите **Импорт списка** , чтобы открыть диалоговое окно **Импорт списка** .
3. В диалоговом окне **Импорт списка** перейдите к расположению `.cilx` файла, выберите файл и нажмите кнопку **Открыть**.
4. В диалоговом окне **средство управления активацией корпоративных лицензий** нажмите **кнопку ОК**, чтобы начать импорт. VAMT отображает сообщение о ходе импорта файла. Нажмите **кнопку ОК** , когда появится сообщение и подтвердится, что импорт успешно завершен.

Экспорт данных VAMT

Экспорт данных VAMT с главного компьютера VAMT, который не подключен к Интернету, является первым шагом активации прокси-сервера с помощью нескольких узлов VAMT. Экспорт данных активации продукта в `.cilx` файл:

1. В левой области выберите продукт, для которого нужно экспортировать данные, или выберите **Продукты** , если список содержит данные для всех продуктов.
2. Если вы хотите экспортировать только часть данных в списке продуктов, в представлении списка продуктов в центральной области выберите продукты, которые нужно экспортировать.
3. В правой части области **Действия** выберите **Экспорт списка** , чтобы открыть диалоговое окно **Экспорт списка** .
4. В диалоговом окне **Экспорт списка** нажмите кнопку **Обзор** , чтобы перейти к файлу `.cilx` .
5. В разделе **Параметры экспорта** выберите один из следующих параметров типа данных:
   - Экспорт продуктов и ключей продуктов
   - Экспорт только продуктов
   - Экспортируйте только данные активации прокси-сервера. Выбор этого параметра гарантирует, что экспорт содержит только сведения о лицензировании, необходимые веб-службе прокси-сервера для получения CID от Корпорации Майкрософт. При выборе этого параметра в экспортируемом `.cilx` файле не содержится личных сведений.
6. Если вы выбрали экспортируемые продукты, установите флажок **Экспортировать только строки выбранных продуктов** проверка.
7. Выберите **Сохранить**. VAMT отображает сообщение о ходе экспорта данных. Нажмите **кнопку OK** , когда появится сообщение и подтвердится, что экспорт успешно завершен.

Связанные статьи

Прокси-активация с помощью VAMT

Last updated on 14.05.2025

Использование VAMT в Windows PowerShell

Статья • 20.11.2024

Командлеты PowerShell средство управления активацией корпоративных лицензий (VAMT) можно использовать для выполнения той же функции, что и средство командной строки Vamt.exe.

Настройка VAMT в Windows PowerShell

Установка PowerShell 3.0

Командлетам PowerShell VAMT требуется Windows PowerShell, который входит в состав Windows 10 и более поздних версий. Сведения о том, как скачать последнюю версию PowerShell, см. в статье Установка PowerShell в Windows.

Установка комплекта средств оценки и развертывания Windows

В дополнение к PowerShell необходимо импортировать модуль VAMT PowerShell. Модуль входит в папку VAMT 3.0 после установки комплекта средств оценки и развертывания Windows (Windows ADK).

Подготовка среды PowerShell VAMT

Чтобы открыть PowerShell с учетными данными администратора, нажмите кнопку **Пуск** и введите , `PowerShell` чтобы найти программу. Щелкните **правой** кнопкой мыши Windows PowerShell и выберите **Запуск от имени администратора**. Чтобы открыть PowerShell в Windows 7, выберите **Пуск**, **Все программы**, **Стандартные**, **Windows PowerShell**, щелкните **правой** кнопкой мыши Windows PowerShell, а затем выберите **Запуск от имени администратора**.

> ⓘ **Важно!**
>
> Если вы используете компьютер с 64-разрядным процессором, выберите **Windows PowerShell (x86)**. Командлеты PowerShell VAMT поддерживаются

только для архитектуры x86. Для импорта модуля VAMT необходимо использовать версию Windows PowerShell x86.

Версии x86 Windows PowerShell доступны в следующих каталогах:

- PowerShell: `C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe`
- Среда интегрированной среды сценариев PowerShell: `C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell_ise.exe`

Для всех поддерживаемых операционных систем можно использовать модуль VAMT PowerShell, входящий в состав Windows ADK. По умолчанию модуль устанавливается вместе с Windows ADK в папке VAMT. Измените каталоги на каталог, в котором находится VAMT. Например, если Windows ADK установлен в расположении `C:\Program Files(x86)\Windows Kits\10` по умолчанию , введите:

PowerShell

```
cd "C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\VAMT3"
```

Импорт модуля PowerShell VAMT

Чтобы импортировать модуль PowerShell VAMT, введите следующую команду в командной строке PowerShell:

PowerShell

```
Import-Module .\VAMT.psd1
```

где **Import-Module** импортирует модуль только в текущий сеанс. Чтобы импортировать модуль во все сеансы, добавьте команду **Import-Module** в профиль Windows PowerShell. Для получения дополнительных сведений о профилях введите `get-help about_profiles`.

Получение справки по командлетам PowerShell VAMT

Вы можете просмотреть все разделы справки для командлета PowerShell VAMT или просмотреть только интересующий вас раздел. Чтобы просмотреть все содержимое справки для командлета VAMT, введите:

PowerShell

```
get-help <cmdlet name> -all
```

Например, введите:

PowerShell

```
get-help get-VamtProduct -all
```

> ⚠ **Предупреждение**
>
> Командлет update-help не поддерживается для командлетов PowerShell VAMT. Чтобы просмотреть справку по командлетам VAMT в Интернете, можно использовать `-online` параметр с командлетом `get-help` . Дополнительные сведения см. в статье Командлеты средство управления активацией корпоративных лицензий (VAMT) в Windows PowerShell.

Просмотр разделов справки По PowerShell ДЛЯ VAMT

1. Чтобы получить синтаксис для использования с командлетом, введите следующую команду в командной строке PowerShell:

   PowerShell

   ```
   get-help <cmdlet name>
   ```

   Например, введите:

   PowerShell

   ```
   get-help get-VamtProduct
   ```

2. Чтобы просмотреть примеры с помощью командлета, введите:

   PowerShell

   ```
   get-help <cmdlet name> -examples
   ```

   Например, введите:

   ```
   
   ```

PowerShell

```
get-help get-VamtProduct -examples
```

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

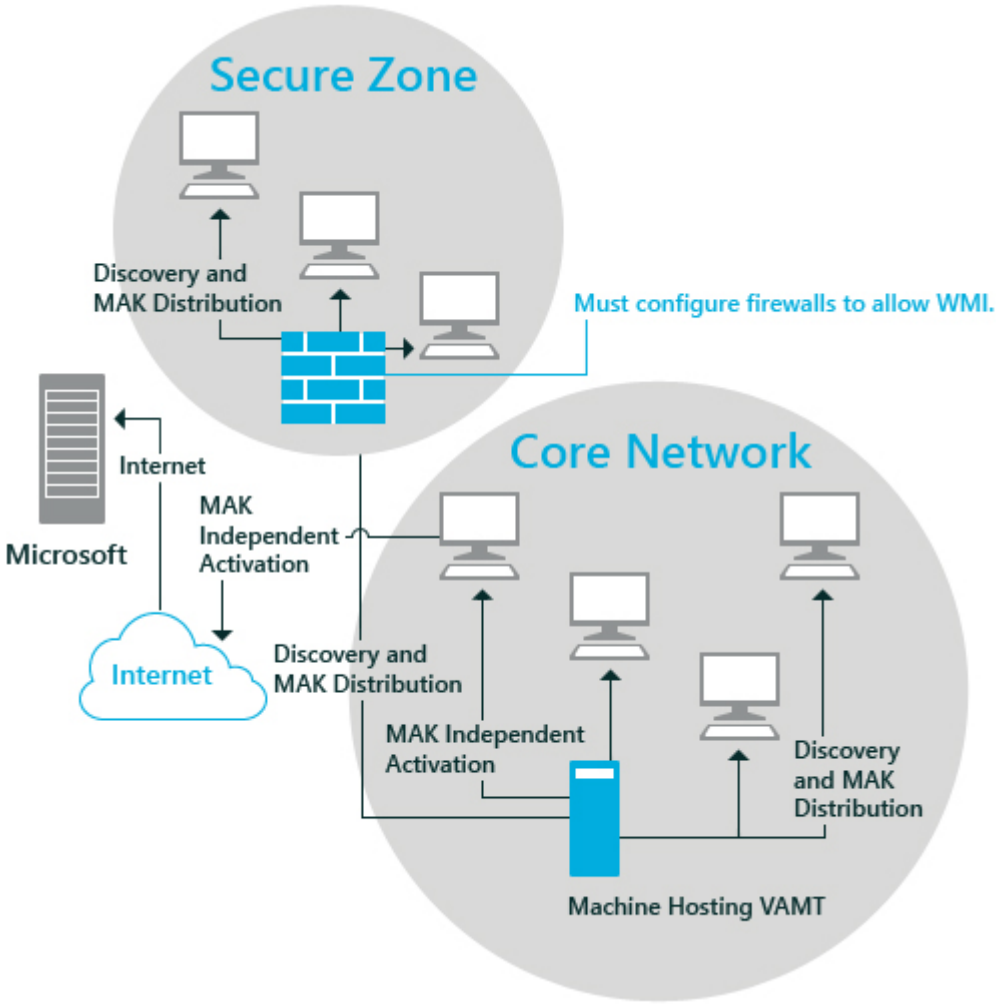
Отзыв о продукте

Сценарий 1. Активация через Интернет

Статья • 18.03.2023

В этом сценарии средство управления активацией корпоративных лицензий (VAMT) развертывается в основной сетевой среде. VAMT устанавливается на центральном компьютере, который имеет сетевой доступ ко всем клиентским компьютерам. Как узел VAMT, так и клиентские компьютеры имеют доступ к Интернету. На следующем рисунке показана схема сценария активации по сети для нескольких ключей активации (MAK). Этот сценарий можно использовать для активации по сети следующих типов ключей:

- Ключ множественной активации (MAK)
- Ключи службы управления ключами Windows (KMS):
  - Ключ узла KMS (CSVLK)
  - Универсальный ключ корпоративной лицензии (GVLK) или ключ клиента KMS
- Розничная торговля. Безопасная зона представляет собой основные сетевые компьютеры с более высоким уровнем безопасности, которые имеют дополнительную защиту брандмауэра.



Шаг 1. Установка и запуск VAMT на сетевом хост-компьютере

1. Установите VAMT на главный компьютер.

2. Щелкните значок VAMT в меню **Пуск** , чтобы открыть VAMT.

Шаг 2. Настройка исключения брандмауэра инструментария управления Windows на целевых компьютерах

- Убедитесь, что для всех целевых компьютеров включено исключение брандмауэра инструментария управления Windows (WMI). Дополнительные сведения см. в разделе Настройка клиентских компьютеров.

  ⓘ **Примечание**

Чтобы получить состояние лицензии на продукт, VAMT должна иметь административные разрешения на удаленных компьютерах, а WMI должен быть доступен через брандмауэр Windows. Кроме того, для компьютеров рабочей группы необходимо создать раздел реестра, чтобы включить удаленные административные действия в разделе Контроль учетных записей пользователей (UAC). Дополнительные сведения см. в разделе **Настройка клиентских компьютеров**.

Шаг 3. Подключение к базе данных VAMT

1. Если вы еще не подключены к базе данных, при открытии VAMT появится диалоговое окно **Параметры подключения к базе данных** . Выберите сервер и базу данных, где находятся ключи, которые необходимо активировать.

2. Выберите **Подключиться**.

3. Если вы уже подключены к базе данных, VAMT отображает список продуктов и ключей продуктов в центральной области, а также обзор лицензий компьютеров в базе данных. Если необходимо подключиться к другой базе данных, выберите **Успешно подключено к серверу** , чтобы открыть **диалоговое окно Параметры подключения к базе данных** . Дополнительные сведения о создании баз данных VAMT и добавлении данных VAMT см. в разделе Управление данными VAMT.

Шаг 4. Обнаружение продуктов

1. В левой области в узле **Продукты** Продукты выберите продукт, который требуется активировать.

2. Чтобы открыть диалоговое окно **Обнаружение продуктов** , выберите **Обнаружение продуктов** в меню **Действия** на панели справа.

3. В диалоговом окне **Обнаружение продуктов** выберите **Поиск компьютеров в Active Directory** , чтобы отобразить параметры поиска, а затем выберите нужные параметры поиска. Вы можете искать компьютеры в домене Active Directory, по имени отдельного компьютера или IP-адресу, в рабочей группе или с помощью общего запроса LDAP:

    - Чтобы найти компьютеры в домене Active Directory, выберите **Поиск компьютеров в Active Directory**. Затем в разделе **Критерии фильтра домена** в списке доменных имен выберите имя домена, который

требуется выполнить поиск. Вы можете еще больше сузить поиск, введя имя в поле **Фильтр по имени компьютера** , чтобы найти определенные компьютеры в домене. Этот фильтр поддерживает подстановочный знак звездочки (*). Например, при вводе "a*" будут отображаться только те имена компьютеров, которые начинаются с буквы "a".

- Чтобы выполнить поиск по имени или IP-адресу отдельного компьютера, выберите **Вручную ввести имя или IP-адрес**. Затем введите полное имя или IP-адрес в текстовое поле **Один или несколько имен компьютеров или IP-адресов, разделенных запятыми** . Разделите несколько записей с помощью запятой. VAMT поддерживает адресацию IPv4 и IPV6.

- Чтобы найти компьютеры в рабочей группе, выберите **Поиск компьютеров в рабочей группе**. Затем в разделе **Условия фильтра рабочей группы** в списке имен рабочих групп выберите имя рабочей группы, в которой требуется выполнить поиск. Вы можете еще больше сузить поиск, введя имя в поле **Фильтр по имени компьютера** , чтобы найти конкретный компьютер в рабочей группе. Этот фильтр поддерживает подстановочный знак звездочки (*). Например, при вводе "a*" будут отображаться только имена компьютеров, начинающиеся с буквы "a".

- Чтобы выполнить поиск компьютеров с помощью общего запроса LDAP, выберите **Поиск с запросом LDAP** и введите запрос в появившемся текстовом поле. VAMT проверит синтаксис запроса LDAP, но в противном случае выполнит запрос без дополнительных проверок.

4. Выберите **Поиск**.

   После завершения поиска продукты, обнаруженные VAMT, отображаются в представлении списка продуктов в центральной области.

Шаг 5. Сортировка и фильтрация списка компьютеров

Вы можете отсортировать список продуктов, чтобы было проще найти компьютеры, для которых требуется активировать ключи продуктов:

1. В строке меню в верхней части центральной области выберите **Группировать по**, а затем выберите **Продукт**, **Тип ключа продукта** или **Состояние лицензии**.

2. Чтобы отсортировать список дальше, можно выбрать один из заголовков столбцов для сортировки по столбцу.

3. Функцию **Фильтр** также можно использовать для сужения поиска компьютеров, щелкнув **Фильтр** в правой области, чтобы открыть диалоговое окно **Фильтр продуктов** .

4. В диалоговом окне **Filter Products** можно отфильтровать список по имени компьютера, названию продукта, типу ключа продукта, состоянию лицензии или любому сочетанию этих параметров.

    - Чтобы отфильтровать список по имени компьютера, введите нужное имя в поле **Computer Name**.

    - Чтобы отфильтровать список по названию продукта, типу ключа продукта или состоянию лицензии, выберите список, который вы хотите использовать для фильтра, и выберите параметр. При необходимости выберите **очистить все фильтры** , чтобы создать новый фильтр.

5. Выберите **Фильтр**. VAMT отображает отфильтрованный список в представлении списка продуктов в центральной области.

Шаг 6. Сбор сведений о состоянии с компьютеров в списке

Чтобы получить сведения о состоянии с избранных компьютеров в базе данных, можно выбрать компьютеры в представлении списка продуктов с помощью одного из следующих методов:

- Чтобы выбрать блок последовательно перечисленных компьютеров, выберите первый компьютер, который нужно выбрать, а затем выберите последний компьютер при нажатии клавиши **SHIFT** .

- Чтобы выбрать компьютеры, которые не перечислены подряд, удерживайте нажатой клавишу **CTRL** и выберите каждый компьютер, для которого требуется собрать сведения о состоянии.

Сбор сведений о состоянии с выбранных компьютеров

- В правой части области **Действия** выберите **Обновить состояние лицензии** в меню **Выбранные элементы** , а затем выберите параметр учетных данных.

Выберите **Альтернативные учетные данные** , только если вы обновляете продукты, для которых требуются учетные данные администратора, отличные от тех, которые использовались для входа на компьютер. В противном случае выберите **Текущие учетные данные** и перейдите к шагу 2. Если вы предоставляете альтернативные учетные данные, в диалоговом окне **Безопасность Windows** введите соответствующее имя пользователя и пароль, а затем нажмите кнопку **OK**.

- VAMT отображает диалоговое окно **Сбор сведений о продукте** при сборе состояния лицензии для всех поддерживаемых продуктов на выбранных компьютерах. По завершении процесса обновленное состояние лицензии каждого продукта появится в представлении списка продуктов в центральной области.

  > ⓘ **Примечание**
  >
  > Если на компьютере установлено несколько поддерживаемых продуктов, VAMT добавляет запись для каждого продукта. Запись отображается под соответствующим заголовком продукта.

Шаг 7. Добавление ключей продукта и определение оставшегося количества активаций

1. Выберите узел **Ключи продуктов** в левой области, а затем выберите **Добавить ключи продуктов** в области справа, чтобы открыть диалоговое окно **Добавление ключей продуктов** .

2. В диалоговом окне **Добавление ключа продукта** можно выбрать один из следующих способов добавления ключей продукта:

   - Чтобы добавить ключи продукта вручную, выберите **Ввести ключи продукта, разделенные разрывами строк**, введите один или несколько ключей продукта, а затем нажмите **кнопку Добавить ключи**.

   - Чтобы импортировать файл с разделимы-запятыми (CSV), содержащий список ключей продукта, выберите **Выберите файл ключа продукта для импорта**, перейдите к расположению файла, нажмите кнопку **Открыть** , чтобы импортировать файл, а затем нажмите **кнопку Добавить ключи**.

Добавленные ключи отображаются в представлении списка **Ключи продуктов** в центральной области.

> **ⓘ Важно!**
>
> Если вы активируете многие продукты с помощью MAK, обновите число активаций MAK, чтобы обеспечить поддержку необходимого количества активаций. В списке ключей продукта в центральной области выберите MAK, а затем щелкните **Обновить данные ключа продукта в интернете** в области справа, чтобы связаться с корпорацией Майкрософт и получить количество оставшихся активаций для MAK. Для этого шага требуется доступ к Интернету. Вы можете получить только оставшееся число активаций для MAK.

Шаг 8. Установка ключей продукта

1. В области слева выберите продукт, в который нужно установить ключи.
2. При необходимости отсортируйте и отфильтруйте список продуктов, чтобы было проще найти компьютеры, на которых должен быть установлен ключ продукта. См . раздел Шаг 5. Сортировка и фильтрация списка компьютеров.
3. В области Список **продуктов** выберите отдельные продукты, для которых должны быть установлены ключи. Можно выбрать несколько продуктов с помощью клавиши **CTRL** или **SHIFT**.
4. Выберите **Установить ключ продукта** в меню **Выбранные элементы** в области справа, чтобы открыть диалоговое окно **Установка ключа продукта** .
5. В диалоговом окне **Select Product Key** отображаются ключи, которые доступны для установки. В разделе **Рекомендуемые пакеты MAK** в VAMT могут отображаться один или несколько рекомендуемых MAK на основе выбранных продуктов. Если вы устанавливаете MAK, вы можете выбрать рекомендуемый ключ продукта или любой другой mak из **списка Все ключи продуктов**. Если вы не устанавливаете MAK, выберите ключ продукта из списка **Все ключи продукта** . Используйте полосу прокрутки, если хотите просмотреть **описание** для каждой клавиши. Выбрав ключ продукта, который требуется установить, выберите **Установить ключ**. Одновременно можно установить только один ключ.

6. VAMT отображает диалоговое окно **Installing product key** во время попытки установить ключ продукта для выбранных продуктов. По окончании этого процесса его состояние отобразится в столбце **Action Status** диалогового окна. Нажмите **кнопку Закрыть** , чтобы закрыть диалоговое окно. Вы также можете выбрать флажок **Автоматически закрывать по завершении** проверка при появлении диалогового окна.

   То же состояние отображается в столбце **Состояние последнего действия** в представлении списка продуктов в центральной области.

   > ⓘ **Примечание**
   >
   > Установка ключа продукта завершится ошибкой, если VAMT найдет несоответствующие типы или выпуски ключей. VAMT отобразит состояние сбоя и продолжит установку со следующего продукта в списке. Дополнительные сведения о выборе правильного ключа продукта см. в статье **Выбор правильного ключа корпоративной лицензии для Windows.**

Шаг 9. Активация клиентских продуктов

1. Выберите отдельные продукты, которые нужно активировать, в области представления списка.

2. В строке меню выберите **Действие**, наведите указатель мыши на **кнопку Активировать** и выберите **Пункт Активация по сети**. Вы также можете щелкнуть правой кнопкой мыши выбранные компьютеры, чтобы открыть меню **Действие** , наведите указатель мыши на **пункт Активировать** и выберите **Пункт Активация в сети**. Вы также можете выбрать **Активировать** в меню **Выбранные элементы** на правой панели, чтобы открыть параметр **Активировать** .

3. Если вы активизируете ключи продукта с помощью текущих учетных данных, выберите **Текущие учетные данные** и перейдите к шагу 5. Если вы активизируете продукты, для которых требуются учетные данные администратора, отличные от используемых в настоящее время, выберите параметр **Альтернативные учетные данные** .

4. Введите альтернативное имя пользователя и пароль и нажмите **кнопку OK**.

5. Параметр **Активировать** связывается с сервером активации продуктов Майкрософт через Интернет и запрашивает активацию выбранных продуктов. VAMT отображает диалоговое окно **Активация продуктов** до завершения запрошенных действий.

> **Примечание**
>
> Установка MAK и перезапись GVLK в клиентских продуктах должны выполняться с осторожностью. Если rtM-версия Windows Vista установлена на компьютере более 30 дней, то ее первоначальный льготный период истек. В результате он перейдет в режим ограниченной функциональности (RFM), если активация по сети не будет успешно завершена перед следующей попыткой входа. Однако вы можете использовать активацию по сети для восстановления правильно настроенных компьютеров из RFM, если компьютеры доступны в сети. RFM применяется только к RTM-версии Windows Vista или розничным выпускам Microsoft Office 2010. Windows Vista с пакетом обновления 1 (SP1) или более поздней версии, Windows 7, Windows 8, Windows 10, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012 и корпоративные выпуски Office 2010 не будут входить в RFM.

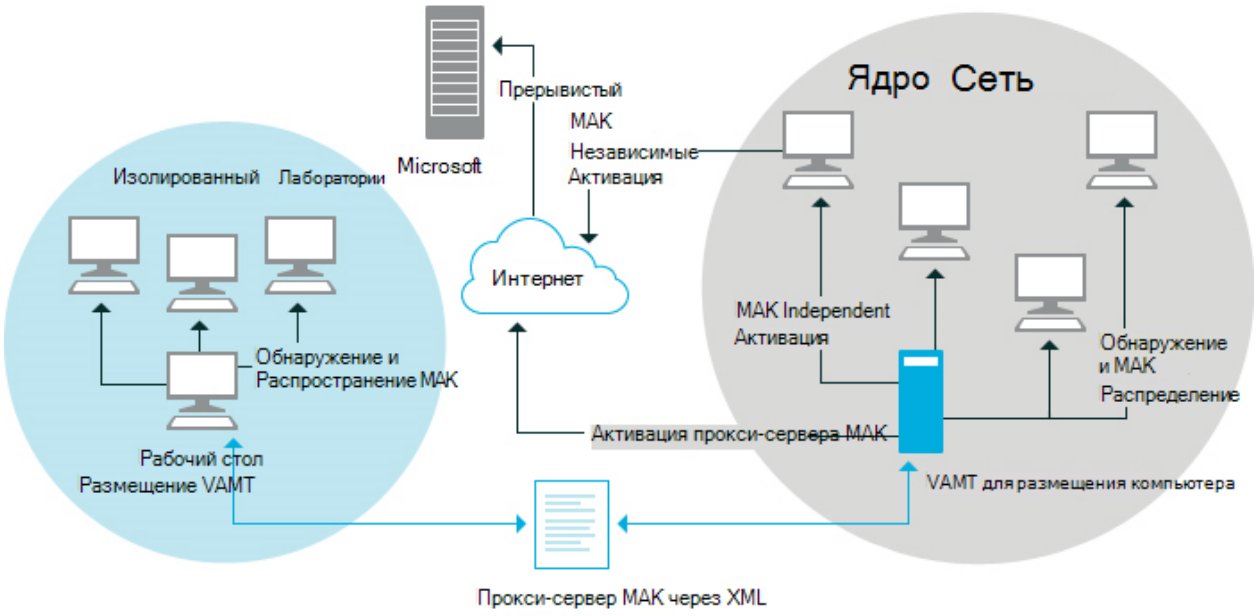
Связанные статьи

- Пошаговые сценарии VAMT

Сценарий 2. Прокси-активация

Статья • 18.03.2023

В этом сценарии средство управления активацией корпоративных лицензий (VAMT) используется для активации продуктов, установленных на компьютерах рабочей группы в изолированной лабораторной среде. Для рабочих групп, изолированных от более крупной сети, можно активировать прокси-сервер для нескольких ключей активации (MAK), ключей узла KMS (CSVLK), универсальных ключей корпоративной лицензии (GVLK) (или ключей клиента KMS) или ключей розничной торговли. Активация прокси-сервера выполняется путем установки второго экземпляра VAMT на компьютере в изолированной рабочей группе. Затем можно использовать съемный носитель для передачи списков сведений о компьютерах VAMT (CILX) между экземпляром VAMT в изолированной рабочей группе и другим узлом VAMT с доступом к Интернету. На следующей схеме показан сценарий активации прокси-сервера с несколькими ключами активации (MAK).



Шаг 1. Установка VAMT на компьютере рабочей группы в изолированной лаборатории

1. Установите VAMT на главный компьютер в изолированной рабочей группе лаборатории. Этот компьютер может работать под управлением Windows 7, Windows 8, Windows 10, Windows Server 2008 R2 или Windows Server® 2012.

2. Щелкните значок VAMT в меню **Пуск** , чтобы открыть VAMT.

Шаг 2. Настройка исключения брандмауэра инструментирования управления Windows на целевых компьютерах

- Убедитесь, что для всех целевых компьютеров включено исключение брандмауэра инструментария управления Windows (WMI). Дополнительные сведения см. в разделе Настройка клиентских компьютеров.

  > ⓘ **Примечание**
  >
  > Чтобы получить состояние лицензии на выбранных компьютерах, VAMT должна иметь административные разрешения на удаленных компьютерах, а WMI должен быть доступен через брандмауэр Windows. Кроме того, для компьютеров рабочей группы необходимо создать раздел реестра, чтобы включить удаленные административные действия в разделе Контроль учетных записей пользователей (UAC). Дополнительные сведения см. в разделе **Настройка клиентских компьютеров**.

Шаг 3. Подключение к базе данных VAMT

1. Если главный компьютер в изолированной рабочей группе лаборатории еще не подключен к базе данных, при открытии VAMT появляется диалоговое окно **Параметры подключения к базе данных** . Выберите сервер и базу данных, содержащие компьютеры в рабочей группе.

2. Выберите **Подключиться**.

3. Если вы уже подключены к базе данных, в центральной области VAMT отображается список продуктов и ключей продуктов, а также обзор лицензий компьютеров в базе данных. Если необходимо подключиться к другой базе данных, выберите **Успешно подключено к серверу** , чтобы открыть диалоговое окно **Параметры подключения к базе данных** . Дополнительные сведения о создании баз данных VAMT и добавлении данных VAMT см. в разделе Управление данными VAMT.

Шаг 4. Обнаружение продуктов

1. В левой области в узле **Продукты** выберите продукт, который нужно активировать.

2. Чтобы открыть диалоговое окно **Обнаружение продуктов** , выберите **Обнаружение продуктов** в области справа.

3. В диалоговом окне **Обнаружение продуктов** выберите **Поиск компьютеров в Active Directory** , чтобы отобразить параметры поиска, а затем выберите нужные параметры поиска. Вы можете искать компьютеры в домене Active Directory, по имени отдельного компьютера или IP-адресу, в рабочей группе или с помощью общего запроса LDAP:

    - Чтобы найти компьютеры в домене Active Directory, выберите **Поиск компьютеров в Active Directory**. Затем в разделе **Критерии фильтра домена** в списке доменных имен выберите имя домена, который требуется выполнить поиск. Вы можете еще больше сузить поиск, введя имя в поле **Фильтр по имени компьютера** , чтобы найти определенные компьютеры в домене. Этот фильтр поддерживает подстановочный знак звездочки (*). Например, при вводе "a*" будут отображаться только имена компьютеров, начинающиеся с буквы "a".

    - Чтобы выполнить поиск по имени или IP-адресу отдельного компьютера, выберите **Вручную ввести имя или IP-адрес**. Затем введите полное имя или IP-адрес в текстовое поле **Один или несколько имен компьютеров или IP-адресов, разделенных запятыми** . Разделите несколько записей с помощью запятой. Поддерживаются IPv4 и IPv6addressing.

    - Чтобы найти компьютеры в рабочей группе, выберите **Поиск компьютеров в рабочей группе**. Затем в разделе **Условия фильтра рабочей группы** в списке имен рабочих групп выберите имя рабочей группы, в которой требуется выполнить поиск. Вы можете еще больше сузить поиск, введя имя в поле **Фильтр по имени компьютера** , чтобы найти конкретный компьютер в рабочей группе. Этот фильтр поддерживает подстановочный знак звездочки (`*`). Например, при вводе `a*` будут отображаться только те имена компьютеров, которые начинаются с буквы **a**.

    - Чтобы выполнить поиск компьютеров с помощью общего запроса LDAP, выберите **Поиск с запросом LDAP** и введите запрос в появившемся текстовом поле. VAMT проверит синтаксис запроса LDAP, но в противном случае выполнит запрос без дополнительных проверок.

4. Выберите **Поиск**.

Откроется окно **Поиск компьютеров** , в котором отображается ход поиска по мере обнаружения компьютеров.

После завершения поиска продукты, обнаруженные VAMT, отображаются в представлении списка в центральной области.

Шаг 5. Сортировка и фильтрация списка компьютеров

Вы можете отсортировать список продуктов, чтобы было проще найти компьютеры, для которых требуется активировать ключи продуктов:

1. В строке меню в верхней части центральной области выберите **Группировать по**, а затем выберите **Продукт**, **Тип ключа продукта** или **Состояние лицензии**.
2. Чтобы отсортировать список дальше, можно выбрать один из заголовков столбцов для сортировки по столбцу.
3. Функцию **Фильтр** также можно использовать для сужения поиска компьютеров, щелкнув **Фильтр** в правой области, чтобы открыть диалоговое окно **Фильтр продуктов** .
4. В диалоговом окне **Filter Products** можно отфильтровать список по имени компьютера, названию продукта, типу ключа продукта, состоянию лицензии или любому сочетанию этих параметров.
    - Чтобы отфильтровать список по имени компьютера, введите нужное имя в поле **Computer Name**.
    - Чтобы отфильтровать список по названию продукта, типу ключа продукта или состоянию лицензии, выберите список, который вы хотите использовать для фильтра, и выберите параметр. При необходимости выберите **очистить все фильтры** , чтобы создать новый фильтр.
5. Выберите **Фильтр**. VAMT отображает отфильтрованный список в представлении списка продуктов в центральной области.

Шаг 6. Сбор сведений о состоянии с компьютеров в изолированной лаборатории

Чтобы получить сведения о состоянии с избранных компьютеров в базе данных, можно выбрать компьютеры в представлении списка продуктов с помощью

одного из следующих методов:

- Чтобы выбрать блок последовательно перечисленных компьютеров, выберите первый компьютер, который нужно выбрать, а затем выберите последний компьютер при нажатии клавиши **SHIFT** .
- Чтобы выбрать компьютеры, которые не перечислены подряд, удерживайте нажатой клавишу **CTRL** и выберите каждый компьютер, для которого требуется собрать сведения о состоянии. **Сбор сведений о состоянии с выбранных компьютеров**
- В правой части области **Действия** выберите **Обновить состояние лицензии** в меню **Выбранные элементы** , а затем выберите параметр учетных данных. Выберите **Альтернативные учетные данные** , только если вы обновляете продукты, для которых требуются учетные данные администратора, отличающиеся от тех, которые использовались для входа на компьютер. В противном случае выберите **Текущие учетные данные** и перейдите к шагу 2. Если вы предоставляете альтернативные учетные данные, в диалоговом окне **Безопасность Windows** введите соответствующее имя пользователя и пароль, а затем нажмите **кнопку OK**.
- VAMT отображает диалоговое окно **Сбор сведений о продукте** при сборе состояния лицензии для всех поддерживаемых продуктов на выбранных компьютерах. По завершении процесса обновленное состояние лицензии каждого продукта появится в представлении списка продуктов в центральной области.

  > ⓘ **Примечание**
  >
  > Если на компьютере установлено несколько поддерживаемых продуктов, VAMT добавляет запись для каждого продукта. Запись отображается под соответствующим заголовком продукта.

Шаг 7. Добавление ключей продукта

1. Выберите узел **Ключи продуктов** в левой области, а затем выберите **Добавить ключи продуктов** в области справа, чтобы открыть диалоговое окно **Добавление ключей продуктов** .
2. В диалоговом окне **Добавление ключей продуктов** можно выбрать один из следующих способов добавления ключей продукта:

- Чтобы добавить один ключ продукта, выберите **Ввести ключи продукта, разделенные разрывами строк**, введите один или несколько ключей продукта, а затем выберите **Добавить ключи**.
- Чтобы импортировать файл с разделяющимися запятыми (CSV) со списком ключей продукта, выберите **Выбрать ключ продукта для импорта**, перейдите в расположение файла, нажмите кнопку **Открыть** , чтобы импортировать файл, а затем выберите **Добавить ключи**.

Добавленные ключи отображаются в представлении списка **Ключи продуктов** в центральной области.

Шаг 8. Установка ключей продуктов на изолированных компьютерах лаборатории

1. В левой области в узле **Продукты** выберите продукт, на который нужно установить ключи.
2. При необходимости отсортируйте и отфильтруйте список продуктов, чтобы было проще найти компьютеры, на которых должен быть установлен ключ продукта. См . раздел Шаг 5. Сортировка и фильтрация списка компьютеров.
3. В области Список **продуктов** выберите отдельные продукты, для которых должны быть установлены ключи. Можно выбрать несколько продуктов с помощью клавиши **CTRL** или **SHIFT**.
4. Выберите **Установить ключ продукта** в меню **Выбранные элементы** в области справа, чтобы открыть диалоговое окно **Установка ключа продукта** .
5. В диалоговом окне **Select Product Key** отображаются ключи, которые доступны для установки. В разделе **Рекомендуемые пакеты MAK** в VAMT могут отображаться один или несколько рекомендуемых MAK на основе выбранных продуктов. Если вы устанавливаете MAK, вы можете выбрать рекомендуемый ключ продукта или любой другой mak из **списка Все ключи продуктов**. Если вы не устанавливаете MAK, выберите ключ продукта из списка **Все ключи продукта** . Используйте полосу прокрутки, чтобы просмотреть описания каждого ключа в разделе **Description**. Выбрав ключ продукта, который требуется установить, выберите **Установить ключ**. Одновременно можно установить только один ключ.
6. VAMT отображает диалоговое окно **Installing product key** во время попытки установить ключ продукта для выбранных продуктов. По окончании этого

процесса его состояние отобразится в столбце **Action Status** диалогового окна. Нажмите **кнопку Закрыть** , чтобы закрыть диалоговое окно. Вы также можете выбрать флажок **Автоматически закрывать по завершении** проверка при появлении диалогового окна.

То же состояние отображается в столбце **Состояние последнего действия** в представлении списка продуктов в центральной области.

> ⓘ **Примечание**
>
> Установка ключа продукта завершится ошибкой, если VAMT найдет несоответствующие типы или выпуски ключей. VAMT отображает состояние сбоя и продолжает установку для следующего продукта в списке. Дополнительные сведения о выборе правильного ключа продукта см. в статье **Выбор правильного ключа корпоративной лицензии для Windows.**

> ⓘ **Примечание**
>
> Установка MAK и перезапись GVLK в клиентских продуктах должны выполняться с осторожностью. Если rtM-версия Windows Vista установлена на компьютере более 30 дней, то ее первоначальный льготный период истек. В результате он перейдет в режим ограниченной функциональности (RFM), если активация по сети не будет успешно завершена перед следующей попыткой входа. Однако вы можете использовать активацию по сети для восстановления правильно настроенных компьютеров из RFM, если компьютеры доступны в сети. RFM применяется только к RTM-версии Windows Vista или розничным выпускам Microsoft Office 2010. Windows Vista с пакетом обновления 1 (SP1) или более поздней версии, Windows 7, Windows 8, Windows 10, Windows Server 2008, Windows Server 2008 R2 и Windows Server 2012, а также корпоративные выпуски Office 2010 не будут входить в RFM.

Шаг 9. Экспорт данных VAMT в `.cilx` файл

На этом шаге вы экспортируете VAMT с главного компьютера рабочей группы и сохраните `.cilx` его в файле. Затем вы копируете файл на `.cilx` съемный носитель, чтобы вы могли отправить его на главный компьютер VAMT, подключенный к Интернету. При активации прокси-сервера MAK важно сохранить

этот файл, так как VAMT использует его для применения идентификаторов подтверждения (CID) к соответствующим продуктам.

1. Выберите отдельные продукты, которые успешно получили ключ продукта на шаге 8. При необходимости отсортируйте и отфильтруйте список, чтобы найти продукты.

2. В правой части области **Действия** выберите **Экспорт списка** , чтобы открыть диалоговое окно **Экспорт списка** .

3. В диалоговом окне **Экспорт списка** нажмите кнопку **Обзор** , чтобы перейти к файлу `.cilx` , или введите имя `.cilx` файла, в который нужно экспортировать данные.

4. В разделе **Параметры экспорта** выберите один из следующих параметров типа данных:

    - Экспорт продуктов и ключей продуктов.
    - Экспортируйте только продукты.
    - Экспортируйте только данные активации прокси-сервера. Выбор этого параметра гарантирует, что экспорт содержит только сведения о лицензии, необходимые веб-службе прокси-сервера для получения CID от Корпорации Майкрософт. При выборе этого параметра в экспортируемом файле в экспортируемом `.cilx` файле не содержится личных сведений. Этот параметр следует использовать, если в политике безопасности предприятия указано, что никакие сведения, которые могут идентифицировать конкретный компьютер или пользователя, не могут быть переданы из изолированной лаборатории, и, следовательно, этот тип данных должен быть исключен из `.cilx` файла, который передается на узел VAMT core network.

5. Если вы выбрали продукты для экспорта, а не весь набор данных из базы данных, установите флажок **Экспорт выбранных строк продукта только** проверка.

6. Выберите **Сохранить**. VAMT отображает сообщение о ходе экспорта данных. Нажмите **кнопку ОК** , когда появится сообщение и подтвердится, что экспорт успешно завершен.

7. Если вы экспортировали список в файл на жестком диске главного компьютера, скопируйте файл на съемный носитель, например на диск, компакт-диск или DVD-диск или USB-устройство хранения.

> ⓘ **Важно!**
>
> При выборе параметра **Экспортировать только данные активации прокси-сервера** исключается сохранение персональных данных в `.cilx` файле. Таким образом, `.cilx` файл необходимо повторно импортировать в базу данных SQL Server на основном компьютере VAMT изолированной рабочей группы лаборатории, чтобы идентификаторы CID, запрошенные у корпорации Майкрософт (как описано на шаге 10), можно было правильно назначить компьютерам в изолированной группе лаборатории.

Шаг 10. Получение идентификаторов подтверждения от корпорации Майкрософт на хост-компьютере, подключенном к Интернету

1. Вставьте съемный носитель в узел VAMT с доступом к Интернету.
2. Откройте VAMT. Убедитесь, что вы находитесь на корневом узле и что **представление средство управления активацией корпоративных лицензий** отображается в центральной области.
3. В правой области **Действия** выберите **Получение идентификаторов подтверждения для CILX** , чтобы открыть диалоговое окно **Получение идентификаторов подтверждения для файла** .
4. В диалоговом окне **Получение идентификаторов подтверждения для файла** перейдите к расположению файла, экспортированного с изолированного `.cilx` главного компьютера лаборатории, выберите файл и нажмите кнопку **Открыть**. VAMT отображает сообщение **идентификаторов подтверждения получения** , когда оно связывается с корпорацией Майкрософт и собирает идентификаторы CID.
5. Когда процесс сбора CID будет завершен, VAMT отображает **средство управления активацией корпоративных лицензий** сообщение, в котором отображается количество успешно полученных идентификаторов подтверждения и имя файла, в котором были сохранены идентификаторы. Нажмите **кнопку ОК** , чтобы закрыть сообщение.

Шаг 11. Импорт файла на `.cilx` узел VAMT в рабочей группе изолированной лаборатории

1. Удалите запоминающее устройство, содержащее `.cilx` файл, с подключенного к Интернету главного компьютера VAMT и вставьте его в главный компьютер VAMT в изолированной лаборатории.

2. Откройте VAMT и убедитесь, что вы подключены к базе данных, содержащей компьютер с ключами продукта, которые вы активируете.

3. В правой области **Действия** выберите **Импорт списка** , чтобы открыть диалоговое окно **Импорт списка** .

4. В **диалоговом окне Импорт списка** перейдите к расположению `.cilx` файла, содержащего идентификаторы CID, выберите файл и нажмите кнопку **Открыть**.

5. Нажмите **кнопку ОК** , чтобы импортировать файл и перезаписать все конфликтующие данные в базе данных данными из файла.

6. VAMT отображает сообщение о ходе импорта данных. Нажмите **кнопку ОК** , когда появится сообщение и подтвердится, что данные успешно импортированы.

Шаг 12. Применение идентификаторов CID и активация изолированных компьютеров лаборатории

1. Выберите продукты, к которым требуется применить CID. При необходимости отсортируйте и отфильтруйте список, чтобы найти продукты.

2. В меню **Выбранные элементы** справа выберите **Активировать**, **применить идентификатор подтверждения**, а затем выберите соответствующий параметр учетных данных. Если выбрать параметр **Альтернативные учетные данные** , вам будет предложено ввести альтернативное имя пользователя и пароль.

   VAMT отображает диалоговое окно **Применение идентификатора подтверждения** при установке ИДЕНТИФИКАТОРов CID на выбранные продукты. Когда VAMT завершит установку CID, состояние отображается в

столбце **Состояние действия** диалогового окна. Нажмите **кнопку Закрыть** , чтобы закрыть диалоговое окно. Вы также можете выбрать флажок **Автоматически закрывать по завершении** проверка при появлении диалогового окна. То же состояние отображается в столбце **Состояние последнего действия** в представлении списка продуктов в центральной области.

Шаг 13. (Необязательно) Повторная активация переимогаемых компьютеров в изолированной лаборатории

Если вы захватили новые образы компьютеров в изолированной лаборатории, но базовое оборудование этих компьютеров не изменилось, VAMT может повторно активировать эти компьютеры с помощью ИДЕНТИФИКАТОРов CID, хранящихся в базе данных.

1. Повторное развертывание продуктов на каждом компьютере с теми же именами компьютеров, что и раньше.

2. Откройте VAMT.

3. В меню **Выбранные элементы** справа выберите **Активировать**, **применить идентификатор подтверждения**, а затем выберите соответствующий параметр учетных данных. Если выбрать параметр **Альтернативные учетные данные** , вам будет предложено ввести альтернативное имя пользователя и пароль.

   VAMT отображает диалоговое окно **Применение идентификатора подтверждения** при установке ИДЕНТИФИКАТОРов CID на выбранные продукты. Когда VAMT завершит установку CID, состояние отображается в столбце **Состояние действия** диалогового окна. Нажмите **кнопку Закрыть** , чтобы закрыть диалоговое окно. Вы также можете выбрать флажок **Автоматически закрывать по завершении** проверка при появлении диалогового окна. То же состояние отображается в столбце **Состояние последнего действия** в представлении списка продуктов в центральной области.

   > ⓘ **Примечание**
   >
   > Установка MAK и перезапись GVLK на клиентских продуктах должны выполняться с осторожностью. Если первоначальный льготный период

активации Windows истек, Windows перейдет в режим ограниченной функциональности (RFM), если активация через Интернет не завершена успешно до следующей попытки входа. Однако вы можете использовать активацию по сети для восстановления правильно настроенных компьютеров из RFM, если компьютеры доступны в сети.

RFM применяется только к RTM-версии Windows Vista или розничным выпускам Microsoft Office 2010. Windows Vista с пакетом обновления 1 (SP1) или более поздней версии, Windows 7, Windows 8, Windows 10, Windows Server 2008, Windows Server 2008 R2 и Windows Server 2012, а также корпоративные выпуски Office 2010 не будут использовать RFM.

> ⓘ **Примечание**
>
> Повторное применение того же CID позволяет сохранить оставшиеся активации в MAK.

Связанные статьи

- Пошаговые сценарии VAMT

Сценарий 3. Активация клиента KMS

Статья • 18.03.2023

В этом сценарии вы используете средство управления активацией корпоративных лицензий (VAMT) для активации клиентских ключей службы управления ключами (KMS) или универсальных ключей корпоративной лицензии (GVLK). Этот тип активации может выполняться на компьютерах Core Network или Isolated Lab. По умолчанию в выпусках Windows Vista, Windows® 7, Windows 8, Windows 10, Windows Server 2008, Windows Server 2008 R2, Windows Server® 2012 и Microsoft® Office 2010 с корпоративными лицензиями для активации используется KMS. Ключи GVLK уже установлены в выпусках этих продуктов с корпоративными лицензиями. Вам не нужно вводить ключ для активации продукта в качестве GVLK, если вы не преобразуете продукт, активированный MAK, в активацию KMS. Дополнительные сведения см. в разделе Установка ключа клиента KMS.

Процедура, описанная ниже, предполагает следующую конфигурацию:

- Служба KMS включена и доступна для всех клиентов KMS.
- VAMT установлен, а компьютеры добавлены в базу данных VAMT. Дополнительные сведения см. в разделах с 1 по 4 в разделе Сценарий 1. Активация через Интернет или Сценарий 2. Активация прокси-сервера .

Активация клиентов KMS

1. Откройте VAMT.
2. Чтобы задать параметры активации KMS, в строке меню выберите **Вид**. Затем выберите **Параметры**, чтобы открыть диалоговое окно **Параметры средство управления активацией корпоративных лицензий**.
3. В диалоговом окне **Параметры средство управления активацией корпоративных лицензий** в разделе **Узел служб управления KMS** выберите один из следующих вариантов:
    - **Автоматические поиск узла KMS с помощью DNS**. Этот параметр является параметром по умолчанию. VAMT укажет компьютеру запросить службу доменных имен (DNS), чтобы найти узел KMS и выполнить активацию. Если клиент содержит раздел реестра с допустимым узлом KMS, вместо него будет использоваться это значение.

- **Найдите узел KMS с помощью DNS в этом домене для поддерживаемых продуктов**. Выберите этот параметр, если используется определенный домен, и введите имя домена.

- **Используйте определенный узел KMS**. Выберите этот параметр для сред, которые не используют DNS для идентификации узла KMS, и вручную введите имя узла KMS и выберите порт узла KMS. VAMT задаст указанное имя узла KMS и порт узла KMS на целевом компьютере, а затем укатит компьютеру выполнить активацию с определенным узлом KMS.

4. В левой области в узле **Продукты** выберите продукт, который нужно активировать.

5. При необходимости в представлении списка продуктов в центральной области отсортируйте список. Можно воспользоваться функцией **Filter**, чтобы сузить область поиска компьютеров. Для этого нажмите **Filter** на панели справа, чтобы открыть диалоговое окно **Filter Products**.

6. В диалоговом окне **Filter Products** можно отфильтровать список по имени компьютера, названию продукта, типу ключа продукта, состоянию лицензии или любому сочетанию этих параметров.

    - Чтобы отфильтровать список по имени компьютера, введите нужное имя в поле **Computer Name**.

    - Чтобы отфильтровать список по названию продукта, типу ключа продукта или состоянию лицензии, выберите список, который вы хотите использовать для фильтра, и выберите параметр . При необходимости выберите **очистить все фильтры** , чтобы создать новый фильтр.

7. Выберите **Фильтр**. VAMT отображает отфильтрованный список на центральной панели.

8. Выберите продукты, которые нужно активировать.

9. Выберите **Активировать** в меню **Выбранные элементы** на правой панели **Действия** , выберите **Активировать**, наведите указатель мыши на кнопку **Активация тома**, а затем выберите соответствующий параметр учетных данных. Если выбрать параметр **Альтернативные учетные данные** , вам будет предложено ввести альтернативное имя пользователя и пароль.

10. VAMT отображает диалоговое окно **Активация продуктов** , пока не завершит запрошенное действие. После завершения активации состояние отображается

в столбце **Состояние действия** диалогового окна. Нажмите **кнопку Закрыть** , чтобы закрыть диалоговое окно. Вы также можете выбрать флажок **Автоматически закрывать по завершении** проверка при появлении диалогового окна.

То же состояние отображается в столбце **Состояние последнего действия** в представлении списка продуктов в центральной области.

Связанные статьи

- Пошаговые сценарии VAMT

Известные проблемы VAMT

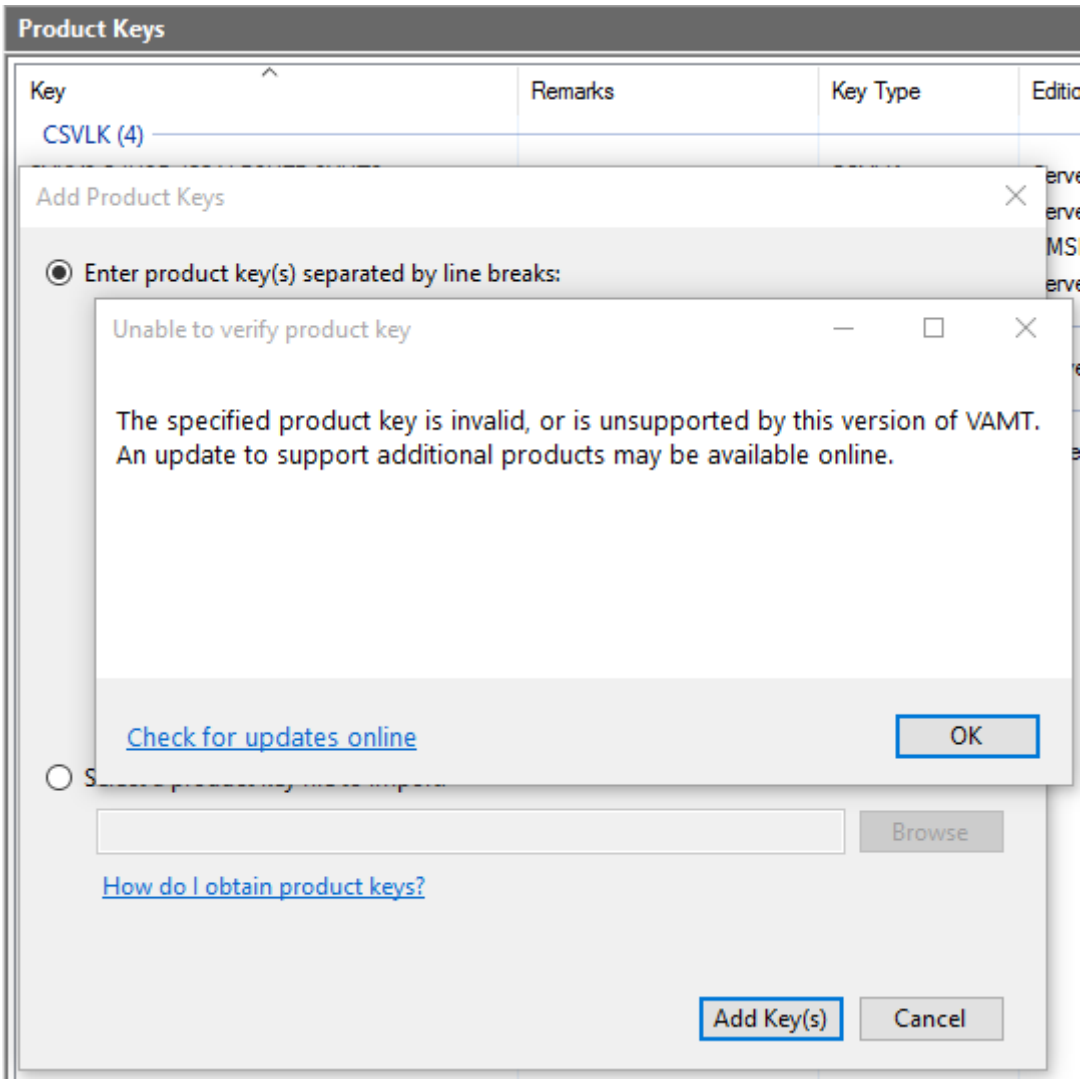
Статья • 18.03.2023

Текущие известные проблемы с средство управления активацией корпоративных лицензий (VAMT) версии 3.0. и 3.1:

- Удаленные операции инфраструктуры управления Windows (WMI) VAMT могут выполняться дольше, если целевой компьютер находится в спящем или резервном состоянии.
- При открытии файла списка сведений о компьютере (CIL), сохраненного с помощью предыдущей версии VAMT, сведения о выпуске не отображаются для каждого продукта в центральной области. Чтобы получить сведения о выпуске, необходимо снова обновить состояние продукта.
- Оставшееся количество активаций можно получить только для нескольких ключей активации (MAK).

Обходные решения для добавления CSV-файлов для активации Windows 10 в VAMT 3.1

Другая известная проблема заключается в том, что при попытке добавить ключ узла Windows 10 службы управления ключами (KMS) (CSVLK) или Windows Server 2012 R2 для Windows 10 CSVLK в VAMT 3.1 (версия 10.0.10240.0), появляется сообщение об ошибке, показанное здесь.



Эта проблема возникает из-за того, что VAMT 3.1 не содержит правильные файлы Pkconfig для распознавания такого рода ключей. Чтобы обойти эту проблему, используйте один из следующих методов.

Способ 1

Не добавляйте CSVLK в средство VAMT 3.1. Вместо этого используйте `slmgr.vbs /ipk <CSVLK>` команду для установки CSVLK на узле KMS. В этой команде *<CSVLK>* представляет конкретный ключ, который требуется установить. Дополнительные сведения об использовании средства см. в `Slmgr.vbs`Slmgr.vbs параметрах для получения сведений об активации корпоративных лицензий.

Способ 2

На хост-компьютере KMS выполните следующие действия.

1. Скачайте накопительный пакет обновления за июль 2016 г. для Windows 8.1 и Windows Server 2012 R2 .

2. В Windows Обозреватель щелкните правой кнопкой мыши **485392_intl_x64_zip** и извлеките исправление в папку C:\KB3058168.

3. Чтобы извлечь содержимое обновления, выполните следующую команду:

   Командная строка Windows

   ```
   expand c:\KB3058168\Windows8.1-KB3058168-x64.msu -f:* C:\KB3058168\
   ```

4. Чтобы извлечь содержимое Windows8.1-KB3058168-x64.cab, выполните следующую команду:

   Командная строка Windows

   ```
   expand c:\KB3058168\Windows8.1-KB3058168-x64.cab -f:pkeyconfig-csvlk.xrm-ms c:\KB3058168
   ```

5. В раскрывающемся списке

   `C:\KB3058168\x86_microsoft-windows-s..nent-sku-csvlk-pack_31bf3856ad364e35_6.3.9600.17815_none_bd26b4f34d049716`

   папка, скопируйте

   `pkeyconfig-csvlk.xrm-ms`

   Файл. Вставьте этот файл в

   `C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\VAMT3\pkconfig`

   Windows".

6. Перезапустите VAMT.

Обзор отчетов Центра обновления Windows для бизнеса

Применяется к: ✅ Windows 11, ✅ Windows 10

Отчеты клиентский компонент Центра обновления Windows для бизнеса — это облачное решение, которое предоставляет сведения о соответствии Microsoft Entra присоединенных устройств обновлениям Windows. Отчеты клиентский компонент Центра обновления Windows для бизнеса предлагаются через портал Azure и включены в состав Windows 10 или Windows 11 необходимых лицензий. Отчеты клиентский компонент Центра обновления Windows для бизнеса помогают:

- Мониторинг безопасности, качества, драйверов и обновлений компонентов для устройств Windows 11 и Windows 10
- Отчет об устройствах с проблемами соответствия обновлений
- Анализ и отображение данных несколькими способами

Преимущества отчетов клиентский компонент Центра обновления Windows для бизнеса

Ниже приведены некоторые преимущества отчетов клиентский компонент Центра обновления Windows для бизнеса.

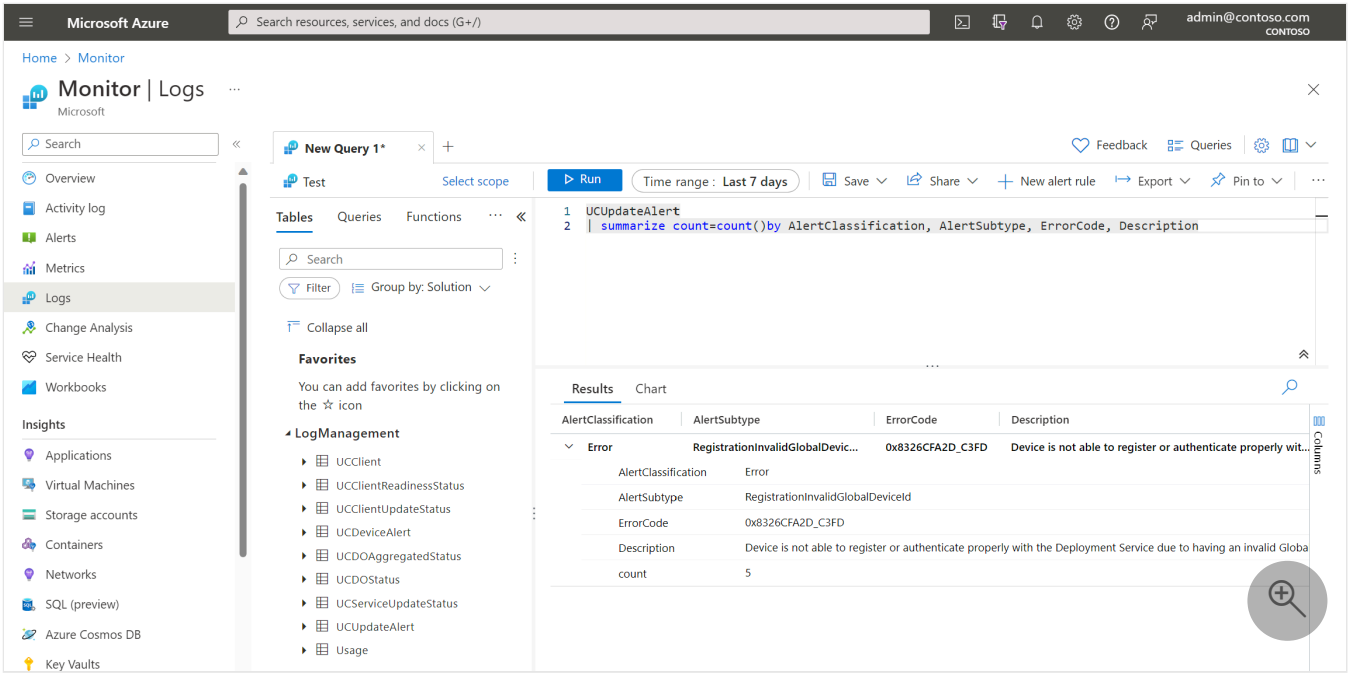
- Совместимость с обновлениями компонентов и политиками ускорения обновлений качества Windows в Intune.
- Новый тип данных **Alerts** , помогающий определить устройства, на которые возникают проблемы во время процесса обновления. Для устранения проблем с обновлением предоставляются сведения о коде ошибки.

В настоящее время отчеты клиентский компонент Центра обновления Windows для бизнеса содержат следующие функции:

- Книга отчетов Центра обновления Windows для бизнеса
- Диаграммы состояния соответствия в администраторе Microsoft 365
- Доступ к следующим таблицам отчетов клиентский компонент Центра обновления Windows для бизнеса:
  - UCClient
  - UCClientReadinessStatus
  - UCClientUpdateStatus
  - UCDeviceAlert

- UCDOAggregatedStatus
- UCDOStatus
- UCServiceUpdateStatus
- UCUpdateAlert

- Сбор данных клиента для заполнения таблиц отчетов клиентский компонент Центра обновления Windows для бизнеса



Ограничения

Отчеты клиентский компонент Центра обновления Windows для бизнеса — это служба Windows, размещенная в Azure, которая использует диагностические данные Windows. Следует помнить, что отчеты клиентский компонент Центра обновления Windows для бизнеса не соответствуют требованиям сообщества государственных организаций США (GCC). Список предложений GCC для продуктов и служб Майкрософт см. в центре управления безопасностью Майкрософт. Отчеты клиентский компонент Центра обновления Windows для бизнеса доступны в коммерческом облаке Azure, но недоступны для клиентов GCC High или США Министерства обороны.

Принципы работы отчетов клиентский компонент Центра обновления Windows для бизнеса

Вы настроите отчеты клиентский компонент Центра обновления Windows для бизнеса, зарегистрируясь в службе из портал Azure. Затем вы настроите устройства,

присоединенные к Microsoft Entra, для отправки диагностических данных клиента Windows в службу. клиентский компонент Центра обновления Windows для бизнеса отчеты используют Log Analytics в Azure Monitor для хранения диагностических данных, отправляемых клиентами. Эти данные можно использовать для создания отчетов об обновлениях для устройств. Отчеты клиентский компонент Центра обновления Windows для бизнеса собирают системные данные, такие как:

- Ход развертывания обновления
- Данные об использовании оптимизации доставки
- клиентский компонент Центра обновления Windows данных конфигурации политики клиента

Плата за прием и хранение в Azure Log Analytics не взимается в подписке Azure для данных отчетов клиентский компонент Центра обновления Windows для бизнеса. Вы также выбираете рабочие области Azure Log Analytics , которые вам принадлежат для диагностических данных клиента. Собранные диагностические данные заполняют таблицы отчетов клиентский компонент Центра обновления Windows для бизнеса, что позволяет легко запрашивать данные.

Использование данных отчетов клиентский компонент Центра обновления Windows для бизнеса

Так как данные клиентов хранятся в рабочей области Log Analytics, вы можете выйти за рамки стандартных отчетов для анализа и отображения данных несколькими способами. Ниже приведены некоторые из способов отображения данных.

- Использование данных в создаваемых пользовательских книгах
- Создание пользовательских запросов Kusto (KQL)
- Разработка собственных пользовательских представлений путем интеграции данных Log Analytics в другие средства, такие как:
  - Operations Management Suite
  - Power BI
  - Другие средства для запроса данных

Дальнейшие действия

- Ознакомьтесь с предварительными условиями для отчетов клиентский компонент Центра обновления Windows для бизнеса

Last updated on 01.04.2025

Предварительные требования отчетов Центра обновления Windows для бизнеса

Статья • 15.10.2024 • Применяется к: ✅ Windows 11, ✅ Windows 10

Прежде чем приступить к добавлению отчетов клиентский компонент Центра обновления Windows для бизнеса в подписку Azure, убедитесь, что выполнены необходимые условия.

Azure и Microsoft Entra ID

- Подписка Azure с Microsoft Entra ID.
- Устройства должны быть Microsoft Entra присоединены и соответствовать приведенным ниже требованиям к ОС, диагностике и доступу к конечным точкам.
  - Устройства можно Microsoft Entra присоединение или Microsoft Entra гибридное присоединение.
- Устройства, Microsoft Entra зарегистрированные только (присоединенные к рабочему месту), не поддерживаются с отчетами клиентский компонент Центра обновления Windows для бизнеса.
- Рабочая область Log Analytics должна находиться в поддерживаемом регионе.
- Данные на вкладке **Обновления драйверов**книги доступны только для устройств, получающих обновления драйверов и встроенного ПО из автозапавление Windows.

Разрешения

Для типичного доступа к отчетам клиентский компонент Центра обновления Windows для бизнеса требуются разрешения из нескольких источников, включая:

- Microsoft Entra ID или Intune: используется для управления службами клиентский компонент Центра обновления Windows для бизнеса через Microsoft API Graph, например для регистрации в отчетах.
- Azure: используется для управления доступом к ресурсам Azure с помощью службы "Управление ресурсами Azure", например для доступа к рабочей области Log Analytics.
- Центр администрирования Microsoft 365. Управляет доступом к Центр администрирования Microsoft 365, что позволяет входить только пользователям с определенными Microsoft Entra ролями.

Роли, которые могут регистрироваться в отчетах клиентский компонент Центра обновления Windows для бизнеса

Для регистрации в отчетах клиентский компонент Центра обновления Windows для бизнеса из портал Azure или Центр администрирования Microsoft 365 требуется одна из следующих ролей:

- роль Microsoft Entra администратора Intune
- роль администратора развертывания клиентский компонент Центра обновления Windows Microsoft Entra
- Роль Microsoft Intune диспетчера политик и профилей
  - Microsoft Intune роли RBAC не разрешают доступ к Центр администрирования Microsoft 365

Роли Azure, разрешающие доступ к рабочей области Log Analytics

Данные для отчетов клиентский компонент Центра обновления Windows для бизнеса направляются в рабочую область Log Analytics для выполнения запросов и анализа. Для отображения или запроса любых данных отчетов клиентский компонент Центра обновления Windows для бизнеса пользователи должны иметь следующие роли или эквивалентные разрешения для рабочей области:

- Роль читателя Log Analytics можно использовать для чтения данных
- Роль участника Log Analytics можно использовать, если требуется создание новой рабочей области или доступ на запись

Примеры часто назначаемых ролей для пользователей отчетов клиентский компонент Центра обновления Windows для бизнеса:

Развернуть таблицу

Роли	Регистрация с помощью книги	Регистрация через Центр администрирования Microsoft 365	Отображение книги	доступ Центр администрирования Microsoft 365	Создание рабочей области Log Analytics
Администратор Intune и участник Log Analytics	Да	Да	Да	Да	Да
администратор развертывания клиентский компонент Центра обновления Windows и читатель Log Analytics	Да	Да	Да	Да	Нет

Роли	Регистрация с помощью книги	Регистрация через Центр администрирования Microsoft 365	Отображение книги	доступ Центр администрирования Microsoft 365	Создание рабочей области Log Analytics
Диспетчер политик и профилей (роль Intune)+ читатель Log Analytics	Да	Нет	Да	Нет	Нет
Средство чтения Log Analytics	Нет	Нет	Да	Нет	Нет
Глобальное средство чтения и средство чтения Log Analytics	Нет	Нет	Да	Да	Нет

> **ⓘ Примечание**
>
> Роли Microsoft Entra, рассматриваемые в этой статье, для доступа к Центр администрирования Microsoft 365 относятся специально к вкладке **Windows** на странице **Обновления программного обеспечения**. Дополнительные сведения о вкладке **Приложения Microsoft 365** см. в разделе Приложения Microsoft 365 обновления в Центре администрирования.

Операционные системы и выпуски

- Windows 11 выпуски Professional, Education, Enterprise и Enterprise с несколькими сеансами
- Windows 10 выпуски professional, education, Enterprise и Enterprise с несколькими сеансами

Отчеты клиентский компонент Центра обновления Windows для бизнеса предоставляют данные только для стандартной версии классического клиента Windows и в настоящее время несовместимы с Windows Server, Surface Hub, IoT или другими версиями.

> **ⓘ Важно!**
>
> В настоящее время существует известная проблема, из-за которой клиентский компонент Центра обновления Windows отчеты для бизнеса не отображают данные

для корпоративных устройств с несколькими сеансами.

Каналы обслуживания клиентов Windows

Отчеты клиентский компонент Центра обновления Windows для бизнеса поддерживают клиентские устройства Windows по следующим каналам:

- Канал общей доступности
- Отчеты клиентский компонент Центра обновления Windows для бизнеса *учитываются* Windows Insider Preview устройствах, но в настоящее время подробные сведения о развертывании для них не предоставляются.

Обновления операционной системы Windows для клиентских устройств

Для регистрации клиентов в отчетах клиентский компонент Центра обновления Windows для бизнеса требуется установка накопительного обновления за февраль 2023 г. или более поздней версии эквивалентного обновления. Это обновление помогло включить изменения в сбор диагностических данных Windows, от которого зависит клиентский компонент Центра обновления Windows отчетов для бизнеса.

Дополнительные сведения о доступных обновлениях см. в разделе сведения о выпуске Windows 11 и сведения о выпуске Windows 10.

Требования к диагностическим данным

Как минимум, для отчетов клиентский компонент Центра обновления Windows для бизнеса требуется, чтобы устройства отправляли диагностические данные на *обязательном* уровне (ранее — *базовый*). Дополнительные сведения о том, какие данные включает каждый уровень диагностики, см. в статье Настройка диагностических данных Windows в организации.

Рекомендуется использовать следующие уровни, но не обязательные:

- *Расширенный* уровень для Windows 10 устройств.
- Уровень "*Необязательный*" для устройств Windows 11 (ранее *полный*).

Имена устройств не отображаются в отчетах клиентский компонент Центра обновления Windows для бизнеса, если вы не по отдельности согласитесь на использование устройств с помощью политики. Скрипт конфигурации выполняет это действие за вас, но при использовании других методов конфигурации клиента задайте одну из следующих политик для отображения имен устройств:

- CSP: System/AllowDeviceNameInDiagnosticData

- групповая политика: **разрешить отправку имени устройства в диагностические данные Windows в** разделе **Конфигурация компьютера\Административные шаблоны\Компоненты Windows\Сбор данных и предварительные сборки**

> **Совет**
>
> клиентский компонент Центра обновления Windows отчетах для бизнеса **используется конфигурация служб**, также называемая OneSettings. Отключение конфигурации служб может привести к тому, что некоторые данные клиента будут неверными или отсутствовать в отчетах. Дополнительные сведения см. в разделе Параметры политики **DisableOneSettingsСкачать** .

Корпорация Майкрософт стремится предоставлять эффективные элементы управления данными и обеспечивать прозрачность наших способов обработки ваших данных. Дополнительные сведения об обработке и конфиденциальности диагностических данных Windows см. в разделах Настройка диагностических данных Windows в организации и Изменения в сборе диагностических данных Windows.

Конечные точки

Устройства должны иметь возможность связаться со следующими конечными точками для проверки подлинности и отправки диагностических данных:

Развернуть таблицу

Конечная точка	Функция
`*v10c.events.data.microsoft.com` `eu-v10c.events.data.microsoft.com` для клиентов с адресом выставления счетов на границе данных ЕС	Конечная точка компонента "Взаимодействие с пользователем и диагностика" для Windows 10 версии 1803 и более поздних версий. DeviceCensus.exe должны выполняться регулярно и обращаться к этой конечной точке, чтобы получить большую часть информации для отчетов клиентский компонент Центра обновления Windows для бизнеса.
`umwatsonc.events.data.microsoft.com` `eu-watsonc.events.data.microsoft.com` для клиентов с адресом выставления счетов на границе данных ЕС	отчеты об ошибках Windows (WER), используемый для предоставления расширенных отчетов об ошибках при возникновении определенных сбоев развертывания обновления компонентов.
`v10.vortex-win.data.microsoft.com`	Конечная точка компонента "Взаимодействие с пользователем и диагностика" для Windows 10 версии 1709 или более ранней.
`settings-win.data.microsoft.com`	Используется компонентами и приложениями Windows для динамического обновления конфигурации. Требуется для клиентский компонент

Конечная точка	Функция
	Центра обновления Windows функциональных возможностей.
`adl.windows.com`	Требуется для клиентский компонент Центра обновления Windows функциональных возможностей.
`oca.telemetry.microsoft.com`	Анализ сбоев в сети, используемый для предоставления рекомендаций для конкретных устройств и подробных ошибок при наличии определенных сбоев.
`login.live.com`	Эта конечная точка упрощает доступ к учетной записи Майкрософт и требуется для создания основного идентификатора, используемого для устройств. Без этой службы устройства не видны в решении. Служба помощника по входу в учетную запись Майкрософт также должна работать (wlidsvc).

`ceuswatcab01.blob.core.windows.net`
`ceuswatcab02.blob.core.windows.net`
`eaus2watcab01.blob.core.windows.net`
`eaus2watcab02.blob.core.windows.net`
`weus2watcab01.blob.core.windows.net`
`weus2watcab02.blob.core.windows.net`
	Хранилище данных BLOB-объектов Azure.

Примечание

Регистрация в отчетах клиентский компонент Центра обновления Windows для бизнеса из Azure CLI или регистрация программным способом в настоящее время не поддерживается. Необходимо вручную добавить отчеты клиентский компонент Центра обновления Windows для бизнеса в подписку Azure.

Регионы Log Analytics

Отчеты клиентский компонент Центра обновления Windows для бизнеса могут использовать рабочую область Log Analytics в следующих регионах:

Развернуть таблицу

Совместимые регионы Log Analytics
Центральная Австралия
Восточная Австралия
Юго-Восточная Австралия
Южная Бразилия

Совместимые регионы Log Analytics
Центральная Канада
Центральная Индия
Центральная часть США
Восточная Азия
Восточная часть США
Восточная часть США 2
Eastus2euap(canary)
Центральная Франция
Восточная Япония
Центральная Корея
Центрально-северная часть США
Северная Европа
Северная часть Южной Африки
Центрально-южная часть США
Юго-Восточная Азия
Северная Швейцария
Западная Швейцария
Западная часть Соединенного Королевства
Южная часть Соединенного Королевства
Центрально-западная часть США
Западная Европа
Западная часть США
Западная часть США 2

Дальнейшие действия

- Включение решения отчетов клиентский компонент Центра обновления Windows для бизнеса в портал Azure

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Включение отчетов Центра обновления Windows для бизнеса

Статья • 25.02.2025 • Применяется к: ✅ Windows 11, ✅ Windows 10

Убедившись, что предварительные требования выполнены, можно приступить к настройке отчетов клиентский компонент Центра обновления Windows для бизнеса. Ниже приведены два main шага по настройке отчетов клиентский компонент Центра обновления Windows для бизнеса.

1. Добавьте отчеты клиентский компонент Центра обновления Windows для бизнеса в подписку Azure. Этот шаг состоит из следующих этапов:
   a. Выберите или создайте рабочую область Log Analytics для использования с отчетами клиентский компонент Центра обновления Windows для бизнеса.
   b. Зарегистрируйтесь в отчетах клиентский компонент Центра обновления Windows для бизнеса с помощью одного из следующих методов:

      - Регистрация с помощью книги Azure (предпочтительный метод)
      - Зарегистрируйтесь из Центр администрирования Microsoft 365.

2. Настройте клиенты для отправки данных в отчеты клиентский компонент Центра обновления Windows для бизнеса. Клиенты можно настроить следующими тремя способами:

   - Использование скрипта
   - Использование Microsoft Intune
   - Настройка вручную

> **ⓘ Важно!**
>
> Отчеты клиентский компонент Центра обновления Windows для бизнеса — это служба Windows, размещенная в Azure, которая использует диагностические данные Windows. Следует помнить, что отчеты клиентский компонент Центра обновления Windows для бизнеса не соответствуют требованиям **сообщества государственных организаций США (GCC).** Список предложений GCC для продуктов и служб Майкрософт см. в **центре управления безопасностью Майкрософт**. Отчеты клиентский компонент Центра обновления Windows для бизнеса доступны в коммерческом облаке Azure, но недоступны для клиентов GCC High или США Министерства обороны.

Добавление отчетов клиентский компонент Центра обновления Windows для бизнеса в подписку Azure

Прежде чем настраивать клиенты для отправки данных, необходимо добавить отчеты клиентский компонент Центра обновления Windows для бизнеса в подписку Azure, чтобы данные можно было получать. Сначала выберите или создадите рабочую область Log Analytics для использования. Во-вторых, вы регистрируете клиентский компонент Центра обновления Windows отчетов для бизнеса в рабочую область.

Выбор или создание рабочей области Log Analytics для отчетов клиентский компонент Центра обновления Windows для бизнеса

клиентский компонент Центра обновления Windows для бизнеса отчеты используют принадлежащие вам рабочие области Azure Log Analytics для хранения диагностических данных клиента. Определите существующую рабочую область или создайте новую, выполнив следующие действия.

1. Войдите в портал Azure по адресу https://portal.azure.com .

    - Хотя подписка Azure является обязательной, плата за прием данных отчетов клиентский компонент Центра обновления Windows для бизнеса не взимается.

2. В портал Azure введите **Log Analytics** в строке поиска. Когда вы начнете вводить текст, список фильтруется на основе ваших входных данных.
3. Выберите **Рабочие области Log Analytics**.
4. Если у вас уже есть рабочая область Log Analytics, определите, какую рабочую область Log Analytics вы хотите использовать для отчетов клиентский компонент Центра обновления Windows для бизнеса. Убедитесь, что рабочая область находится в **совместимом регионе Log Analytics** из таблицы, указанной в предварительных требованиях.

    - Пользователи службы "Управление обновлениями Azure" должны использовать одну и ту же рабочую область для отчетов клиентский компонент Центра обновления Windows для бизнеса.

5. Если у вас нет рабочей области Log Analytics или вы не хотите использовать текущую рабочую область, создайте новую рабочую область в совместимом регионе.

> **Примечание**
>
> - Можно сопоставить только один клиент с одной рабочей областью Log Analytics. Сопоставление одного клиента с несколькими рабочими областями не поддерживается.
> - Если изменить рабочую область Log Analytics для отчетов клиентский компонент Центра обновления Windows для бизнеса, устаревшие данные будут отображаться около 24 часов, пока новая рабочая область не будет полностью подключена. Вам также потребуется перенастроить параметры клиентский компонент Центра обновления Windows для бизнес-отчетов, чтобы снова зарегистрироваться.

Регистрация в отчетах клиентский компонент Центра обновления Windows для бизнеса

Зарегистрируйтесь в отчетах клиентский компонент Центра обновления Windows для бизнеса, настроив их параметры с помощью книги Azure или из Центр администрирования Microsoft 365. Используйте один из следующих методов для регистрации в отчетах клиентский компонент Центра обновления Windows для бизнеса:

Регистрация с помощью книги Azure (рекомендуемый метод)

1. В портал Azure выберите **Мониторинг**>**книг** в строке меню.
    - Вы также можете ввести **Monitor** в строке поиска. Когда вы начнете вводить текст, список фильтруется на основе ваших входных данных.
2. Когда коллекция откроется, выберите книгу **отчетов клиентский компонент Центра обновления Windows для бизнеса**. При необходимости книги можно фильтровать по имени в коллекции.
3. Нажмите кнопку **Начало работы**, когда книга предложит открыть всплывающее **окно регистрации отчетов клиентский компонент Центра**

обновления Windows для бизнеса.

4. Во всплывающем окне укажите **подписку** и **рабочую область Azure Log Analytics**, которые вы хотите использовать для отчетов клиентский компонент Центра обновления Windows для бизнеса.

    - Если вам нужно создать рабочую область Log Analytics, выберите **Создать рабочую область** и следуйте инструкциям, чтобы создать новую рабочую область.

5. Выберите **Сохранить параметры**, чтобы сохранить параметры и зарегистрироваться в отчетах клиентский компонент Центра обновления Windows для бизнеса.

    > **Совет**
    >
    > При возникновении `403 Forbidden` ошибки убедитесь, что у используемой учетной записи есть **разрешения на регистрацию в отчетах** клиентский компонент Центра обновления Windows для бизнеса.

6. Начальная настройка может занять до 24 часов. В течение этого времени в книге будет отображаться сообщение о том, что она **ожидает клиентский компонент Центра обновления Windows данных отчетов для бизнеса**.

    - Регистрация в отчетах клиентский компонент Центра обновления Windows для бизнеса не влияет на скорость отправки необходимых данных с устройств. Подключение устройства к Интернету и его активность влияет на то, сколько времени потребуется, прежде чем устройство появится в отчетах. Устройства, которые активны и подключены к Интернету ежедневно, могут быть полностью загружены в течение одной недели (обычно менее 72 часов). Менее активные устройства могут занять до двух недель, прежде чем данные будут полностью доступны.

Регистрация через Центр администрирования Microsoft 365

1. Перейдите к Центр администрирования Microsoft 365 и войдите в систему.

2. Разверните узел **Работоспособности**, а затем выберите **Программное обеспечение Обновления**. Для отображения **работоспособности** в меню навигации может потребоваться использовать параметр **Показать все**.

- Если в меню не отображается запись об **обновлениях программного обеспечения** , попробуйте перейти по следующему URL-адресу: https://admin.microsoft.com/Adminportal/Home#/softwareupdates.

3. На странице **Программное обеспечение Обновления** выберите вкладку **Windows**.

4. При первом выборе вкладки **Windows** вам будет предложено **настроить параметры**. Эта вкладка заполняется данными из отчетов клиентский компонент Центра обновления Windows для бизнеса. Проверьте или предоставьте следующие сведения о параметрах отчетов клиентский компонент Центра обновления Windows для бизнеса:

   - Подписка Azure
   - Рабочая область Log Analytics

5. Начальная настройка может занять до 24 часов. В течение этого времени на вкладке **Windows** отображается сообщение **Ожидание клиентский компонент Центра обновления Windows данных отчетов для бизнеса**.

   - Регистрация в отчетах клиентский компонент Центра обновления Windows для бизнеса не влияет на скорость отправки необходимых данных с устройств. Подключение устройства к Интернету и его активность влияет на то, сколько времени потребуется, прежде чем устройство появится в отчетах. Устройства, которые активны и подключены к Интернету ежедневно, могут быть полностью загружены в течение одной недели (обычно менее 72 часов). Менее активные устройства могут занять до двух недель, прежде чем данные будут полностью доступны.

6. После завершения начальной настройки на вкладке **Windows** на диаграммах будут отображаться данные отчетов клиентский компонент Центра обновления Windows для бизнеса.

   > **Примечание**
   >
   > Количество устройств на вкладке **Windows** может отличаться от **Приложения Microsoft 365** вкладки, так как их требования отличаются.

Дальнейшие действия

После добавления отчетов клиентский компонент Центра обновления Windows для бизнеса в рабочую область в подписке Azure и настройки параметров с помощью Центр администрирования Microsoft 365 необходимо настроить все устройства, которые вы хотите отслеживать. Регистрация устройств в отчетах клиентский компонент Центра обновления Windows для бизнеса с помощью любого из следующих методов:

- Настройка клиентов с помощью сценария
- Настройка клиентов вручную
- Настройка клиентов с помощью Microsoft Intune

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Настройка устройств с помощью скрипта конфигурации отчетов клиентский компонент Центра обновления Windows для бизнеса

Статья • 25.02.2025 • Применяется к: ✅ Windows 11, ✅ Windows 10

Скрипт конфигурации отчетов клиентский компонент Центра обновления Windows для бизнеса — это рекомендуемый метод настройки устройств для отправки данных в Корпорацию Майкрософт для использования с отчетами клиентский компонент Центра обновления Windows для бизнеса. Скрипт настраивает политики поддержки разделов реестра, обеспечивает выполнение необходимых служб и многое другое. Этот скрипт является рекомендуемым дополнением к настройке необходимых политик, описанных в статье Ручная настройка устройств для отчетов клиентский компонент Центра обновления Windows для бизнеса, так как он может предоставлять отзывы о наличии проблем с конфигурацией вне настраиваемых политик.

Сведения о скрипте

Скрипт конфигурации настраивает разделы реестра напрямую. Разделы реестра могут быть перезаписаны параметрами политики, такими как групповая политика или MDM. *Перенастройка устройств с помощью скрипта не приводит к перенастройке ранее заданных политик, как в случае групповая политика, так и MDM*. Если между конфигурациями групповая политика или MDM и необходимыми конфигурациями, перечисленными в разделе Ручная настройка устройств для отчетов клиентский компонент Центра обновления Windows для бизнеса, данные устройства могут не отображаться в клиентский компонент Центра обновления Windows для бизнес-отчетов правильно.

Скрипт можно скачать из Центра загрузки Майкрософт.

Порядок упорядочения этого скрипта

Два основных файла этого скрипта: `ConfigScript.ps1` и `RunConfig.bat`. Вы настраиваете `RunConfig.bat` в соответствии с указаниями в самом , который затем будет выполняться `ConfigScript.ps1` с параметрами, введенными в

`.bat` `RunConfig.bat`. Скрипт можно использовать двумя способами: в **пилотном** режиме или в режиме **развертывания** .

> ⓘ **Важно!**
>
> PsExec используется для запуска скрипта в системном контексте. После настройки устройства удалите PsExec.exe с устройства.

Использование этого скрипта

Измените файл, `RunConfig.bat` чтобы настроить следующие переменные, а затем запустите измененный файл .bat:

⛶ **Развернуть таблицу**

Переменная	Допустимые значения и описание	Пример
runMode	**Пилотный проект** (по умолчанию): подробный режим с дополнительными диагностика и ведением журнала. Пилотный режим лучше всего подходит для тестового запуска скрипта или для устранения неполадок. **Развертывание**: не выполняет никаких дополнительных диагностика и не добавляет дополнительного ведения журнала.	`runMode=Pilot`
logPath	Путь, по которому сохраняются журналы. Расположение журналов по умолчанию — `.\UCLogs`.	`logPath=C:\temp\logs`
logMode	**0**. Вход в консоль только **1** (по умолчанию): вход в файл и консоль. **2**. Только вход в файл.	`logMode=2`
DeviceNameOptIn	**true** (по умолчанию): имя устройства отправляется в корпорацию Майкрософт. **false**: имя устройства не отправляется в корпорацию Майкрософт.	`DeviceNameOptIn=true`
ClientProxy	**Прямой** (по умолчанию): прокси-сервер не используется. Подключение к конечным точкам осуществляется напрямую. **Система**. Используется системный прокси-сервер без проверки подлинности. Этот тип прокси-сервера обычно настраивается с помощью netsh и может быть проверен с помощью `netsh winhttp`	`ClientProxy=Direct`

Переменная	Допустимые значения и описание	Пример
	`show proxy`. **Пользователь**. Прокси-сервер настраивается через IE и может потребовать или не требует проверки подлинности пользователя. Дополнительные сведения см. в разделе Как клиент клиентский компонент Центра обновления Windows определяет, какой прокси-сервер следует использовать для подключения к веб-сайту клиентский компонент Центра обновления Windows.	
источник	Используется файлом .bat и скриптом PowerShell для поиска зависимостей. Рекомендуется не изменять это значение.	`source=%~dp0`

Ошибки скрипта

Развернуть таблицу

Ошибка	Описание
1	Непредвиденная ошибка
12	Сбой CheckVortexConnectivity, проверка выходные данные журнала для получения дополнительных сведений.
12	Непредвиденный сбой при запуске CheckVortexConnectivity.
16	На устройстве ожидается перезагрузка. Перезапустите устройство, а затем повторно запустите сценарий.
17	Непредвиденное исключение в CheckRebootRequired.
27	Не системная учетная запись.
30	Не удается отключить прокси-сервер корпоративной проверки подлинности. Для работы в среде прокси-сервера, прошедшей проверку подлинности, это значение реестра должно быть равно 0.
34	Непредвиденное исключение при попытке проверка параметров прокси-сервера.
35	Непредвиденное исключение при проверке прокси-сервера пользователя.
37	Непредвиденное исключение при сборе журналов.

Ошибка	Описание
40	Непредвиденное исключение при проверке и настройке телеметрии.
41	Не удается олицетворить вошедшего в систему пользователя.
42	Непредвиденное исключение при попытке олицетворения пользователя, выполнившего вход.
43	Непредвиденное исключение при попытке олицетворения пользователя, выполнившего вход.
44	Ошибка при запуске службы CheckDiagTrack.
45	DiagTrack.dll не найден.
50	Служба DiagTrack не запущена.
51	Непредвиденное исключение при попытке запустить Census.exe.
52	Не удалось найти Census.exe.
54	Служба Помощника по входу в учетную запись Майкрософт (MSA) отключена.
55	Не удалось создать путь к реестру для SetDeviceNameOptIn.
56	Не удалось создать свойство для SetDeviceNameOptIn по пути к реестру.
57	Не удалось обновить значение для SetDeviceNameOptIn.
58	Неожиданное исключение в SetDeviceNameOptIn.
59	Не удалось удалить свойство LastPersistedEventTimeOrFirstBoot по пути реестра при попытке очистить OneSettings.
60	Не удалось удалить раздел реестра при попытке очистить OneSettings.
61	Неожиданное исключение при попытке очистить OneSettings.
62	Раздел реестра AllowTelemetry не является правильным типом REG_DWORD.
63	Параметр AllowTelemetry не имеет соответствующего значения и не может быть задан скриптом.
64	AllowTelemetry не является правильным типом REG_DWORD.
66	Не удалось проверить подключение UTC и последние отправки.
67	Непредвиденный сбой при проверке utc CSP.
99	Устройство не является Windows 10 или Windows 11.
100	Чтобы использовать отчеты клиентский компонент Центра обновления Windows для бизнеса, устройство должно быть Microsoft Entra присоединено или Microsoft

Ошибка	Описание
	Entra гибридное присоединение.
101	Проверьте, Microsoft Entra сбой соединения с непредвиденным исключением.
102	Политика DisableOneSettingsСкачать политику не должна быть включена. Отключите эту политику.

Дальнейшие действия

Использование отчетов Центра обновления Windows для бизнеса

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Настройка вручную устройств для отчетов Центра обновления Windows для бизнеса

Статья • 09.07.2024 • Применяется к: ✅ Windows 11, ✅ Windows 10

Существует множество требований, которые следует учитывать при настройке вручную устройств для отчетов Центра обновления Windows для бизнеса. Эти требования могут измениться в более поздних версиях клиента Windows. При изменении каких-либо требований к конфигурации мы обновим скрипт конфигурации отчетов Центра обновления Windows для бизнеса. В этом случае необходимо только повторно развернуть сценарий.

Требования разделены на различные категории:

1. Обеспечение правильной настройки **необходимых политик** для отчетов Центра обновления Windows для бизнеса.
2. Устройства в каждой топологии сети должны отправлять данные в **необходимые конечные точки** для отчетов Центра обновления Windows для бизнеса. Например, устройства в главном и вспомогательном офисах, которые могут иметь разные конфигурации сети, должны иметь возможность доступа к конечным точкам.
3. Убедитесь, что **обязательные службы Windows** запущены или запланированы для запуска. Для правильной функциональности оставьте для служб Windows стандартные конфигурации по умолчанию.

Обязательные политики

Служба отчетов Центра обновления Windows для бизнеса имеет несколько политик, которые необходимо настроить соответствующим образом. Эти политики позволяют корпорации Майкрософт обрабатывать устройства и отображать их в отчетах Центра обновления Windows для бизнеса. Политики перечислены в следующих подразделах, разделенных управлением мобильными устройствами (MDM) или групповой политикой.

Для обеих таблиц применяются следующие определения:

- **Политика**: расположение и имя политики.
- **Значение**: задайте для политики это значение. Для отчетов Центра обновления Windows для бизнеса требуются по крайней мере *обязательные* (ранее *базовые*) диагностические данные, но они могут работать с *расширенными* или *необязательными* (ранее *полными*).
- **Функция**: сведения о том, почему требуется политика и какую функцию она служит для отчетов Центра обновления Windows для бизнеса. В нем также описана минимальная версия, требуемая политикой, если она есть.

Политики MDM

Каждая политика MDM ссылается на более подробную документацию в иерархии поставщика служб конфигурации (CSP).

Развернуть таблицу

Политика	Тип данных	Значение	Функция	Обязательный или рекомендуемый
System/AllowTelemetry	целое число	`1`: базовый (обязательный)	Настраивает устройство для отправки минимально необходимых диагностических данных.	Обязательный
System/ConfigureTelemetryOptInSettingsUx	целое число	`1`: отключение параметров согласия на использование диагностических данных	Определяет, могут ли пользователи устройства настраивать диагностические данные на уровни ниже, чем определено *политикой AllowTelemetry* . Задайте рекомендуемое значение, чтобы отключить параметры согласия, иначе пользователи могут изменить эффективный уровень диагностических данных, который может оказаться недостаточным.	Рекомендуется
System/AllowDeviceNameInDiagnosticData	целое число	`1`:Дозволенный	Позволяет устройству отправлять свое имя с диагностическими данными Windows. Если вы не настроили эту политику или не присвоили ей `0`значение : Отключено, то данные не будут содержать имя устройства. Если данные не содержат имя устройства, устройство не отображается в отчетах Центра обновления Windows для бизнеса. В этом случае вместо	Рекомендуется

Политика	Тип данных	Значение	Функция	Обязательный или рекомендуемый
			этого отображаются `#` отчеты.	
System/ConfigureTelemetryOptInChangeNotification	целое число	`1`:Нетрудоспособный	Отключает уведомления пользователей об изменениях на уровне диагностических данных.	Рекомендуется

Групповые политики

Все групповые политики, которые необходимо настроить для отчетов Центра обновления Windows для бизнеса, находятся по следующему пути: **Конфигурация > компьютера Административные шаблоны > Сбор данных компонентов > Windows и Предварительные сборки**. Все эти политики должны находиться в состоянии *Включено* и иметь определенное *значение*.

Развернуть таблицу

Политика	Значение	Функция	Обязательный или рекомендуемый
Разрешить диагностические данные	Отправлять обязательные диагностические данные	Настраивает устройство для отправки минимально необходимых диагностических данных.	Обязательный
Настройка согласия на предоставление диагностических данных, настройка пользовательского интерфейса	Отключение параметров согласия на использование диагностических данных	Определяет, могут ли пользователи устройства настраивать диагностические данные на уровни ниже, чем определено политикой *Разрешить диагностические данные* . Задайте рекомендуемое значение, чтобы отключить параметры согласия, иначе пользователи могут изменить эффективный уровень диагностических данных, который может оказаться недостаточным.	Рекомендуется
Разрешить отправку имени устройства в диагностических данных Windows	Enabled	Позволяет устройству отправлять свое имя с диагностическими данными Windows. Если вы не настроили эту политику или не установили для нее значение *Отключено*, данные не будут содержать имя устройства. Если данные не содержат имя устройства, устройство не отображается в отчетах Центра обновления Windows для бизнеса. В этом случае вместо этого отображаются `#` отчеты.	Рекомендуется
Настройка уведомлений об изменениях в диагностических данных	Отключение уведомлений об изменении диагностических данных	Отключает уведомления пользователей об изменениях на уровне диагностических данных.	Рекомендуется

Обязательные конечные точки

Устройства должны иметь возможность связаться со следующими конечными точками для проверки подлинности и отправки диагностических данных:

Развернуть таблицу

Конечная точка	Функция
`*v10c.events.data.microsoft.com` `eu-v10c.events.data.microsoft.com` для клиентов с адресом выставления счетов на границе данных ЕС	Конечная точка компонента "Взаимодействие с пользователем и диагностика" для Windows 10 версии 1803 и более поздних версий. DeviceCensus.exe должны выполняться регулярно и обращаться к этой конечной точке, чтобы получить большую часть сведений об отчетах Центра обновления Windows для бизнеса.
`umwatsonc.events.data.microsoft.com` `eu-watsonc.events.data.microsoft.com` для клиентов с адресом выставления счетов на границе данных ЕС	Отчеты об ошибках Windows (WER), используемые для предоставления расширенных отчетов об ошибках при возникновении определенных сбоев развертывания обновления компонентов.
`v10.vortex-win.data.microsoft.com`	Конечная точка компонента "Взаимодействие с пользователем и диагностика" для Windows 10 версии 1709 или более ранней.
`settings-win.data.microsoft.com`	Используется компонентами и приложениями Windows для динамического обновления конфигурации. Требуется для функциональных возможностей Центра обновления Windows.
`adl.windows.com`	Требуется для функциональных возможностей Центра обновления Windows.
`oca.telemetry.microsoft.com`	Анализ сбоев в сети, используемый для предоставления рекомендаций для конкретных устройств и подробных ошибок при наличии определенных сбоев.
`login.live.com`	Эта конечная точка упрощает доступ к учетной записи Майкрософт и требуется для создания основного идентификатора, используемого для устройств. Без этой службы устройства не видны в решении. Служба помощника по входу в учетную запись Майкрософт также должна работать (wlidsvc).

`ceuswatcab01.blob.core.windows.net`
`ceuswatcab02.blob.core.windows.net`
`eaus2watcab01.blob.core.windows.net`
`eaus2watcab02.blob.core.windows.net`
`weus2watcab01.blob.core.windows.net`
`weus2watcab02.blob.core.windows.net`
	Хранилище данных BLOB-объектов Azure.

Обязательные службы

Многие службы Windows необходимы для отчетов Центра обновления Windows для бизнеса для просмотра данных устройства. Разрешить работу всех служб по умолчанию из стандартного интерфейса. Используйте скрипт конфигурации отчетов Центра обновления Windows для бизнеса, чтобы проверить, запущены ли необходимые службы или разрешено ли выполняться автоматически.

Дальнейшие действия

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Настройка Microsoft Intune устройств для отчетов клиентский компонент Центра обновления Windows для бизнеса

Статья • 10.03.2023

(Применимо к: Windows 11 & Windows 10 управляется Microsoft Intune

Эта статья посвящена настройке устройств, зарегистрированных для Microsoft Intune для отчетов клиентский компонент Центра обновления Windows для бизнеса, в Microsoft Intune самом Microsoft Intune. Настройка устройств для отчетов клиентский компонент Центра обновления Windows для бизнеса в Microsoft Intune позволяет выполнить следующие действия.

1. Создайте профиль конфигурации для устройств, которые требуется зарегистрировать. Профиль конфигурации содержит параметры для всех политик mobile Управление устройствами (MDM), которые необходимо настроить.
2. Дождитесь заполнения данных. Длительность этого процесса зависит от того, на компьютере, который включен, подключен к Интернету и правильно настроен. Для отображения некоторых типов данных требуется больше времени, чем для других. Дополнительные сведения см. в разделе Использование отчетов клиентский компонент Центра обновления Windows для бизнеса.

Совет

- Если вам нужно устранить неполадки с регистрацией клиента, рассмотрите возможность развертывания **скрипта конфигурации** в качестве приложения Win32 на нескольких устройствах и просмотра журналов, которые он создает. С помощью скрипта выполняются дополнительные проверки, чтобы убедиться, что устройства настроены правильно.
- Intune предоставляет отчеты о соответствии требованиям, и у них есть собственные предварительные требования для использования. Количество устройств, отображаемых в отчетах Intune, также может отличаться от клиентский компонент Центра обновления Windows

отчетов для бизнеса. Дополнительные сведения см. **в разделе Intune отчетов о соответствии требованиям для обновлений**.

Создание профиля конфигурации

Создайте профиль конфигурации, который будет задавать необходимые политики для отчетов клиентский компонент Центра обновления Windows для бизнеса. Существует два типа профилей, которые можно использовать для создания профиля конфигурации для отчетов клиентский компонент Центра обновления Windows для бизнеса (выберите один):

- Каталог параметров
- Шаблон для пользовательского профиля на основе OMA URI

Каталог параметров

1. В Центре администрирования Intune перейдите в раздел**Профили конфигурацииWindows**>**устройства**>.
2. В **представлении Профили конфигурации** выберите **Создать профиль**.
3. Выберите следующие параметры, а затем нажмите кнопку **Создать** по завершении:
   - **Платформа**: Windows 10 и более поздних версий
   - **Тип профиля**: Каталог параметров
4. Теперь вы перейдете на страницу создание профиля конфигурации. На вкладке **Основные сведения** укажите **имя** и **описание** профиля.
5. На странице **Параметры конфигурации** вы добавите несколько параметров из категории **Система** . С помощью **средства выбора параметров** выберите категорию **Система** .
6. Добавьте следующие обязательные параметры и значения в категорию **Система** :
   - **Параметр**: Разрешить телеметрию
     - **Значение**: Базовый
       - Базовый — это минимальное значение, но его можно безопасно задать на более высокое значение. Базовый также называется необходимыми диагностическими данными.

7. Добавьте следующие рекомендуемые параметры и значения из категории **Система** :

   > ⓘ **Примечание**
   >
   > Эти параметры не требуются, но они рекомендуются, чтобы пользователи устройства не могли переопределить уровень диагностических данных устройства.

   - **Параметр**. Настройка согласия телеметрии в параметрах Ux
     - **Значение**: Отключено
       - Включив этот параметр, пользователь отключит возможность переопределить уровень диагностических данных устройств, чтобы данные не были доступны для этих устройств в отчетах клиентский компонент Центра обновления Windows для бизнеса.
   - **Параметр**. Настройка согласия телеметрии в уведомлении об изменениях
     - **Значение**: Отключено
       - Включив этот параметр, вы отключаете уведомления об изменениях диагностических данных.
   - **Параметр**: Разрешить отправку имени устройства в диагностических данных Windows
     - **Значение**: Разрешено
       - Если эта политика отключена, имя устройства не будет отправлено и не будет видно в отчетах клиентский компонент Центра обновления Windows для бизнеса.

8. Перейдите к следующему набору вкладок **Теги области**, **Назначения** и **Правила применимости** , чтобы назначить профиль конфигурации устройствам, которые вы хотите зарегистрировать.

9. Просмотрите параметры и нажмите кнопку **Создать**.

Пользовательский профиль на основе OMA URI

1. В Центре администрирования Intune перейдите в раздел**Профили конфигурацииWindows**>**устройства**>.

2. В **представлении Профили конфигурации** выберите **Создать профиль**.

3. Выберите следующие параметры, а затем нажмите кнопку **Создать** по завершении:

   - **Platform**:Windows 10 и более поздних версий
   - **Тип профиля**: Шаблоны
   - **Имя шаблона**: Настраиваемое

4. Теперь вы перейдете на экран создания профиля конфигурации. На вкладке **Основные сведения** укажите **имя** и **описание**.

5. На странице **Параметры конфигурации** вы добавите несколько параметров OMA-URI, которые соответствуют политикам, описанным в статье Настройка устройств для клиентский компонент Центра обновления Windows для бизнеса.

   Обязательные параметры:

   a. Добавьте параметр, настроив **уровень диагностических данных Windows** для устройств:

      - **Имя**: Разрешить телеметрия
      - **Описание**. Задает максимально допустимые диагностические данные для отправки в корпорацию Майкрософт, необходимые для клиентский компонент Центра обновления Windows отчетов для бизнеса.
      - **OMA-URI**: `./Vendor/MSFT/Policy/Config/System/AllowTelemetry`
      - **Тип данных**: Целое число
      - **Значение**: 1
        - *1 — это минимальное значение, означающее обязательные или базовые диагностические данные, но для него можно безопасно задать более высокое значение.*

   Рекомендуемые параметры, но не обязательные:

   a. Добавьте параметры **для интерфейса "Отключить параметры диагностических данных устройств".** Если они не отключены, пользователи каждого устройства могут переопределить уровень диагностических данных устройств таким образом, чтобы данные не были доступны для этих устройств в отчетах клиентский компонент Центра обновления Windows для бизнеса:

      - **Имя**: отключить интерфейс согласия телеметрии
      - **Описание**. Отключает возможность для конечных пользователей устройств настраивать диагностические данные на уровни ниже, чем определено параметром Разрешить телеметрию.

- **OMA-URI**: `./Vendor/MSFT/Policy/Config/System/ConfigureTelemetryOptInSettingsUx`
- **Тип данных**: Целое число
- **Значение**: 1

b. Добавьте параметр **Разрешить имя устройства в диагностических данных**; В противном случае имя устройства не будет находиться в клиентский компонент Центра обновления Windows отчетах для бизнеса:

- **Имя**: разрешить имя устройства в диагностических данных
- **Описание**. Разрешает имя устройства в диагностических данных.
- **OMA-URI**: `./Vendor/MSFT/Policy/Config/System/AllowDeviceNameInDiagnosticData`
- **Тип данных**: Целое число
- **Значение**: 1

c. Добавьте параметр **Настроить телеметрия в уведомлении об изменениях**. Уведомления об изменении диагностических данных не будут отображаться при внесении изменений.

- **Имя**: настройка согласия телеметрии в уведомлении об изменениях
- **Описание**: отключение телеметрии в уведомлении об изменениях
- **OMA-URI**: `./Vendor/MSFT/Policy/Config/System/ConfigureTelemetryOptInChangeNotification`
- **Тип данных**: Целое число
- **Значение**: 1

6. Перейдите к следующему набору вкладок **Теги области**, **Назначения** и **Правила применимости** , чтобы назначить профиль конфигурации устройствам, которые вы хотите зарегистрировать.

7. Просмотрите параметры и нажмите кнопку **Создать**.

Развертывание скрипта конфигурации

Скрипт конфигурации отчетов клиентский компонент Центра обновления Windows для бизнеса — это полезное средство для правильной регистрации устройств в отчетах клиентский компонент Центра обновления Windows для бизнеса, хотя это и не обязательно. Он проверяет наличие необходимых служб, работающих на устройствах, и проверяет подключение к конечным точкам, описанным в разделе Настройка устройств вручную для отчетов клиентский компонент Центра

обновления Windows для бизнеса. Скрипт можно развернуть как приложение Win32. Дополнительные сведения см. в статье Управление приложениями Win32 в Microsoft Intune.

> ⓘ **Примечание**
>
> Использование скрипта необязательно при настройке устройств с помощью Intune. Скрипт можно использовать в качестве средства устранения неполадок, чтобы убедиться, что устройства правильно настроены для клиентский компонент Центра обновления Windows отчетов для бизнеса.

При развертывании скрипта конфигурации в качестве приложения Win32 вы не сможете получить результаты журналов на устройстве без доступа к устройству или сохранения результатов журналов в общей файловой системе. Рекомендуется развернуть скрипт в пилотном режиме на подмножестве устройств, к которым можно получить доступ. После выполнения этого руководства скрипт конфигурации можно развернуть в режиме развертывания в качестве приложения Win32 на всех устройствах клиентский компонент Центра обновления Windows для бизнес-отчетов.

Дальнейшие действия

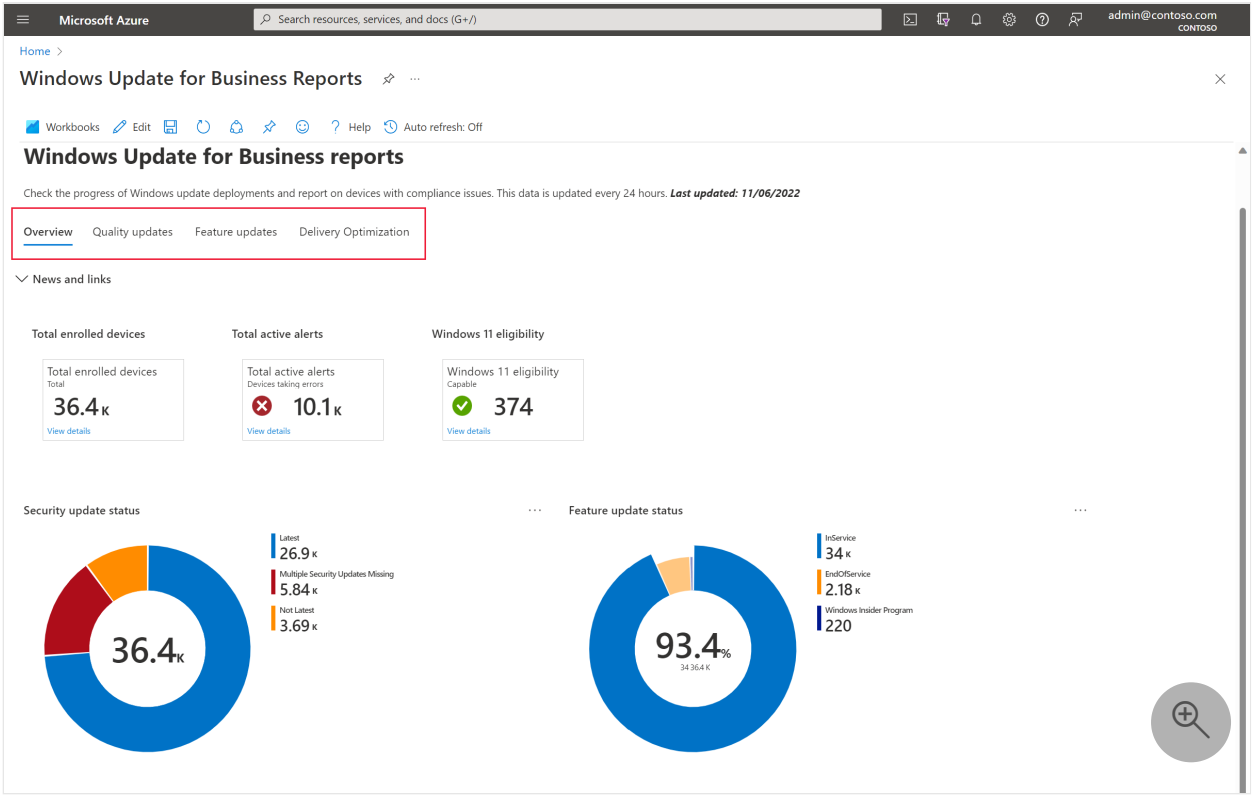
Использование отчетов клиентский компонент Центра обновления Windows для бизнеса

Книга отчетов Центра обновления Windows для бизнеса

Статья • 29.01.2024 • Применяется к: ✅ Windows 11, ✅ Windows 10

Отчеты клиентский компонент Центра обновления Windows для бизнеса содержат сведения, часто необходимые администраторам обновлений, в простом в использовании формате. клиентский компонент Центра обновления Windows для бизнеса отчеты используют книги Azure для визуального представления данных о соответствии требованиям. Книга разбита на разделы табуляции:

- Сводка
- Исправления
- Обновления компонентов
- Оптимизация доставки
- Обновления драйверов



Открытие книги отчетов клиентский компонент Центра обновления Windows для бизнеса

Чтобы получить доступ к книге отчетов клиентский компонент Центра обновления Windows для бизнеса:

1. В портал Azure выберите **Мониторинг**>**книг** в строке меню.

    - Вы также можете ввести **Monitor** в строке поиска. Когда вы начнете вводить текст, список фильтруется на основе ваших входных данных.

2. Когда коллекция откроется, выберите книгу **отчетов клиентский компонент Центра обновления Windows для бизнеса**. При необходимости книги можно фильтровать по имени в коллекции.

3. При открытии книги может потребоваться указать **подписку** и **рабочую область**, которые использовались при включении отчетов клиентский компонент Центра обновления Windows для бизнеса.

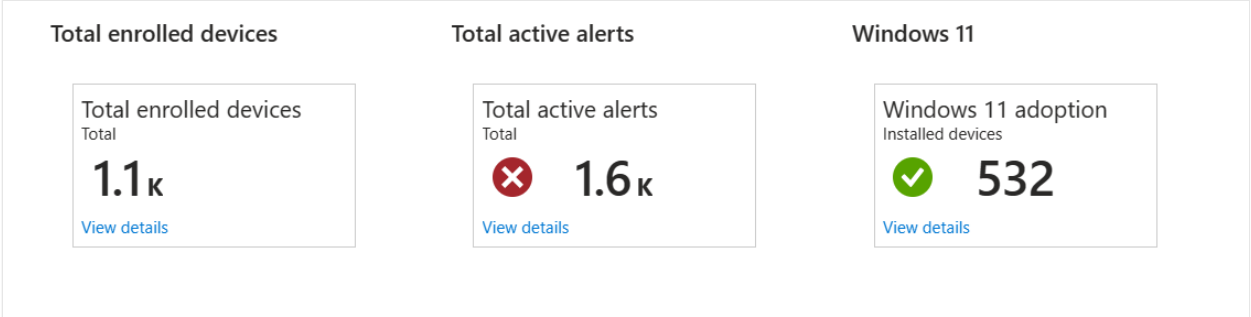
> **Важно!**
>
> Не закрепляйте книгу отчетов клиентский компонент Центра обновления Windows для бизнеса на панели мониторинга Azure. При использовании закрепленного отчета загружается более старая копия отчета, и в нем не отображаются обновления шаблона отчета.

Вкладка "Сводка"

На вкладке **Сводка** представлен краткий обзор устройств, зарегистрированных в отчетах клиентский компонент Центра обновления Windows для бизнеса. **Вкладка Сводка** содержит плитки над диаграммой **Общее состояние обновлений безопасности**.

Плитки вкладки "Сводка"

Каждая из этих плиток содержит параметр **Просмотреть сведения**. Если для плитки выбран параметр **Просмотреть сведения** , появится всплывающее окно с дополнительными сведениями.



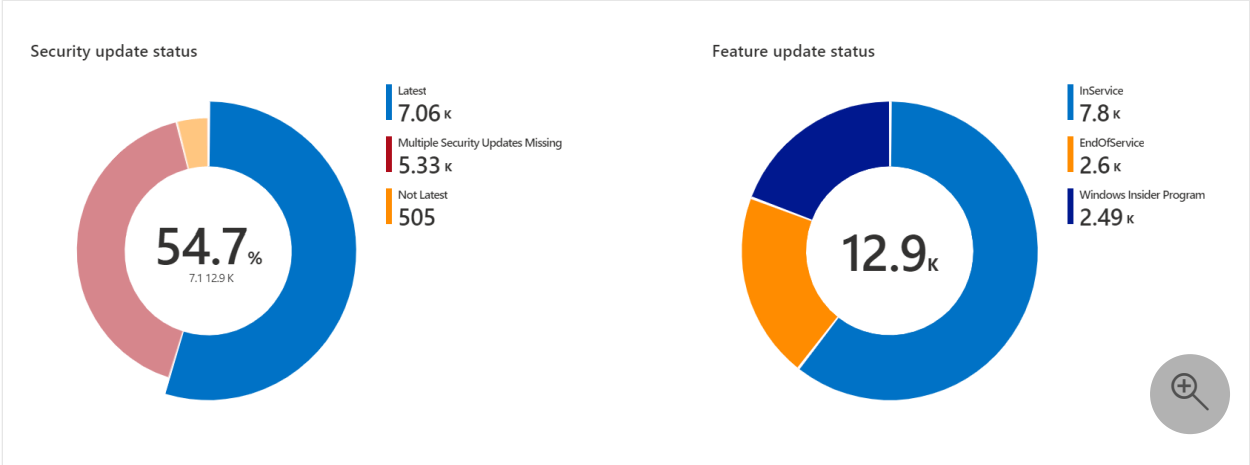
Развернуть таблицу

Имя плитки	Описание	Просмотр описания сведений
Зарегистрированные устройства	Общее количество устройств, зарегистрированных в отчетах клиентский компонент Центра обновления Windows для бизнеса	Отображает несколько диаграмм об операционных системах (ОС) для зарегистрированных устройств: **версия** **ОС OS Edition** OS**Servicing Channel**
Активные оповещения	Общее количество активных оповещений на зарегистрированных устройствах	Отображает три основных подтипа активных оповещений и количество устройств в каждом из них. Выберите количество **устройств** , чтобы отобразить таблицу устройств. Эта таблица ограничена первыми 1000 строками. Выберите `...` , чтобы экспортировать полный список или отобразить запрос в Log Analytics. Выберите **AlertSubtype** , чтобы отобразить список, содержащий: - Каждый **код ошибки** в подтипе оповещения - **Описание** кода ошибки - **Рекомендация** по исправлению кода ошибки - Количество **устройств** с определенным кодом ошибки
внедрение Windows 11	Количество устройств под управлением Windows 11	Отображаются следующие элементы: - **диаграмма Windows 11 число устройств** с разбивкой по версии - Windows 11 **Windows 11 состояние готовности** содержит диаграмму **состояния готовности**, в котором указано количество устройств по версиям ОС, которые либо поддерживают, либо не поддерживают Windows 11. — **Список устройств** позволяет выбрать причину Windows 11 **для** отображения устройств, которые не соответствуют выбранному требованию.

Диаграммы вкладок "Сводка"

Диаграммы, отображаемые на вкладке **Сводка** , дают общее представление об общем состоянии устройств. Две отображаемые диаграммы:

- **Общее состояние обновления для системы безопасности**. Предоставляет общие сведения о текущем состоянии соответствия обновлений зарегистрированным устройствам. Например, если на диаграмме показано, что большое количество устройств не хватает нескольких обновлений для системы безопасности, это может указывать на проблему в процессе обновления программного обеспечения.
- **Состояние обновления компонентов**. Дает общее представление о том, сколько устройств подходит для обновления компонентов в зависимости от жизненного цикла операционной системы.



Вкладка "Исправления"

На вкладке **Исправления** в верхней части экрана отображаются обобщенные данные с помощью плиток. Данные о качестве обновления становятся более конкретными при переходе ниже на этой вкладке. В верхней части вкладки **Исправления** содержатся плитки со следующими сведениями и параметрами детализации:

Развернуть таблицу

Имя плитки	Описание	Описание детализации
Последнее обновление для системы безопасности	Количество устройств, которые сообщили об успешной	— Выберите **Просмотреть сведения** , чтобы отобразить всплывающий элемент с диаграммой, на котором отображаются первые 1000 элементов. — Выберите `...` из всплывающего меню, чтобы

Имя плитки	Описание	Описание детализации
	установке последнего обновления для системы безопасности.	экспортировать полный список или отобразить запрос в Log Analytics.
Отсутствует одно обновление для системы безопасности	Количество устройств, на которых не установлено последнее обновление для системы безопасности.	— Выберите **Просмотреть сведения** , чтобы отобразить всплывающий элемент с диаграммой, на котором отображаются первые 1000 элементов. — Выберите `...` из всплывающего меню, чтобы экспортировать полный список или отобразить запрос в Log Analytics.
Отсутствие нескольких обновлений для системы безопасности	Количество устройств, на которых не хватает двух или более обновлений для системы безопасности.	— Выберите **Просмотреть сведения** , чтобы отобразить всплывающий элемент с диаграммой, на котором отображаются первые 1000 элементов. — Выберите `...` из всплывающего меню, чтобы экспортировать полный список или отобразить запрос в Log Analytics.
Активные оповещения	Количество активных обновлений и оповещений устройств об обновлениях качества.	
Состояние ускорения	Обзор хода выполнения ускоренного развертывания последнего обновления для системы безопасности.	Выберите **Просмотреть сведения** , чтобы отобразить всплывающее меню с двумя **вкладками: Развертывания** и **Готовность** . На вкладке **Развертывания** отображается диаграмма, отображающая общий ход каждого развертывания, количество оповещений и количество устройств. • Выберите счетчик в столбце **Оповещения** , чтобы отобразить оповещения по имени для развертывания. При выборе числа устройств для имени оповещения отображается список устройств с оповещением. • Выберите счетчик в столбце **TotalDevices** , чтобы отобразить список клиентов и их сведения для развертывания.

Имя плитки	Описание	Описание детализации
		— Вкладка "**Готовность** " содержит диаграмму с количеством устройств, которые **имеют право** и **не имеют права** на установку ускоряемых udpates. Вкладка "**Готовность** " также содержит таблицу, в которой перечислены развертывания для ускоренного обновления. • Выберите счетчик в столбце **Оповещения** , чтобы отобразить устройства с состоянием **RegistrationMissingUpdateClient**, что означает, что на устройстве отсутствует средство обновления работоспособности. Средства работоспособности обновлений устанавливаются, начиная с KB4023057 или из автономного пакета из Центра загрузки Майкрософт. Пример скрипта PowerShell для проверки установки средств: `Get-CimInstance -ClassName Win32_Product | Where-Object {$_.Name -match "Microsoft Update Health Tools"}` • Выберите значение **TotalDevices,** чтобы отобразить список устройств в развертывании.

Под плитками вкладка **Исправления обновлений** подразделяется на группы **Состояние обновления** и **Состояние устройства** . Эти различные группы диаграмм позволяют легко обнаруживать тенденции в данных соответствия требованиям. Например, вы помните, что около трети ваших устройств находились в состоянии установки вчера, но это число изменилось не так сильно, как вы ожидали. Эта неожиданная тенденция может привести к изучению и устранению потенциальной проблемы до того, как пользователи будут затронуты.

Обновление группы состояния для обновлений качества

Группа **состояния обновления** для обновлений качества содержит следующие элементы:

- **Состояния обновлений для всех выпусков системы безопасности**. Состояния обновлений для последних 3 обновлений безопасности используются для заполнения этой диаграммы. Общее количество состояний обновления примерно в 3 раза больше, чем количество устройств, которые сообщили об

обновлении данных в клиентский компонент Центра обновления Windows для бизнес-отчетов за последние 30 дней.
- **Оповещения об обновлении для всех выпусков системы безопасности**: диаграмма, содержащая количество активных ошибок и предупреждений для обновлений системы безопасности.

В таблице **Состояние развертывания обновления** отображаются обновления качества для каждой версии операционной системы, выпущенной за последние 60 дней. Для каждого обновления выполните детализацию, выбрав значение из следующих столбцов:

Развернуть таблицу

Имя столбца	Описание	Описание детализации
Оповещения	Количество различных кодов ошибок, обнаруженных устройствами при обновлении.	При выборе этого номера выводится имя оповещения для каждого кода ошибки и количество устройств с ошибкой. Выберите число устройств, чтобы отобразить список устройств с активным оповещением о коде ошибки.
Номер базы знаний	Номер базы знаний для обновления	При выборе номера базы знаний откроется веб-страница сведений о поддержке для обновления.
Всего устройств	Количество устройств, на которых было предложено обновление или которые устанавливают, установили или отменили обновление.	При выборе счетчика устройств откроется таблица списка устройств. Эта таблица ограничена первыми 1000 строками. Выберите `...` , чтобы экспортировать полный список или отобразить запрос в Log Analytics.

Группа состояния устройств для обновлений качества

Группа **состояния устройства** для обновлений качества содержит следующие элементы:

- **Номер сборки ОС**: диаграмма, содержащая количество устройств по сборке ОС, получающих обновления для системы безопасности.
- **Оповещения устройств**: диаграмма, содержащая количество активных ошибок и предупреждений об обновлениях качества.
- **Состояние соответствия устройств**. Таблица, содержащая список устройств, получающих обновления для системы безопасности и сведения об установке обновлений, включая активные оповещения для устройств.

- Эта таблица ограничена первыми 1000 строками. Выберите `...` , чтобы экспортировать полный список или отобразить запрос в Log Analytics.

Вкладка "Обновления компонентов"

На **вкладке Обновления компонентов** в верхней части экрана отображаются обобщенные данные с помощью плиток. Данные об обновлении компонентов становятся более конкретными при переходе ниже на этой вкладке. В верхней части вкладки **Обновления компонентов** содержатся плитки со следующими сведениями:

- **В обновлении компонентов службы**: количество устройств, установленных с поддерживаемой версией обновления компонентов Windows.
- **Обновление компонентов окончания обслуживания**: количество устройств, на которых не установлена поддерживаемая версия обновления компонентов Windows. Дополнительные сведения см. в статье Вопросы и ответы о жизненном цикле Windows.
- **Приближается EOS** Количество устройств, находящихся в течение 18 месяцев с даты окончания обслуживания.
- **Активные оповещения**: количество активных обновлений и оповещений устройств для обновлений компонентов.

Как и на вкладке **Исправления обновлений**, вкладка **Обновления компонентов** также подразделяется на группы **Состояние обновления** и **Состояние устройства** под плитками. При выборе **пункта Просмотреть сведения** на любой из плиток отображается всплывающее меню с диаграммой, на котором отображаются первые 1000 элементов. Выберите `...` из всплывающего меню, чтобы экспортировать полный список или отобразить запрос в Log Analytics.

Группа состояния обновления для обновлений компонентов

Группа **состояния обновления** для обновлений компонентов содержит следующие элементы:

- **Целевая версия**: диаграмма, содержащая количество устройств для каждой версии целевой операционной системы.
- **Удержание защиты**: диаграмма, содержащая количество устройств для каждой версии операционной системы, которые находятся под удержанием для обновления компонентов.

- **Оповещения об обновлении**: диаграмма, содержащая количество активных ошибок и предупреждений для обновлений компонентов.

Таблица состояния развертывания обновления для обновлений компонентов отображает состояние установки по целевой версии операционной системы. Для каждой целевой версии операционной системы доступны следующие столбцы:

Развернуть таблицу

Имя столбца	Описание	Описание детализации
Общий ход выполнения	Процент устройств, на которые установлено обновление компонентов целевой версии операционной системы за последние 30 дней.	Линейчатая диаграмма включена в этот столбец. Дополнительные сведения см. в разделе **Всего устройств** .
Оповещения	Количество различных кодов ошибок, обнаруженных устройствами при обновлении.	При выборе этого номера выводится имя оповещения для каждого кода ошибки и количество устройств с ошибкой. Выберите число устройств, чтобы отобразить список устройств с активным оповещением о коде ошибки.
Всего устройств	Количество устройств для каждой целевой версии операционной системы, для которых было предложено обновление, устанавливается, установлено или отменено обновление компонентов.	При выборе счетчика устройств откроется таблица списка устройств. Эта таблица ограничена первыми 1000 строками. Выберите `...` , чтобы экспортировать полный список или отобразить запрос в Log Analytics.

Группа состояния устройств для обновлений компонентов

Группа **состояния устройства** для обновлений компонентов содержит следующие элементы:

- **Windows 11 состояние готовности**: диаграмма, содержащая количество устройств, которые имеют состояние "поддержка", "не поддерживает" или "неизвестно" для Windows 11 готовности.
- **Оповещения устройств**. Количество активных оповещений устройств для обновлений компонентов в каждой классификации оповещений.

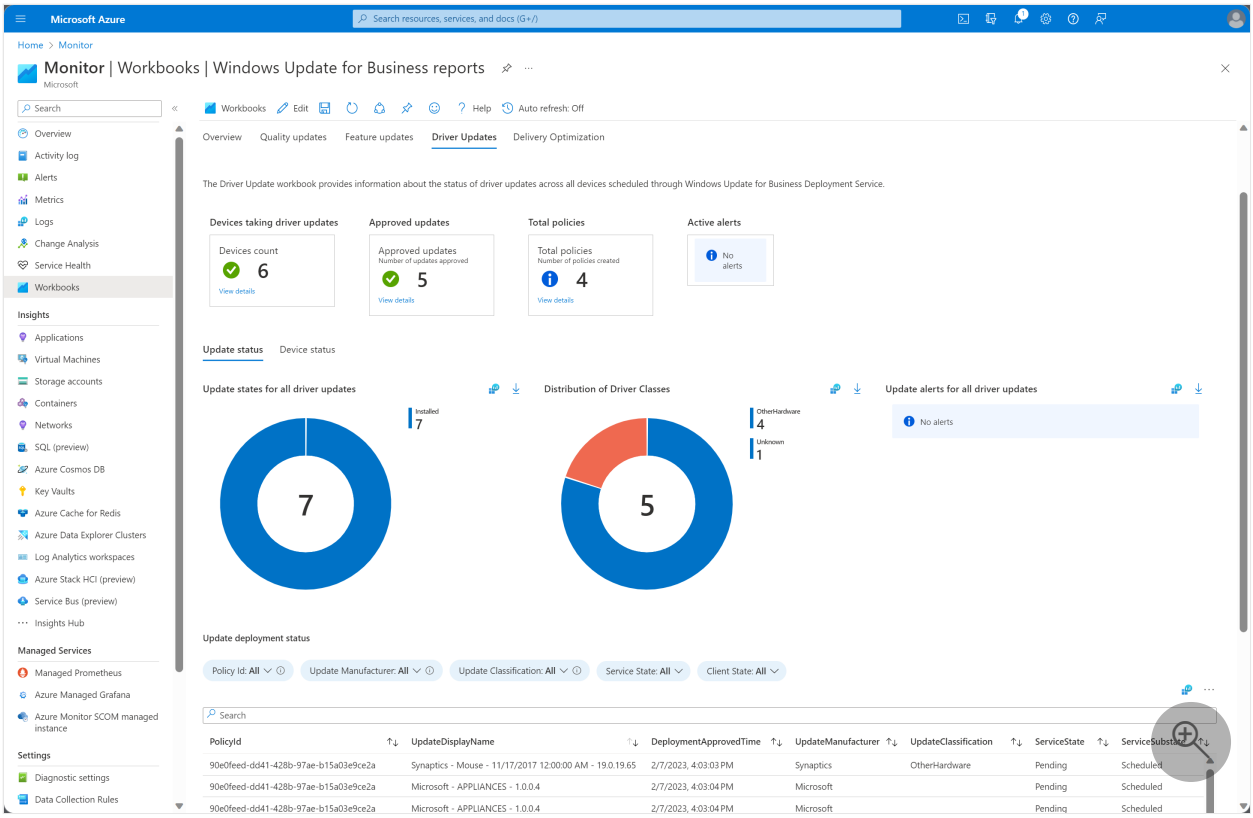
- **Состояние соответствия устройств**. Таблица, содержащая список устройств, получающих сведения об обновлении компонентов и установке, включая активные оповещения для устройств.
  - Эта таблица ограничена первыми 1000 строками. Выберите `...` , чтобы экспортировать полный список или отобразить запрос в Log Analytics.

Вкладка "Обновления драйверов"

На вкладке **Обновление драйверов** содержатся сведения о развертываниях обновлений драйверов и встроенного ПО из службы развертывания клиентский компонент Центра обновления Windows для бизнеса. Обобщенные данные отображаются в верхней части страницы на плитках. Данные становятся более конкретными при переходе вниз на этой вкладке. В верхней части вкладки Обновления драйверов содержатся плитки со следующими сведениями:

Устройства, принимающие обновления драйверов: количество устройств, устанавливающих обновления драйверов и встроенного ПО. **Утвержденные обновления**: количество утвержденных обновлений драйверов **Всего политик**: общее количество политик развертывания для обновлений драйверов и встроенного ПО из службы развертывания клиентский компонент Центра обновления Windows для бизнеса**Активные оповещения**: количество активных оповещений для развертываний драйверов

При выборе **пункта Просмотреть сведения** на любой из плиток отображается всплывающее меню с диаграммой, на котором отображаются первые 1000 элементов. Выберите `...` из всплывающего меню, чтобы экспортировать полный список или отобразить запрос в Log Analytics.



Как и на вкладках **Обновления качества** и **Обновления компонентов** , вкладка **Обновления драйверов** также подразделяется на группы **Состояние обновления** и **Состояние устройства** под плитками. Эти различные группы диаграмм позволяют легко обнаруживать тенденции в данных соответствия требованиям.

Обновление группы состояния для драйверов

Группа **состояния обновления** для обновлений драйверов содержит следующие элементы:

- **Состояния обновлений для всех обновлений драйверов**: диаграмма, содержащая количество устройств в определенном состоянии, например установка, для обновлений драйверов.
- **Распределение классов драйверов**: диаграмма, содержащая количество драйверов в определенном классе.
- **Оповещения об обновлении для всех обновлений драйверов**: диаграмма, содержащая количество активных ошибок и предупреждений для обновлений драйверов.

В таблице **Состояние развертывания обновления** отображаются сведения о развернутых обновлениях драйверов для ваших устройств. Затем выполните детализацию, выбрав значение из столбца **TotalDevices** , чтобы отобразить состояние конкретного драйвера для определенной политики, а также сведения о состоянии установки для каждого устройства.

Группа состояния устройств для обновлений драйверов

Группа **состояния устройства** для обновлений драйверов содержит следующие элементы:

- **Оповещения устройств**. Количество активных оповещений устройств об обновлениях драйверов в каждой классификации оповещений.
- **Состояние соответствия устройств**. Таблица, содержащая список устройств, получающих сведения об обновлении и установке драйверов, включая активные оповещения для устройств.
  - Эта таблица ограничена первыми 1000 строками. Выберите `...` , чтобы экспортировать полный список или отобразить запрос в Log Analytics.

Оптимизация доставки

На вкладке **Оптимизация доставки** представлено обобщенное представление об эффективности пропускной способности. Этот новый пересмотренный отчет также содержит сведения о подключенном кэше Майкрософт . Дополнительные сведения см. в статье Данные оптимизации доставки в отчетах клиентский компонент Центра обновления Windows для бизнеса.

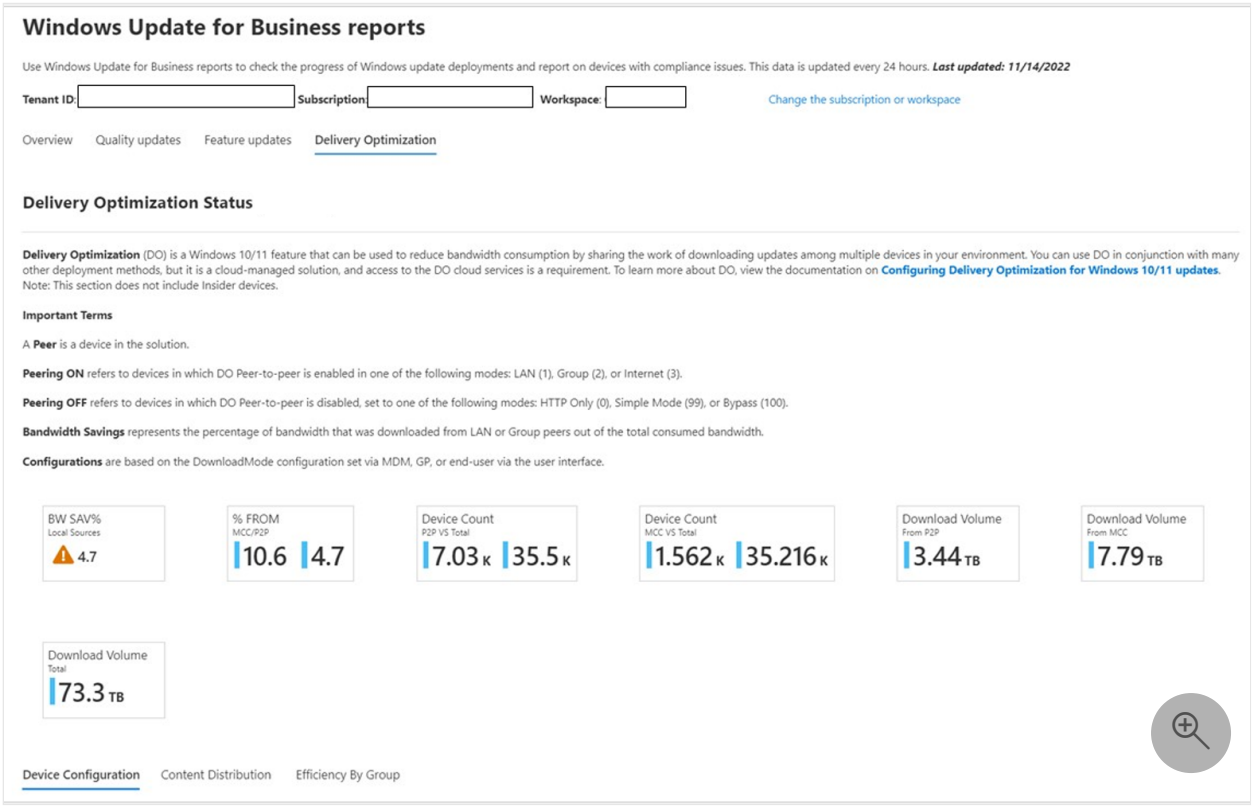
В верхней части отчета на плитках отображаются следующие сведения:

- Процент общей экономии пропускной способности
- Процент сохраненной пропускной способности с разбивкой по одноранговой сети и MCC
- Количество устройств, показывающее процент байтов, доставленных между одноранговым подключением и MCC
- Разбивка общего числа скачанных ГБ.

Вкладка Оптимизация доставки разделена на следующие группы:

- **Конфигурация устройства**. Диаграмма, в основе которого указано количество устройств с одноранговым подключением и без нее. И таблица разбивки конфигурации режима загрузки между числами устройств. Если этот параметр выбран, устройства в этой группе можно просмотреть, отфильтровав в отдельной таблице.
- **Распределение содержимого**. Включает диаграммы, показывающие процентные тома и тома ГБ по источнику по типам контента. Все типы контента связаны с таблицей для более глубокой фильтрации по **ContentType**, **AzureADTenantId** и **GroupID**.

- **Эффективность по группам**. Это представление предоставляет фильтры, часто используемые способы группирования устройств. К предоставленным фильтрам относятся : **GroupID**, **City**, **Country** и **ISP**.



Основные сведения о состояниях обновления

Обновления может пройти несколько этапов, начиная с первоначального развертывания до установки на устройстве. Переход из одного состояния в другое может быть быстрым, что делает некоторые состояния менее вероятными для отображения в отчетах. Книга может сообщать о следующих состояниях высокого уровня для обновления устройства:

- **Предложение**: обновление предлагается устройству для установки
- **Установка**: обновление устанавливается на устройстве.
- **Установлено**: обновление установлено на устройстве.
- **Отменено**: обновление было отменено из службы развертывания перед установкой.
- **Удалено**: обновление было удалено с устройства администратором или пользователем.
- **OnHold**: обновление было отложено из службы развертывания перед установкой

- **Неизвестно**. Это состояние возникает, когда в таблице UCClient есть запись для устройства, но в таблице UCClientUpdateStatus нет записи для конкретного обновления для конкретного устройства. Это означает, что отсутствует запись об обновлении для соответствующего устройства.

Настройка книги

Так как книга отчетов клиентский компонент Центра обновления Windows для бизнеса является шаблоном книги Azure, ее можно настроить в соответствии с вашими потребностями. Если вы открываете шаблон, вносите некоторые изменения и сохраняете его, шаблон сохраняется как книга. Эта книга отображается зеленым цветом. Исходный шаблон остается нетронутым. Дополнительные сведения о книгах см. в статье Начало работы с книгами Azure.

Дальнейшие действия

- Изучение схемы отчетов клиентский компонент Центра обновления Windows для бизнеса
- Просмотр отзывов, поддержки и устранения неполадок для отчетов клиентский компонент Центра обновления Windows для бизнеса

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Данные оптимизации доставки в отчетах клиентский компонент Центра обновления Windows для бизнеса

Применимо к: ✅ Windows 11, ✅ Windows 10

Оптимизация доставки (DO) — это функция Windows, которая может использоваться для снижения потребления пропускной способности путем совместного скачивания обновлений между несколькими устройствами в вашей среде. Вы можете использовать DO со многими другими методами развертывания, но это облачное решение, и доступ к облачным службам DO является обязательным.

Отчеты клиентский компонент Центра обновления Windows для бизнеса предоставляют сведения об оптимизации доставки в следующих местах:

- Книга отчетов клиентский компонент Центра обновления Windows для бизнеса
- UCDOAggregatedStatus
- UCDOStatus

клиентский компонент Центра обновления Windows отчеты для бизнеса не включают данные оптимизации доставки для устройств предварительной оценки Windows.

Условия оптимизации доставки

клиентский компонент Центра обновления Windows отчетах для бизнеса используются следующие условия оптимизации доставки:

- **Одноранговый узел**: устройство в решении
- **Пиринг "ON"** — устройства, где одноранговая связь DO включена в одном из следующих режимов:
  - Локальная сеть (1)
  - Группа (2)
  - Интернет (3)
- **Пиринг "OFF"**: устройства, на которых отключена одноранговая связь DO, задается один из следующих режимов:
  - Только HTTP (0)
  - Простой режим (99)
  - Обход (100), устаревший в Windows 11

- **Экономия пропускной способности**. Процент пропускной способности, загруженной из альтернативных источников (одноранговых узлов или подключенного кэша Майкрософт), от общего объема скачанных данных.
- Если экономия пропускной способности <составляет 60 %, отображается значок *предупреждения* .
- Если экономия пропускной способности составляет <10 %, отображается значок *Ошибки* .
- **Конфигурации**. На основе набора конфигурации DownloadMode через MDM, групповая политика или конечный пользователь через пользовательский интерфейс.
- **Число устройств P2P**. Количество устройств — это количество устройств, настроенных для использования пиринга.
- **Подключенный кэш (Майкрософт**). Подключенный кэш (Майкрософт) — это программное решение для кэширования, которое предоставляет содержимое Майкрософт. Дополнительные сведения см. в статье Обзор подключенного кэша (Майкрософт).
- **Число устройств MCC**. Число устройств — это количество устройств, которые получили байты с сервера кэша для поддерживаемых типов контента.
- **Общее число устройств**: общее число устройств с активностью за последние 28 дней.
- **Байты локальной сети**: байты, доставляемые из одноранговых узлов локальной сети.
- **Байты группы**: байты из одноранговых узлов группы. Если устройство использует group DownloadMode, оптимизация доставки сначала ищет одноранговые узлы в локальной сети, а затем в группе. Таким образом, если байты доставляются из одноранговых узлов локальной сети, они вычисляются в "байтах локальной сети".
- **Байты CDN**: байты, доставленные из сети доставки содержимого (CDN).
- **Город**. Город определяется на основе расположения устройства, на котором загружается максимальный объем данных.
- **Страна**: страна определяется на основе расположения устройства, на котором загружается максимальный объем данных.
- **Поставщик услуг Интернета**. Поставщик услуг интернета определяется на основе того, что поставщик услуг Интернета доставляет максимальное количество байтов на устройство.

Вычисления для оптимизации доставки

Вычисляемые значения, используемые в отчете об оптимизации доставки, перечислены ниже.

Вычисления эффективности (%)

- Экономия пропускной способности (BW SAV%) = 100 * (BytesFromPeers + BytesFromGroupPeers + BytesFromCache) / (BytesFromPeers + BytesFromGroupPeers +BytesFromCDN + BytesFromCache)
  - Таблица UCDOAggregatedStatus
- % эффективности P2P = 100 * (BytesFromPeers + BytesFromGroupPeers) / (BytesFromPeers + BytesFromGroupPeers+BytesFromCDN+BytesFromCache)
  - Таблица UCDOStatus
- Процент эффективности подключенного кэша = 100 * BytesFromCache / (BytesFromPeers + BytesFromGroupPeers+BytesFromCDN+BytesFromCache)
  - Таблица UCDOStatus

Вычисления байтов:

- TotalBytes = BytesFromCDN + BytesFromEnterpriseCache + BytesFromPeers + BytesFromGroupPeers
  - Таблица UCDOAggregatedStatus
- BytesFromCDN = BytesFromCDN
  - Таблица UCDOAggregatedStatus
- BytesFromPeers = BytesFromLAN
  - Таблица UCDOAggregatedStatus
- BytesFromGroupPeers = BytesFromGroupPeers
  - Таблица UCDOAggregatedStatus
- BytesFromCache = BytesFromCache
  - Таблица UCDOAggregatedStatus

Вычисления томов:

- Том по P2P = BytesFromPeers + BytesFromGroupPeers
  - Таблица UCDOStatus
- Volume by Connected Cache = BytesFromCache
  - Таблица UCDOStatus
- Том по CDN = BytesF from CDN
  - Таблица UCDOStatus

Сопоставление GroupID

В подразделе **Efficiency By Group (Эффективность по группе)** **идентификатор GroupID** отображается в виде закодированного хэша SHA256 и учитывает регистр. Вы можете создать сопоставление исходных идентификаторов с идентификаторами groupID с помощью следующего примера PowerShell:

PowerShell

```
$text = "<myOriginalGroupID>`0" ; # The `0 null terminator is required

$hashObj = [System.Security.Cryptography.HashAlgorithm]::Create('sha256') ; $dig =
$hashObj.ComputeHash([System.Text.Encoding]::Unicode.GetBytes($text)) ; $digB64 =
[System.Convert]::ToBase64String($dig) ; Write-Host "$text ==> $digB64"
```

Кроме того, в журналах оптимизации доставки можно просмотреть закодированные и декодированные идентификаторы GroupID.

PowerShell

```
Get-DeliveryOptimizationLog -Flush | Set-Content C:\dosvc.log
```

Следующие две строки объединяются в подробных журналах:

text

```
2023-02-15T12:33:11.3811337Z 1514  1F4          {CGlobalConfigManager::GetGroupId}
Using groupID = **<myOriginalGroupId>**
2023-02-15T12:33:11.3811432Z 1514  1F4          {CGlobalConfigManager::GetGroupId}
Hashed groupID = **<myEncodedGroupId>**
```

Примеры запросов

Вы можете использовать данные в UCDOAggregatedStatus и UCDOStatus для создания собственных запросов. Создавайте пользовательские запросы с помощью язык запросов Kusto (KQL), но обратите внимание, что в отчетах клиентский компонент Центра обновления Windows для бизнеса используется Azure Monitor, поэтому некоторые операторы не поддерживаются. В документации по KQL указано, какие операторы не поддерживаются монитором Azure, или они имеют разные функции. Дополнительные сведения о KQL в Azure Monitor см. в статье Запросы журналов в Azure Monitor. Ниже приведены примеры использования данных.

Пример запроса таблицы UCDOAggregatedStatus

Следующий запрос используется для отображения значения общей экономии пропускной способности в процентах:

Kusto

```
UCDOAggregatedStatus| where TimeGenerated == _SnapshotTime
| extend LocalSourceBytes = BytesFromCache + BytesFromGroupPeers + BytesFromPeers
| summarize LocalSources_BWSAV = round((sum(0.0 + LocalSourceBytes)/
sum(LocalSourceBytes+BytesFromCDN)) * 100.0 ,2)
| extend Title = "BW SAV%" , SubTitle = "Local Sources"
```

Пример запроса к таблице UCDOStatus

Следующий запрос используется для отображения 10 идентификаторов групп:

Kusto

```
UCDOStatus  | where TimeGenerated == _SnapshotTime
| summarize sum(BytesFromCDN) ,  sum(BytesFromGroupPeers) , sum(BytesFromPeers) ,
sum(BytesFromCache) ,
DeviceCount = count_distinct(GlobalDeviceId) by GroupID | top 10 by DeviceCount desc
| extend TotalBytes = (sum_BytesFromPeers +
sum_BytesFromGroupPeers+sum_BytesFromCDN+sum_BytesFromCache)
| extend P2PPercentage = ((0.0 + sum_BytesFromPeers +
sum_BytesFromGroupPeers)/TotalBytes ) * 100.0
| extend  MCCPercentage = ((0.0 + sum_BytesFromCache)/ TotalBytes) * 100.0  ,
 VolumeBytesFromPeers = sum_BytesFromPeers + sum_BytesFromGroupPeers
| extend VolumeBytesFromMCC = sum_BytesFromCache , VolumeByCDN = sum_BytesFromCDN
| project  GroupID , P2PPercentage , MCCPercentage ,  VolumeBytesFromPeers ,
VolumeBytesFromMCC ,VolumeByCDN , DeviceCount
```

Поддерживаемые типы контента для оптимизации доставки

Существует множество типов контента Майкрософт, поддерживаемых оптимизацией доставки. Все эти типы контента отображаются в разделе "Распространение содержимого" отчета об оптимизации доставки. Ознакомьтесь с полной таблицей о типах поддержки P2P и подключенного кэша.

> **Заметка**
>
> С 22 июля 2025 г. Обновления программного обеспечения, которые являются обновлениями, не относящихся к Windows и не из Магазина, будут перемещены из категории "Другое" в категорию "Обновления компонентов". Примеры: Visual Studio, Exchange, SQL Server.

Развернуть таблицу

Категория содержимого	Включенные типы контента
Приложения	приложения магазина Windows 10, Windows 11 приложения магазина UWP
Обновления драйвера	Обновления драйверов клиентский компонент Центра обновления Windows
Обновления компонентов	обновления компонентов клиентский компонент Центра обновления Windows
Office	Приложения Microsoft 365 и обновления
Другое	Языковые пакеты Windows, обновления определений Защитника Windows, Intune приложения Win32, обновления браузера Edge, Configuration Manager экспресс-обновления, динамические обновления, агент MDM, Xbox Game Pass (PC), Диспетчер пакетов Windows, установщик MSIX (включает приложения Win32 Windows 11 Store, обновления Windows 11 Teams)
Исправления	Обновления качества windows Обновления
Teams Обновления (поддержка P2P, начиная с версии 25122.1415.3698.6812)	Обновления Teams

Вопросы по частоте

- **Какой период времени включает данные оптимизации доставки?** Данные создаются или агрегируются за последние 28 дней для активных устройств. Чтобы данные оптимизации доставки регистрировались в отчете, устройство должно выполнить некоторое действие оптимизации доставки в 28-дневном окне скользящего окна. Сюда входят сведения о конфигурации устройства.
- **Данные отображаются как "Неизвестные", что это означает?** Данные могут отображаться в отчете как "Неизвестные". Это состояние указывает, что параметр DownloadMode оптимизации доставки является недопустимым или пустым.
- **Как определяются группы "Топ-10"?** Верхние группы представлены количеством устройств в определенной группе для любого из четырех типов групп (GroupID, City, Country и ISP).
- **Идентификаторы GroupID не выглядят знакомыми, почему они отличаются?** Значения GroupID кодируются для требований телеметрии защиты данных. Дополнительные сведения см. в разделе "Сопоставление идентификаторов групп" выше.

- **Как просмотреть данные для устройства в офисе и вне офиса?** Сегодня у нас нет различий для данных, скачанных по расположению.
- **Что представляют данные в таблице UCDOStatus?** Строка в UCDOStatus представляет данные, скачанные сочетанием одного идентификатора устройства (AzureADDeviceId) по типу контента (ContentType).
- **Что представляют данные в таблице UCDOAggregatedStatus?** Строка в UCDOAggregatedStatus представляет данные, суммированные на уровне клиента (AzureADTenantID) для каждого типа контента (ContentType).
- **Как вычисляется BytesFromCache при наличии сервера подключенного кэша, используемого поставщиком услуг Интернета?** Если есть сервер подключенного кэша на уровне поставщика услуг Интернета, BytesFromCache отфильтровывает все байты, поступающие в подключенный кэш поставщика услуг Интернета.
- **Как результаты командлетов PowerShell для оптимизации доставки сравниваются с результатами в отчете?**Командлеты PowerShell для оптимизации доставки могут быть мощным инструментом, используемым для мониторинга данных оптимизации доставки на устройстве. Эти командлеты используют кэш на устройстве. Данные, вычисляемые в отчете, берутся из событий телеметрии оптимизации доставки.
- **Отчет представляет данные за последние 28 дней. Почему некоторые запросы включают >= семь дней?** Данные в отчете представляют данные за последние 28 дней. Запрос за последние семь дней предназначен только для получения данных за последние snapshot за последние семь дней. Возможно, данные задерживаются на некоторое время и недоступны за текущий день, поэтому мы ищем последние snapshot за последние 7 дней в log Analytics и показываем последние snapshot.

Last updated on 03.12.2025

страница обновлений программного обеспечения Центр администрирования Microsoft 365

Статья • 08.05.2024 •

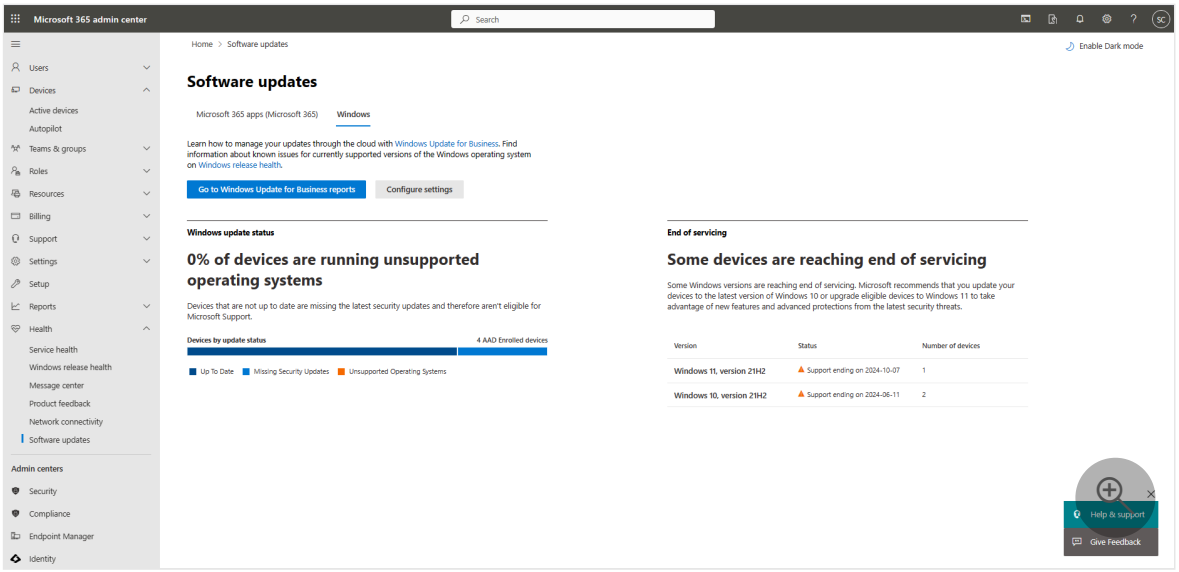
Применяется к: ✅ Windows 11, ✅ Windows 10, ✅ Windows Update for Business reports, ✅ Microsoft 365 admin center

На странице **Обновления программного обеспечения** в Центр администрирования Microsoft 365 отображается общий обзор состояния установки обновлений Приложения Microsoft 365 и Windows в вашей среде. Исправления, содержащие исправления безопасности, обычно выпускаются во второй вторник каждого месяца. Обеспечение установки этих обновлений важно, так как они помогают защитить вас от известных уязвимостей. На странице **Обновления программного обеспечения** можно легко определить общее соответствие обновлений для ваших устройств.

На странице **Обновления программного обеспечения** есть следующие вкладки, которые помогут вам отслеживать состояние обновлений для ваших устройств:

- **Приложения Microsoft 365**: отображает состояние обновления для Приложения Microsoft 365.
  - Дополнительные сведения о вкладке **Приложения Microsoft 365** см. в разделе Приложения Microsoft 365 обновления в Центре администрирования.

- **Windows**: отображаются диаграммы соответствия для накопительных обновлений и обновлений компонентов для клиентов Windows. Эта статья содержит сведения о вкладке **Windows** .



Ограничения

Отчеты клиентский компонент Центра обновления Windows для бизнеса — это служба Windows, размещенная в Azure, которая использует диагностические данные Windows. Отчеты клиентский компонент Центра обновления Windows для бизнеса доступны в коммерческом облаке Azure, но недоступны для клиентов GCC High или США Министерства обороны, так как они не соответствуют требованиям сообщества государственных организаций США (GCC). Список предложений GCC для продуктов и служб Майкрософт см. в центре управления безопасностью Майкрософт.

Get started

Убедившись, что выполнены предварительные требования и разрешения для отчетов клиентский компонент Центра обновления Windows для бизнеса, при необходимости зарегистрируйтесь, используя приведенные ниже инструкции.

1. Перейдите к Центр администрирования Microsoft 365 и войдите в систему.

2. Разверните узел **Работоспособности**, а затем выберите **Программное обеспечение Обновления**. Для отображения **работоспособности** в меню навигации может потребоваться использовать параметр **Показать все**.

    - Если в меню не отображается запись об **обновлениях программного обеспечения** , попробуйте перейти по следующему URL-адресу: https://admin.microsoft.com/Adminportal/Home#/softwareupdates .

3. На странице **Программное обеспечение Обновления** выберите вкладку **Windows**.

4. При первом выборе вкладки **Windows** вам будет предложено **настроить параметры**. Эта вкладка заполняется данными из отчетов клиентский компонент Центра обновления Windows для бизнеса. Проверьте или предоставьте следующие сведения о параметрах отчетов клиентский компонент Центра обновления Windows для бизнеса:

    - Подписка Azure
    - Рабочая область Log Analytics

5. Начальная настройка может занять до 24 часов. В течение этого времени на вкладке **Windows** отображается сообщение **Ожидание клиентский компонент Центра обновления Windows данных отчетов для бизнеса**.

    - Регистрация в отчетах клиентский компонент Центра обновления Windows для бизнеса не влияет на скорость отправки необходимых данных с устройств. Подключение устройства к Интернету и его активность влияет на то, сколько времени потребуется, прежде чем устройство появится в отчетах. Устройства, которые активны и подключены к Интернету ежедневно, могут быть полностью загружены в течение одной недели (обычно менее 72 часов). Менее активные устройства могут занять до двух недель, прежде чем данные будут полностью доступны.

6. После завершения начальной настройки на вкладке **Windows** на диаграммах будут отображаться данные отчетов клиентский компонент Центра обновления Windows для бизнеса.

    > ⓘ **Примечание**
    >
    > Количество устройств на вкладке **Windows** может отличаться от **Приложения Microsoft 365** вкладки, так как их требования отличаются.

Вкладка Windows

Вкладка **Windows** на странице **Обновления программного обеспечения** в Центре администрирования Майкрософт заполняется данными из отчетов клиентский компонент Центра обновления Windows для бизнеса. Вкладка содержит общий обзор соответствия обновлений для клиентов Windows в вашей среде. На вкладке отображаются две диаграммы **Состояние обновления Windows** и **Окончание службы**. Данные клиентский компонент Центра обновления Windows для бизнеса, заполняющие эти диаграммы, обновляются каждые 24 часа. Дополнительные

сведения см. в разделе задержка данных клиентский компонент Центра обновления Windows для бизнеса.

Диаграмма состояния центра обновления Windows

Диаграмма **состояния обновлений Windows** дает визуальное представление о том, сколько устройств находятся в следующих состояниях для ежемесячных накопительных обновлений:

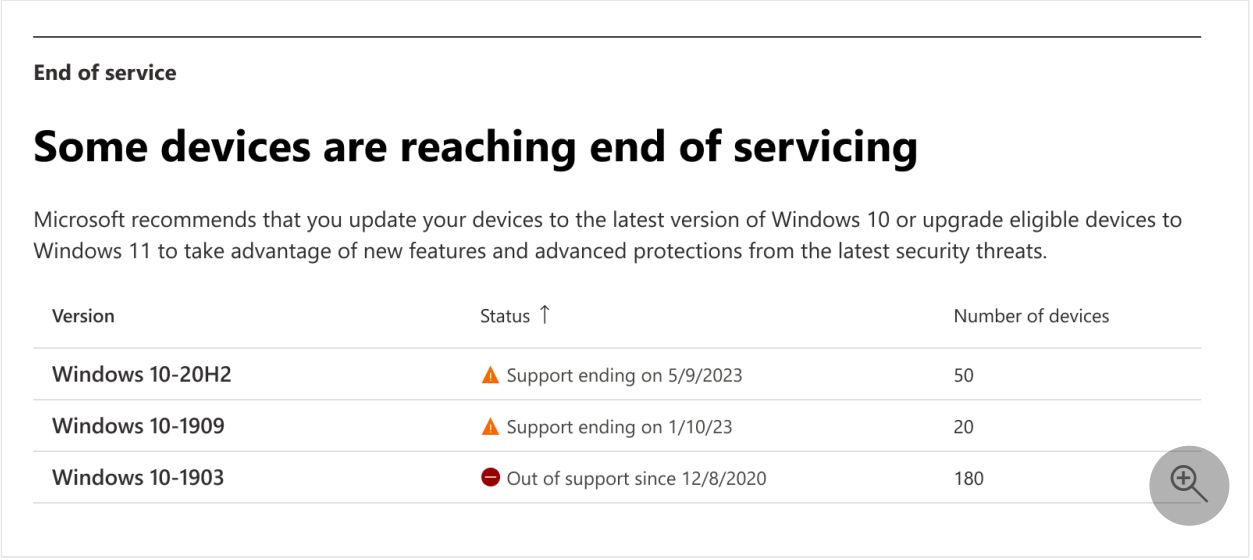
- Современный
- Отсутствующие обновления для системы безопасности
- Неподдерживаемая операционная система

Устройство считается **актуальным** на этой диаграмме, если оно установило обновления для системы безопасности , выпущенные в течение последних двух месяцев. Устройства, которые отстают от установки более двух месяцев, находятся в классификации **отсутствующих обновлений для системы безопасности** . **Неподдерживаемая операционная система** больше не поддерживается жизненным циклом продукта Майкрософт.

Диаграмма конца службы

На **диаграмме Окончание службы** отображается количество устройств с версией операционной системы, которая приближается к жизненному циклу продукта Майкрософт. На **диаграмме Конец службы** перечислены все версии операционной системы, которые не являются последней версией, и подсчитывается количество устройств для каждой версии. Эта диаграмма поможет определить, сколько устройств необходимо для установки последнего обновления компонентов операционной системы. Если вы сейчас развертываете обновления

компонентов на этих устройствах, на диаграмме также можно получить представление о ходе развертывания.



Дальнейшие действия

Используйте отчеты клиентский компонент Центра обновления Windows для бизнеса для отображения дополнительных данных о состоянии обновлений Windows.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Использование отчетов клиентский компонент Центра обновления Windows для бизнеса

Статья • 18.03.2023

(Применимо к: Windows 11 & Windows 10)

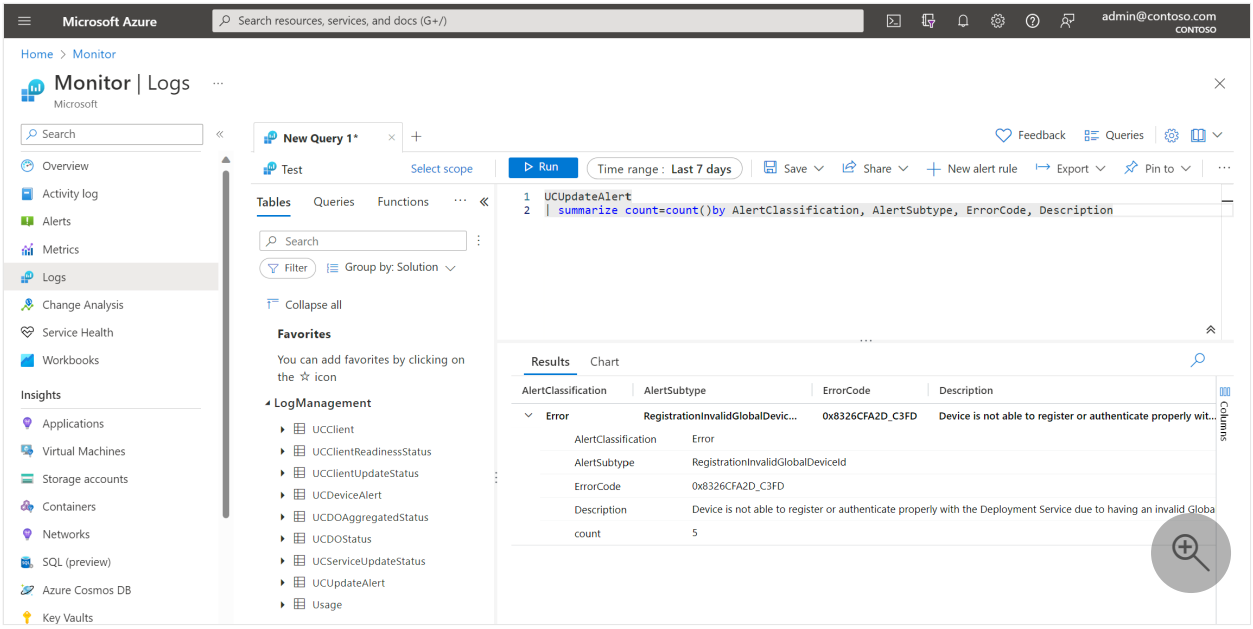
В этой статье вы узнаете, как использовать отчеты клиентский компонент Центра обновления Windows для бизнеса для мониторинга обновлений Windows для ваших устройств. Сведения о настройке среды для использования с отчетами клиентский компонент Центра обновления Windows для бизнеса см. в статье Включение отчетов клиентский компонент Центра обновления Windows для бизнеса.

Отображение данных отчетов клиентский компонент Центра обновления Windows для бизнеса

1. Войдите в портал Azure.
2. В портал Azure введите **Log Analytics** в строке поиска. Когда вы начнете вводить текст, список фильтруется на основе ваших входных данных.
3. Выберите **Рабочие области Log Analytics**.
4. Выберите рабочую область, используемую для отчетов клиентский компонент Центра обновления Windows для бизнеса.
5. Выберите **Журналы** в группе **Общие** в рабочей области.
6. Если в Log Analytics включен параметр **Всегда показывать запросы** , закройте окно запроса, чтобы получить доступ к схеме.
7. В разделе **Схемы и фильтр** выберите **Группировать по: Решение** , а затем разверните схему **Управления журналами** . Если выбран параметр **Группировать по категории** , схема отображается в категории **Другие** .
8. Используйте схему отчетов клиентский компонент Центра обновления Windows для бизнеса для пользовательских запросов Kusto (KQL), для создания пользовательских книг или создания собственного решения для отображения данных отчетов клиентский компонент Центра обновления Windows для бизнеса. Например, можно запросить данные, чтобы просмотреть сведения о различных типах оповещений за последние 7 дней и сколько раз возникало каждое оповещение.

Kusto

```
UCUpdateAlert
| summarize count=count() by AlertClassification, AlertSubtype, ErrorCode,
Description
```



Задержка данных

Отчеты клиентский компонент Центра обновления Windows для бизнеса используют диагностические данные клиента Windows в качестве источника данных. После добавления отчетов клиентский компонент Центра обновления Windows для бизнеса и соответствующей настройки устройств может потребоваться 48–72 часа.

Отчеты клиентский компонент Центра обновления Windows для бизнеса обновляются каждые 24 часа и обновляются с помощью последних данных со всех устройств вашей организации, которые были замечены за последние 28 дней. Весь набор данных обновляется в каждой ежедневной snapshot, что означает, что одни и те же данные могут приниматься снова, даже если с устройства с последнего snapshot не поступало новых данных. Время создания моментального снимка можно определить по полю TimeGenerated для каждой записи, в то время как LastScan можно использовать для приблизительного определения актуальности данных каждой записи. Подключение устройства к Интернету и, как правило, его активность влияет на то, сколько времени потребуется, прежде чем оно появится в отчетах клиентский компонент Центра обновления Windows для бизнеса.

Тип данных	Скорость передачи данных с устройства	Задержка данных

Тип данных	Скорость передачи данных с устройства	Задержка данных
UCClient	Один раз в день	4 часа
UCClientUpdateStatus	Каждое событие обновления (скачивание, установка и т. д.)	24–36 часов
UCServiceUpdateStatus	Каждое событие обновления (скачивание, установка и т. д.)	24–36 часов
UCUpdateAlert	Каждое событие	24–36 часов
UCDeviceAlert	Каждое событие	24–36 часов
UCClientReadinessStatus	После Windows 11 оценки готовности	24–36 часов
UCDOStatus	События скачивания	24–36 часов
UCDOAggregatedStatus	События скачивания	24–36 часов

Работа с журналами Azure Monitor

Отчеты клиентский компонент Центра обновления Windows для бизнеса основаны на платформе журналов Azure Monitor. Все данные, связанные с отчетами клиентский компонент Центра обновления Windows для бизнеса, собираются в рабочей области Log Analytics, где данные доступны для запросов. Понимание доступных в вашем распоряжении средств и функций журналов Azure Monitor, интегрированных в портал Azure, может значительно улучшить ваши возможности и дополнить клиентский компонент Центра обновления Windows отчетов для бизнеса.

Сведения о том, как это сделать, см. в следующих статьях журналов Azure Monitor:

- Эффективно запрашивать данные журнала в журналах Azure Monitor.
- Создание панелей мониторинга данных и совместное использование их в рабочей области Log Analytics.
- Настройте оповещения в Azure Monitor , чтобы всегда быть в курсе критически важных проблем, которые вас больше всего волнуют.

Часто задаваемые вопросы об отчетах клиентский компонент Центра обновления Windows для бизнеса

В этой статье приведены ответы на часто задаваемые вопросы об отчетах клиентский компонент Центра обновления Windows для бизнеса.

Общие вопросы:

- Что такое клиентский компонент Центра обновления Windows отчетов для бизнеса?
- Являются ли отчеты клиентский компонент Центра обновления Windows для бизнеса бесплатными?
- Какие версии Windows поддерживаются?

Вопросы по настройке:

- Как настроить отчеты клиентский компонент Центра обновления Windows для бизнеса?
- Почему на странице отображается сообщение "Ожидание данных отчетов клиентский компонент Центра обновления Windows для бизнеса"
- Почему появляется сообщение об ошибке "400 Bad Request: The указанный ресурс уже существует"?

Вопросы об использовании отчетов клиентский компонент Центра обновления Windows для бизнеса:

- Почему имя устройства имеет значение null(#)?
- Почему в отчетах отсутствуют устройства?
- В чем разница между версией ОС и целевой версией?
- Почему существует несколько записей для одного устройства?
- Почему на устройствах отображается неизвестное состояние?
- Когда следует использовать таблицы UCClient, UCClientUpdateStatus или UCUpdateAlert?
- В чем разница между исправлениями и обновлениями для системы безопасности?
- Разделы справки убедиться, что устройства отправляют данные?
- Почему книга не отображает данные, даже если в таблице UCClient есть данные?

Данные оптимизации доставки.

- Какой период времени включает данные оптимизации доставки?
- Данные отображаются как "Неизвестные", что это означает?
- Как определяются группы "Топ-10"?

- Идентификаторы GroupID не выглядят знакомыми, почему они отличаются?
- Как просмотреть данные для устройства в офисе и вне офиса?
- Что представляют данные в таблице UCDOStatus?
- Что представляют данные в таблице UCDOAggregatedStatus?
- Как вычисляется BytesFromCache при наличии сервера подключенного кэша, используемого поставщиком услуг Интернета?
- Как результаты командлетов PowerShell для оптимизации доставки сравниваются с результатами в отчете?
- Отчет представляет данные за последние 28 дней. Почему некоторые запросы включают >= семь дней?

Общее

Что такое клиентский компонент Центра обновления Windows отчетов для бизнеса?

Отчеты клиентский компонент Центра обновления Windows для бизнеса — это облачное решение, которое предоставляет сведения о соответствии Microsoft Entra присоединенных устройств обновлениям Windows. Отчеты клиентский компонент Центра обновления Windows для бизнеса предлагаются через портал Azure и включены в состав Windows 10 или Windows 11 необходимых лицензий.

Являются ли отчеты клиентский компонент Центра обновления Windows для бизнеса бесплатными?

Данные, передаваемые в рабочую область Log Analytics, могут храниться бесплатно в течение первых 31 дней (или 90 дней, если в рабочей области включена Microsoft Sentinel). Данные, передаваемые в Application Insights(классическая или рабочая область), хранятся в течение 90 дней без каких-либо затрат. За данные, сохраненные за эти безвозмездные периоды, взимается плата за каждый ГБ данных, сохраненных в течение месяца, с пропорциональной оценкой ежедневно. Дополнительные сведения см. в разделе **Хранение данных журнала** в ценах на Azure Monitor.

Какие версии Windows поддерживаются?

Отчеты клиентский компонент Центра обновления Windows для бизнеса поддерживают клиенты с поддерживаемой версией многосеансового выпуска Windows 10 или Windows 11 Professional, Education, Enterprise и Enterprise. Отчеты клиентский компонент Центра

обновления Windows для бизнеса предоставляют данные только для стандартной версии клиента Windows для настольных компьютеров и в настоящее время несовместимы с Windows Server, Surface Hub, IoT или другими версиями.

> ⓘ **Внимание**
>
> В настоящее время существует известная проблема, из-за которой клиентский компонент Центра обновления Windows отчеты для бизнеса не отображают данные для корпоративных устройств с несколькими сеансами.

Вопросы по настройке

Как настроить отчеты клиентский компонент Центра обновления Windows для бизнеса?

Убедившись, что предварительные требования выполнены, можно приступить к настройке отчетов клиентский компонент Центра обновления Windows для бизнеса. Ниже приведены два main шага по настройке отчетов клиентский компонент Центра обновления Windows для бизнеса.

1. Добавьте отчеты клиентский компонент Центра обновления Windows для бизнеса в подписку Azure. Этот шаг состоит из следующих этапов:
2. Выберите или создайте рабочую область Log Analytics для использования с отчетами клиентский компонент Центра обновления Windows для бизнеса.
3. Зарегистрируйтесь в отчетах клиентский компонент Центра обновления Windows для бизнеса с помощью одного из следующих методов:

- Регистрация с помощью книги Azure (предпочтительный метод) — регистрация из Центр администрирования Microsoft 365.

1. Настройте клиенты для отправки данных в отчеты клиентский компонент Центра обновления Windows для бизнеса. Клиенты можно настроить следующими тремя способами:

    - Использование скрипта
    - Использование Microsoft Intune
    - Настройка вручную

Почему на странице отображается сообщение "Ожидание клиентский компонент Центра

обновления Windows данных отчетов для бизнеса"?

Как правило, сообщение **"Ожидание клиентский компонент Центра обновления Windows для бизнеса"** отображается по следующим причинам:

- Возможно, у вас нет правильных разрешений на отображение данных.
- Начальная регистрация может быть еще не завершена.
- Возможно, устройства не обмен данными. Если вы получили сообщение об успешном сохранении во время регистрации, но по-прежнему не видели никаких данных через 48 часов, попробуйте использовать сценарий конфигурации на устройствах, чтобы убедиться, что они настроены правильно. Если вы проверили указанные выше элементы, но по-прежнему не видите данные, вы можете отменить регистрацию, а затем повторно зарегистрироваться. Однако регистрация занимает еще 24–48 часов. Если проблема не исчезнет, обратитесь в службу поддержки.

Почему появляется сообщение об ошибке "400 Bad Request: The указанный ресурс уже существует"?

Сообщение `400 Bad Request: The specified resource already exists` об ошибке указывает, что в службе уже сохранена подписка и сопоставление рабочей области. Если вы пытаетесь повторно зарегистрироваться с теми же параметрами конфигурации, подождите несколько минут, а затем обновите страницу, прежде чем снова сохранить подписку и рабочую область. Иногда для регистрации сохранения может потребоваться время, поэтому важно не выполнять повторную регистрацию слишком быстро.

Использование отчетов клиентский компонент Центра обновления Windows для бизнеса

Почему имя устройства имеет значение null(#)?

Если вы видите идентификатор устройства, но не имя устройства, возможно, что необходимая политика для отображения имени устройства не задана на клиенте. Убедитесь, что на клиентах настроена политика.

- CSP: System/AllowDeviceNameInDiagnosticData

- групповая политика: разрешить отправку имени устройства в диагностических данных Windows
  - Находится в **разделе Конфигурация**> компьютера**Административные шаблоны**>**Компоненты**> Windows**Сбор данных и Предварительные сборки**. Отображение всех имен устройств в отчетах может занять до 21 дня при условии, что они включено и активно.

Почему в отчетах отсутствуют устройства?

Ниже приведены некоторые причины, по которым устройства могут не отображаться в отчетах.

- **Устройство не зарегистрировано с помощью Microsoft Entra**. Для устройств необходимо Microsoft Entra присоединение или гибридное присоединение Microsoft Entra.
- **Устройство не отправляет данные**. Возможно, устройства не обмениваются данными из-за неправильно настроенной политики или конфигурации прокси-сервера или брандмауэра. Попробуйте использовать скрипт конфигурации на устройствах, чтобы убедиться, что они настроены правильно.
- **Устройство недостаточно активно**: клиенты должны быть активными и подключены к Интернету для проверки на наличие Центра обновления Майкрософт. Убедитесь, что устройства включены и были активны по крайней мере один раз за последние 28 дней.
- **Книга имеет ограниченные результаты**: по умолчанию для строк в книгах Azure установлено ограничение в 1000. Это ограничение позволяет избежать задержки во время загрузки интерфейса. Если вы заметили, что не можете найти определенное устройство, можно экспортировать выходные данные в Excel или открыть результаты в представлении журналов для полного результата, выбрав три точки рядом с каждым компонентом.

Почему существует несколько записей для одного устройства?

Устройства имеют несколько записей при запросе к таблицам `UCClientUpdateStatus` или `UCClientServiceStatus` . Эти таблицы содержат несколько записей, так как они содержат журнал для всех устройств, на которых за последние 28 дней обнаружены применимые обновления. Например, в течение последних 28 дней устройство обнаружило несколько обновлений для системы безопасности, каждое из которых имеет разные состояния обновления. Также возможно, что устройство может находиться в нескольких развертываниях, поэтому отображается несколько записей.

Почему на устройствах отображается неизвестное состояние?

Если для устройства нет записи обновления, отображается неизвестное состояние клиента. Это состояние может произойти по многим причинам, например, устройство неактивно, не может проверить клиентский компонент Центра обновления Windows или в настоящее время не выполняет никаких действий, связанных с обновлением.

В чем разница между версией ОС и целевой версией?

Слово *target* в метках данных ссылается на версию обновления, сборку или базу знаний, которые клиент планирует обновить. Как правило, поля, начиная с *ОС*, такие как OSbuild и OSversion, представляют, что в настоящее время работает на устройстве.

Когда следует использовать таблицы UCClient, UCClientUpdateStatus или UCUpdateAlert?

Эти таблицы можно использовать для получения следующих сведений:

- **UCClient**: представляет запись отдельного устройства. Он содержит такие данные, как имя устройства, установленная в настоящее время сборка и выпуск OS Edition. Каждое устройство имеет одну запись в этой таблице. Используйте эту таблицу, чтобы получить общее состояние соответствия устройств.
  - Чтобы отобразить сведения о конкретном устройстве по Microsoft Entra идентификатору устройства, выполните следующие действия:
    `UCClient where AzureADDeviceId contains "01234567-89ab-cdef-0123-456789abcdef"`
  - Чтобы отобразить все записи устройств с любой версией ОС Windows 11, выполните следующие действия:
    `UCClient | where OSVersion contains "Windows 11"`

- **UCClientUpdateStatus**: содержит записи для каждого обновления, которое устройство определило, применимо. Если за последние 60 дней было обнаружено несколько применимых обновлений для устройства, может быть несколько записей. Используйте эту таблицу, если вы хотите получить подробные сведения о состоянии обновления для активных развертываний. Как правило, для последних 3 обновлений системы безопасности на каждое устройство будет 3 записи о состоянии обновления.
  - Чтобы найти записи устройств, которые определили применимо обновление от 14 марта 2023 г., выполните следующие действия:

`UCClientUpdateStatus | where UpdateCategory =="WindowsQualityUpdate" and UpdateReleaseTime == "3/14/2023"`

  - Чтобы отобразить устройства, которые находятся в подсостояние перезапуска, выполните следующие действия: `UCClientUpdateStatus |where ClientSubstate =="RestartRequired"`

- **UCUpdateAlert**. Используйте эту таблицу, чтобы понять сбои обновлений и действовать на устройствах с помощью рекомендаций по оповещениям. Эта таблица содержит сведения, которые требуют внимания относительно одного устройства, одного обновления и одного развертывания (если это необходимо).
  - Чтобы отобразить сведения о коде ошибки, выполните следующие действия: `UCUpdateAlert|where ErrorCode =="0X8024000b"`
  - Чтобы отобразить количество устройств с активными оповещениями по подтипам, выполните следующие действия: `UCUpdateAlert |where AlertStatus =="Active"|summarize Devices=count() by AlertSubtype`

В чем разница между исправлениями и обновлениями для системы безопасности?

Обновления качества Windows — это ежемесячные обновления, выпущенные во второй или четвертый вторник месяца. Накопительные обновления, выпущенные во второй вторник месяца, могут содержать обновления для системы безопасности и обновления, не связанные с безопасностью. Накопительные обновления, выпущенные в четвертый вторник месяца, являются необязательными предварительными выпусками без безопасности. Используйте поля в таблице UCClient для получения дополнительных сведений, таких как:

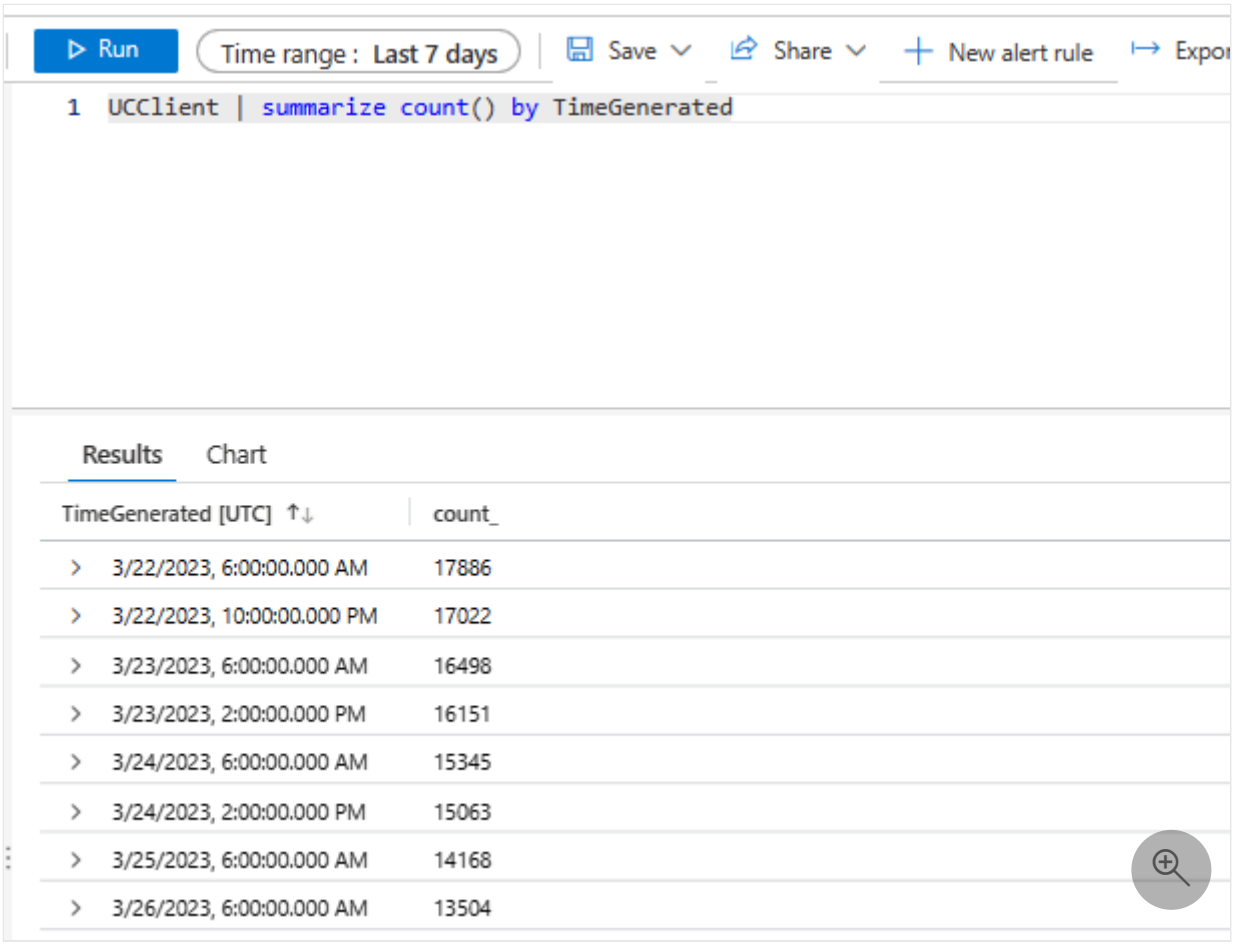
- **OSSecurityUpdateStatus**: указывает состояние ежемесячного обновления, выпущенного во второй вторник.
- **OSQualityUpdateStatus**: указывает состояние ежемесячного обновления, выпущенного в четвертый вторник.

Разделы справки убедиться, что устройства отправляют данные?

После завершения регистрации и правильной настройки устройств для совместного использования данных подождите 48 часов, пока данные начнут отображаться в отчетах. Отображение всех устройств в отчетах может занять до 14 дней в некоторых случаях, когда устройства не активны. Вы можете проверка, чтобы узнать, заполняются ли таблицы Log Analytics в рабочей области. Данные ежедневно подается службой для

создания отчетов. Если вы заметили, что день отсутствует, возможно, служба отчетов пропустила прием. Чтобы убедиться, что устройства отправляют данные, запроситетаблицу UCClient. В следующем запросе показано общее количество зарегистрированных устройств за время создания:

```
UCClient | summarize count() by TimeGenerated
```



Почему книга не отображает данные, даже если в таблице UCClient есть данные?

Если таблица UCClient содержит данные, но книга не отображает данные, убедитесь, что у пользователя есть правильные разрешения на чтение данных. Роль читателя Log Analytics необходима для просмотра данных в книгах. Роль Участника Log Analytics необходима для внесения любых изменений в запросы и книги.

Данные оптимизации доставки

Какой период времени включает данные оптимизации доставки?

Данные агрегируются за последние 28 дней для активных устройств.

Данные отображаются как "Неизвестные", что это означает?

Данные могут отображаться в отчете как "Неизвестные". Это состояние указывает, что параметр DownloadMode оптимизации доставки является недопустимым или пустым.

Как определяются группы "Топ-10"?

Верхние группы представлены количеством устройств в определенной группе для любого из четырех типов групп (GroupID, City, Country и ISP).

Идентификаторы GroupID не выглядят знакомыми, почему они отличаются?

Значения GroupID кодируются в соответствии с требованиями к защите данных. Дополнительные сведения см. в разделе Сопоставление идентификаторов групп.

Как просмотреть данные для устройства в офисе и вне офиса?

Сегодня у нас нет различий для данных, скачанных по расположению.

Что представляют данные в таблице UCDOStatus?

Строка в UCDOStatus представляет данные, скачанные сочетанием одного идентификатора устройства (AzureADDeviceId) по типу контента (ContentType).

Что представляют данные в таблице UCDOAggregatedStatus?

Строка в UCDOAggregatedStatus представляет данные, суммированные на уровне клиента (AzureADTenantID) для каждого типа контента (ContentType).

Как вычисляется BytesFromCache при наличии сервера подключенного кэша, используемого поставщиком услуг Интернета?

Если есть сервер подключенного кэша на уровне поставщика услуг Интернета, BytesFromCache отфильтровывает все байты, поступающие в подключенный кэш поставщика услуг Интернета.

Как результаты командлетов PowerShell для оптимизации доставки сравниваются с результатами в отчете?

Командлеты PowerShell для оптимизации доставки могут быть мощным инструментом, используемым для мониторинга данных оптимизации доставки на устройстве. Эти командлеты используют кэш на устройстве. Данные, вычисляемые в отчете, берутся из событий оптимизации доставки.

Отчет представляет данные за последние 28 дней. Почему некоторые запросы включают >= семь дней?

Данные в отчете представляют данные за последние 28 дней. Запрос за последние семь дней предназначен только для получения данных за последние snapshot за последние семь дней. Возможно, данные задерживаются на некоторое время и недоступны для текущего дня, поэтому мы ищем последние семь дней snapshot в аналитике журналов и показываем последние snapshot.

отзывы, поддержка и устранение неполадок в отчетах клиентский компонент Центра обновления Windows для бизнеса

Статья • 20.11.2024 • Применяется к: ✅ Windows 11, ✅ Windows 10

Существует несколько ресурсов, которые можно использовать для поиска справки по отчетам клиентский компонент Центра обновления Windows для бизнеса. Если вы только начинаете работу или опытный администратор, используйте следующие ресурсы, когда вам нужна помощь с отчетами клиентский компонент Центра обновления Windows для бизнеса:

- Отправка отзывов о продуктах об отчетах клиентский компонент Центра обновления Windows для бизнеса
- Открыть обращение в службу поддержки Майкрософт
- Отзывы о документации
- Следите за блогом Windows IT Pro, чтобы узнать о предстоящих изменениях в отчетах клиентский компонент Центра обновления Windows для бизнеса
- Использование Microsoft Q&A для получения вопросов о продукте

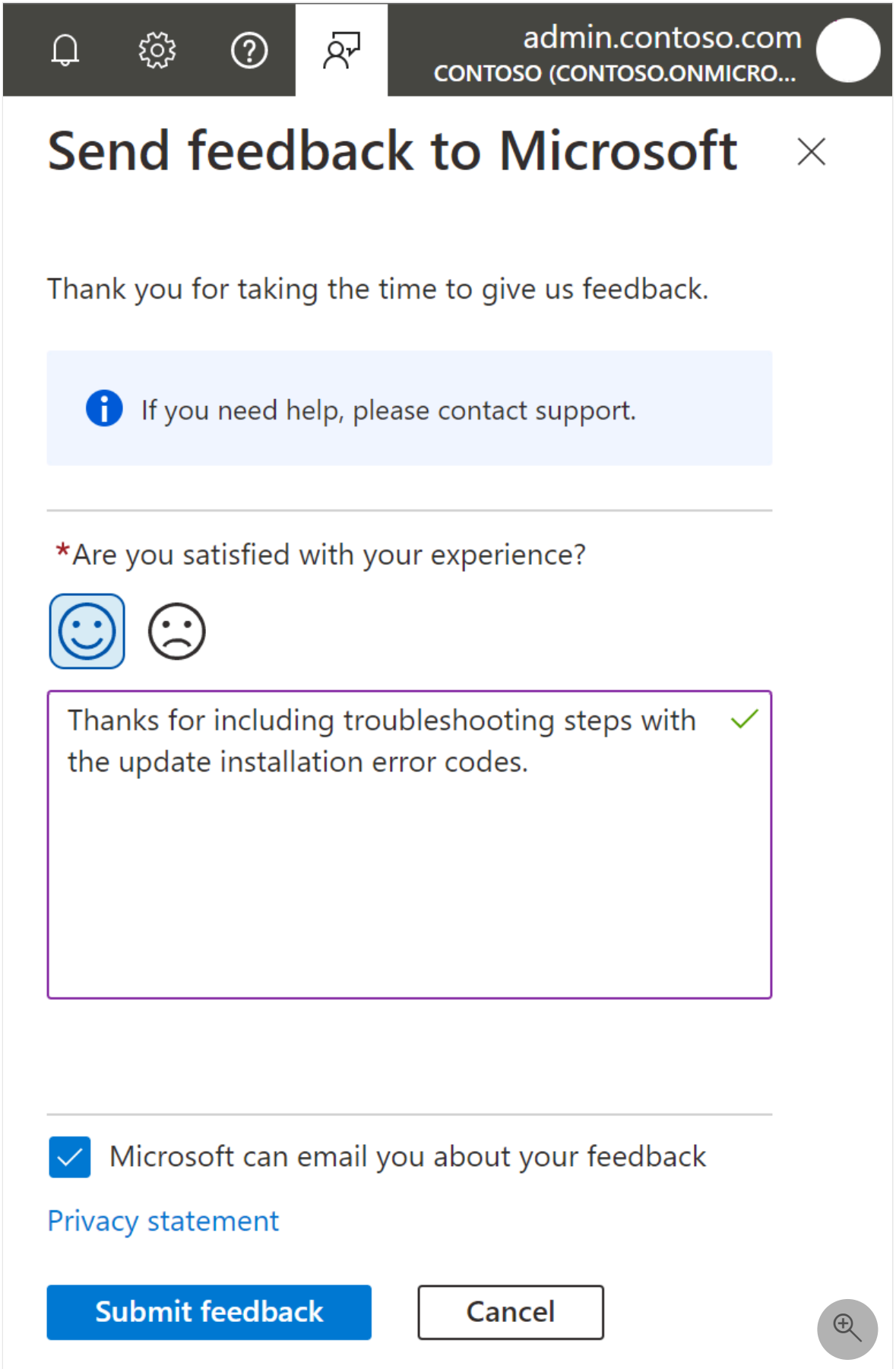
Отправка отзывов о продукте

Используйте вариант обратной связи о продукте, чтобы предложить предложения по новым функциям и функциям или предложить изменения в текущих клиентский компонент Центра обновления Windows функций отчетов для бизнеса. Вы можете предоставить отзыв непосредственно группе продуктов отчетов клиентский компонент Центра обновления Windows для бизнеса. Чтобы предоставить отзыв о продукте, выполните следующие действия.

1. В правом верхнем углу портал Azure щелкните значок обратной связи.
2. Выберите улыбку или нахмуренный, чтобы оценить ваше удовлетворение от вашего опыта.
3. В текстовом поле опишите, что вам понравилось или что не понравилось. Предоставляя отзыв о проблеме, обязательно включите в описание

достаточно подробных сведений, чтобы ее можно было правильно определить в группе продуктов.

4. Выберите, хотите ли вы разрешить корпорации Майкрософт отправлять вам сообщения о вашем отзыве.
5. Выберите **Отправить отзыв** после заполнения формы обратной связи.



Открыть обращение в службу поддержки Майкрософт

Запросы на поддержку можно открывать непосредственно из портал Azure. Если страница **Справка и поддержка** не отображается, убедитесь, что у вас есть доступ к открытию запросов на поддержку. Дополнительные сведения об элементах управления доступом на основе ролей для запросов на поддержку см. в статье Создание запроса на поддержка Azure. Чтобы создать новый запрос на поддержку для отчетов клиентский компонент Центра обновления Windows для бизнеса, выполните приведенные далее действия.

1. Откройте страницу **Справка и поддержка** из следующих расположений:

- Во всплывающем окне Отправить отзыв о продукте выберите ссылку **контактная служба поддержки** .
- В портал Azure выберите **Новый запрос на поддержку** в разделе **Поддержка и устранение неполадок**.

1. Выберите **Создать запрос на поддержку**, чтобы открыть новую страницу запроса на поддержку.

2. На вкладке **Описание проблемы** укажите сведения о проблеме. Для обеспечения того, чтобы инженер отчетов клиентский компонент Центра обновления Windows для бизнеса получил ваш запрос на поддержку, следует использовать следующие ***пункты курсивным курсивом***:

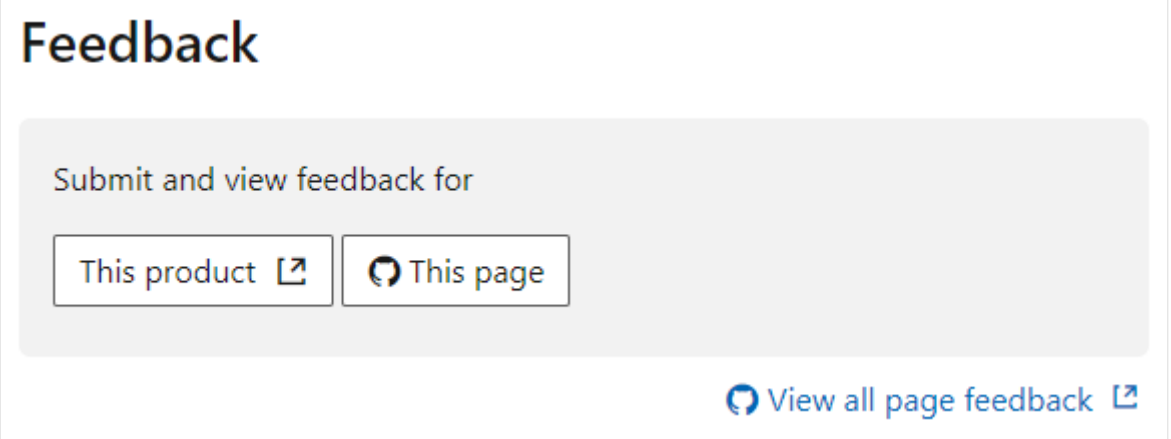
    - **Сводка** — краткое описание проблемы
    - **Тип** - проблемы***Технический***
    - **Подписка** — выберите подписку, используемую для отчетов клиентский компонент Центра обновления Windows для бизнеса.
    - **Служба** - ***Мои службы***
    - **Тип службы**— выберите ***отчеты клиентский компонент Центра обновления Windows для бизнеса*** в разделе ***Мониторинг и управление.***

3. На основе предоставленных сведений отображаются рекомендуемые **решения** , которые можно использовать для устранения проблемы.

4. Перейдите на вкладку **Дополнительные сведения** и создайте запрос на вкладке **Просмотр и создание** .

Отзывы о документации

Щелкните ссылку **Отзыв** в правом верхнем углу любой статьи, чтобы перейти к разделу Отзывы внизу. Обратная связь интегрирована с GitHub Issues. Дополнительные сведения об интеграции с GitHub Issues см. в записи блога платформы документации.



Чтобы поделиться отзывом о текущей статье, выберите **Эта страница**. Учетная запись GitHub является необходимым условием для предоставления отзывов по документации. После входа в систему вы получите одноразовую авторизацию для организации MicrosoftDocs. Затем откроется форма новой проблемы GitHub. Добавьте описательное название и подробный отзыв в текст, но не изменяйте раздел сведений о документе. Затем выберите **Отправить новую проблему** , чтобы отправить новую проблему для целевой статьи в репозитории GitHub Windows-ITPro-docs.

Чтобы узнать, есть ли отзыв по этой статье, выберите **Просмотреть все отзывы о странице**. Это действие открывает запрос проблемы GitHub для этой статьи. По умолчанию отображаются как открытые, так и закрытые проблемы. Просмотрите все существующие отзывы, прежде чем отправлять новую проблему. Если вы обнаружили связанную проблему, щелкните значок лица, чтобы добавить реакцию, добавить комментарий в поток или **подписаться на** получение уведомлений.

Используйте GitHub Issues для отправки отзывов следующих типов:

- Ошибка в документации: содержимое устарело, неясно, запутано или неработано.
- Улучшение документации. Предложение по улучшению статьи.
- Вопрос документации. Вам нужна помощь с поиском существующей документации.
- Идея документа: предложение для новой статьи.
- Kudos: положительный отзыв о полезной или информативной статье.
- Локализация: отзыв о переводе содержимого.

- Оптимизация поисковой системы (SEO): отзывы о проблемах с поиском контента. Включите поисковую систему, ключевые слова и целевую статью в комментарии.

Если вы создаете проблему для чего-то, не связанного с документацией, корпорация Майкрософт закроет ее и перенаправит вас на более качественный канал отзывов. Пример:

- Отзывы о продуктах для отчетов клиентский компонент Центра обновления Windows для бизнеса
- Вопросы о продукте (с помощью Microsoft Q&A)
- Запросы на поддержку для отчетов клиентский компонент Центра обновления Windows для бизнеса

Чтобы поделиться отзывами о платформе Microsoft Learn, ознакомьтесь с отзывами о Microsoft Learn. Платформа включает все компоненты оболочки, такие как заголовок, оглавление и правое меню. Кроме того, как статьи отображаются в браузере, например шрифт, поля оповещений и привязки страницы.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Схема отчетов клиентский компонент Центра обновления Windows для бизнеса

Статья • 06.12.2023 • Применяется к: ✅ Windows 11, ✅ Windows 10

Если визуализации, предоставляемые в интерфейсе по умолчанию, не соответствуют вашим потребностям в отчетах или если вам нужно устранить проблемы с устройствами, полезно понимать схему отчетов клиентский компонент Центра обновления Windows для бизнеса и иметь общее представление о возможностях запросов журналов Azure Monitor. для включения дополнительных панелей мониторинга, интеграции с внешними средствами анализа данных, автоматического оповещения и многого другого.

Схемы для отчетов клиентский компонент Центра обновления Windows для бизнеса

В следующей таблице перечислены различные таблицы, которые являются частью решения отчетов клиентский компонент Центра обновления Windows для бизнеса. Сведения о том, как перемещаться по журналам Azure Monitor для поиска этих данных, см. в статье Начало работы с запросами журналов в Azure Monitor.

> **Примечание**
>
> Данные собираются ежедневно. В поле TimeGenerated отображается время сбора данных. Он добавляется Log Analytics при сборе данных. Данные устройства за последние 28 дней собираются, даже если с момента последнего времени не было создано никаких новых данных. LastScan — это более четкий индикатор актуальности данных (то есть время последнего обновления значений), в то время как TimeGenerated указывает на актуальность данных в Log Analytics.

Expand table

Table	Категория	Описание
UCClient	Запись устройства	UCClient выступает в качестве записи отдельного устройства. Он содержит такие данные, как установленная сборка, имя устройства, выпуск

Table	Категория	Описание
		операционной системы и часы активности (количественные).
UCClientReadinessStatus	Запись устройства	UCClientReadinessStatus — это запись отдельного устройства о готовности к обновлению до Windows 11. Если устройство не поддерживает работу Windows 11, в записи указаны Windows 11 требования к оборудованию, которым устройство не соответствует.
UCClientUpdateStatus	Запись устройства	Событие обновления, объединяющее последние данные на основе клиента с последними данными на основе службы, чтобы создать полную картину для одного устройства (клиента) и одного обновления.
UCDeviceAlert	Запись службы и устройства	Эти оповещения активируются в результате проблемы, которая связана с устройством. Это не зависит от сочетания конкретного обновления и определенного устройства. Как и UpdateAlerts, alertType указывает, откуда поступает оповещение, например ServiceDeviceAlert или ClientDeviceAlert.
UCDOAggregatedStatus	Запись устройства	UCDOAggregatedStatus — это агрегат всех отдельных записей UDDOStatus в клиенте и суммирует экономию пропускной способности на всех устройствах, зарегистрированных с помощью оптимизации доставки и подключенного кэша Майкрософт.
UCDOStatus	Запись устройства	UCDOStatus предоставляет сведения об использовании пропускной способности для одного устройства в разных типах контента в случае использования оптимизации доставки и подключенного кэша Майкрософт.
UCServiceUpdateStatus	Запись службы	Событие обновления, которое поступает непосредственно на стороне службы. Событие содержит только сведения на стороне службы для одного устройства (клиента) и одно обновление в одном развертывании.
UCUpdateAlert	Записи служб и устройств	Оповещение об обновлении клиента и службы. Содержит сведения, которые требуют внимания относительно одного устройства (клиента), одного обновления и одного развертывания, если это необходимо. Некоторые поля могут быть пустыми в зависимости от поля AlertType UpdateAlert. Например, ServiceUpdateAlert не обязательно будет

Table	Категория	Описание
		содержать состояния на стороне клиента и может быть пустым.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

UCClient

Статья • 15.10.2024 • Применяется к: ✅ Windows 11, ✅ Windows 10

UCClient выступает в качестве записи отдельного устройства. Он содержит такие данные, как установленная сборка, имя устройства, выпуск ОС и часы активности (количественные).

Схема для UCClient

Развернуть таблицу

Поле	Тип	Перечислимый тип	Пример	Описание
AzureADDeviceID	струна	Нет	`71db1a1a-f1a6-4a25-b88f-79c2f513dae0`	Microsoft Entra идентификатор устройства
AzureADTenantId	струна	Нет	`69ca04b0-703d-4b3a-9184-c4e3c15d6f5e`	идентификатор клиента Microsoft Entra
Город	струна	Нет		В настоящее время данные не собираются для заполнения этого поля. Город устройства, основанный на IP-адресе.
Страна	струна	Нет	`US`	Последнее зарегистрированное расположение устройства (страна или регион) на основе IP-адреса. Отображается как код страны.
DeviceFamily	струна	Нет	`PC, Phone`	Семейство устройств, например КОМПЬЮТЕР, Телефон.
DeviceFormFactor	струна	Нет	`Notebook, Desktop, Phone.`	В настоящее время данные не собираются для заполнения этого поля. Форм-фактор устройства
DeviceManufacturer	струна	Нет	`Hewlett-Packard.`	В настоящее время данные не собираются для заполнения этого поля. Изготовитель oem устройства
DeviceModel	струна	Нет	`The device's OEM model`	В настоящее время данные не собираются для заполнения этого поля. Модель oem устройства
DeviceName	струна	Нет	`JohnPC-Contoso`	Имя устройства, предоставленное клиентом
GlobalDeviceId	струна	Нет	`g:9832741921341`	Глобальный идентификатор устройства
IsVirtual	bool	Нет	`Yes, No`	Указывает, является ли устройство виртуальным устройством.
LastCensusScanTime [UTC]	datetime	Нет	`2020-05-14 09:26:03.478039`	Последний раз, когда это устройство выполняло успешное сканирование переписи, если таковое имеется.
LastWUScanTime [UTC]	datetime	Нет	`2020-05-14 09:26:03.478039`	В последний раз, когда это устройство успешно выполняло проверку клиентский компонент Центра обновления Windows, если таковое имеется.
OSArchitecture	струна	Да	`x86`	Архитектура операционной системы (а не устройства) на этом устройстве в данный момент включена.
OSBuild	струна	Нет	`10.0.22621.1702`	Полная сборка операционной системы, установленная на этом

Поле	Тип	Перечислимый тип	Пример	Описание
				устройстве, например Major.Minor.Build.Revision
OSBuildNumber	int	Нет	`22621`	Основной номер сборки в формате int, который использует устройство.
OSEdition	струна	Да	`Professional`	Выпуск Windows
OSFeatureUpdateComplianceStatus	струна	Да	`Compliant`	Указывает, находится ли устройство в последнем обновлении функций, доступном из автопаттинга Windows, в противном случае — NotApplicable.
OSFeatureUpdateEOSTime [UTC]	datetime	Нет	`2020-05-14 09:26:03.478039`	Дата окончания обслуживания обновления компонентов, установленного на устройстве.
OSFeatureUpdateReleaseTime [UTC]	datetime	Нет	`2020-05-14 09:26:03.478039`	Дата выпуска обновления компонентов, установленного на устройстве.
OSFeatureUpdateStatus	струна	Да	`InService;EndOfService`	Указывает, находится ли устройство в последнем доступном обновлении компонентов для обновления компонентов.
OSQualityUpdateComplianceStatus	струна	Да	`NotCompliant`	Указывает, находится ли устройство в последнем обновлении качества, доступном из автоматического исправления Windows, в противном случае — NotApplicable.
OSQualityUpdateReleaseTime [UTC]	datetime	Нет	`2020-05-14 09:26:03.478039`	Дата выпуска обновления качества, установленного на устройстве.
OSQualityUpdateStatus	струна	Да	`Latest;NotLatest`	Указывает, находится ли устройство в последнем доступном обновлении качества для обновления компонентов.
OSRevisionNumber	int	Нет	`836`	Редакция в формате int, это устройство включено.
OSSecurityUpdateComplianceStatus	струна	Да	`NotCompliant`	Указывает, находится ли устройство в последнем обновлении для системы безопасности (обновление качества, где классификация=безопасность), которое предлагается из автоматического исправления Windows, в противном случае — NotApplicable.
OSSecurityUpdateStatus	струна	Да	`Latest;NotLatest;MultipleSecurityUpdatesMissing`	Указывает, установлена ли на устройстве последнее доступное обновление для системы безопасности для обновления компонентов.
OSServicingChannel	струна	Да	`SAC`	Выбранный Windows 10 канал обслуживания устройства.
OSVersion	струна	Нет	`1909`	Версия операционной системы Windows 10, установленная на устройстве, например 19H2, 20H1, 20H2.
PrimaryDiskFreeCapacityMb		Нет		В настоящее время данные не собираются для заполнения этого поля. Бесплатная емкость основного диска в мегабайтах.

Поле	Тип	Перечислимый тип	Пример	Описание
SCCMClientId	струна	Нет	`5AB72FAC-93AB-4954-9AB0-6557D0EFA245`	Configuration Manager идентификатор клиента, если он доступен.
SourceSystem	струна	Нет	`Azure`	
Идентификатор клиента	струна	Нет	`69ca04b0-703d-4b3a-9184-c4e3c15d6f5e`	Microsoft Entra идентификатор клиента устройства.
ВремяGenerated [UTC]	datetime	Нет	`2020-05-14 09:26:03.478039`	Время создания этой конкретной записи snapshot. Это поле предназначено для определения того, к какому пакету snapshot относится эта запись.
Тип	струна	Нет	`UCClient`	Тип сущности
UpdateConnectivityLevel		Да		В настоящее время данные не собираются для заполнения этого поля. Независимо от того, поддерживает ли это устройство достаточное совокупное и непрерывное подключение к клиентский компонент Центра обновления Windows, чтобы обновление двигалось оптимально.
WUAutomaticUpdates		Нет		В настоящее время данные не собираются для заполнения этого поля. Управление поведением автоматического обновления для сканирования, скачивания и установки обновлений.
WUDeadlineNoAutoRestart		Нет		В настоящее время данные не собираются для заполнения этого поля. Устройства не будут автоматически перезапускаться в нерабочее время, пока не будет достигнут крайний срок. По умолчанию это значение равно 1 и указывает, что включено, 0 указывает, что отключено.
WUDODownloadMode		Нет		В настоящее время данные не собираются для заполнения этого поля. Конфигурация клиентский компонент Центра обновления Windows DO DownloadMode.
WUFeatureDeadlineDays	int	Нет	`0`	CSP: ConfigureDeadlineForFeatureUpdates. Конфигурация крайнего срока обновления компонентов в днях. -1 указывает, что не настроено. 0 указывает, что настроено, но для параметра задано значение 0. Значения > 0 указывают крайний срок в днях.
WUFeatureDeferralDays	int	Нет	`0`	CSP: DeferFeatureUpdates. Конфигурация отсрочки обновления компонентов в днях. -1 указывает, что не настроено. 0 указывает, что настроено, но для параметра задано значение 0. Значения > 0 указывают параметр политики.
WUFeatureGracePeriodDays	int	Нет	`7`	Льготный период клиентский компонент Центра обновления Windows для обновления

Поле	Тип	Перечислимый тип	Пример	Описание
				компонентов в днях. -1 указывает, что не настроено. 0 указывает, что настроено и задано значение 0. Значения больше 0 указывают на льготный период в днях.
WUFeaturePauseEndTime [UTC]	datetime	Нет	`2020-05-14 09:26:03.478039`	В настоящее время данные не собираются для заполнения этого поля. Время, клиентский компонент Центра обновления Windows приостановки обновления компонентов, заканчивается, если активация, в противном случае значение NULL.
WUFeaturePauseStartTime [UTC]	datetime	Нет	`2020-05-14 09:26:03.478039`	В настоящее время данные не собираются для заполнения этого поля. Время активации клиентский компонент Центра обновления Windows приостановки обновления компонентов, в противном случае — значение NULL. Обновления компонентов приостанавливаются на 35 дней с указанной даты начала.
WUFeaturePauseState	струна	Нет	`NotConfigured`	Указывает состояние приостановки устройства для обновления компонентов. Возможные значения: Paused, NotPaused, NotConfigured.
WUNotificationLevel		Нет		В настоящее время данные не собираются для заполнения этого поля. Эта политика позволяет определить, какие клиентский компонент Центра обновления Windows уведомления видят пользователи. 0 (по умолчанию) — используйте уведомления по умолчанию клиентский компонент Центра обновления Windows. 1. Отключите все уведомления, за исключением предупреждений о перезапуске. 2. Отключение всех уведомлений, включая предупреждения о перезапуске
WUPauseUXDisabled		Нет		В настоящее время данные не собираются для заполнения этого поля. Эта политика позволяет ИТ-администратору отключить функцию приостановки Обновления. Если эта политика включена, пользователь не сможет получить доступ к функции приостановки обновлений. Поддерживаемые значения 0, 1.
WUQualityDeadlineDays	int	Нет	`7`	CSP: ConfigureDeadlineForQualityUpdates. Конфигурация крайнего срока обновления качества обновления Windows в днях. -1 указывает, что не настроено. 0 указывает, что настроено, но для параметра задано значение 0. Значения > 0 указывают крайний срок в днях.
WUQualityDeferralDays	int	Нет	`-1`	CSP: DeferQualityUpdates. Конфигурация отсрочки обновления клиентский компонент

Поле	Тип	Перечислимый тип	Пример	Описание
				Центра обновления Windows качества в днях. -1 указывает, что не настроено. 0 указывает, что настроено, но для параметра задано значение 0. Значения, превышающие 0, указывают на параметр политики.
WUQualityGracePeriodDays	int	Нет	`0`	Льготный период клиентский компонент Центра обновления Windows для обновления качества в днях. -1 указывает, что не настроено. 0 указывает, что настроено и задано значение 0. Значения больше 0 указывают на льготный период в днях.
WUQualityPauseEndTime [UTC]	datetime	Нет	`2020-05-14 09:26:03.478039`	В настоящее время данные не собираются для заполнения этого поля. Время окончания приостановки обновления качества, если она активирована, в противном случае значение NULL.
WUQualityPauseStartTime [UTC]	datetime	Нет	`2020-05-14 09:26:03.478039`	В настоящее время данные не собираются для заполнения этого поля. Время, клиентский компонент Центра обновления Windows приостановке обновления качества; если активировано; в противном случае — значение NULL.
WUQualityPauseState	струна	Нет	`NotConfigured`	Указывает состояние приостановки устройства для обновления качества. Возможные значения: Paused, NotPaused, NotConfigured.
WURestartNotification		Нет		В настоящее время данные не собираются для заполнения этого поля. Позволяет ИТ-администратору указать метод, с помощью которого автоматическое перезапуск необходимое уведомление будет отклонено. В следующем списке показаны поддерживаемые значения: 1 (по умолчанию) = Автоматическое закрытие. 2. Увольнение пользователя.
WUServiceURLConfigured		Нет		В настоящее время данные не собираются для заполнения этого поля. Устройство проверяет наличие обновлений в Центре обновления Майкрософт. Задайте URL-адрес, например http://abcd-srv:8530. Устройство проверяет наличие обновлений с сервера WSUS по указанному URL-адресу. Не настроено. Устройство проверяет наличие обновлений в Центре обновления Майкрософт. Задайте URL-адрес, например http://abcd-srv:8530. Устройство проверяет наличие обновлений с сервера WSUS по указанному URL-адресу.
WUUXDisabled		Нет		В настоящее время данные не собираются для заполнения этого поля. Эта политика позволяет ИТ-администратору удалять доступ к

Поле	Тип	Перечислимый тип	Пример	Описание
				проверке клиентский компонент Центра обновления Windows. Если эта политика включена, пользователь не сможет получить доступ к клиентский компонент Центра обновления Windows сканировать, скачивать и устанавливать компоненты. Значение по умолчанию — 0. Поддерживаемые значения 0, 1.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

UCClientReadinessStatus

Статья • 06.12.2023 • Применяется к: ✅ Windows 11, ✅ Windows 10

UCClientReadinessStatus — это запись отдельного устройства о готовности к обновлению до Windows 11. Если устройство не поддерживает работу Windows 11, в записи указаны Windows 11 требования к оборудованию, которым устройство не соответствует.

Схема для UCClientReadinessStatus

Expand table

Поле	Тип	Перечислимый тип	Пример	Описание
AzureADDeviceId	Строка	Нет	`71db1a1a-f1a6-4a25-b88f-79c2f513dae0`	Microsoft Entra идентификатор устройства
AzureADTenantId	Строка	Нет	`69ca04b0-703d-4b3a-9184-c4e3c15d6f5e`	идентификатор клиента Microsoft Entra
DeviceName	Строка	Нет	`JohnPC-Contoso`	Имя устройства, предоставленное клиентом
GlobalDeviceId	Строка	Нет	`g:9832741921341`	Глобальный идентификатор устройства.
OSBuild	Строка	Нет	`10.0.18363.836`	Полная сборка ОС, установленная на этом устройстве, например Major.Minor.Build.Revision
ИМЯ OSName	Строка	Нет	`Windows 10`	Имя операционной системы.
OSVersion	Строка	Нет	`1909`	Версия ОС Win10 (например, 19H2, 20H1, 20H2), установленная на устройстве.
ReadinessExpiryTime [UTC]	Datetime	Нет	`2020/05/14 09:26:03.478 AM`	Дата и время истечения срока действия оценки готовности.
ReadinessReason	Строка	Нет	`CPU;TPM`	Список требований к оборудованию, которые блокируют возможность установки Windows 11 на устройстве. Поле имеет

Поле	Тип	Перечислимый тип	Пример	Описание
				значение NULL, если устройство поддерживает. Это состояние определяется клиентский компонент Центра обновления Windows применимости.
ReadinessScanTime [UTC]	Datetime	Нет	`2020/05/14 09:26:03.478 AM`	Дата и время оценки готовности и отправки оценки.
ReadinessStatus	Строка	Нет	`Not capable`	Состояние готовности устройства либо поддерживается, не поддерживается, либо неизвестно. Это состояние определяется клиентский компонент Центра обновления Windows.
SCCMClientId	Строка	Нет	`5AB72FAC-93AB-4954-9AB0-6557D0EFA245`	Configuration Manager идентификатор клиента, если он доступен.
SetupReadinessExpiryTime [UTC]	Datetime	Нет	`2020/05/14 09:26:03.478 AM`	Дата и время истечения срока действия оценки готовности к настройке.
SetupReadinessReason	Строка	Нет	`CPU;TPM`	Список требований к оборудованию, которые блокируют возможность установки Windows 11 на устройстве. Поле имеет значение NULL, если устройство поддерживает. Это состояние определяется программой установки Windows.
SetupReadinessStatus	Строка	Нет	`Not capable`	Состояние готовности устройства либо поддерживается, не поддерживается, либо неизвестно. Это состояние определяется программой установки Windows.

Поле	Тип	Перечислимый тип	Пример	Описание
SetupReadinessTime [UTC]	Datetime	Нет	`2020/05/14 09:26:03.478 AM`	Дата и время оценки готовности с помощью настройки и отправки оценки.
SourceSystem	Строка	Нет	`Azure`	
TargetOSBuild	Строка	Нет	`10.0.22000.1`	Полный номер сборки операционной системы, предназначенный для устройства для этой записи готовности.
TargetOSName	Строка	Нет	`Windows 11`	Имя операционной системы, предназначенной для устройства для этой записи готовности.
TargetOSVersion	Строка	Нет	`21H2`	Версия операционной системы, предназначенная для устройства для этой записи готовности.
Идентификатор клиента	Строка	Нет	`69ca04b0-703d-4b3a-9184-c4e3c15d6f5e`	Microsoft Entra идентификатор клиента устройства.
ВремяGenerated [UTC]	Datetime	Нет	`2020/05/14 09:26:03.478 AM`	Дата и время приема этой записи журналами Azure Monitor для рабочей области Log Analytics.
Тип	Строка	Нет	`UCClientReadinessStatus`	Тип сущности

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

UCClientUpdateStatus

Статья • 15.10.2024 • Применяется к: ✅ Windows 11, ✅ Windows 10

Событие обновления, объединяющее последние данные на основе клиента с последними данными на основе службы, чтобы создать полную картину для одного устройства (клиента) и одного обновления.

Схема для UCClientUpdateStatus

Развернуть таблицу

Поле	Тип	Перечислимый тип	Пример	Описание
AzureADDeviceId	струна	Нет	`71db1a1a-f1a6-4a25-b88f-79c2f513dae0`	Microsoft Entra идентификатор устройства
AzureADTenantId	струна	Нет	`69ca04b0-703d-4b3a-9184-c4e3c15d6f5e`	идентификатор клиента Microsoft Entra
CatalogId	струна	Нет	`b0f410599615e2ce15e6614ac3fc4ec62d80324020351e172edef89091a64f2f`	Это поле применяется только к драйверам. Идентификатор каталога обновления из автоматического исправления Windows.
ClientState	струна	Да	`Installing`	Это поле применяется только к драйверам. Контейнер clientSubstate более высокого уровня.
ClientSubstate	струна	Да	`DownloadStart`	Последнее известное состояние этого обновления относительно устройства из клиента.
ClientSubstateRank	int	Нет	`2300`	Ранжирование клиентских подстатов для последовательного упорядочения в представлениях типа воронки. Ранжирование между ServiceSubstate и ClientSubstate можно использовать вместе.
ClientSubstateTime [UTC]	datetime	Нет	`2020/05/14 09:26:03.478 AM`	Дата и время последнего перехода подсостояния клиента
DeploymentId	струна	Нет	`cf1b12a3-3d84-4ce3-bc8e-de48459e252d`	Идентификатор развертывания, которое предназначено для этого обновления для этого устройства, в

Поле	Тип	Перечислимый тип	Пример	Описание
				противном случае пустой.
DeviceName	струна	Нет	`JohnPC-Contoso`	Заданное имя устройства
EventData	струна	Нет		В настоящее время данные не собираются для заполнения этого поля. Json для заполнения произвольными парами K/V. Используется для заполнения контекстных данных, которые в противном случае были бы заполнены разреженно при повышении до поля, всегда присутствующего в схеме.
FurthestClientSubstate	струна	Нет	`DownloadComplete`	Самый дальний клиентSubstate
FurthestClientSubstateRank	int	Нет	`2400`	Рейтинг самых дальних клиентовSubstate
GlobalDeviceId	струна	Нет	`g:9832741921341`	Внутренний глобальный идентификатор устройства Майкрософт
IsUpdateHealthy	струна	Нет	`1`	В настоящее время данные не собираются для заполнения этого поля. True. Проблемы, препятствующие обновлению этого устройства до этого обновления, не обнаружены. False: есть что-то, что может помешать обновлению этого устройства.
OfferReceivedTime [UTC]	datetime	Нет	`2020/05/14 09:26:03.478 AM`	Дата и время последнего сообщения устройства о вводе OfferReceived, в противном случае пустые.
RestartRequiredTime [UTC]	datetime	Нет	`2020/05/14 09:26:03.478 AM`	Дата и время, когда устройство впервые сообщило о вводе RebootRequired (или RebootPending), в противном случае пустое.

Поле	Тип	Перечислимый тип	Пример	Описание
SCCMClientId	струна	Нет	`5AB72FAC-93AB-4954-9AB0-6557D0EFA245`	Строка, соответствующая идентификатору клиента Configuration Manager на устройстве.
SourceSystem	струна	Нет	`Azure`	
TargetBuild	струна	Нет	`10.0.18363.836`	Полная сборка содержимого, отслеживаемого deviceUpdateEvent. Для Windows 10 обновлений это значение будет соответствовать полной сборке (10.0.14393.385).
TargetBuildNumber	струна	Нет	`18363`	Целое число основной части сборки.
TargetKBNumber	струна	Нет	`KB4524570`	Статья базы знаний.
TargetRevisionNumber	струна	Нет	`836`	Целочисленная или дополнительная (или редакция) часть сборки.
TargetVersion	струна	Нет	`1909`	Целевая версия операционной системы, например 1909.
Идентификатор клиента	струна	Нет	`69ca04b0-703d-4b3a-9184-c4e3c15d6f5e`	Microsoft Entra идентификатор клиента устройства.
ВремяGenerated [UTC]	datetime	Нет	`2020/05/14 09:26:03.478 AM`	Время создания этой конкретной записи snapshot. Это необходимо, чтобы определить, к какому пакету snapshot принадлежит эта запись.
Тип	струна	Нет	`UCClientUpdateStatus`	Тип сущности
UpdateCategory	струна	Да	`WindowsFeatureUpdate`	Тип содержимого, отслеживаемого устройством DeviceUpdateEvent.
UpdateClassification	струна	Да	`Upgrade`	Является ли классификация обновлений обновлением (обновление компонентов), безопасностью (обновлением качества), отсутствием безопасности (обновлением качества) или драйвером.

Поле	Тип	Перечислимый тип	Пример	Описание
UpdateConnectivityLevel		Да		В настоящее время данные не собираются для заполнения этого поля. Независимо от того, поддерживает ли это устройство достаточное совокупное и непрерывное подключение к клиентский компонент Центра обновления Windows, чтобы обновление двигалось оптимально.
UpdateDisplayName	струна	Нет	`Windows 10 1909`	Отображаемое имя в длинной форме для данного обновления. Зависит от типа контента (обновление компонентов. обновление качества)
UpdateHealthGroupL1	струна	Нет		В настоящее время данные не собираются для заполнения этого поля. Схема группирования для описания текущей установки обновления "работоспособности", L1 (самый высокий уровень).
UpdateHealthGroupL2	струна	Нет		В настоящее время данные не собираются для заполнения этого поля. Целое число для ранжирования L1 UpdateHealthGroup.
UpdateHealthGroupL3	струна	Нет		В настоящее время данные не собираются для заполнения этого поля. Второе группирование, подмножество L1, более подробное.
UpdateHealthGroupRankL1	int	Нет		В настоящее время данные не собираются для заполнения этого поля. Целое число для ранжирования L2 UpdateHealthGroup.
UpdateHealthGroupRankL2	int	Нет		В настоящее время данные не собираются для

Поле	Тип	Перечислимый тип	Пример	Описание
				заполнения этого поля. Третье группирование, подмножество L3, более подробное.
UpdateHealthGroupRankL3	int	Нет		В настоящее время данные не собираются для заполнения этого поля. Целое число для ранжирования L3 UpdateHealthGroup.
UpdateId	струна	Нет	`10e519f0-06ae-4141-8f53-afee63e995f0`	Это поле применяется только к драйверам. Идентификатор обновления целевого обновления
UpdateInstalledTime [UTC]	datetime	Нет	`2020/05/14 09:26:03.478 AM`	DateTime, когда событие переключено в UpdateInstalled, в противном случае пусто.
UpdateManufacturer	струна	Нет	`Microsoft`	Это поле применяется только к драйверам. Производитель обновления. Майкрософт для обновлений компонентов или исправлений, для драйверов — имя производителя драйвера.
UpdateReleaseTime [UTC]	datetime	Нет	`2020/05/14 09:26:03.478 AM`	Дата выпуска обновления
UpdateSource	струна	Да	`UUP`	Источник обновления, например UUP, MUv6, Media

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

UCDeviceAlert

Статья • 15.10.2024 • Применяется к: ✅ Windows 11, ✅ Windows 10

Эти оповещения активируются в результате проблемы, которая связана с устройством. Это не зависит от сочетания конкретного обновления и определенного устройства. Как и UpdateAlerts, alertType указывает, откуда поступает оповещение (ServiceDeviceAlert, ClientDeviceAlert). Например, оповещение EndOfService — это ClientDeviceAlert, так как сборка больше не обслуживается (EOS) является состоянием на уровне клиента. Между тем, DeviceRegistrationIssues в Windows Autopatch будет serviceDeviceAlert, так как это состояние на уровне всего устройства в службе, которое не должно быть зарегистрировано правильно.

Схема для UCDeviceAlert

Развернуть таблицу

Поле	Тип	Перечислимый тип	Пример	Описание
AlertClassification	струна	Да	`Error`	Является ли это оповещение ошибкой, предупреждением или информационным
AlertData	струна	Нет		В настоящее время данные не собираются для заполнения этого поля. Необязательная строка, отформатированная в виде полезных данных JSON, содержащих метаданные для оповещения.
AlertId	струна	Нет	`9e107d9d372bb6826bd81d3542a419d6`	Уникальный идентификатор этого оповещения
AlertRank	int	Нет	`1000`	Целочисленное ранжирование оповещения для

Поле	Тип	Перечислимый тип	Пример	Описание
				определения приоритетов во время устранения неполадок
AlertStatus	струна	Да	`Active`	Является ли это оповещение активным, разрешенным или удаленным.
AlertSubtype	струна	Да	`DiskFull`	Подтип оповещения.
AlertType	струна	Да	`ClientUpdateAlert`	Тип оповещения, например ClientUpdateAlert или ServiceUpdateAlert. Указывает, какие поля присутствуют.
AzureADDeviceId	струна	Нет	`71db1a1a-f1a6-4a25-b88f-79c2f513dae0`	Microsoft Entra идентификатор устройства
AzureADTenantId	струна	Нет	`69ca04b0-703d-4b3a-9184-c4e3c15d6f5e`	идентификатор клиента Microsoft Entra
Описание	струна	Нет	`Disk full`	Локализованная строка, переведенная из сочетания других полей оповещений и языковых предпочтений, в котором подробно описывается проблема.
DeviceName	струна	Нет	`JohnPC-Contoso`	Имя заданного устройства
ErrorCode	струна	Нет		В настоящее время данные не собираются для заполнения этого поля. Код ошибки , если таковой есть, который

Поле	Тип	Перечислимый тип	Пример	Описание
				активировал это оповещение. В случае явных оповещений на основе клиента коды ошибок могут иметь расширенные коды ошибок, которые добавляются к коду ошибки с разделителем подчеркивания.
ErrorSymName	струна	Нет		В настоящее время данные не собираются для заполнения этого поля. Символическое имя, которое сопоставляется с кодом ошибки, если оно есть. В противном случае пусто.
GlobalDeviceId	струна	Нет	`g:1298371934870`	Внутренний глобальный идентификатор Майкрософт, если он доступен.
Рекомендации	струна	Нет	`Free up disk space.`	Локализованная строка, переведенная из RecommendedAction, Message и других полей (в зависимости от источника оповещения), которая предоставляет рекомендуемое действие.
ResolvedTime [UTC]	datetime	Нет	`2020-05-14 09:26:03.478039`	Время разрешения этого оповещения, в

Поле	Тип	Перечислимый тип	Пример	Описание
				противном случае пустое.
SCCMClientId	струна	Нет	`5AB72FAC-93AB-4954-9AB0-6557D0EFA245`	Configuration Manager идентификатор клиента устройства, если он доступен.
SourceSystem	струна	Нет	`Azure`	
StartTime [UTC]	datetime	Нет	`2020-05-14 09:26:03.478039`	Время активации этого оповещения.
Идентификатор клиента	струна	Нет	`69ca04b0-703d-4b3a-9184-c4e3c15d6f5e`	Microsoft Entra идентификатор клиента устройства.
ВремяGenerated [UTC]	datetime	Нет	`2020-05-14 09:26:03.478039`	Время создания этой конкретной записи snapshot. Это необходимо, чтобы определить, к какому пакету snapshot принадлежит эта запись.
Тип	струна	Нет	`UCDeviceAlert`	Тип сущности
URL-адрес	струна	Нет	`aka.ms/errordetail32152`	В настоящее время данные не собираются для заполнения этого поля. Необязательный URL-адрес для получения более подробных сведений, связанных с этим оповещением.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

UCDOAggregatedStatus

Статья • 25.10.2024 • Применяется к: ✅ Windows 11, ✅ Windows 10

UCDOAggregatedStatus — это агрегат всех отдельных записей UDDOStatus в клиенте и суммирует экономию пропускной способности на всех устройствах, зарегистрированных с помощью оптимизации доставки и подключенного кэша Майкрософт.

Схема для UCDOAggregatedStatus

Развернуть таблицу

Поле	Тип	Пример	Описание
AzureADDeviceId	струна	`71db1a1a-f1a6-4a25-b88f-79c2f513dae0`	Microsoft Entra идентификатор устройства
AzureADTenantId	струна	`69ca04b0-703d-4b3a-9184-c4e3c15d6f5e`	идентификатор клиента Microsoft Entra
BWOptPercent28Days	реальный	`10.61`	Оптимизация пропускной способности (в процентах от экономии общей пропускной способности в противном случае) для этого устройства. Скользящий 28-дневный базис.
BytesFromCache	long	`285212672`	Общее количество байтов, доставленных из подключенного кэша Майкрософт.
BytesFromCDN	long	`11463008693388`	Общее количество байтов, доставленных из сети доставки содержимого (CDN).
BytesFromGroupPeers	long	`30830657175`	Общее количество байтов, которые были доставлены из одноранговых узлов группы с общим идентификатором GroupId.
BytesFromIntPeers	long	`285212672`	Общее количество байтов, доставленных из одноранговых узлов Интернета.

Поле	Тип	Пример	Описание
BytesFromPeers	long	`285212672`	Общее количество байтов, доставленных через все одноранговые узлы.
ContentType	струна	`Driver Updates`	Один из поддерживаемых типов содержимого.
DeviceCount	long	`27077`	Количество устройств.
Идентификатор клиента	струна	`6yy5y416-2d35-3yyf-ab5f-aea713e489d2`	Идентификатор клиента
TimeGenerated	datetime	`2022-11-17T22:11:40.1132971Z`	Время создания этой конкретной записи snapshot. Это необходимо, чтобы определить, к какому пакету snapshot принадлежит эта запись.
Тип	струна	`UCDOAggregatedStatus`	Тип сущности.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

UCDOStatus

Применяется к: ✅ Windows 11, ✅ Windows 10

UCDOStatus предоставляет сведения об использовании пропускной способности для одного устройства в разных типах контента в случае использования оптимизации доставки и подключенного кэша Майкрософт.

Схема данных для UCDOStatus

Развернуть таблицу

Поле	Тип	Пример	Описание
AzureADDeviceId	струна	`71db1a1a-f1a6-4a25-b88f-79c2f513dae0`	Microsoft Entra идентификатор устройства
AzureADTenantId	струна	`69ca04b0-703d-4b3a-9184-c4e3c15d6f5e`	идентификатор клиента Microsoft Entra
BWOptPercent28Days	реальный	`10.61`	Оптимизация пропускной способности (в процентах от экономии общей пропускной способности в противном случае) для этого устройства. Скользящий 28-дневный базис.
BWOptPercent7Days	реальный	`10.61`	Оптимизация пропускной способности (в процентах от экономии общей пропускной способности в противном случае) для этого устройства. Последовательная 7-дневная основа.

Поле	Тип	Пример	Описание
BytesFromCache	long	`285212672`	Общее количество байтов, доставленных из подключенного кэша Майкрософт.
BytesFromCDN	long	`11463008693388`	Общее количество байтов, доставленных из сети доставки содержимого (CDN).
BytesFromGroupPeers	long	`30830657175`	Общее количество байтов, которые были доставлены из одноранговых узлов группы с общим идентификатором GroupId.
BytesFromIntPeers	long	`285212672`	Общее количество байтов, доставленных из одноранговых узлов Интернета.
BytesFromPeers	long	`285212672`	Общее количество байтов, доставленных через одноранговые узлы локальной сети.
Город	струна	`Redmond`	Приблизительный город, в котором находилось устройство при скачивании содержимого, на основе IP-адреса.

Поле	Тип	Пример	Описание
ContentDownloadMode	int	`1`	Режим загрузки оптимизации доставки устройства, используемый для скачивания содержимого.
ContentType	струна	`Driver Updates`	Один из поддерживаемых типов содержимого.
Страна	струна	`US`	Приблизительная страна, в которой устройство находилось при скачивании содержимого, на основе IP-адреса.
DeviceName	струна	`DESKTOP-DO`	Имя устройства, предоставленное пользователем или организацией. Если значение отображается как "#", настройте устройство для отправки имени устройства.
DOStatusDescription	струна	`Downloading`	Краткое описание состояния оптимизации доставки, если оно имеется.
DownloadMode	струна	`LAN (1)`	Режим загрузки оптимизации доставки, настроенный на устройстве.
DownloadModeSrc	струна	`MDM`	Источник конфигурации режима загрузки.

Поле	Тип	Пример	Описание
GlobalDeviceId	струна	`g:9832741921341`	Глобальный идентификатор устройства Майкрософт. Этот идентификатор используется корпорацией Майкрософт для внутренних целей.
GroupID	струна	`3suvw1efol0nmy8y9g8tfhtj1onwpsk9g9swpwnvfra=`	Значение GUID идентификатора группы оптимизации доставки.
Поставщик услуг Интернета	струна	`Microsoft Corporation`	Оценка поставщика услуг Интернета.
LastCensusSeenTime	datetime	`2020-05-14 09:26:03.478039`	Последний раз, когда это устройство выполняло успешное сканирование переписи, если таковое имеется.
NoPeersCount	long	`4`	Количество одноранговых узлов, с которыми взаимодействовал устройство.
OSVersion	струна	`1909`	Версия операционной системы Windows 10/11, установленная на устройстве, например 20H1, 21H2.
PeerEligibleTransfers	long	`5`	Общее количество допустимых передач по

Поле	Тип	Пример	Описание
			одноранговым узлам.
PeeringStatus	струна	`On`	Состояние пиринга оптимизации доставки.
PeersCannotConnectCount	long	`1`	Число одноранговых узлов, к которому не удалось подключиться к оптимизации доставки.
PeersSuccessCount	long	`2`	Число одноранговых узлов, к которому успешно подключена оптимизация доставки.
PeersUnknownCount	long	`0`	Число одноранговых узлов с неизвестным отношением.
Идентификатор клиента	струна	`6yy5y416-2d35-3yyf-ab5f-aea713e489d2`	Идентификатор клиента
TimeGenerated	datetime	`2022-11-17T22:11:40.1132971Z`	Время создания этой конкретной записи snapshot. Это необходимо, чтобы определить, к какому пакету snapshot принадлежит эта запись.
TotalTimeForDownload	струна	`00:02:11`	Общее время загрузки содержимого.
TotalTransfers	long	`304`	Общее количество

Поле	Тип	Пример	Описание
			передач данных, необходимых для скачивания содержимого.
Тип	струна	`UCDOAggregatedStatus`	Тип сущности.

Last updated on 04.08.2025

UCServiceUpdateStatus

Статья • 15.10.2024 • Применяется к: ✅ Windows 11, ✅ Windows 10

Событие обновления, которое поступает непосредственно на стороне службы. Событие содержит только сведения на стороне службы для одного устройства (клиента) и одно обновление в одном развертывании. Это событие имеет определенные поля, удаленные из него, чтобы иметь возможность отображать данные практически в реальном времени.

Схема для UCServiceUpdateStatus

Развернуть таблицу

Поле	Тип	Перечислимый тип	Пример	Описание
AzureADDeviceId	струна	Нет	`71db1a1a-f1a6-4a25-b88f-79c2f513dae0`	Microsoft Entra идентификатор устройства
AzureADTenantId	струна	Нет	`69ca04b0-703d-4b3a-9184-c4e3c15d6f5e`	идентификатор клиента Microsoft Entra
CatalogId	струна	Нет	`b0f410599615e2ce15e6614ac3fc4ec62d80324020351e172edef89091a64f2f`	Это поле применяется только к драйверам. Идентификатор каталога обновления из автоматического исправления Windows.
DeploymentApprovedTime [UTC]	datetime	Нет	`2020-05-14 09:26:03.478039`	Это поле применяется только к драйверам. Дата и время утверждения обновления
DeploymentId	струна	Нет	`cf1b12a3-3d84-4ce3-bc8e-de48459e252d`	Если это deviceUpdateEvent из содержимого, развернутого политикой службы планировщика развертывания, этот GUID сопоставляется с этой политикой, в противном случае он пуст.
DeploymentIsExpedited	bool	Нет	`1`	В настоящее время данные не собираются для заполнения этого поля. Он указал, ускоряется ли содержимое
DeploymentName	струна	Нет	`My deployment`	В настоящее время данные не собираются для заполнения этого

Поле	Тип	Перечислимый тип	Пример	Описание
				поля. Понятное имя созданного развертывания
DeploymentRevokeTime [UTC]	datetime	Нет	`2020-05-14 09:26:03.478039`	Это поле применяется только к драйверам. Дата и время отзыва обновления
GlobalDeviceId	струна	Нет	`g:9832741921341`	В настоящее время данные не собираются для заполнения этого поля. Внутренний глобальный идентификатор устройства Майкрософт
OfferReadyTime [UTC]	datetime	Нет	`2020-05-14 09:26:03.478039`	DateTime перехода OfferReady. Если он пуст, еще не был предложен.
PolicyCreatedTime [UTC]	datetime	Нет	`2020-05-14 09:26:03.478039`	Это поле применяется только к драйверам. Дата и время создания политики
PolicyId (Идентификатор политики)	струна	Нет	`9011c330-1234-5678-9abc-def012345678`	Это поле применяется только к драйверам. Идентификатор политики, предназначенный для обновления для этого устройства
PolicyName	струна	Нет	`My policy`	В настоящее время данные не собираются для заполнения этого поля. Это поле применяется только к драйверам. Понятное имя политики.
ProjectedOfferReadyTime [UTC]	datetime	Нет	`2020-05-14 09:26:03.478039`	Для устройства будет предложено обновление прогнозируемого времени. Если пуст, неизвестно.
ServiceState	струна	Да	`Offering`	Состояние обновления на высоком уровне относительно устройства, на стороне службы.

Поле	Тип	Перечислимый тип	Пример	Описание
ServiceSubstate	струна	Да	`OfferReady`	Низкоуровневое состояние состояния обновления относительно устройства, на стороне службы.
ServiceSubstateRank	int	Нет		В настоящее время данные не собираются для заполнения этого поля. Ранжирование вложенных состояний для последовательного упорядочения в представлениях типа воронки. Ранжирование между ServiceSubstate и ClientSubstate можно использовать вместе.
ServiceSubstateTime [UTC]	datetime	Нет	`2020-05-14 09:26:03.478039`	Дата и время последнего перехода ServiceSubstate.
SourceSystem	струна	Нет	`Azure`	
TargetBuild	струна	Нет	`10.0.18363.836`	Полная сборка для содержимого, отслеживаемого этим событием. Для Windows 10 эта строка соответствует "10.0.Build.Revision"
TargetVersion	струна	Нет	`1909`	Версия содержимого, отслеживаемого устройством DeviceUpdateEvent. Для Windows 10 обновлений это число будет соответствовать используемому формату версии года или месяца, например 1903.
Идентификатор клиента	струна	Нет	`9011c330-1234-5678-9abc-def012345678`	идентификатор клиента Microsoft Entra
ВремяGenerated [UTC]	datetime		`2020-05-14 09:26:03.478039`	Время выполнения snapshot также может совпадать с EventDateTimeUTC в некоторых случаях.

Поле	Тип	Перечислимый тип	Пример	Описание
Тип	струна	Нет	`UCServiceUpdateStatus`	Тип сущности
UdpateIsSystemManifest	струна	Нет		В настоящее время данные не собираются для заполнения этого поля. Это поле применяется только к драйверам.
UpdateCategory	струна	Да	`WindowsFeatureUpdate`	Тип содержимого, отслеживаемого устройством DeviceUpdateEvent.
UpdateClassification	струна	Да	`Upgrade`	Является ли это обновление обновлением (обновление компонентов), безопасностью (обновлением качества), отсутствием безопасности (обновлением качества) или драйвером.
UpdateDisplayName	струна	Нет	`Windows 10 1909`	Отображаемое имя в длинной форме для данного обновления. Зависит от типа контента (обновление компонентов. обновление качества)
UpdateId	струна	Нет	`10e519f0-06ae-4141-8f53-afee63e995f0`	Это поле применяется только к драйверам. Идентификатор обновления целевого обновления
UpdateManufacturer	струна	Нет	`Microsoft`	Это поле применяется только к драйверам. Производитель обновления. Майкрософт для обновлений компонентов или исправлений, для драйверов — имя производителя драйвера.
UpdateProvider	струна	Нет	`Microsoft`	Это поле применяется только к

Поле	Тип	Перечислимый тип	Пример	Описание
				драйверам. Поставщик обновлений драйверов и встроенного ПО
UpdateRecommendedTime [UTC]	datetime	Нет	`2020-05-14 09:26:03.478039`	Это поле применяется только к драйверам. Дата и время, когда для устройства было рекомендовано обновление
UpdateReleaseTime [UTC]	datetime	Нет	`2020-05-14 09:26:03.478039`	В настоящее время данные не собираются для заполнения этого поля. Дата выпуска обновления
UpdateVersion	струна	Нет	`20.0.19.3`	Это поле применяется только к драйверам. Обновление версии драйверов или встроенного ПО
UpdateVersionTime [UTC]	datetime	Нет	`2020-05-14 09:26:03.478039`	Это поле применяется только к драйверам. Обновление метки времени даты версии для драйверов и встроенного ПО

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

UCUpdateAlert

Статья • 15.10.2024 • Применяется к: ✅ Windows 11, ✅ Windows 10

Оповещение об обновлениях клиента и службы. Содержит сведения, которые требуют внимания относительно одного устройства (клиента), одного обновления и одного развертывания (если применимо). Некоторые поля могут быть пустыми в зависимости от поля AlertType UpdateAlert; Например, ServiceUpdateAlert не обязательно будет содержать состояния на стороне клиента.

Схема для UCUpdateAlert

Развернуть таблицу

Поле	Тип	ENUM	Пример	Описание
AlertClassification	струна	Да	`Error`	Является ли это оповещение ошибкой, предупреждением или информационным
AlertData	струна	Нет	`{ "freeDiskCapacityMb": 3213, "contentSizeMb": 4381}`	Необязательная строка, отформатированная в виде полезных данных JSON, содержащих метаданные для оповещения.
AlertId	струна	Нет	`9e107d9d372bb6826bd81d3542a419d6`	Уникальный идентификатор этого оповещения
AlertRank	int	Нет	`1000`	Целочисленное ранжирование оповещения для определения приоритетов во время устранения неполадок
AlertStatus	струна	Да	`Active`	Является ли это оповещение активным, разрешенным или удаленным
AlertSubtype	струна	Да	`DiskFull`	Подтип оповещения
AlertType	струна	Да	`ClientUpdateAlert`	Тип оповещения, например ClientUpdateAlert или ServiceUpdateAlert. Указывает, какие поля присутствуют.
AzureADDeviceId	струна	Нет	`71db1a1a-f1a6-4a25-b88f-79c2f513dae0`	Microsoft Entra идентификатор

Поле	Тип	ENUM	Пример	Описание
				устройства
AzureADTenantId	струна	Нет	`69ca04b0-703d-4b3a-9184-c4e3c15d6f5e`	идентификатор клиента Microsoft Entra
CatalogId	струна	Нет	`b0f410599615e2ce15e6614ac3fc4ec62d80324020351e172edef89091a64f2f`	Это поле применяется только к драйверам. Идентификатор каталога обновления из автоматического исправления Windows.
ClientSubstate	струна	Да	`DownloadStart`	Если оповещение от клиента, значение ClientSubstate на момент активации или обновления оповещения, в противном случае пустое.
ClientSubstateRank	int	Нет	`2300`	Ранг clientSubstate
DeploymentId	струна	Нет	`cf1b12a3-3d84-4ce3-bc8e-de48459e252d`	Развертывание это оповещение относится к , если оно есть.
Описание	струна	Нет	`Disk full`	Локализованная строка, переведенная из сочетания других полей оповещений и языковых настроек, в котором подробно описывается проблема.
DeviceName	струна	Нет	`JohnPC-Contoso`	Имя заданного устройства
ErrorCode	струна	Нет	`0x8326CFA2D_C3FD`	Код ошибки , если таковой есть, который активировал это оповещение. В случае явных оповещений на основе клиента коды ошибок могут иметь расширенные коды ошибок, которые добавляются к коду ошибки с разделителем подчеркивания.

Поле	Тип	ENUM	Пример	Описание
ErrorSymName	струна	Нет	`WU_E_DISK_FULL`	Символическое имя, которое сопоставляется с кодом ошибки, если оно есть, в противном случае пусто.
GlobalDeviceId	струна	Нет	`g:1298371934870`	Внутренний глобальный идентификатор Майкрософт, если он доступен.
Рекомендации	струна	Нет	`Free up disk space.`	Локализованная строка, переведенная из RecommendedAction, Message и других полей (в зависимости от источника оповещения), которая предоставляет рекомендуемое действие.
ResolvedTime [UTC]	datetime	Нет	`2020-05-14 09:26:03.478039`	Время разрешения этого оповещения, в противном случае пустое.
SCCMClientId	струна	Нет	`5AB72FAC-93AB-4954-9AB0-6557D0EFA245`	Идентификатор клиента Configuration Manager устройства, если он доступен.
ServiceSubstate	струна	Да	`OfferReady`	Если оповещение от службы, значение ServiceSubstate на момент активации или обновления оповещения, в противном случае пустое.
ServiceSubstateRank	int	Нет		Ранг "ClientSubstate"
SourceSystem	струна	Нет	`Azure`	
StartTime [UTC]	datetime	Нет	`2020-05-14 09:26:03.478039`	Время активации этого оповещения.
TargetBuild	струна	Нет	`18363.836`	Майор Windows 10. Редакция этого параметра UpdateAlert относится к.
TargetVersion	струна	Нет	`1909`	Относительно Windows 10 сборки

Поле	Тип	ENUM	Пример	Описание
				этого UpdateAlert.
Идентификатор клиента	струна	Нет	`69ca04b0-703d-4b3a-9184-c4e3c15d6f5e`	Microsoft Entra идентификатор клиента устройства.
ВремяGenerated [UTC]	datetime	Нет	`2020-05-14 09:26:03.478039`	Время создания этой конкретной записи snapshot. Это необходимо, чтобы определить, к какому пакету snapshot принадлежит эта запись.
Тип	струна	Нет	`UCUpdateAlert`	Тип сущности
UpdateCategory	струна	Да	`WindowsFeatureUpdate`	Тип содержимого, отслеживаемого устройством DeviceUpdateEvent.
UpdateClassification	струна	Да	`Upgrade`	Является ли это обновление обновлением (обновление компонентов), безопасностью (обновлением качества), отсутствием безопасности (обновлением качества) или драйвером.
UpdateId	струна	Нет	`10e519f0-06ae-4141-8f53-afee63e995f0`	Это поле применяется только к драйверам. Идентификатор обновления целевого обновления.
URL-адрес	струна	Нет	`aka.ms/errordetail32152`	Необязательный URL-адрес для получения более подробных сведений, связанных с этим оповещением.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Перечисление типов для отчетов клиентский компонент Центра обновления Windows для бизнеса

Статья • 06.12.2023 • Применяется к: ✅ Windows 11, ✅ Windows 10

В отчетах клиентский компонент Центра обновления Windows для бизнеса используются следующие перечислимые типы:

OSEdition

SKU Windows, на котором работает устройство.

Expand table

Значение	Описание
Корпоративная	Windows Корпоративная
Профессиональная	Windows Professional
ProfessionalWorkstation	Рабочая станция Windows Professional
ProfessionalN	Аналогично выпуску Windows Professional, но не включает проигрыватель Windows Media.
Education	Windows для образовательных учреждений

OSArchitecture

Архитектура операционной системы, работающей на клиенте.

Expand table

Значение	Описание
amd64	ОС является 64-разрядной
x86	ОС является 32-разрядной
Unknown (неизвестно).	Архитектура ОС неизвестна

OSFeatureUpdateStatus

Состояние обновлений компонентов

Expand table

Значение	Описание
Неизвестна	Значение по умолчанию отправляется, если данные клиента недоступны.
InService	Клиент использует версию Windows 10, которая обслуживается.
EndOfService	Клиент находится в версии Windows 10, которая больше не обслуживается.

OSQualityUpdateStatus

Состояние обновлений качества

Expand table

Значение	Описание
Последнее	Клиент находится на последнем обновлении качества
NotLatest	Клиент не включен в последнее обновление качества

OSSecurityUpdateStatus

Состояние обновлений системы безопасности

Expand table

Значение	Описание
Последнее	На клиенте установлена последняя версия обновления для системы безопасности
NotLatest	Клиент не использует последнее обновление для системы безопасности
MultipleSecurityUpdatesMissing	На клиенте отсутствует несколько обновлений для системы безопасности

OSFeatureUpdateComplianceStatus, OSSecurityUpdateComplianceStatus, OSQualityUpdateComplianceStatus

Состояние соответствия

Expand table

Значение	Описание
Совместимый	Последнее развертывание из службы развертывания клиентский компонент Центра обновления Windows для бизнеса устанавливается на клиенте.
NotCompliant	Последнее развертывание из службы развертывания клиентский компонент Центра обновления Windows для бизнеса не установлено на клиенте.
NotApplicable	Клиент не является частью каких-либо клиентский компонент Центра обновления Windows развертываний службы развертывания для бизнеса

OSServicingChannel

Канал обслуживания клиента

Expand table

Значение	Описание
Неизвестна	По умолчанию не удается определить ветвь выпуска.
МЕШОК	Канал полугодового выпуска
LTSC	Канал долгосрочного обслуживания
WIP-S	Windows Insider Preview — медленное кольцо
WIP-F	Windows Insider Preview — быстрый круг
Внутренние	Идентифицируемое, но внутреннее кольцо выпуска

ServiceState

Состояние службы высокого уровня OSServicingChannel

Expand table

Значение	Описание
Состояние Pending (ожидание)	служба развертывания клиентский компонент Центра обновления Windows для бизнеса не предназначена для этого устройства, так как обновление не готово.
Предлагая	Служба предлагает обновление для устройства. Обновление доступно устройству, если оно сканирует клиентский компонент Центра обновления Windows.
OnHold	Служба задерживает предложение обновления для устройства на неопределенный срок. Пока служба или администратор не изменит какое-либо условие, устройства остаются в этом состоянии.
Canceled (Отменено)	Служба отменяется, предлагая обновление для устройства, и устройство подтверждает, что не устанавливает обновление.

ServiceSubstate

Состояние службы нижнего уровня

Expand table

Значение	ServiceState
Проверки	Обновление не может быть предложено устройству из-за проблемы с проверкой устройства и службы развертывания.
Назначенные	Обновление не готово к предложению устройству, но планируется его предложить позже.
OfferReady	Обновление в настоящее время предлагается устройству с клиентский компонент Центра обновления Windows.
RemovedFromDeployment	Предложение обновлений было отменено, так как оно было удалено из развертывания из-за явного действия администратора.
AdminCancelled	Предложение обновления было отменено из-за явного действия администратора.
ServiceCancelled	Предложение обновлений было отменено из-за автоматического действия службы развертывания.
AdminPaused	Обновление приостановлено, так как развертывание было приостановлено явным действием администратора.

Значение	ServiceState
ServicePaused	Обновление находится на удержании из-за автоматического действия службы развертывания.
Защита	Обновление не предлагается, так как на устройстве существует удержание средств защиты.

ClientState

Состояние клиента высокого уровня

Expand table

Значение	Описание
Неизвестна	Значение по умолчанию, если clientSubstate неизвестно (другими словами, нет данных клиента).
Предлагая	Обновление предлагается для устройства
Установка	Обновление выполняется на устройстве
Удаление	Обновление удаляется с устройства
Установлено	Обновление установлено на устройстве
Удалить	Обновление удалено с устройства
Canceled (Отменено)	Обновление отменено с устройства
OnHold	Обновление было отложено

ClientSubstate

Состояние клиента нижнего уровня

Expand table

Значение	Описание
Неизвестна	Значение по умолчанию, если clientSubstate неизвестно (другими словами, нет данных клиента).
Предлагая	Обновление предлагается для устройства

Значение	Описание
Установка	Обновление выполняется на устройстве
Удаление	Обновление удаляется с устройства
Установлено	Обновление установлено на устройстве
Удалить	Обновление удалено с устройства
Canceled (Отменено)	Обновление отменено с устройства
OnHold	Обновление было отложено

UpdateCategory

Тип обновления.

Expand table

Значение	Описание
WindowsQualityUpdate	Обновление компонентов Windows
WindowsFeatureUpdate	Обновление качества Windows
DriverUpdate	Обновление драйвера

UpdateClassification

Является ли это обновление обновлением, безопасностью, отсутствием безопасности или драйвером.

Expand table

Значение	Описание
Безопасность	Обновление — это обновление качества, содержащее исправления для системы безопасности.
Небезопасность	Обновление — это исправление качества, не содержащее исправлений системы безопасности.
Обновление с более ранней версии:	Обновление — это обновление компонентов

UpdateSource

Источник обновления

Expand table

Значение	Описание
Вывести	
MuV6	Обновление через старую клиентский компонент Центра обновления Windows или с помощью WSUS (используется старый протокол)
UUP	Обновление с помощью современных клиентский компонент Центра обновления Windows

ReadinessStatus

Может ли устройство принимать целевую ОС и версию.

Expand table

Значение	Описание
Способны	Устройство соответствует всем требованиям для обновления до Windows 11.
Не поддерживается	Устройство не соответствует требованиям для обновления до Windows 11. Проверьте причину готовности.
Unknown (неизвестно).	Корпорация Майкрософт не имеет достаточного количества точек данных для определения статуса соответствия требованиям.

ReadinessReason

Причина, по которой устройство не поддерживает обновление до целевой ОС и версии.

Expand table

Значение	Описание
Tpm	Требуется доверенный платформенный модуль (TPM) версии 2.0. Если устройство не соответствует минимальным требованиям из-за доверенного платформенного модуля, см. статью Включение доверенного

Значение	Описание
	платформенного модуля 2.0 на компьютере , чтобы узнать, есть ли какие-либо действия по исправлению.
cpufms	ЦП не поддерживается. Дополнительные сведения см. в разделе Требования к процессору Windows.
sysdrivesize	Требуется запоминающее устройство размером 64 ГБ или больше. Если на компьютере недостаточно большого дискового пространства, иногда существуют варианты обновления диска. Обратитесь к веб-сайту изготовителя компьютера или к розничному продавцу, чтобы узнать, есть ли варианты для удовлетворения минимальных требований для Windows 11.
UefiSecureBoot	UEFI (единый расширяемый интерфейс встроенного ПО) и возможность безопасной загрузки. Если устройство не соответствует минимальным требованиям, так как оно не поддерживает безопасную загрузку. Дополнительные сведения см. в разделах Windows 11 и безопасная загрузка, чтобы узнать, можно ли включить безопасную загрузку. Безопасную загрузку можно включить только с помощью UEFI.

AlertType

Тип оповещения.

Expand table

Значение	Описание
ServiceUpdateAlert	Оповещение относится к предложению клиентский компонент Центра обновления Windows службы развертывания для бизнеса клиенту.
ClientUpdateAlert	Оповещение относится к возможности клиента выполнить установку содержимого обновления.
ServiceDeviceAlert	Оповещение относится к состоянию устройства в службе развертывания клиентский компонент Центра обновления Windows для бизнеса
ClientDeviceAlert	Оповещение относится к состоянию устройства
DeploymentAlert	Оповещение относится ко всему развертыванию или к значительному числу устройств в развертывании.

AlertSubtype

Подтип оповещения.

Expand table

Значение	Описание
CancelledByUser	Пользователь отменил обновление.
CertificateIssue	Обнаружен сертификат с истекшим сроком действия.
Поврежденнаямедиа	Файл обновления поврежден.
DeviceRegistrationInvalidAzureADJoin	Устройство не может правильно зарегистрировать или пройти проверку подлинности в службе развертывания из-за отсутствия присоединения к идентификатору Entra на уровне устройства. Устройства, присоединенные к рабочему месту, несовместимы со службой развертывания.
DiskFull	Не удалось выполнить операцию, так как диск заполнен.
DiskIssue	клиентский компонент Центра обновления Windows обнаружено повреждение диска.
DownloadCancelled	Скачивание было отменено.
DownloadCredentialsIssue	Для прокси-сервера или брандмауэра в сети могут потребоваться учетные данные.
DownloadIssue	Возникла проблема с загрузкой.
DownloadIssueServiceDisabled	Служба, от нее зависит скачивание, отключена.
DownloadTimeout	Истекло время ожидания.
EndOfService	Клиентская ОС больше не обслуживается
EndOfServiceApproaching	Период обслуживания клиентской ОС завершается менее чем через 60 дней
FileNotFound	Установщику не удалось найти необходимый компонент Windows.
InstallAccessDenied	Доступ запрещен.
InstallCancelled	Установка отменена.
InstallFileLocked	Не удалось получить доступ к файлу, так как он уже используется.
InstallIssue	Возникла проблема с установкой.

Значение	Описание
InstallSetupBlock	Обновление блокируется приложением или драйвером.
InstallSetupError	Произошла ошибка при установке новой версии Windows.
InstallSetupRestartRequired	Требуется перезагрузка.
InstallSharingViolation	Приложение, скорее всего, мешает клиентский компонент Центра обновления Windows.
InstallSystemError	При установке новой версии Windows произошла системная ошибка.
InsufficientUpdateConnectivity	Устройство не имеет достаточного количества подключений для клиентский компонент Центра обновления Windows для выполнения процесса обновления и будет испытывать задержки.
MultipleSecurityUpdatesMissing	На клиенте отсутствует несколько обновлений для системы безопасности
NetworkIssue	Время ожидания сервера истекло.
PathNotFound	Не удается найти указанный путь.
RestartIssue	Перезапуск для применения обновлений блокируется одним или несколькими приложениями.
Защита	Не удается установить обновление из-за известного удержания защиты.
UnexpectedShutdown	Установка остановлена, так как Windows завершает работу или перезапускается.
WindowsComponentCorruption	Это устройство имеет поврежденный компонент Windows
WUBusy	клиентский компонент Центра обновления Windows пытались установить обновление, пока уже выполнялся другой процесс установки.
WUComponentMissing	клиентский компонент Центра обновления Windows может отсутствовать компонент или файл обновления может быть поврежден.
WuDamaged	Файл обновления может быть поврежден.

Значение	Описание
WUFileCorruption	клиентский компонент Центра обновления Windows обнаружены поврежденные файлы.
WUIssue	Во время установки возникла непредвиденная проблема.
WUSetupError	Процесс настройки приостановлен.

AlertStatus

Состояние оповещения

Expand table

Значение	Описание
Active	Оповещение активно и по-прежнему требует внимания.
Устранено	Оповещение устранено и больше не требует внимания.
Удалено	Оповещение было удалено из серверной системы.

AlertClassification

Является ли это оповещение ошибкой, предупреждением или информационным.

Expand table

Значение	Описание
Информационный	Оповещение является информационным по своей природе.
Warning	Оповещение — это предупреждение
Ошибка	Оповещение является ошибкой или связано с ошибкой. Должен быть код ошибки, который сопоставляется с клиентом или службой.
Рекомендации	Оповещение — это рекомендация, что-то для оптимизации.

Обратная связь

Были ли сведения на этой странице полезными?

Да Нет

Отзыв о продукте

Устранение ошибок обновления Windows: Техническая информация для ИТ-специалистов

Применяется к: ✅ Windows 11, ✅ Windows 10

> ⓘ **Внимание**
>
> Эта статья содержит технические инструкции для ИТ-администраторов. Эта статья не предназначена для администраторов, не относящихся к ИТ, таких как домашние или потребительские пользователи.

В этой статье содержатся краткие сведения о процессах установки Windows и приводятся процедуры устранения неполадок, которые ИТ-администраторы могут использовать для устранения проблем с обновлением Windows.

Статья разделена на подтемы разных технических уровней. Базовый уровень предоставляет общие процедуры, которые позволяют устранить несколько типов ошибок обновления. Для расширенного уровня требуется определенный опыт работы с подробными методами устранения неполадок.

Назначаются следующие четыре уровня:

- Уровень 100: базовый
- Уровень 200: Средний
- Уровень 300: средний расширенный
- Уровень 400: расширенный

В этом руководстве

См. следующие статьи в этом разделе:

- Быстрые исправления: (уровень 100) Действия, которые необходимо предпринять для устранения многих ошибок обновления Windows.
- SetupDiag(уровень 300) SetupDiag — это новое средство, помогающий изолировать первопричину сбоя обновления.
- Устранение ошибок обновления: (уровень 300) Общие советы и методы устранения ошибок обновления Windows, а также описание этапов, используемых в процессе обновления.

- отчеты об ошибках Windows: (уровень 300) Использование Просмотр событий для просмотра сведений об обновлении Windows.
- Коды ошибок обновления(уровень 400). Компоненты кода ошибки объясняются.
  - Коды результатов: сведения о кодах результатов.
  - Коды расширений: сведения о кодах расширений.
- Файлы журнала (уровень 400) — список и описание файлов журналов, полезных для устранения неполадок.
  - Структура записи журнала: описание формата записи журнала.
  - Анализ файлов журналов: общие процедуры для анализа файлов журналов и пример.
- Процедуры разрешения: (уровень 200) Причины и процедуры по устранению неполадок, связанные с определенными кодами ошибок.
  - 0xC1900101: сведения о коде результата 0xC1900101.
  - 0x800xxxxx: сведения о кодах результатов, которые начинаются с 0x800.
  - Другие коды результатов: дополнительные причины и процедуры устранения проблем для некоторых кодов результатов.
  - Другие коды ошибок: дополнительные причины и процедуры устранения проблем для некоторых кодов ошибок.
- Отправка ошибок обновления Windows: (уровень 100) Отправка ошибок обновления в корпорацию Майкрософт для анализа.

Связанные статьи

- Исправьте ошибки клиентский компонент Центра обновления Windows с помощью средства DISM или средства проверки готовности к обновлению системы.

Last updated on 09.04.2025

Быстрые исправления обновления Windows 10

15.01.2025

Применимо к: Windows 10

> **Примечание**
>
> Это 100 раздел уровня (базовый).
>
> Для ИТ-специалистов ознакомьтесь с дополнительными сведениями об **ошибках** обновления Windows 10.

В следующем списке исправлений можно устранить множество проблем с обновлением Windows. Эти действия следует выполнить перед обращением в службу поддержки Майкрософт или попыткой более расширенного анализа сбоя обновления Windows. Дополнительные сведения см. в справке по Windows 10.

> **Совет**
>
> Вы также можете попробовать новое средство, доступное от Корпорации Майкрософт, которое помогает диагностировать многие ошибки обновления Windows. Дополнительные сведения и скачивание этого средства см. в разделе **SetupDiag**. Этот раздел более сложный (уровень 300), так как для использования средства доступны несколько дополнительных параметров. Однако теперь вы можете просто скачать и дважды щелкнуть средство, чтобы запустить его. По умолчанию при нажатии кнопки "Сохранить" средство сохраняется в *папке* " Загрузки". Дважды щелкните средство в папке и дождитесь завершения работы (может потребоваться несколько минут), а затем дважды щелкните *файл SetupDiagResults.log* и откройте его с помощью Блокнота, чтобы просмотреть результаты анализа.

Список исправлений

Ниже приведены пошаговые инструкции.

1. Удалите непреднаправленное внешнее оборудование, например док-станции и USB-устройства.
2. Проверьте системный диск для ошибок и попытайтесь восстановить.

3. Запустите средство устранения неполадок Обновл. Windows.
4. Попытайтесь восстановить и восстановить системные файлы.
5. Обновите Windows таким образом, чтобы все доступные рекомендуемые обновления были установлены, и убедитесь, что компьютер перезагружается, если необходимо завершить установку обновления.
6. Временно удалите антивирусное программное обеспечение, отличное от Майкрософт.
7. Удалите все нетентичные программы.
8. Обновление встроенного ПО и драйверов.
9. Убедитесь, что "Загрузка и установка обновлений (рекомендуется)" принимается в начале процесса обновления.
10. Убедитесь, что доступно не менее 16 ГБ свободного места для обновления 32-разрядной ОС или 20 ГБ для 64-разрядной ОС.

Удаление внешнего оборудования

Если компьютер переносим и он находится в док-станции, открепите компьютер.

Распакуние невенсиальных внешних аппаратных устройств с компьютера, таких как:

- Наушники
- Джойстики
- Принтеры
- Плоттеры
- Проекторы
- Сканеры
- Докладчики
- USB-устройств флэш-памяти;
- Переносимые жесткие диски
- Переносимые диски CD/DVD/Blu-ray
- Микрофоны
- Средства чтения карт мультимедиа
- Камеры и веб-камеры
- Смартфонов
- Вторичные мониторы, клавиатуры, мыши

Дополнительные сведения об отключении внешних устройств см. в статье "Безопасное удаление оборудования в Windows 10"

Восстановление системного диска

Системный диск — это диск, содержащий системную секцию. Обычно это диск C:

Чтобы проверить и исправить ошибки на системном диске, выполните следующие действия.

1. Выберите **Пуск**.
2. Команда *type*.
3. Щелкните правой кнопкой мыши **командную строку** и выберите команду "**Запуск от имени администратора**".
4. Если вы запрашиваете UAC, нажмите кнопку "**Да**".
5. Введите `chkdsk /F` и нажмите клавишу ВВОД.
6. При появлении запроса на планирование проверки при следующем перезапуске системы введите `Y`.
7. См. следующий пример.

   Консоль

   ```
   C:\WINDOWS\system32>chkdsk /F
   The type of the file system is NTFS.
   Cannot lock current drive.

   Chkdsk cannot run because the volume is in use by another
   process.  Would you like to schedule this volume to be
   checked the next time the system restarts? (Y/N) Y

   This volume will be checked the next time the system restarts.
   ```

8. Перезагрузите компьютер. Компьютер приостанавливается перед загрузкой Windows и выполняет восстановление жесткого диска.

Средство устранения неполадок Обновл. Windows

Средство устранения неполадок Обновл. Windows автоматически анализирует и исправляет проблемы с Обновл. Windows, например поврежденное скачивание. Он также сообщит вам, есть ли ожидающая перезагрузка, которая препятствует обновлению Windows.

Скачайте средство для Windows 10.

Чтобы запустить средство, выберите соответствующую ссылку выше. Веб-браузер предложит сохранить или открыть файл. Выберите "**Открыть** ", а средство автоматически запустится. Это средство поможет вам проанализировать и устранить некоторые распространенные проблемы.

Восстановление системных файлов

Это исправление также подробно описано в answers.microsoft.com .

Чтобы проверить и восстановить системные файлы, выполните приведенные ниже действия.

1. Выберите **Пуск**.
2. Команда *type*.
3. Щелкните правой кнопкой мыши **командную строку** и выберите команду "**Запуск от имени администратора**".
4. Если вы запрашиваете UAC, нажмите кнопку "**Да**".
5. Введите `sfc /scannow` и нажмите клавишу ВВОД. См. следующий пример.

```
Консоль

C:\>sfc /scannow

Beginning system scan.  This process will take some time.

Beginning verification phase of system scan.
Verification 100% complete.

Windows Resource Protection did not find any integrity violations.
```

6. Если вы используете Windows 8.1 или более поздней версии, введите `DISM.exe /Online /Cleanup-image /Restorehealth` и нажмите клавишу ВВОД (`DISM` параметры команды недоступны для Windows 7). См. следующий пример.

```
Консоль

C:\>DISM.exe /Online /Cleanup-image /Restorehealth

Deployment Image Servicing and Management tool
Version: 10.0.16299.15

Image Version: 10.0.16299.309
```

```
[==========================100.0%==========================] The restore
operation completed successfully.
The operation completed successfully.
```

> ⓘ **Примечание**
>
> Выполнение операций команд может занять несколько минут. Дополнительные сведения см. в статье "Восстановление образа Windows" и использование средства проверки системных файлов.

Обновление Windows

Перед попыткой обновления необходимо установить все важные обновления. Сюда входят обновления драйверов оборудования на компьютере.

Отвечайте на вопросы, которые запрашивает агент, и следуйте инструкциям, чтобы убедиться, что Windows обновлена. Вы также можете запустить средство устранения неполадок Обновл. Windows, описанное выше.

Выберите "**Пуск**", выберите "**Параметры** питания" и перезагрузите компьютер.

Удаление антивирусного программного обеспечения, отличного от Майкрософт

Используйте Защитник Windows для защиты во время обновления.

Проверьте сведения о совместимости и при необходимости переустановите антивирусные приложения после обновления. Если вы планируете переустановить приложение после обновления, убедитесь, что у вас есть носитель установки и все необходимые сведения о активации перед удалением программы.

Чтобы удалить приложение, перейдите к **панель управления**> **Programs**>**Programs and Features** и выберите антивирусное приложение, а затем нажмите кнопку **"Удалить".** Нажмите кнопку "**Да** ", когда вам будет предложено подтвердить удаление программы.

Дополнительные сведения см. в разделе Windows 7. Как правильно удалить программы или восстановить или удалить программы в Windows 10.

Удаление неисключаемого программного обеспечения

Устаревшие приложения могут вызвать проблемы с обновлением Windows. Поэтому удаление старых или неуклюжных приложений с компьютера может помочь.

Если вы планируете переустановить приложение позже, убедитесь, что у вас есть установочный носитель и все необходимые сведения о активации перед его удалением.

Чтобы удалить программы, выполните те же действия, что и приведенные выше для удаления антивирусного программного обеспечения, отличного от Майкрософт, но вместо удаления антивирусного приложения повторите действия для всех неиспользуемых, неиспользуемых или устаревших программ.

Обновление встроенного ПО и драйверов

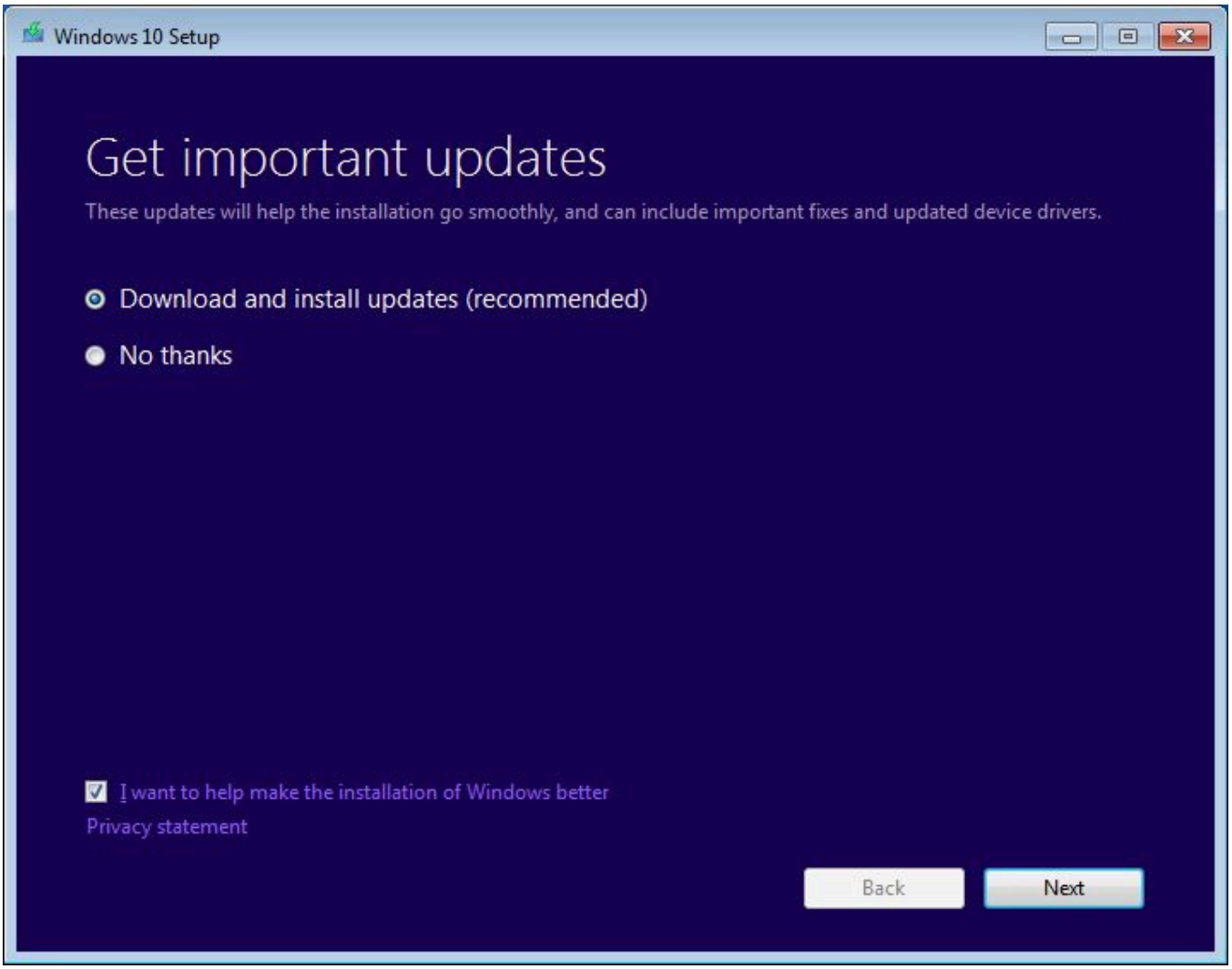
Обновление встроенного ПО (например, BIOS) и установка аппаратных драйверов — это расширенная задача. Не пытайтесь обновить BIOS, если вы не знакомы с параметрами BIOS или не знаете, как восстановить предыдущую версию BIOS, если возникли проблемы. Большинство обновлений BIOS предоставляются в виде обновления flash. Изготовитель может предоставить средство для выполнения обновления или может потребоваться ввести BIOS и обновить его вручную. Не забудьте сохранить рабочие параметры BIOS, так как некоторые обновления могут сбросить конфигурацию и завершить загрузку компьютера, если (например) конфигурация RAID изменена.

Большинство обновлений BIOS и других компонентов оборудования можно получить с веб-сайта, поддерживаемого производителем компьютера. Например, драйверы устройств Microsoft Surface можно получить по адресу: скачайте последнюю версию встроенного ПО и драйверов для устройств Surface.

Чтобы получить соответствующие драйверы встроенного ПО, найдите самую обновленную версию драйвера, предоставляемую производителем компьютера. Установите эти обновления и перезагрузите компьютер после установки. Обратитесь за помощью к производителю, если у вас возникли вопросы.

Убедитесь, что выбран параметр "Скачивание и установка обновлений"

При запуске Обновл. Windows процесс установки попросит вас **получить важные обновления**. Ответ " **Да",** если компьютер, который вы обновляете, подключен к Интернету. См. следующий пример.



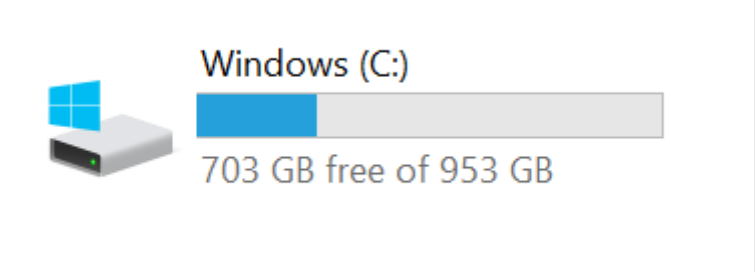
Проверка места на диске

Список требований для Windows 10 можно просмотреть в спецификациях Windows 10 и требованиях к системе. Одним из требований является то, что достаточно места на жестком диске для установки. Для обновления 32-разрядной ОС или 20 ГБ для 64-разрядной ОС должно быть доступно не менее 16 ГБ свободного места.

Чтобы просмотреть объем свободного места на жестком диске на компьютере, откройте проводник. В Windows 7 это было названо проводником Windows.

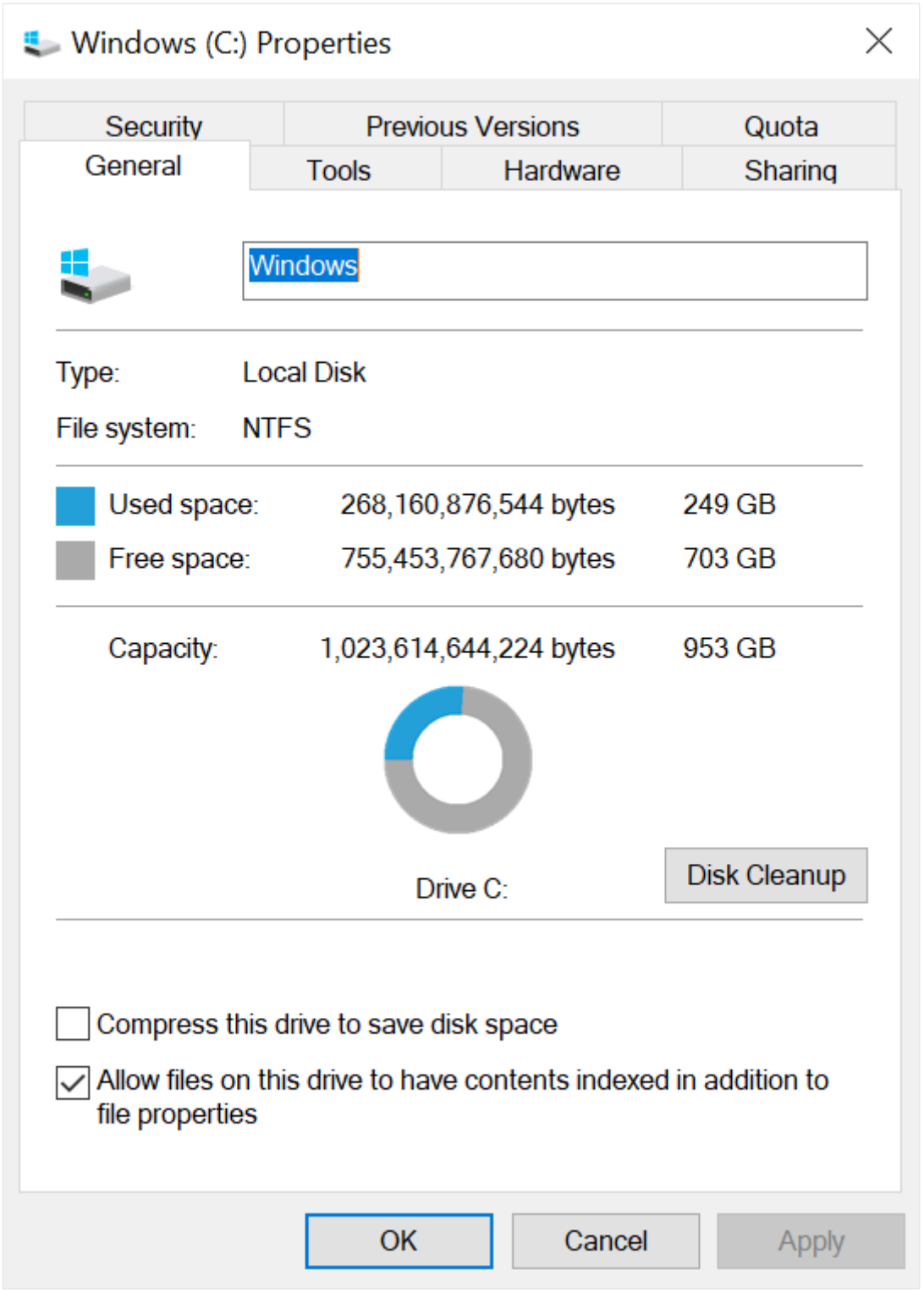
В **проводник выберите компьютер или этот компьютер слева, а затем просмотрите жесткие диски или на устройствах и дисках.** Если есть несколько дисков, системный диск — это диск, который включает логотип Microsoft Windows над значком диска.

Объем свободного места на системном диске будет отображаться под диском. См. следующий пример.



В предыдущем примере на системном диске (C:) доступно 703 ГБ свободного места.

Чтобы освободить больше места на системном диске, начните с запуска очистки диска. Чтобы получить доступ к очистке диска, щелкните правой кнопкой мыши значок жесткого диска и выберите пункт "Свойства". См. следующий пример.



Инструкции по очистке диска и другим предложениям по освобождению места на жестком диске см . в советах по освобождению места на диске на компьютере .

При запуске очистки диска и включении параметра очистки системных файлов можно удалить предыдущие установки Windows, что может освободить большое количество места. Это следует сделать только в том случае, если вы не планируете восстановить старую версию ОС.

Откройте командную строку с повышенными привилегиями

> **Совет**
>
> Для запуска **средства SetupDiag** больше не требуется открывать командную строку с повышенными привилегиями. Однако это по-прежнему оптимальный способ запуска средства.

Чтобы запустить командную строку с повышенными привилегиями, нажмите клавишу Windows на клавиатуре, введите *cmd*, нажмите клавиши CTRL+SHIFT+ВВОД, а затем нажмите **кнопку "Да** ", чтобы подтвердить запрос на повышение прав. Дополнительные сведения о снимках экранах и других шагах для открытия командной строки с повышенными привилегиями см. в статье "Командная строка (администратор) Windows 7".

> **Примечание**
>
> При открытии командной строки с повышенными привилегиями обычно запускается в каталоге *C:\WINDOWS\system32* . Чтобы запустить программу, которую вы недавно скачали, необходимо изменить каталог, в котором находится программа. Кроме того, можно переместить или скопировать программу в каталог в переменной PATH. Эти каталоги автоматически ищутся. Введите `echo %PATH%` каталоги в переменной PATH.

Другим вариантом является использование проводник для создания новой папки в C: с коротким именем, например "new", а затем скопируйте или переместите программы, которые нужно запустить (например, SetupDiag) в эту папку с помощью проводник. При открытии командной строки с повышенными привилегиями перейдите в этот каталог, введя `cd c:\new`его, и теперь вы можете запускать программы в этой папке.

Если вы скачали *программу SetupDiag.exe* на компьютер, скопировали ее в папку *C:\new*, а затем открыли командную строку с повышенными привилегиями, а затем введите `cd c:\new` в этот каталог, просто введите `setupdiag` и нажмите клавишу ВВОД, чтобы запустить программу. Эта программа анализирует файлы на компьютере, чтобы узнать, почему сбой обновления Windows, и если причина была распространенной, он сообщит об этой причине. Это не исправит проблему для вас, но зная, почему обновление завершилось сбоем, позволяет предпринять шаги по устранению проблемы.

Сбор данных

Если вам нужна помощь службы поддержки Microsoft, мы рекомендуем собирать информацию путем выполнения действий, описанных в разделе Сбор информации с

помощью TSS для решения проблем, связанных с развертыванием.

Справочные материалы

- Вопросы и ответы о Windows 10 для ИТ-специалистов
- требования к системе Windows 10 Корпоративная
- Спецификации Windows 10
- Форумы ИТ-специалистов в Windows 10
- Исправление Обновл. Windows ошибок с помощью средства подготовки к обновлению системы или DISM

SetupDiag

Применяется к: ✅ Windows 11, ✅ Windows 10

> ⓘ **Примечание.**
>
> Эта статья представляет собой статью уровня 300 (средний расширенный). Полный список статей этого раздела см. в статье Устранение ошибок обновления Windows .

Сведения об установкеDiag

> ⓘ **Внимание**
>
> При запуске SetupDiag вручную корпорация Майкрософт рекомендует запустить последнюю версию SetupDiag. Последняя версия доступна по следующей ссылке:
>
> Скачайте последнюю версию SetupDiag
>
> Запуск последней версии обеспечивает последнюю функциональность и устраняет известные проблемы.

SetupDiag — это средство диагностики, которое можно использовать для получения сведений о причинах неудачного обновления Windows.

SetupDiag работает путем изучения файлов журнала программы установки Windows. Он пытается проанализировать эти файлы журнала, чтобы определить основную причину сбоя при обновлении компьютера или обновлении до Windows. SetupDiag можно запустить на компьютере, который не удалось обновить. Журналы также можно экспортировать с компьютера в другое расположение, а затем запустить SetupDiag в автономном режиме.

SetupDiag входит в программу установки Windows во всех поддерживаемых в настоящее время версиях Windows.

В процессе обновления программа установки Windows извлекает все свои исходные файлы, включая `SetupDiag.exe`, в `%SystemDrive%\$Windows.~bt\Sources` каталог . Если с обновлением возникла проблема, программа SetupDiag автоматически запускается, чтобы определить причину сбоя.

При запуске с помощью программы установки Windows используются следующие параметры :

- `/ZipLogs:False`
- `/Format:xml`
- `/Output:%windir%\logs\SetupDiag\SetupDiagResults.xml`
- `/RegPath:HKEY_LOCAL_MACHINE\SYSTEM\Setup\SetupDiag\Results`

Результирующий анализ SetupDiag можно найти по адресу `%WinDir%\Logs\SetupDiag\SetupDiagResults.xml` и в реестре в разделе `HKLM\SYSTEM\Setup\SetupDiag\Results`.

> ⓘ **Примечание.**
>
> Если программа установки Windows запускает setupDiag автоматически, путь к реестру не совпадает с путем реестра по умолчанию при запуске SetupDiag вручную. Если setupDiag запускается вручную, а `/RegPath` параметр не указан, данные сохраняются в реестре по адресу `HKLM\SYSTEM\Setup\MoSetup\Volatile\SetupDiag`.

> ⓘ **Внимание**
>
> Если setupDiag указывает, что произошло несколько сбоев, последний сбой в файле журнала обычно является неустранимой ошибкой, а не первой.

Если процесс обновления продолжается в обычном режиме `Sources` , каталог, в том числе `SetupDiag.exe` , перемещается в для `%SystemDrive%\Windows.Old` очистки. `Windows.old` Если каталог будет удален позже, `SetupDiag.exe` он также удаляется.

> **Совет**
>
> Если `SetupDiag.exe` это необходимо после `Windows.old` удаления каталога, его можно скачать из Центра загрузки Майкрософт.

Требования

1. Целевая версия Windows должна быть поддерживаемой в настоящее время версией Windows. Изначально установленная версия Windows может быть версией Windows, которая не поддерживается, если:

    - Целевая версия Windows является поддерживаемой в настоящее время версией Windows.

- Обновление до целевой версии Windows поддерживается с исходной установленной версии Windows.

2. необходимо установить платформа .NET Framework 4.7.2 или более поздней версии. Чтобы определить, какая версия .NET предустановлена с определенной версией Windows, см. платформа .NET Framework требования к системе: Поддерживаемые клиентские операционные системы. Сведения о том, какая версия .NET установлена в настоящее время, см. в статье Практическое руководство. Определение установленных версий платформа .NET Framework.

   Следующий запрос командной строки можно использовать для отображения текущей установленной версии .NET:

   Командная строка Windows

   ```
   reg.exe query "HKLM\SOFTWARE\Microsoft\Net Framework Setup\NDP\v4" /s
   ```

   До тех пор, пока установлена по крайней мере требуемая версия .NET, никаких дополнительных действий не требуется, в том числе при установке более новой версии.

3. **Setupdiag.exe** следует запускать из командной строки с повышенными привилегиями, чтобы она работала правильно.

Использование SetupDiag

Чтобы использовать SetupDiag, выполните следующие действия:

1. Убедитесь, что система соответствует требованиям.

2. Скачайте последнюю версию SetupDiag.

3. Если веб-браузер спрашивает, что делать с файлом, нажмите кнопку **Сохранить**. По умолчанию файл сохраняется в папке **Загрузки**, которая отображается в проводник в разделе **Быстрый доступ** в области навигации слева. При необходимости файл также можно сохранить в другом расположении с помощью **команды Сохранить как**.

4. После завершения загрузки SetupDiag откройте командную строку с повышенными привилегиями и перейдите в каталог, в который `setupdiag.exe` был скачан и сохранен.

5. В командной строке с повышенными привилегиями выполните команду `setupdiage.exe` в интерактивном режиме, используя требуемые параметры, как

описано в разделах Параметры и примеры .

6. Дождитесь завершения setupDiag.
7. После завершения установкиDiag в той же папке, из которой была запущена программа SetupDiag, создаются два файла:
   - Файл конфигурации.
   - Файл журнала.
8. Используйте Блокнот, чтобы открыть файл журнала **SetupDiagResults.log**.
9. Просмотрите отображаемые сведения. Если правило было сопоставлено, эта информация может сказать, почему не удалось выполнить обновление компьютера, и, возможно, как устранить проблему. См. раздел Пример текстового журнала.

> **Совет**
>
> Инструкции по запуску средства в автономном режиме в Среде предустановки Windows см. в разделах **Параметры** и **Примеры**.

Параметры

Развернуть таблицу

Параметр	Описание
/?	Отображение справочных сведений
/Output:[Полный путь и имя файла выходного журнала]	Этот необязательный параметр указывает имя и расположение файла журнала результатов. Выходной файл содержит анализ из SetupDiag. Поддерживаются только выходные данные в текстовом формате. UNC-пути работают при условии, что контекст, в котором выполняется SetupDiag, имеет доступ к UNC-пути. Если путь содержит пробел, весь путь должен быть заключен в двойные кавычки ("). Пример см. в разделах Примеры . По умолчанию. Если параметр не указан, SetupDiag создает **файл SetupDiagResults.log** в том же каталоге, где выполняется **SetupDiag.exe** .
/LogsPath:[Полный путь к журналам]	Этот необязательный параметр указывает расположение журналов для анализа и место поиска файлов журналов для автономного анализа. Эти файлы журнала могут быть в формате неструктурированных папок или содержать несколько подкаталогов. SetupDiag рекурсивно выполняет поиск по всем дочерним каталогам. По умолчанию проверяет текущую систему на наличие журналов.

Параметр	Описание
/ZipLogs:[True | False]	Этот необязательный параметр сообщает **SetupDiag.exe** о создании ZIP-файла, содержащего результаты и все файлы журналов, которые были проанализированы. ZIP-файл создается в том же каталоге, где выполняется **SetupDiag.exe** . По умолчанию: если не указано, используется значение true.
/Format:[xml | json]	Этот необязательный параметр задает формат выходных данных для файлов журнала в формате XML или JSON. Если этот параметр не указан, текстовый формат используется по умолчанию.
/Scenario: [Восстановление | Отладка]	Этот необязательный параметр может выполнять один из следующих двух элементов на основе используемого аргумента: • Восстановление позволяет **SetupDiag.exe** искать и обрабатывать журналы сброса и восстановления, а также игнорировать журналы установки и обновления. • Отладка дает **SetupDiag.exe** инструкции по отладке дампов памяти, если установлены необходимые отладочные двоичные файлы.
/Многословный	Этот необязательный параметр создает журнал диагностики в текущем каталоге с сведениями об отладке, дополнительными данными и сведениями о SetupDiag. По умолчанию SetupDiag создает только запись файла журнала для серьезных ошибок. При использовании **/Verbose** программа SetupDiag всегда создает другой файл журнала со сведениями об отладке. Эти сведения могут быть полезны при отправке сообщения о проблеме с помощью SetupDiag.
/NoTel	Этот необязательный параметр сообщает **SetupDiag.exe** не отправлять диагностические данные телеметрии в корпорацию Майкрософт.
/RegPath	Этот необязательный параметр указывает **SetupDiag.exe** добавить сведения о сбоях в реестр по заданному пути. Пути к реестру должны начинаться с **HKEY_LOCAL_MACHINE** или **HKEY_CURRENT_USER** и быть доступными на уровне повышения прав SetupDiag выполняется в разделе . Если этот параметр не указан, путь по умолчанию — `HKLM\SYSTEM\Setup\MoSetup\Volatile\SetupDiag`.
/AddReg	Этот необязательный параметр Указывает **SetupDiag.exe** добавить сведения о сбоях в реестр в выполняемой системе в автономном режиме. SetupDiag по умолчанию добавляет сведения о сбоях в реестр только в оперативном режиме. Данные реестра будут передаваться, `HKEY_LOCAL_MACHINE\SYSTEM\Setup\MoSetup\Volatile\SetupDiag` если не указано иное.

ⓘ Примечание.

Параметр **/Mode** не рекомендуется использовать в SetupDiag.

В предыдущих версиях параметр **/Mode** использовался с параметром **/LogsPath** в автономном режиме и анализировал набор файлов журнала, которые были записаны на другом компьютере. В текущих версиях SetupDiag, если задан **параметр /LogsPath** , программа SetupDiag автоматически выполняется в автономном режиме, поэтому параметр **/Mode** не требуется.

Примеры:

> ⓘ **Внимание**
>
> **SetupDiage.exe** следует запускать из командной строки с повышенными привилегиями, чтобы она работала правильно.

- В следующем примере программа SetupDiag выполняется без параметров и отображает справочные сведения.

  Командная строка Windows

  ```
  SetupDiag.exe
  ```

- В следующем примере SetupDiag выполняется в интерактивном режиме (этот режим используется по умолчанию). Он знает, где искать журналы в текущей (сбойной) системе, поэтому нет необходимости собирать журналы заранее. Указано пользовательское расположение для результатов.

  Командная строка Windows

  ```
  SetupDiag.exe /Output:C:\SetupDiag\Results.log
  ```

- В следующем примере параметр **/Output** используется для сохранения результатов в имени пути, содержащего пробел:

  Командная строка Windows

  ```
  SetupDiag /Output:"C:\Tools\SetupDiag\SetupDiag Results\Results.log"
  ```

- В следующем примере указывается, что SetupDiag выполняется в автономном режиме и обрабатывает файлы журналов, найденные в **папке D:\Temp\Logs\LogSet1**.

Командная строка Windows

```
SetupDiag.exe /Output:C:\SetupDiag\Results.log /LogsPath:D:\Temp\Logs\LogSet1
```

- Ниже приведен пример режима сброса и восстановления в автономном режиме. SetupDiag предписывает искать журналы сброса и восстановления в указанном расположении LogsPath. Затем он выводит результаты в каталог, указанный параметром **/Output** .

Командная строка Windows

```
SetupDiag.exe /Output:C:\SetupDiag\RecoveryResults.log
/LogsPath:D:\Temp\Cabs\PBR_Log /Scenario:Recovery
```

- В следующем примере показан пример режима сброса и восстановления в сети. SetupDiag предписывает искать журналы сброса и восстановления в текущей системе и выводить результаты в формате XML.

Командная строка Windows

```
SetupDiag.exe /Scenario:Recovery /Format:xml
```

- Ниже приведен пример автономного режима. SetupDiag содержит инструкции по анализу файлов журнала установки и обновления в каталоге LogsPath и выводу результатов в `C:\SetupDiag\Results.txt`.

Командная строка Windows

```
SetupDiag.exe /Output:C:\SetupDiag\Results.txt /LogsPath:D:\Temp\Logs\Logs1
/RegPath:HKEY_CURRENT_USER\SYSTEM\SetupDiag
```

- В следующем примере приведен пример режима "в сети". SetupDiag предписывает искать журналы установки и обновления в текущей системе и выводить результаты в формате XML в `C:\SetupDiag\Results.xml`.

Командная строка Windows

```
SetupDiag.exe /Output:C:\SetupDiag\Results.xml /Format:xml
```

Файлы журнала

Файлы журнала установки Windows и журналы событий содержат сведения о том, где создаются журналы во время установки Windows. Для автономной обработки программа

SetupDiag должна выполняться для содержимого всей папки. Например, в зависимости от того, когда произошел сбой обновления, скопируйте одну из следующих папок в автономное расположение:

- `\$Windows.~bt\sources\panther`
- `\$Windows.~bt\Sources\Rollback`
- `\Windows\Panther`
- `\Windows\Panther\NewOS`

Если родительская папка и все вложенные папки копируются, SetupDiag автоматически выполняет поиск файлов журналов во всех подкаталогах.

Анализ проверка ошибок установки

Когда Microsoft Windows сталкивается с условием, которое скомпрометирует безопасную работу системы, система останавливается. Это условие называется ошибкой проверка. Это условие также часто называется сбоем системы, ошибкой ядра, stop-ошибкой или BSOD. Обычно эта ошибка возникает на аппаратном устройстве, драйвере оборудования или связанном программном обеспечении.

Если в системе включены аварийные дампы, создается файл аварийного дампа. Если ошибка проверка возникает во время обновления, программа установки Windows извлекает файл minidump (`setupmem.dmp`). SetupDiag также может выполнять отладку этих мини-модулей, связанных с установкой.

Чтобы выполнить отладку проверка ошибок, связанных с установкой, выполните следующее:

- Укажите параметр **/LogsPath** . Дампы памяти не могут быть отлажены в оперативном режиме.
- Соберите файл дампа памяти установки (setupmem.dmp) из системы, включающей сбой.

  `Setupmem.dmp` создается в **%SystemDrive%\$Windows.~bt\Sources\Rollback** или в **%WinDir%\Panther\NewOS\Rollback** в зависимости от того, когда произошла ошибка проверка.
- Установите средства отладки Windows на компьютере, на котором запущена программа SetupDiag.

В следующем примере файл копируется в `D:\Dump` каталог, `setupmem.dmp` а перед запуском SetupDiag устанавливаются средства отладки Windows:

Командная строка Windows

```
SetupDiag.exe /Output:C:\SetupDiag\Dumpdebug.log /LogsPath:D:\Dump
```

Известные проблемы

- Обработка некоторых правил может занять много времени, если задействованные файлы журнала имеют большой размер.

Пример выходных данных

Следующая команда является примером, в котором SetupDiag выполняется в автономном режиме.

Командная строка Windows

```
D:\SetupDiag>SetupDiag.exe /output:c:\setupdiag\result.xml
/logspath:D:\Tests\Logs\f55be736-beed-4b9b-aedf-c133536c946e /format:xml

SetupDiag v1.7.0.0
Copyright (c) Microsoft Corporation. All rights reserved.

Searching for setup logs...
Found d:\tests\Logs\f55be736-beed-4b9b-aedf-c133536c946e\setupact_6.log with update
date 6/12/2023 2:44:20 PM to be the correct setup log.
Found d:\tests\Logs\f55be736-beed-4b9b-aedf-c133536c946e\setupact_1.log with update
date 6/12/2023 2:45:19 PM to be the correct rollback log.

Gathering baseline information from setup logs...

SetupDiag: processing rule: CompatScanOnly.
...No match.

...

SetupDiag: processing rule: DISMImageSessionFailure.
..
Error: SetupDiag reports DISM provider failure.
Last Phase: Safe OS
Last Operation: Apply Optional Component status
Message = Failed to get the IDismImage instance from the image session
Function: CDISMManager::CloseImageSession
Error: 0x800706ba
Recommend you re-download the update source files, reboot and try the update again.

SetupDiag found 1 matching issue.

SetupDiag results were logged to: c:\setupdiag\results.xml
Logs ZipFile created at: c:\setupdiag\Logs_14.zip
```

Правила

При поиске файлов журнала программа SetupDiag использует набор правил для сопоставления известных проблем. Эти правила содержатся в XML-файле. Xml-файл может быть обновлен новыми и обновленными правилами по мере того, как становятся доступными новые версии SetupDiag.

Имя каждого правила и связанный с ним уникальный идентификатор правила перечислены с описанием известной проблемы, блокирующей обновление. В описаниях правил термин **downlevel** относится к первому этапу процесса обновления, который выполняется в исходной ОС.

Развернуть таблицу

Имя правила	Код GUID	Описание
CompatScanOnly	FFDAFD37-DB75-498A-A893-472D49A1311D	Это правило указывает, что `setup.exe` был вызван с определенным параметром командной строки, который указывает, что программа установки будет выполнять только проверку совместимости, а не обновление.
PlugInComplianceBlock	D912150B-1302-4860-91B5-527907D08960	Обнаруживает все блоки совместимости в подключаемых модулях соответствия сервера. Это правило предназначено только для обновлений сервера. Он выводит блок соответствия требованиям и необходимые исправления.
BitLockerHardblock	C30152E2-938E-44B8-915B-D1181BA635AE	Этот блок является блоком обновления, если целевая ОС не поддерживает BitLocker, но в ос узла включен BitLocker.
VHDHardblock	D9ED1B82-4ED8-4DFD-8EC0-BE69048978CC	Этот блок происходит, когда ОС узла загружается в образ VHD. Обновление не поддерживается, если ОС узла загружается из образа VHD.

Имя правила	Код GUID	Описание
PortableWorkspaceHardblock	5B0D3AB4-212A-4CE4-BDB9-37CA404BB280	Этот блок указывает, что ОС узла загружается с устройства To-Go Windows (USB-ключ. Обновление не поддерживается в среде Windows To-Go.
AuditModeHardblock	A03BD71B-487B-4ACA-83A0-735B0F3F1A90	Этот блок указывает, что ос узла в настоящее время загружается в режиме аудита, специальном режиме для изменения состояния Windows. Обновление из этого состояния не поддерживается.
SafeModeHardblock	404D9523-B7A8-4203-90AF-5FBB05B6579B	Этот блок указывает, что ОС узла загружается в безопасном режиме, где обновление не поддерживается.
InsufficientSystemPartitionDiskSpaceHardblock	3789FBF8-E177-437D-B1E3-D38B4C4269D1	Этот блок возникает, когда программа установки определяет, что системный раздел не имеет достаточно места для обслуживания с новыми загрузочными файлами, необходимыми в процессе обновления. Системный раздел — это место, где хранятся файлы загрузчика.
CompatBlockedApplicationAutoUninstall	BEBA5BC6-6150-413E-8ACE-5E1EC8D34DD5	Это правило указывает на наличие приложения, которое необходимо удалить, прежде чем продолжить установку.
CompatBlockedApplicationDismissable	EA52620B-E6A0-4BBC-882E-0686605736D9	При запуске установки в режиме **/quiet** сообщения приложения превратятся в блоки, если в командной строке также не указан **параметр /compat ignorewarning**. Это правило указывает, что настройка была выполнена в режиме **/quiet** , но есть сообщение о закрытии приложения, которое

Имя правила	Код GUID	Описание
		препятствует продолжению установки.
CompatBlockedFODDismissable	7B693C42-793E-4E9E-A10B-ED0F33D45E2A	При запуске установки в режиме **/quiet** появляются сообщения о функциях по запросу, которые превратятся в блоки, если в командной строке также не указан **параметр /compat ignorewarning**. Это правило указывает на то, что настройка выполнялась в режиме **/quiet** , но есть сообщение о блоке компонента по запросу, которое не позволяет продолжить установку. Обычно в целевом образе ОС отсутствует компонент по запросу, установленный в текущей ОС. Удаление функции по запросу в текущей ОС также должно устранить проблему.
CompatBlockedApplicationManualUninstall	9E912E5F-25A5-4FC0-BEC1-CA0EA5432FF4	Это правило указывает, что приложение без записи "Установка и удаление программ" присутствует в системе и блокирует продолжение настройки. Этот блок обычно требует удаления файлов, связанных с этим приложением, вручную.
GenericCompatBlock	511B9D95-C945-4F9B-BD63-98F1465E1CF6	Правило указывает, что система не соответствует требованиям к оборудованию для работы Windows. Например, на устройстве отсутствует требование для TPM 2.0. Эта проблема может возникнуть, даже если предпринята попытка обойти требования к оборудованию.
GatedCompatBlock	34A9F145-3842-4A68-	Это правило указывает, что обновление завершилось сбоем из-за временного блока.

Имя правила	Код GUID	Описание
	987F-4622EE0FC162	Временный блок создается, когда обнаружена проблема с определенным программным или аппаратным драйвером, и проблема находится в ожидании исправления. Блок снимается после того, как исправление становится широко доступным.
HardblockDeviceOrDriver	ED3AEFA1-F3E2-4F33-8A21-184ADF215B1B	Эта ошибка указывает, что драйвер устройства, загруженный в ОС узла, несовместим с более новой версией ОС. Перед обновлением необходимо удалить драйвер устройства.
HardblockMismatchedLanguage	60BA8449-CF23-4D92-A108-D6FCEFB95B45	Это правило указывает, что выпуски ос узла и целевого языка ОС не совпадают.
HardblockFlightSigning	598F2802-3E7F-4697-BD18-7A6371C8B2F8	Это правило указывает, что целевая ОС является предварительной версией, сборкой программы предварительной оценки Windows, а на целевом компьютере включена безопасная загрузка. Это правило блокирует загрузку предварительной подписанной сборки, если она установлена на компьютере.
DiskSpaceBlockInDownLevel	6080AFAC-892E-4903-94EA-7A17E69E549E	Этот сбой указывает на то, что в системе не было места на диске во время операций нижнего уровня обновления.
DiskSpaceFailure	981DCBA5-B8D0-4BA7-A8AB-4030F7A10191	Этот сбой указывает, что на системном диске в какой-то момент после первой перезагрузки при обновлении закончился свободное место на диске.

Имя правила	Код GUID	Описание
PreReleaseWimMountDriverFound	31EC76CC-27EC-4ADC-9869-66AABEDB56F0	Фиксирует сбои из-за регистрации в системе нераспознанного `wimmount.sys` драйвера.
DebugSetupMemoryDump	C7C63D8A-C5F6-4255-8031-7459773C3C6	Это автономное правило указывает на ошибку, проверка произошла во время установки. Если средства отладчика доступны в системе, программа SetupDiag выполняет отладку дампа памяти и предоставляет подробные сведения.
DebugSetupCrash	CEEBA202-6F04-4BC3-84B8-7B99AED924B1	Это правило только в автономном режиме указывает, что при настройке произошл сбой, который привел к дампу памяти процесса. Если средства отладчика установлены в системе, программа SetupDiag выполняет отладку дампа памяти и предоставляет дополнительные сведения.
DebugMemoryDump	505ED489-329A-43F5-B467-FCAAF6A1264C	Это автономное правило предназначено для любого файла memory.dmp, который был результатом операции установки или обновления. Если средства отладчика установлены в системе, программа SetupDiag выполняет отладку дампа памяти и предоставляет дополнительные сведения.
DeviceInstallHang	37BB1C3A-4D79-40E8-A556-FDA126D40BC6	Это правило сбоя указывает, что система зависла или проверила ошибку на этапе установки устройства при обновлении.
DriverPackageMissingFileFailure	37BB1C3A-4D79-40E8-A556-FDA126D40BC6	Это правило указывает, что во время установки устройства в пакете драйвера отсутствует файл. Обновление пакета

Имя правила	Код GUID	Описание
		драйверов может помочь устранить проблему.
UnsignedDriverBootFailure	CD270AA4-C044-4A22-886A-F34EF2E79469	Это правило указывает, что неподписанный драйвер вызвал сбой загрузки.
BootFailureDetected	4FB446C2-D4EC-40B4-97E2-67EB19D1CFB7	Это правило указывает, что произошел сбой загрузки на определенном этапе обновления. Правило указывает код сбоя и этап в целях диагностики.
WinSetupBootFilterFailure	C073BFC8-5810-4E19-B53B-4280B79E096C	Обнаруживает сбои в операциях с файлами в режиме ядра.
FindDebugInfoFromRollbackLog	9600EB68-1120-4A87-9FE9-3A4A70ACFC37	Это правило определяет и предоставляет подробные сведения о проверка ошибок во время процесса установки или обновления, что привело к созданию дампа памяти. Однако пакет отладчика не требуется на выполняемом компьютере.
AdvancedInstallerFailed	77D36C96-32BE-42A2-BB9C-AAFFE64FCADC	Находит неустранимые расширенные операции установщика, которые вызывают сбои установки. Указывает на критический сбой в AdvancedInstaller при запуске пакета установщика, включая вызываемые .exe, коды фазы, режима, компонента и ошибок.
AdvancedInstallerPluginInstallFailed	2F784A0E-CEB1-47C5-8072-F1294C7CB4AE	Это правило указывает, что не удалось установить некоторые компоненты, устанавливаемые с помощью расширенного установщика (FeatureOnDemand, языковые пакеты, пакеты .NET и т. д.). Правило вызывает то, что устанавливалось. Если

Имя правила	Код GUID	Описание
		произошел сбой компонента FeatureOnDemand, удалите компонент Windows, перезагрузитесь и повторите попытку обновления. Если неработоченный компонент является языковым пакетом, удалите дополнительный языковой пакет, перезагрузитесь и повторите попытку обновления.
AdvancedInstallerGenericFailure	4019550D-4CAA-45B0-A222-349C48E86F71	Правило для сопоставления ошибок чтения и записи AdvancedInstaller в общем смысле. Триггеры при сбоях расширенного установщика в общем смысле. Он выводит приложение с именем, фазой, режимом, компонентом и кодом ошибки.
FindMigApplyUnitFailure	A4232E11-4043-4A37-9BF4-5901C46FD781	Обнаруживает сбой единицы миграции, который привел к сбою обновления. Это правило выводит имя подключаемого модуля миграции и код ошибки, созданный в целях диагностики.
FindMigGatherUnitFailure	D04C064B-CD77-4E64-96D6-D26F30B4EE29	Обнаруживает сбой единицы сбора данных миграции, который привел к сбою обновления. Это правило выводит имя модуля сбора или подключаемого модуля и код ошибки, созданный в целях диагностики.
FindMigGatherApplyFailure	A9964E6C-A2A8-45FF-B6B5-25E0BD71428E	Отображает ошибки при сбое подсистемы миграции при выполнении операции сбора или применения. Указывает объект миграции (путь к файлу или реестру), миграция
OptionalComponentFailedToGetOCsFromPackage	D012E2A2-99D8-4A8C-	Это правило соответствует определенному сбою дополнительного компонента

Имя правила	Код GUID	Описание
	BBB2-088B92083D78	при попытке перечислить компоненты в пакете. Указывает, что операции миграции необязательных компонентов (ОС) не удалось перечислить необязательные компоненты из пакета ОС. Выводится имя пакета и код ошибки. Это правило заменяет правило OptionalComponentInstallFailure.
OptionalComponentOpenPackageFailed	22952520-EC89-4FBD-94E0-B67DF88347F6	Соответствует определенному сбою дополнительного компонента при попытке открыть пакет ОС. Выводится имя пакета и код ошибки. Указывает, что необязательная операция миграции компонента не смогла открыть необязательный пакет компонента. Выводит имя пакета и код ошибки.
OptionalComponentInitCBSSessionFailed	63340812-9252-45F3-A0F2-B2A4CA5E9317	Соответствует конкретному сбою, при котором служба или компоненты расширенного установщика не работают или не запущены в системе. Указывает на повреждение стека обслуживания в системе нижнего уровня. Выводит код ошибки, обнаруженной при попытке инициализировать компонент обслуживания в существующей ОС.
CriticalSafeOSDUFailure	73566DF2-CA26-4073-B34C-C9BC70DBF043	Это правило указывает на сбой при обновлении образа SafeOS с критическим динамическим обновлением. Он указывает этап и код ошибки, возникшие при попытке обновить образ SafeOS для диагностических целей.
UserProfileCreationFailureDuringOnlineApply	678117CE-F6A9-40C5-	Указывает, что при создании или изменении профиля

Имя правила	Код GUID	Описание
	BC9F-A22575C78B14	пользователя на этапе применения обновления в сети произошел критический сбой. Он указывает на операции и код ошибки, связанные со сбоем в целях диагностики.
UserProfileCreationFailureDuringFinalize	C6677BA6-2E53-4A88-B528-336D15ED1A64	Соответствует определенной ошибке создания профиля пользователя на этапе завершения установки. Выводится код сбоя.
UserProfileSuffixMismatch	B4BBCCCE-F99D-43EB-9090-078213397FD8	Определяет, когда файл или другой объект приводит к сбою миграции или создания профиля пользователя во время обновления.
DuplicateUserProfileFailure	BD7B3109-80F1-4421-8F0A-B34CD25F4B51	Это правило указывает на неустранимую ошибку при переносе профилей пользователей, как правило, с несколькими идентификаторами БЕЗОПАСНОСТИ, связанными с одним профилем пользователя. Эта ошибка обычно возникает, когда программное обеспечение создает локальные учетные записи пользователей, которые никогда не использовались или не вошли в систему. Правило указывает идентификатор безопасности и имя пользователя учетной записи, которая вызывает сбой. Чтобы попытаться устранить проблему, сначала создайте резервную копию всех файлов пользователя для учетной записи затронутого пользователя. После создания резервной копии файлов пользователя удалите учетную запись поддерживаемым способом. Убедитесь, что

Имя правила	Код GUID	Описание
		учетная запись не требуется или используется для входа на устройство. После удаления учетной записи перезагрузитесь и повторите попытку обновления.
WimMountFailure	BE6DF2F1-19A6-48C6-AEF8-D3B0CE3D4549	Это правило указывает, что обновлению не удалось подключить WIM-файл. В нем отображается имя WIM-файла, а также сообщение об ошибке и код ошибки, связанные со сбоем, в целях диагностики.
WimMountDriverIssue	565B60DD-5403-4797-AE3E-BC5CB972FBAE	Обнаруживает сбои при регистрации в `WimMount.sys` системе.
WimApplyExtractFailure	746879E9-C9C5-488C-8D4B-0C811FF3A9A8	Соответствует сбою при применении WIM на этапах установки извлечения WIM. Он выводит расширение, путь и код ошибки.
UpdateAgentExpanderFailure	66E496B3-7D19-47FA-B19B-4040B9FD17E2	Соответствует сбоям расширителя DPX на этапе нижнего уровня обновления с клиентский компонент Центра обновления Windows. Он выводит имя пакета, функцию, выражение и код ошибки.
FindFatalPluginFailure	E48E3F1C-26F6-4AFB-859B-BF637DA49636	Соответствует любому сбою подключаемого модуля, который setupplatform решает неустраним для установки. Он выводит имя подключаемого модуля, операцию и код ошибки.
MigrationAbortedDueToPluginFailure	D07A24F6-5B25-474E-B516-A730085940C9	Указывает на критический сбой в подключаемом модуле миграции, который приводит к прерыванию установки миграции. Предоставляет операцию установки, имя подключаемого модуля,

Имя правила	Код GUID	Описание
		действие подключаемого модуля и код ошибки.
DISMAddPackageFailed	6196FF5B-E69E-4117-9EC6-9C1EAB20A3B9	Указывает на критический сбой во время операции добавления пакета DISM. Указывает имя пакета, ошибку DISM и код ошибки добавления пакета.
DISMImageSessionFailure	61B7886B-10CD-4C98-A299-B987CB24A11C	Записывает сведения о сбоях, когда DISM не удается успешно запустить сеанс образа.
DISMproviderFailure	D76EF86F-B3F8-433F-9EBF-B4411F8141F4	Активируется при сбое поставщика DISM (подключаемого модуля) в критической операции. Выводит файл (имя подключаемого модуля), функцию с именем + код ошибки и сообщение об ошибке от поставщика.
SysPrepLaunchModuleFailure	7905655C-F295-45F7-8873-81D6F9149BFD	Указывает, что подключаемый модуль sysPrep завершился сбоем в критической операции. Указывает имя подключаемого модуля, имя операции и код ошибки.
UserProvidedDriverInjectionFailure	2247C48A-7EE3-4037-AFAB-95B92DE1D980	Драйвер, предоставленный для настройки (через ввод из командной строки), каким-то образом завершился сбоем. Выводит функцию установки драйвера и код ошибки.
DriverMigrationFailure	9378D9E2-256E-448C-B02F-137F611F5CE3	Это правило указывает на неустранимый сбой при переносе драйверов.
UnknownDriverMigrationFailure	D7541B80-5071-42CE-AD14-FBE8C0C4F7FD	Это правило указывает, что в системе находится недопустимый пакет драйвера. Пакет драйвера приводит к сбою обновления при попытке миграции пакета драйвера на

Имя правила	Код GUID	Описание
		новую ОС. Правило обычно указывает имя пакета драйвера, вызвавшего проблему. Исправление заключается в удалении пакета плохого драйвера, перезагрузке и попытке обновления еще раз. Если обновление этого драйвера доступно от изготовителя оборудования, рекомендуется обновить пакет драйвера.
FindSuccessfulUpgrade	8A0824C8-A56D-4C55-95A0-22751AB62F3E	Определяет, была ли данная настройка успешной или нет на основе журналов.
FindSetupHostReportedFailure	6253C04F-2E4E-4F7A-B88E-95A69702F7EC	Предоставляет сведения о сбоях, которые всплыли на ранних этапах процесса обновления. `setuphost.exe`
FindDownlevelFailure	716334B7-F46A-4BAA-94F2-3E31BC9EFA55	Предоставляет сведения об ошибке, которые отображаются в SetupPlatform позже на этапе нижнего уровня.
FindAbruptDownlevelFailure	55882B1A-DA3E-408A-9076-23B22A0472BD	Предоставляет сведения о сбое последней операции при сбое системы в нижнем уровневом режиме, но журнал просто внезапно заканчивается.
FindEarlyDownlevelError	A4CE4FC9-5E10-4BB1-8ECE-3B29EB9D7C52	Обнаруживает сбои на этапе нижнего уровня перед вызовом платформы установки.
FindSPFatalError	A4028172-1B09-48F8-AD3B-86CDD7D55852	Записывает сведения о сбое при обнаружении неустранимой ошибки на платформе установки.
FindSetupPlatformFailedOperationInfo	307A0133-F06B-4B75-	Предоставляет сведения о последнем этапе и об ошибке, если SetupPlatform указывает

Имя правила	Код GUID	Описание
	AEA8-116C3B53C2D1	на критический сбой. Это правило указывает на операцию и ошибку, связанные со сбоем в целях диагностики.
FindRollbackFailure	3A43C9B5-05B3-4F7C-A955-88F991BB5A48	Предоставляет сведения о последней операции, фазе сбоя и об ошибке при откате.

Примеры журналов

Пример текстового журнала

txt

```
Matching Profile found: OptionalComponentOpenPackageFailed - 22952520-EC89-4FBD-
94E0-B67DF88347F6
System Information:
    Machine Name = Offline
    Manufacturer = MSI
    Model = MS-7998
    HostOSArchitecture = x64
    FirmwareType = PCAT
    BiosReleaseDate = 20160727000000.000000+000
    BiosVendor = BIOS Date: 07/27/16 10:01:46 Ver: V1.70
    BiosVersion = 1.70
    HostOSVersion = 10.0.15063
    HostOSBuildString = 15063.0.amd64fre.rs2_release.170317-1834
    TargetOSBuildString = 10.0.16299.15 (rs3_release.170928-1534)
    HostOSLanguageId = 2057
    HostOSEdition = Core
    RegisteredAV = Windows Defender,
    FilterDrivers = WdFilter,wcifs,WIMMount,luafv,Wof,FileInfo,
    UpgradeStartTime = 3/21/2023 9:47:16 PM
    UpgradeEndTime = 3/21/2023 10:02:40 PM
    UpgradeElapsedTime = 00:15:24
    ReportId = dd4db176-4e3f-4451-aef6-22cf46de8bde

Error: SetupDiag reports Optional Component installation failed to open OC Package.
Package Name: Foundation, Error: 0x8007001F
Recommend you check the "Windows Modules Installer" service (Trusted Installer) is
started on the system and set to automatic start, reboot and try the update again.
Optionally, you can check the status of optional components on the system (search
for Windows Features), uninstall any unneeded optional components, reboot and try
the update again.
Error: SetupDiag reports downlevel failure, Operation: Finalize, Error: 0x8007001F -
0x50015
```

```
Refer to https://learn.microsoft.com/windows/deployment/upgrade/upgrade-error-codes
for error information.
```

Пример журнала XML

XML

```
<?xml version="1.0" encoding="utf-16"?>
<SetupDiag xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns="https://learn.microsoft.com/windows/deployment/upgrade/setupdiag">
  <Version>1.7.0.0</Version>
  <ProfileName>FindSPFatalError</ProfileName>
  <ProfileGuid>A4028172-1B09-48F8-AD3B-86CDD7D55852</ProfileGuid>
  <SystemInfo>
    <MachineName>Offline</MachineName>
    <Manufacturer>Gigabyte Technology Co., Ltd.</Manufacturer>
    <Model>X470 AORUS ULTRA GAMING</Model>
    <HostOSArchitecture>1033</HostOSArchitecture>
    <FirmwareType>UEFI</FirmwareType>
    <BiosReleaseDate>20180808000000.000000+000</BiosReleaseDate>
    <BiosVendor>F3</BiosVendor>
    <BiosVersion />
    <HostOSVersion>10.0.18908</HostOSVersion>
    <HostOSBuildString>18908.1000.amd64fre.rs_prerelease.190524-
1658</HostOSBuildString>
    <TargetOSBuildString>10.0.18912.1001 (rs_prerelease.190601-1739)
</TargetOSBuildString>
    <HostOSLanguageId />
    <HostOSEdition>Professional</HostOSEdition>
    <RegisteredAV>Windows Defender</RegisteredAV>
    <FilterDrivers />
    <UpgradeStartTime>2023-06-06T21:19:10</UpgradeStartTime>
    <UpgradeElapsedTime />
    <UpgradeEndTime>2023-06-06T22:21:49</UpgradeEndTime>
    <RollbackStartTime>0001-01-01T00:00:00</RollbackStartTime>
    <RollbackEndTime>0001-01-01T00:00:00</RollbackEndTime>
    <RollbackElapsedTime />
    <FinalizeStartTime>0001-01-01T00:00:00</FinalizeStartTime>
    <PostOOBESuccessTime>0001-01-01T00:00:00</PostOOBESuccessTime>
    <TotalOfflineTime />
    <CommercialId>Offline</CommercialId>
    <CV>MgUweCZk90KdwUiZ</CV>
    <SetupReportId>F21F8FB6-00FD-4349-84FB-2AC75F389E73</SetupReportId>
    <ReportId>F21F8FB6-00FD-4349-84FB-2AC75F389E73</ReportId>
  </SystemInfo>
  <LogErrorLine>2023-06-06 21:47:11, Error                 SP     Error converting
install time 5/2/2023 to structure[gle=0x00000057]</LogErrorLine>
  <FailureData>
Error: SetupDiag reports Fatal Error.
Last Setup Phase = Downlevel
Last Setup Operation: Gather data, scope: EVERYTHING
Error: 0x00000057</FailureData>
```

```
  <FailureData>LogEntry: 2023-06-06 21:47:11, Error                 SP     Error
converting install time 5/2/2023 to structure[gle=0x00000057]</FailureData>
  <FailureData>LogEntry: 2023-06-06 21:47:11, Error                 SP     Error
converting install time 5/2/2023 to structure[gle=0x00000057]</FailureData>
  <FailureData>
Refer to "https://learn.microsoft.com/windows/desktop/Debug/system-error-codes" for
error information.</FailureData>
  <FailureDetails>Err = 0x00000057, LastOperation = Gather data, scope: EVERYTHING,
LastPhase = Downlevel</FailureDetails>
</SetupDiag>
```

Пример журнала JSON

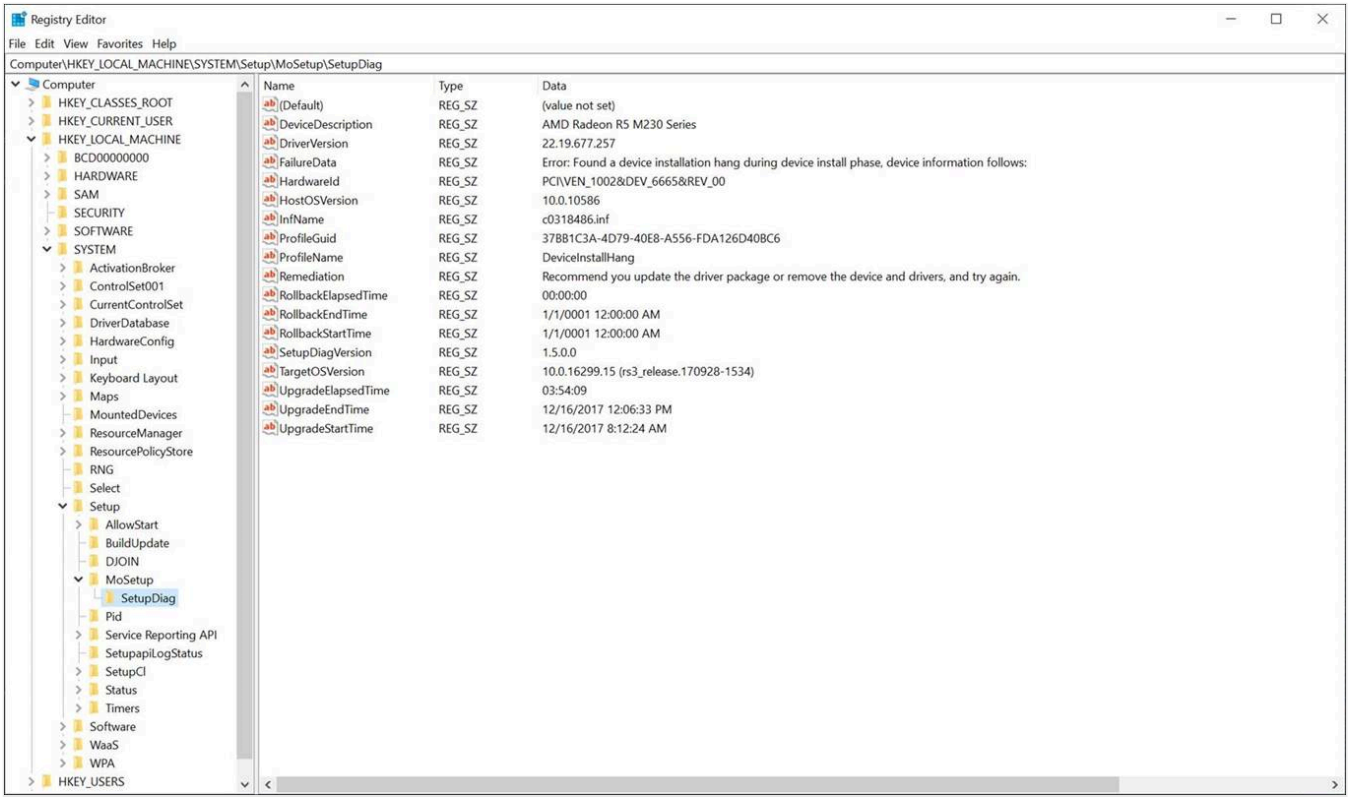
JSON


```
{
    "Version":"1.6.0.0",
    "ProfileName":"FindSPFatalError",
    "ProfileGuid":"A4028172-1B09-48F8-AD3B-86CDD7D55852",
    "SystemInfo":{
        "BiosReleaseDate":"20180808000000.000000+000",
        "BiosVendor":"F3",
        "BiosVersion":"F3",
        "CV":"MgUweCZk90KdwUiZ",
        "CommercialId":"Offline",
        "FilterDrivers":"",
        "FinalizeStartTime":"\/Date(-62135568000000-0800)\/",
        "FirmwareType":"UEFI",
        "HostOSArchitecture":"x64",
        "HostOSBuildString":"18908.1000.amd64fre.rs_prerelease.190524-1658",
        "HostOSEdition":"Professional",
        "HostOSLanguageId":"",
        "HostOSVersion":"",
        "MachineName":"Offline",
        "Manufacturer":"Gigabyte Technology Co., Ltd.",
        "Model":"X470 AORUS ULTRA GAMING",
        "PostOOBESuccessTime":"\/Date(-62135568000000-0800)\/",
        "RegisteredAV":"Windows Defender",
        "ReportId":"F21F8FB6-00FD-4349-84FB-2AC75F389E73",
        "RollbackElapsedTime":"PT0S",
        "RollbackEndTime":"\/Date(-62135568000000-0800)\/",
        "RollbackStartTime":"\/Date(-62135568000000-0800)\/",
        "SetupReportId":"F21F8FB6-00FD-4349-84FB-2AC75F389E73",
        "TargetOSArchitecture":null,
        "TargetOSBuildString":"10.0.18912.1001 (rs_prerelease.190601-1739)",
        "TotalOfflineTime":"PT0S",
        "UpgradeElapsedTime":"PT1H2M39S",
        "UpgradeEndTime":"\/Date(1559884909000-0700)\/",
        "UpgradeStartTime":"\/Date(1559881150000-0700)\/"
    },
    "LogErrorLine":"2023-06-06 21:47:11, Error                 SP     Error
converting install time 5\/2\/2023 to structure[
        gle=0x00000057
```

```
    ]",
    "FailureData":[
        "\u000aError: SetupDiag reports Fatal Error.\u000aLast Setup Phase =
Downlevel\u000aLast Setup Operation: Gather data, scope: EVERYTHING\u000aError:
0x00000057",
        "LogEntry: 2023-06-06 21:47:11, Error                  SP     Error
converting install time 5\/2\/2023 to structure[
            gle=0x00000057
        ]",
        "LogEntry: 2023-06-06 21:47:11, Error                  SP     Error
converting install time 5\/2\/2023 to structure[
            gle=0x00000057
        ]",
        "\u000aRefer to
\"https:\/\/learn.microsoft.com\/windows\/desktop\/Debug\/system-error-codes\" for
error information."
    ],
    "FailureDetails":"Err = 0x00000057, LastOperation = Gather data, scope:
EVERYTHING, LastPhase = Downlevel",
    "DeviceDriverInfo":null,
    "Remediation":[

    ],
    "SetupPhaseInfo":null,
    "SetupOperationInfo":null
}
```


Пример раздела реестра



Связанные статьи

- Устранение ошибок обновления Windows: Техническая информация для ИТ-специалистов.

Last updated on 08.04.2025

Проблемы с обновлением Windows 10

15.01.2025Применяется к: Supported versions of Windows Client

Попробуйте наш виртуальный агент. Он поможет вам быстро определить и устранить распространенные проблемы с загрузкой Windows

> **Примечание**
>
> Это раздел уровня 300 (умеренно расширенный).
>
> Для ИТ-специалистов ознакомьтесь с дополнительными сведениями об **ошибках** обновления Windows 10.

Если обновление Windows 10 не выполнено, полезно понять, когда произошла ошибка в процессе обновления.

> **Важно!**
>
> **Используйте средство SetupDiag**, прежде чем приступить к устранению ошибок обновления вручную. SetupDiag автоматизирует анализ файлов журнала, обнаружение и отчеты о различных типах известных проблем обновления.

Применимо к: Windows 10

Действия, выполняемые во время процессов обновления

Кратко говоря, процесс обновления состоит из четырех этапов, контролируемых программой установки Windows: Downlevel, SafeOS, First boot и Second boot. Компьютер перезагрузится один раз между каждым этапом. Примечание. Ход выполнения отслеживается в реестре во время процесса обновления с помощью следующего раздела. `HKLM\System\Setup\mosetup\volatile\SetupProgress` Этот ключ является переменным и присутствует только во время процесса обновления; Он содержит двоичное значение в диапазоне 0–100.

Эти этапы подробно описаны ниже. Сначала рассмотрим действия, выполняемые на каждом этапе, так как это влияет на тип ошибок, которые могут возникнуть.

1. Этап нижнего уровня: так как этот этап выполняется в исходной ОС, ошибки обновления обычно не видятся. Если возникла ошибка, убедитесь, что исходная ОС стабильна. Также убедитесь, что источник установки Windows и целевой диск доступны.

2. Этап SafeOS: ошибки чаще всего возникают на этом этапе из-за проблем с оборудованием, проблем с встроенного ПО или программного обеспечения шифрования дисков, отличных от Майкрософт.

   Так как компьютер загружается в Windows PE во время этапа SafeOS, полезный способ устранения неполадок заключается в загрузке windows PE с помощью установочного носителя. Вы можете использовать средство создания носителей для создания загрузочного носителя или использовать такие средства, как Windows ADK, а затем загрузить устройство с этого носителя для проверки проблем совместимости оборудования и встроенного ПО.

   > **Совет**
   >
   > Если вы пытаетесь использовать средство создания носителей с USB-накопителем, и это сбой с ошибкой 0x80004005 - 0xa001a, это связано с тем, что USB-диск использует стиль секции GPT. Для этого средства требуется использовать стиль секции MBR. Вы можете использовать `DISKPART` команду для преобразования USB-диска из GPT в MBR. Дополнительные сведения см. в разделе **"Изменение диска таблицы секции GUID" на главный загрузочный диск**.

   Не продолжайте установку Windows 10 после загрузки с этого носителя. Этот метод можно использовать только для выполнения чистой установки, которая не будет переносить какие-либо приложения и параметры, и вам потребуется повторно ввести сведения о лицензии Windows 10.

   Если компьютер не успешно загружается в windows PE с помощью созданного носителя, это, скорее всего, связано с проблемой оборудования или встроенного ПО. Обратитесь к изготовителю оборудования и примените все рекомендуемые обновления BIOS и встроенного ПО. Если вы по-прежнему не можете загрузиться на установочный носитель после применения обновлений, отключить или заменить устаревшее оборудование.

   Если компьютер успешно загружается в Windows PE, но вы не можете просматривать системный диск на компьютере, возможно, что программное обеспечение шифрования дисков, отличное от Майкрософт, блокирует возможность обновления Windows 10. Обновление или временное удаление шифрования дисков.

3. Первый этап загрузки: сбои загрузки на этом этапе относительно редки и почти исключительно вызваны драйверами устройств. Отключите все периферийные устройства, кроме мыши, клавиатуры и дисплея. Получите и установите обновленные драйверы устройств, а затем повторите обновление.

4. Второй этап загрузки: на этом этапе система работает под целевой ОС с новыми драйверами. Сбои загрузки чаще всего возникают из-за вредоносных программ или драйверов фильтров. Отключите все периферийные устройства, кроме мыши, клавиатуры и дисплея. Получите и установите обновленные драйверы устройств, временно удалите антивирусное программное обеспечение, а затем повторите обновление.

Если общие методы устранения неполадок, описанные выше, или быстрые исправления, описанные ниже, не устраняют проблему, можно попытаться проанализировать файлы журналов и интерпретировать коды ошибок обновления. Вы также можете отправить ошибки обновления Windows 10 с помощью Центра отзывов, чтобы корпорация Майкрософт диагностирует вашу проблему.

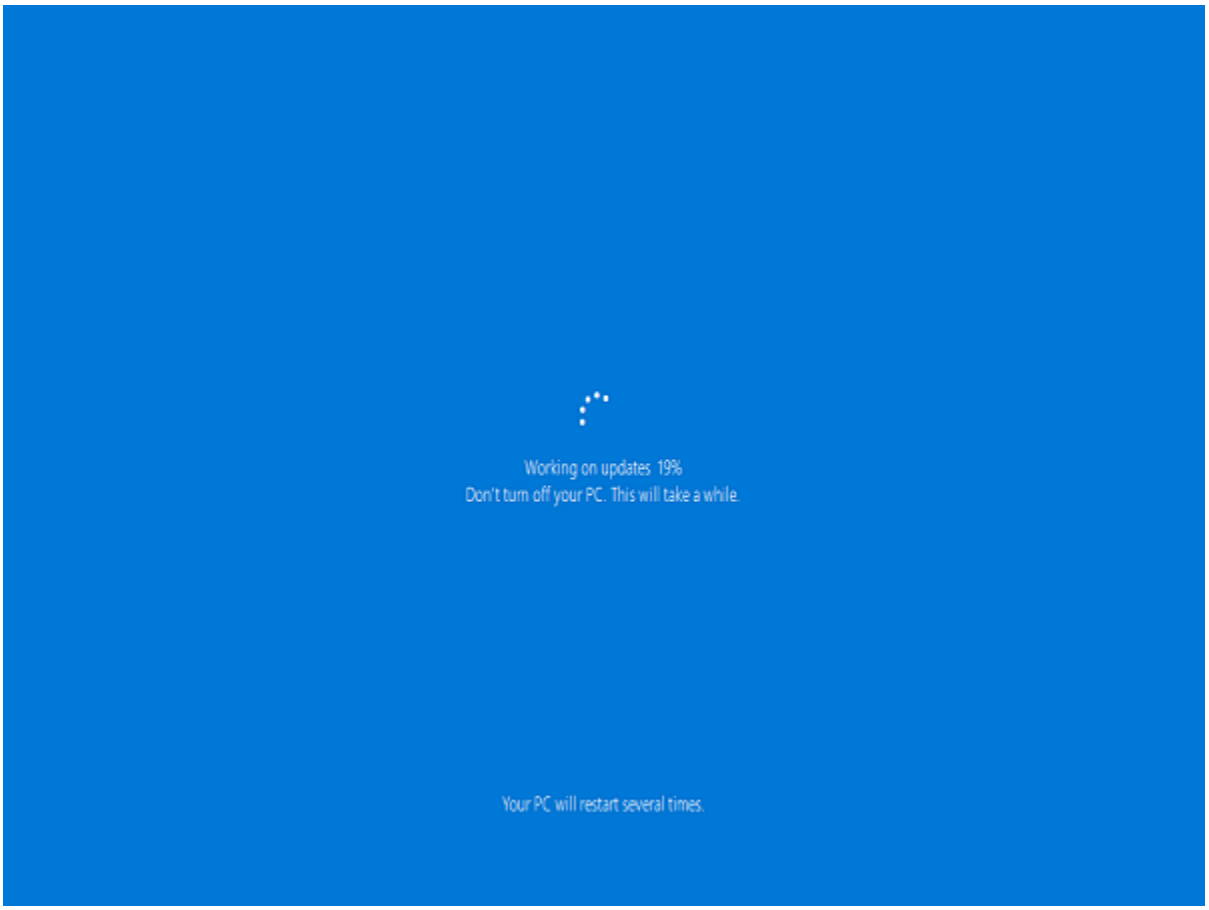
Процесс обновления Windows 10

Приложение установки Windows используется для обновления компьютера до Windows 10 или для выполнения чистой установки. Программа установки Windows запускает и перезагружает компьютер, собирает сведения, копирует файлы и создает или настраивает параметры конфигурации.

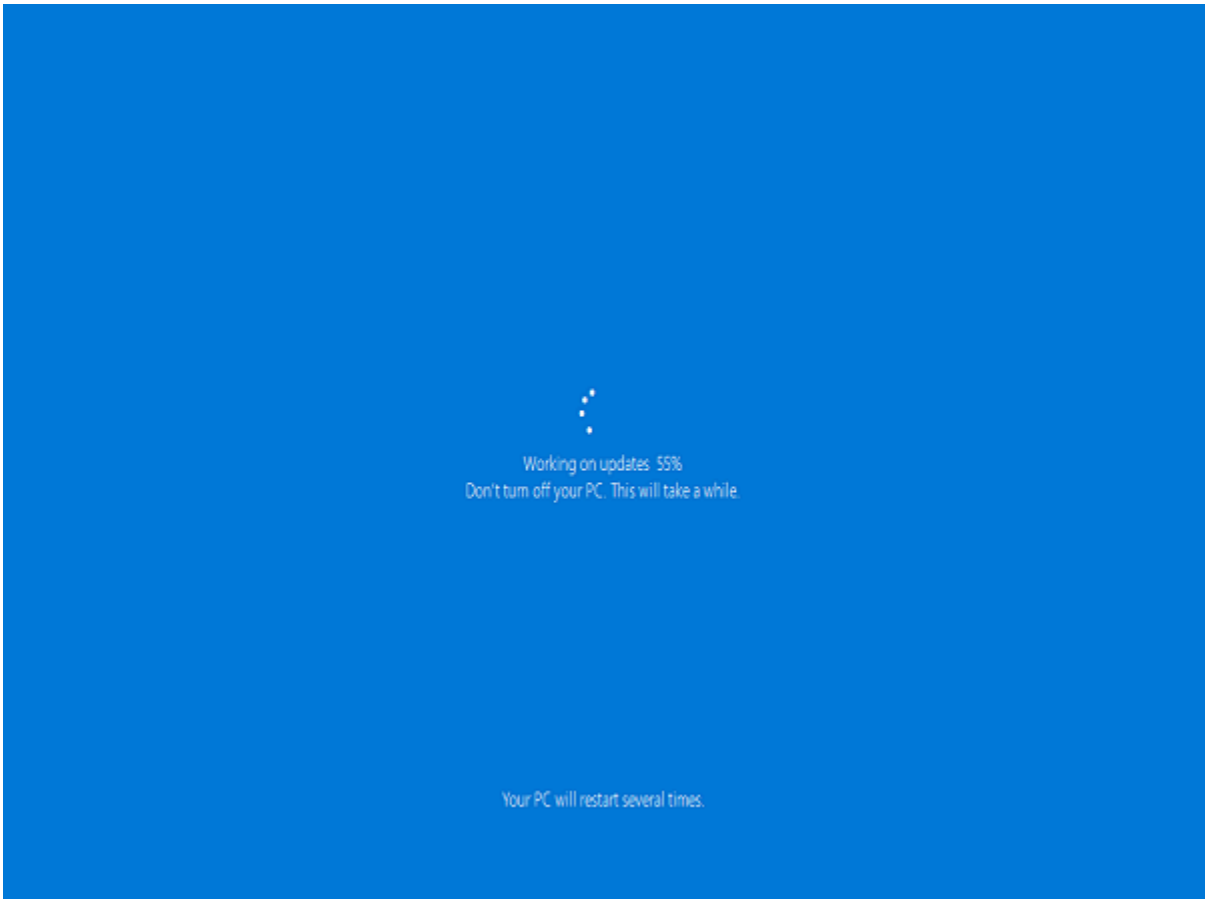
При обновлении операционной системы программа установки Windows использует этапы, описанные ниже. Перезагрузка происходит между каждым из этапов. После первой перезагрузки пользовательский интерфейс останется неизменным до завершения обновления. Процент хода выполнения отображается и будет продвигаться по мере перехода по каждому этапу, достигая 100% в конце второго этапа загрузки.

1. Этап нижнего уровня: этап нижнего уровня выполняется в предыдущей операционной системе. Файлы Windows копируются и собираются компоненты установки.

2. Этап безопасной ОС: настроен раздел восстановления, развернуты файлы Windows и устанавливаются обновления. При необходимости откат ОС подготавливается. Примеры кодов ошибок: 0x2000C, 0x20017.

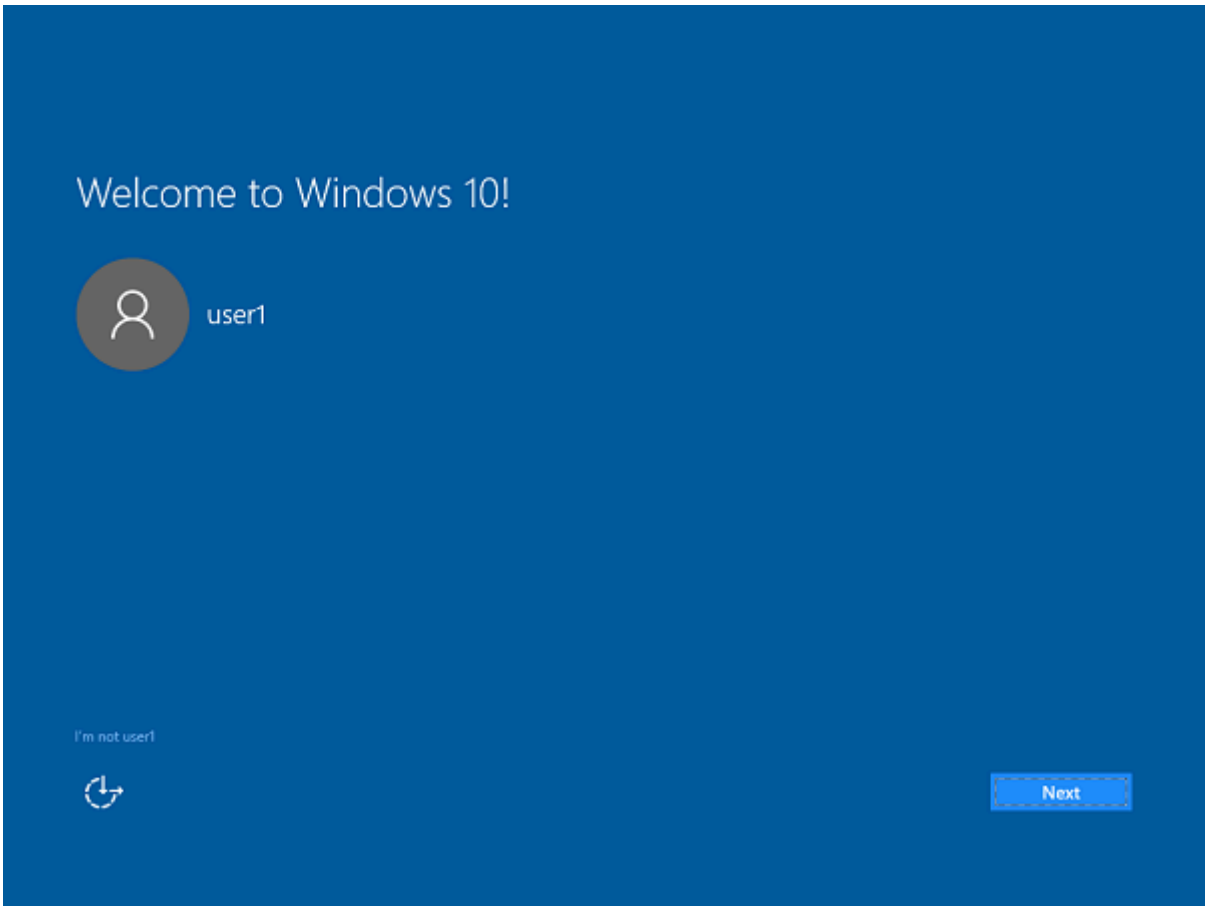


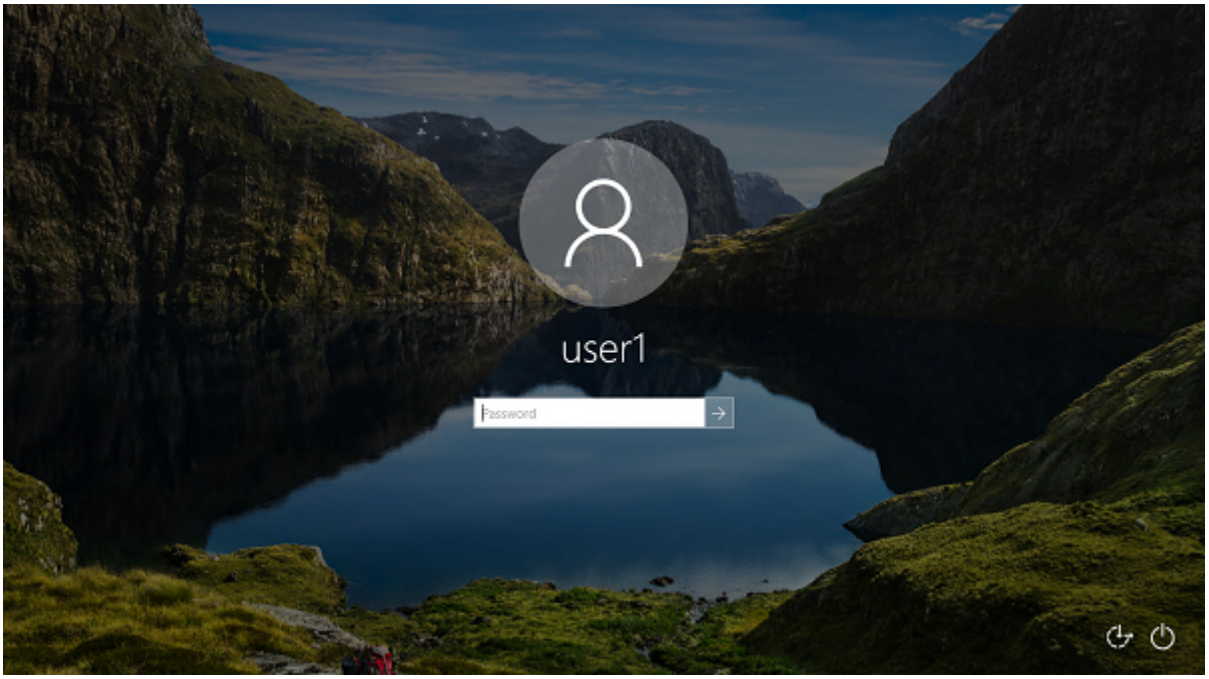
3. Первый этап загрузки: применяются начальные параметры. Примеры кодов ошибок: 0x30018, 0x3000D.

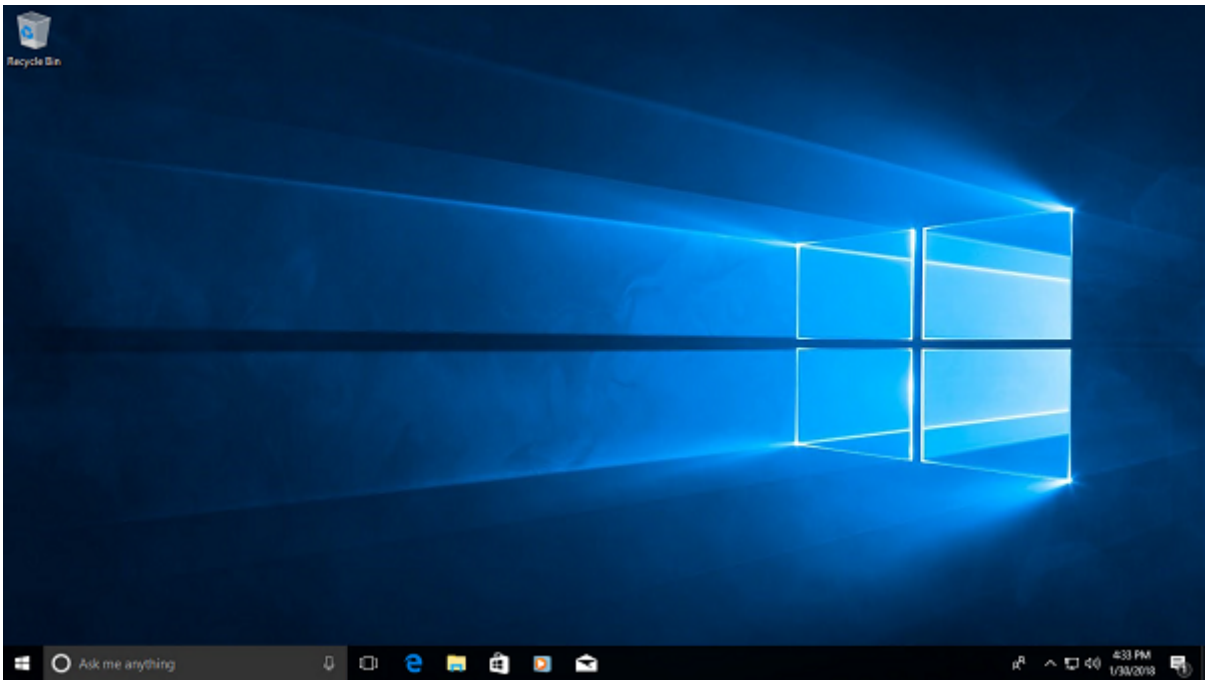


4. Второй этап загрузки: применяются окончательные параметры. Это также называется этапом загрузки OOBE. Примеры кодов ошибок: 0x4000D, 0x40017.

   В конце второго этапа **загрузки отображается экран приветствия в Windows 10** , настроены настройки и отображается запрос на вход в Windows 10.

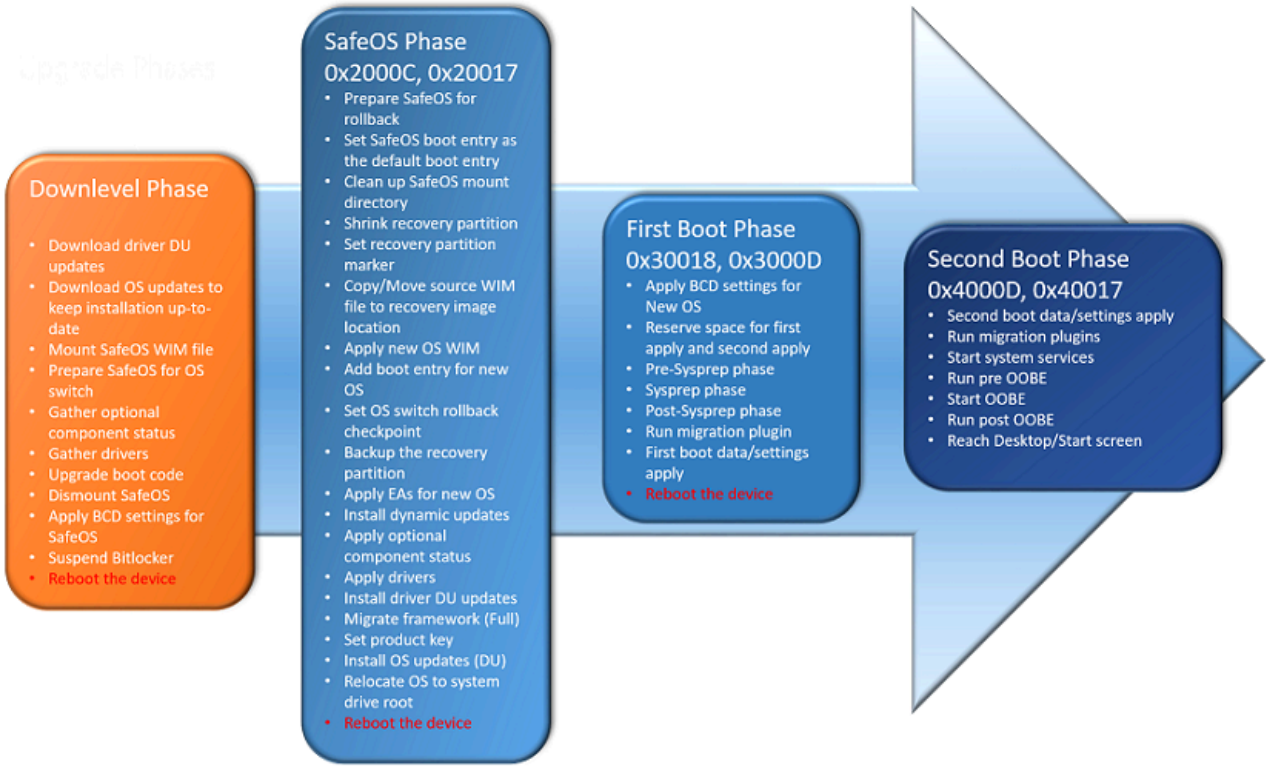

Welcome to Windows 10!
user1
I'm not user1
Next


user1
Password



5. Этап удаления: этот этап происходит, если обновление не выполнено (изображение не отображается). Примеры кодов ошибок: 0x50000, 0x50015.

   Рис. 1. Этапы успешного обновления Windows 10 (удаление не отображается):



DU = обновления драйверов и устройств. OOBE = вне поля взаимодействия. WIM = образ Windows (Майкрософт)

Сбор данных

Если вам нужна помощь службы поддержки Microsoft, мы рекомендуем собирать информацию путем выполнения действий, описанных в разделе Сбор информации с помощью TSS для решения проблем, связанных с развертыванием.

Дополнительная информация

- Вопросы и ответы о Windows 10 для ИТ-специалистов
- требования к системе Windows 10 Корпоративная
- Спецификации Windows 10
- Форумы ИТ-специалистов в Windows 10
- Исправление Обновл. Windows ошибок с помощью средства подготовки к обновлению системы или DISM

Служба Windows Error Reporting

Применяется к: ✅ Windows 11, ✅ Windows 10

> ⓘ **Примечание.**
>
> Эта статья представляет собой 300 уровень статьи (умеренно расширенная).
>
> Полный список статей этого раздела см. в статье **Устранение ошибок обновления Windows** .

При сбое программы установки Windows код результата и код расширения записываются в журнал приложений как информационное событие, отчеты об ошибках Windows как событие 1001. Имя события: **WinSetupDiag02**. для просмотра этого события можно использовать Просмотр событий или Windows PowerShell.

Чтобы использовать Windows PowerShell, введите следующие команды в командной строке Windows PowerShell с повышенными привилегиями:

> ⓘ **Внимание**
>
> Следующие журналы событий доступны только в том случае, если Windows была обновлена с предыдущей версии Windows до новой версии Windows.

PowerShell

```
$events = Get-WinEvent -FilterHashtable
@{LogName="Application";ID="1001";Data="WinSetupDiag02"}
$event = [xml]$events[0].ToXml()
$event.Event.EventData.Data
```

Использование просмотра событий:

1. Откройте окно просмотра событий и перейдите к **Windows Logs\Application**.
2. Выберите **Найти**, а затем найдите **winsetupdiag02**.
3. Двойным щелчком откройте выделенное событие.

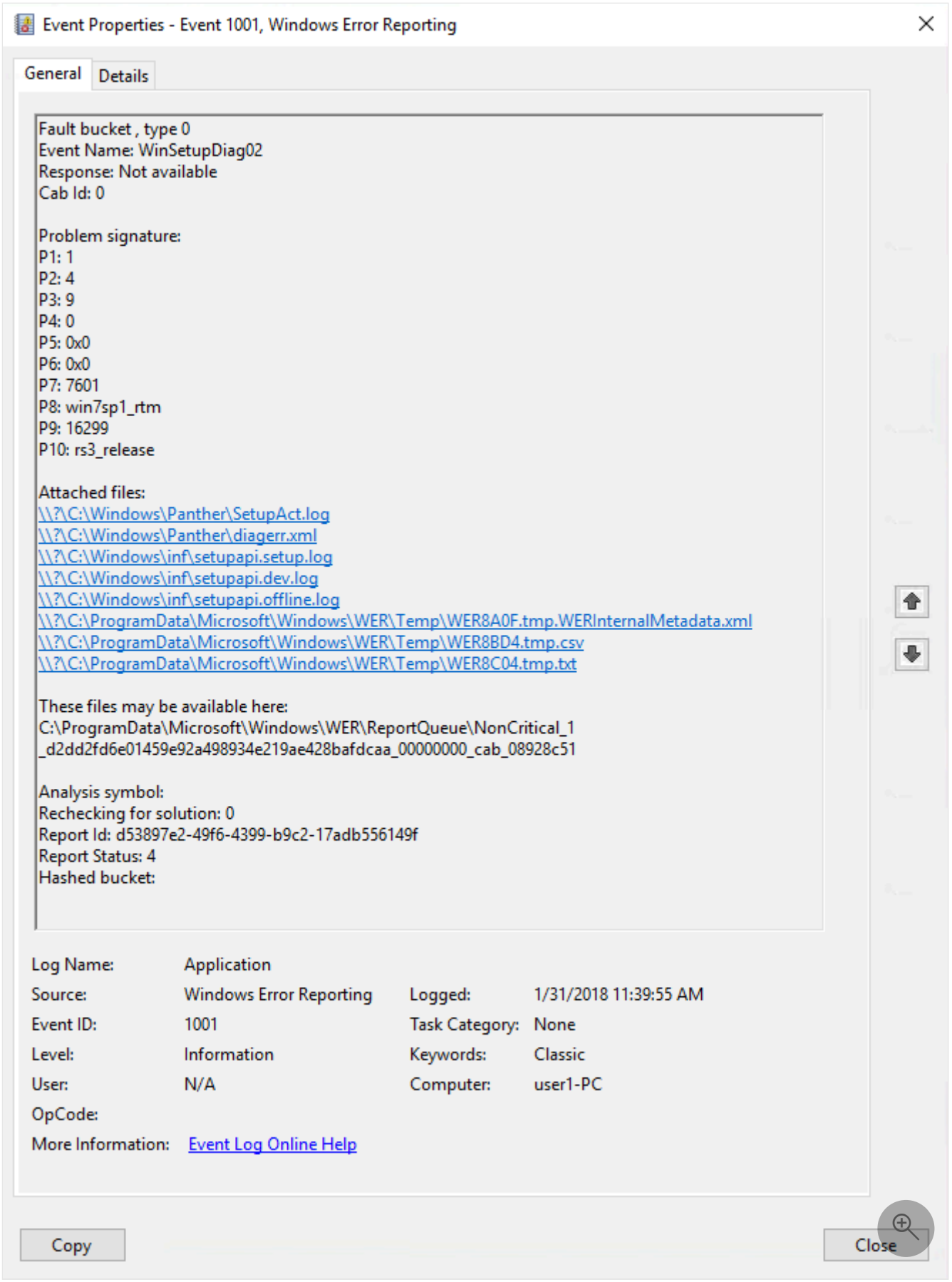
> ⓘ **Примечание.**
>
> Для устаревших операционных систем имя события — WinSetupDiag01.

В событии указаны десять параметров.

Развернуть таблицу

Параметры	Описание	Пример
P1	Сценарий установки	1=Media, 5=WindowsUpdate, 7=Media Creation Tool
P2	Режим установки	x=default, 1=Downlevel, 5=Rollback
P3	Новая архитектура ОС	x=default, 0=X86, 9=AMD64
P4	Результат установки	x=default, 0=Success, 1=Failure,2=Cancel, 3=Blocked
P5	Код ошибки результата	0xc1900101
P6	Расширение кода ошибки	0x20017
P7	Сборка исходной ОС	9600
P8	Исходная ветвь ОС	Обычно недоступен
P9	Новая сборка ОС	16299
P10	Новая ветвь ОС	rs3_release

Событие также содержит ссылки на файлы журнала, которые можно использовать для подробной диагностики ошибки. Следующий пример является примером этого события после успешного обновления:



Связанные статьи

- Исправьте ошибки клиентский компонент Центра обновления Windows с помощью средства DISM или средства проверки готовности к обновлению системы.

Last updated on 09.04.2025

Коды ошибок обновления Windows 10

15.01.2025Применяется к: Supported versions of Windows Client

Применимо к: Windows 10

> **Примечание**
>
> Это 400 раздел уровня (дополнительно).
>
> Для ИТ-специалистов ознакомьтесь с дополнительными сведениями об **ошибках** обновления Windows 10.

Если процесс обновления не выполнен, программа установки Windows вернет два кода:

1. Код результата: код результата соответствует определенной ошибке Win32 или NTSTATUS.
2. Код расширения: код расширения содержит сведения о этапе, в котором произошла ошибка, и операция, выполняемая при возникновении ошибки.

Например, код результата 0xC1900101 с кодом расширения 0x4000D будет возвращен как: 0xC1900101 - 0x4000D.

> **Примечание**
>
> Если возвращается только результирующий код, это может быть вызвано тем, что используется средство, которое не удалось записать код расширения. Например, если вы используете **помощник по обновлению до Windows 10**, может быть возвращен только код результата.

> **Совет**
>
> Если вы не можете найти результат и расширить коды ошибок, можно попытаться найти эти коды с помощью Просмотр событий. Дополнительные сведения см. в разделе **Отчеты об ошибках Windows**.

Коды результатов

Код результата 0xC1900101 является универсальным и указывает, что произошел откат. В большинстве случаев причиной является проблема совместимости драйверов. Чтобы

устранить сбой обновления, который вернул код результата 0xC1900101, проанализируйте код расширения, чтобы определить этап установки Windows, и ознакомьтесь с разделом "Процедуры разрешения" далее в этой статье.

Следующий набор кодов результатов связан с предупреждениями совместимости программы установки Windows:

Развернуть таблицу

Код результата	Сообщение	Описание
0xC1900210	MOSETUP_E_COMPAT_SCANONLY	Программа установки не обнаружила никаких проблем с compat
0xC1900208	MOSETUP_E_COMPAT_INSTALLREQ_BLOCK	Программа установки обнаружила проблему, связанную с действием, например несовместимое приложение
0xC1900204	MOSETUP_E_COMPAT_MIGCHOICE_BLOCK	Выбранный вариант миграции недоступен (например, Enterprise to Home)
0xC1900200	MOSETUP_E_COMPAT_SYSREQ_BLOCK	Компьютер не подходит для Windows 10
0xC190020E	MOSETUP_E_INSTALLDISKSPACE_BLOCK	На компьютере недостаточно свободного места для установки

Список ошибок современной установки (mosetup) с описаниями в диапазоне доступен в разделе процедур разрешения в этой статье.

Другие коды результатов можно сопоставить с определенным типом ошибки. Чтобы сопоставить код результата с ошибкой:

1. Определите тип кода ошибки как Win32 или NTSTATUS с помощью первой шестнадцатеричной цифры:

   8 = код ошибки Win32 (например, 0x80070070) C = ЗНАЧЕНИЕ NTSTATUS (например, 0xC1900107)

2. Запишите последние четыре цифры кода ошибки (например, 0x80070070 = 0070). Эти цифры являются фактическим типом кода ошибки, как определено в структуре HRESULT или NTSTATUS . Другие цифры в коде определяют такие вещи, как тип устройства, который вызвал ошибку.

3. На основе типа кода ошибки, определенного на первом шаге (Win32 или NTSTATUS), соответствуют четыре цифры, производные от второго шага, с кодом ошибки Win32

или значением NTSTATUS, используя следующие ссылки:

- Код ошибки Win32
- Значение NTSTATUS

Примеры:

- 0x80070070

  1. На основе "8" это код ошибки Win32.
  2. Последние четыре цифры 0070, поэтому поиск 0x00000070 в таблице кода ошибки Win32.
  3. Ошибка:

     > ERROR_DISK_FULL (Диск заполнен)

- 0xC1900107

  1. На основе C это код ошибки NTSTATUS.
  2. Последние четыре цифры 0107, поэтому поиск 0x00000107 в таблице значений NTSTATUS.
  3. Ошибка:

     > СТАТУС_НЕКОТОРЫЕ_НЕ_СООТВЕТСТВУЮТ

Некоторые коды результатов являются самообъяснительными, в то время как другие являются более универсальными и требуют дальнейшего анализа. В приведенных выше примерах ERROR_DISK_FULL указывает, что жесткий диск заполнен и требуется дополнительное место для завершения обновления Windows. Сообщение STATUS_SOME_NOT_MAPPED является более неоднозначным и означает, что действие ожидается. В этом случае ожидающее действие часто является операцией очистки из предыдущей попытки установки, которую можно устранить с помощью перезагрузки системы.

Расширение кодов

> ⓘ **Важно!**
>
> Коды расширения отражают текущий процесс обновления Windows 10 и могут измениться в будущих выпусках Windows 10. Коды, рассмотренные в этом разделе,

применяются к Windows 10 версии 1607, также известной как юбилейное обновление.

Коды расширения можно сопоставить с этапом и операцией при возникновении ошибки. Чтобы сопоставить код расширения с этапом и операцией:

1. Используйте первую цифру, чтобы определить этап (например, 0x4000D = 4).
2. Используйте последние две цифры для идентификации операции (например, 0x4000D = 0D).
3. Соответствует этапу и операции значениям в таблицах, приведенных ниже.

В следующих таблицах приведены соответствующие этапы и операции для значений кода расширения:

Расширение кода: этап

Развернуть таблицу

Проклятие	Этап
0	SP_EXECUTION_UNKNOWN
1	SP_EXECUTION_DOWNLEVEL
2	SP_EXECUTION_SAFE_OS
3	SP_EXECUTION_FIRST_BOOT
4	SP_EXECUTION_OOBE_BOOT
5	SP_EXECUTION_UNINSTALL

Расширение кода: операция

Развернуть таблицу

Проклятие	Операция
0	SP_EXECUTION_OP_UNKNOWN
1	КОПИРОВАНИЕ_ПОЛНЫХ_ДАННЫХ_ВО_ВРЕМЯ_ИСПОЛНЕНИЯ
2	SP_EXECUTION_OP_СКАЧАТЬ_ОБНОВЛЕНИЯ
3	SP_EXECUTION_OP_INSTALL_UPDATES

Проклятие	Операция
4	SP_EXECUTION_OP_INSTALL_RECOVERY_ENVIRONMENT
5	SP_EXECUTION_OP_INSTALL_RECOVERY_IMAGE (установка образа восстановления)
6	SP_EXECUTION_OP_REPLICATE_OC
7	SP_EXECUTION_OP_INSTALL_DRIVERS
8	SP_EXECUTION_OP_PREPARE_SAFE_OS
9	SP_EXECUTION_OP_PREPARE_ROLLBACK
а	ОП_ВЫПОЛНЕНИЕ_ПОДГОТОВКА_ПЕРВОЙ_ЗАГРУЗКИ
Б	ОП_ВЫПОЛНЕНИЕ_ПОДГОТОВКА_ООВЕ_ЗАПУСК
С	SP_EXECUTION_OP_APPLY_IMAGE
Д	SP_EXECUTION_OP_MIGRATE_DATA
Е	SP_EXECUTION_OP_SET_PRODUCT_KEY
Ф	SP_EXECUTION_OP_ADD_UNATTEND

Развернуть таблицу

Проклятие	Операция
10	SP_EXECUTION_OP_ADD_DRIVER (добавление драйвера)
11	SP_EXECUTION_OP_ENABLE_FEATURE
12	СП_ИСПОЛНЕНИЕ_ОП_ОТКЛЮЧИТЬ_ФУНКЦИЮ
13 (тринадцать)	SP_EXECUTION_OP_REGISTER_ASYNC_PROCESS
14	SP_EXECUTION_OP_REGISTER_SYNC_PROCESS
15	SP_EXECUTION_OP_CREATE_FILE
16	SP_EXECUTION_OP_СОЗДАНИЕ_РЕЕСТРА
17	SP_EXECUTION_OP_BOOT
18	SP_EXECUTION_OP_SYSPREP
19	SP_EXECUTION_OP_OOBE
1A	Начало первой загрузки

Проклятие	Операция
1 млрд	Завершение первой загрузки
1C	SP_EXECUTION_OP_BEGIN_OOBE_BOOT
1D	SP_EXECUTION_OP_END_OOBE_BOOT
1E	SP_EXECUTION_OP_PRE_OOBE
1F	SP_EXECUTION_OP_POST_OOBE
20	SP_EXECUTION_OP_ADD_PROVISIONING_PACKAGE

Например: код расширения 0x4000D представляет проблему на этапе 4 (0x4) при миграции данных (000D).

Сбор данных

Если вам нужна помощь службы поддержки Microsoft, мы рекомендуем собирать информацию путем выполнения действий, описанных в разделе Сбор информации с помощью TSS для решения проблем, связанных с развертыванием.

Дополнительная информация

- Вопросы и ответы о Windows 10 для ИТ-специалистов
- требования к системе Windows 10 Корпоративная
- Спецификации Windows 10
- Microsoft Windows Q и A
- Исправление Обновл. Windows ошибок с помощью средства подготовки к обновлению системы или DISM

Файлы журнала обновления Windows

Применяется к: ✅ Windows 11, ✅ Windows 10

> ⓘ **Примечание.**
>
> Эта статья представляет собой 400-уровневую статью (расширенная).
>
> Полный список статей этого раздела см. в статье Устранение ошибок обновления Windows .

Во время каждого этапа процесса обновления создаются несколько файлов журнала. Эти файлы журнала необходимы для устранения неполадок при обновлении. По умолчанию папки, содержащие эти файлы журнала, скрыты на компьютере, где выполняется обновление. Для просмотра файлов журнала включите отображение скрытых элементов в проводнике Windows или используйте средство, чтобы автоматически собирать эти журналы. Самый полезный журнал — **setupact.log**. Файлы журнала находятся в разных папках в зависимости от этапа установки Windows. Недавнее, что этап можно определить из кода расширения.

> ⓘ **Примечание.**
>
> Кроме того, сведения о поиске кодов ошибок и файлов журналов см. в отчеты об ошибках Windows статье в этом разделе.

В следующей таблице описаны некоторые файлы журнала и способы их использования для устранения неполадок.

Развернуть таблицу

Файл журнала	Этап: расположение	Описание	Варианты использования
setupact.log	Нижний уровень: $Windows.~BT\Sources\Panther	Содержит сведения о действиях программы установки на низкоуровневом этапе.	Все сбои нижнего уровня и отправная точка для исследования отката. Setup.act — это наиболее важный журнал

Файл журнала	Этап: расположение	Описание	Варианты использования
			для диагностики проблем с установкой.
setupact.log	Готовое взаимодействие (OOBE): $Windows.~BT\Sources\Panther\UnattendGC	Содержит сведения о действиях на этапе запуска при первом включении.	Изучение откатов, завершившиеся сбоем во время этапа и операций OOBE: 0x4001C, 0x4001D, 0x4001E 0x4001F.
setupact.log	Откат: $Windows.~BT\Sources\Rollback	Содержит сведения о действиях во время отката.	Исследование откатов общего характера: 0xC1900101.
setupact.log	Предварительная инициализация (до нижнего уровня): Windows	Содержит сведения об инициализации установки.	Если не удается запустить программу установки.
setupact.log	После обновления (после первого запуска компьютера): Windows\Panther	Содержит сведения о действиях программы установки во время установки.	Исследование проблем, связанных с процессами после обновления.
setuperr.log	Аналогично setupact.log	Содержит сведения об ошибках программы установки во время установки.	Просмотрите все ошибки, возникающие на этапе установки.
miglog.xml	После обновления (после первого запуска компьютера): Windows\Panther	Содержит сведения о том, что было перенесено во	Определение проблем, возникающих после переноса

Файл журнала	Этап: расположение	Описание	Варианты использования
		время установки.	данных обновления.
BlueBox.log	Нижний уровень: Windows\Logs\Mosetup	Содержит обмен данными между `setup.exe` и клиентский компонент Центра обновления Windows.	Используйте во время сбоев WSUS и клиентский компонент Центра обновления Windows нижнего уровня или для 0xC1900107.
Вспомогательные журналы отката: **Setupmem.dmp** **setupapi.dev.log** Журналы событий (*.evtx)	$Windows.~BT\Sources\Rollback	Дополнительные журналы, собранные во время отката.	Setupmem.dmp. Если во время обновления выполняется проверка ошибок ОС, программа установки пытается извлечь мини-дамп. Setupapi: проблемы с установкой устройства — 0x30018 Журналы событий: откаты общего характера (0xC1900101) или неожиданные перезагрузки.

Структура записи журнала

Запись `setupact.log` или `setuperr.log` включает следующие элементы:

1. **Дата и время** — 2023-09-08 09:20:05

2. **Уровень журнала** : Info, Warning, Error, Fatal Error
3. **Компонент ведения журнала** — CONX, MOUPG, PANTHR, SP, IBSLIB, MIG, DISM, CSI, CBS

Компоненты ведения журнала SP (платформа установки), MIG (подсистема миграции) и CONX (сведения о совместимости) полезны для устранения ошибок установки Windows.

1. **Сообщение —** Операция успешно завершена.

См. перечисленные ниже примеры.

Развернуть таблицу

Дата и время	Уровень журнала	Компонент	Сообщение
2023-09-08 09:23:50,	Предупреждение	MIG	Не удалось заменить объект C:\Users\name\Cookies. Не удается удалить целевой объект.

Анализ файлов журнала

Следующие инструкции предназначены для специалистов по ИТ. Чтобы ознакомиться с кодами результатов и расширить коды, см. статью Коды ошибок обновления.

Анализ файлов журнала установки Windows

1. Определите код ошибки программы установки Windows. Программа установки Windows должна вернуть код ошибки, если обновление не прошло успешно.
2. На основе части кода ошибки расширения определите тип и расположение файла журнала для исследования.
3. Откройте файл журнала в текстовом редакторе, например Блокноте.
4. Найдите код результата из кода ошибки программы установки Windows, выполните поиск кода результата в файле и найдите последний экземпляр кода. Или же выполните поиск слов «abort» и «abandoning», которые описано на шаге 7 ниже.
5. Поиск последнего экземпляра кода результата
   a. Прокрутите до конца файла и выберите после последнего символа.
   b. Выберите **Изменить**.
   c. Выберите **Найти**.
   d. Введите код результата.

e. В разделе **Направление** выберите **Вверх**.
f. Нажмите **кнопку Найти далее**.

6. При обнаружении последнего вхождения результирующий код прокрутите несколько строк из этого расположения в файле и просмотрите процессы, которые завершились сбоем, прежде чем создавать код результата.

7. Найдите следующие важные текстовые строки:

   - `Shell application requested abort`
   - `Abandoning apply due to error for object`

8. Декодируйте ошибки Win32, которые отображаются в этом разделе.

9. Запишите метку времени наблюдаемых ошибок в этом разделе.

10. Выполните поиск дополнительных сведений, соответствующих этим меткам времени или ошибкам, в других файлах журналов.

Например, предположим, что код ошибки для ошибки **0x8007042B — 0x2000D**. При поиске **8007042B** отображается следующее содержимое `setuperr.log` из файла:

> ⓘ **Примечание.**
>
> Некоторые строки в следующем тексте сокращены для повышения удобочитаемости. Например:
>
> - Дата и время в начале каждой строки (например, 2023-10-05 15:27:08) сокращается до минут и секунд.
> - Имя файла сертификата, которое является длинной текстовой строкой, сокращается до "CN".

содержимое setuperr.log :

Консоль

```
27:08, Error           SP     Error READ, 0x00000570 while gathering/applying
object: File, C:\ProgramData\Microsoft\Crypto\RSA\S-1-5-18 [CN]. Will return
0[gle=0x00000570]
27:08, Error           MIG    Error 1392 while gathering object
C:\ProgramData\Microsoft\Crypto\RSA\S-1-5-18 [CN]. Shell application requested
abort![gle=0x00000570]
27:08, Error                  Gather failed. Last error: 0x00000000
27:08, Error           SP     SPDoFrameworkGather: Gather operation failed. Error:
0x0000002C
27:09, Error           SP     CMigrateFramework: Gather framework failed. Status: 44
```

```
27:09, Error                 SP     Operation failed: Migrate framework (Full). Error:
0x8007042B[gle=0x000000b7]
27:09, Error                 SP     Operation execution failed: 13. hr =
0x8007042B[gle=0x000000b7]
27:09, Error                 SP     CSetupPlatformPrivate::Execute: Execution of
operations queue failed, abandoning. Error: 0x8007042B[gle=0x000000b7]
```

Первая строка указывает, что **произошла ошибка 0x00000570** с файлом **C:\ProgramData\Microsoft\Crypto\RSA\S-1-5-18 [CN]**:

Консоль

```
27:08, Error                 SP     Error READ, 0x00000570 while gathering/applying
object: File, C:\ProgramData\Microsoft\Crypto\RSA\S-1-5-18 [CN]. Will return
0[gle=0x00000570]
```

Ошибка **0x00000570** — это код ошибки Win32 , соответствующий: **ERROR_FILE_CORRUPT: файл или каталог поврежден и не читается**.

Поэтому программа установки Windows не смогла перенести поврежденный файл **C:\ProgramData\Microsoft\Crypto\RSA\S-1-5-18[CN]**. Этот файл — локальный сертификат системы, и его можно удалить. После поиска дополнительных сведений в `setupact.log` файле фраза **Оболочка, запрошенная прервать приложение** , будет найдена в расположении с той же меткой времени, что и строки в `setuperr.log`. Этот анализ подтверждает подозрение, что этот файл является причиной сбоя обновления:

содержимое setupact.log :

Консоль

```
27:00, Info                  Gather started at 10/5/2023 23:27:00
27:00, Info [0x080489] MIG   Setting system object filter context (System)
27:00, Info [0x0803e5] MIG   Not unmapping HKCU\Software\Classes; it is not mapped
27:00, Info [0x0803e5] MIG   Not unmapping HKCU; it is not mapped
27:00, Info                  SP     ExecuteProgress: Elapsed events:1 of 4, Percent: 12
27:00, Info [0x0802c6] MIG   Processing GATHER for migration unit:
&lt;System&gt;\UpgradeFramework (CMXEAgent)
27:08, Error                 SP     Error READ, 0x00000570 while gathering/applying
object: File, C:\ProgramData\Microsoft\Crypto\RSA\S-1-5-18 [CN]. Will return
0[gle=0x00000570]
27:08, Error                 MIG    Error 1392 while gathering object
C:\ProgramData\Microsoft\Crypto\RSA\S-1-5-18 [CN]. Shell application requested
abort![gle=0x00000570]
27:08, Info                  SP     ExecuteProgress: Elapsed events:2 of 4, Percent: 25
27:08, Info                  SP     ExecuteProgress: Elapsed events:3 of 4, Percent: 37
27:08, Info [0x080489] MIG   Setting system object filter context (System)
27:08, Info [0x0803e5] MIG   Not unmapping HKCU\Software\Classes; it is not mapped
27:08, Info [0x0803e5] MIG   Not unmapping HKCU; it is not mapped
27:08, Info                  MIG    COutOfProcPluginFactory::FreeSurrogateHost: Shutdown
```

```
in progress.
27:08, Info            MIG
COutOfProcPluginFactory::LaunchSurrogateHost::CommandLine: -shortened-
27:08, Info            MIG    COutOfProcPluginFactory::LaunchSurrogateHost:
Successfully launched host and got control object.
27:08, Error                  Gather failed. Last error: 0x00000000
27:08, Info                   Gather ended at 10/5/2023 23:27:08 with result 44
27:08, Info                   Leaving MigGather method
27:08, Error           SP     SPDoFrameworkGather: Gather operation failed. Error:
0x0000002C
```

содержимое setupapi.dev.log :

Консоль

```
>>>  [Device Install (UpdateDriverForPlugAndPlayDevices) - PCI\VEN_8086&DEV_8C4F]
>>>  Section start 2023/09/26 20:13:01.623
      cmd: rundll32.exe
"C:\WINDOWS\Installer\MSI6E4C.tmp",zzzzInvokeManagedCustomActionOutOfProc
SfxCA_95972906 484
ChipsetWiX.CustomAction!Intel.Deployment.ChipsetWiX.CustomActions.InstallDrivers
     ndv: INF path: C:\WINDOWS\TEMP\{15B1CD41-69F5-48EA-9F45-
0560A40FE2D8}\Drivers\lynxpoint\LynxPointSystem.inf
     ndv: Install flags: 0x00000000
     ndv: {Update Device Driver -
PCI\VEN_8086&DEV_8C4F&SUBSYS_05BE1028&REV_04\3&11583659&0&F8}
     ndv:      Search options: 0x00000081
     ndv:      Searching single INF 'C:\WINDOWS\TEMP\{15B1CD41-69F5-48EA-9F45-
0560A40FE2D8}\Drivers\lynxpoint\LynxPointSystem.inf'
     dvi:      {Build Driver List} 20:13:01.643
     dvi:           Searching for hardware ID(s):
     dvi:                pci\ven_8086&dev_8c4f&subsys_05be1028&rev_04
     dvi:                pci\ven_8086&dev_8c4f&subsys_05be1028
     dvi:                pci\ven_8086&dev_8c4f&cc_060100
     dvi:                pci\ven_8086&dev_8c4f&cc_0601
     dvi:           Searching for compatible ID(s):
     dvi:                pci\ven_8086&dev_8c4f&rev_04
     dvi:                pci\ven_8086&dev_8c4f
     dvi:                pci\ven_8086&cc_060100
     dvi:                pci\ven_8086&cc_0601
     dvi:                pci\ven_8086
     dvi:                pci\cc_060100
     dvi:                pci\cc_0601
     sig:           {_VERIFY_FILE_SIGNATURE} 20:13:01.667
     sig:                Key      = lynxpointsystem.inf
     sig:                FilePath = c:\windows\temp\{15b1cd41-69f5-48ea-9f45-
0560a40fe2d8}\drivers\lynxpoint\lynxpointsystem.inf
     sig:                Catalog  = c:\windows\temp\{15b1cd41-69f5-48ea-9f45-
0560a40fe2d8}\drivers\lynxpoint\LynxPoint.cat
     sig:                Success: File is signed in catalog.
     sig:           {_VERIFY_FILE_SIGNATURE exit(0x00000000)} 20:13:01.683
     dvi:           Created Driver Node:
     dvi:                HardwareID   - PCI\VEN_8086&DEV_8C4F
     dvi:                InfName      - c:\windows\temp\{15b1cd41-69f5-48ea-9f45-
```

```
0560a40fe2d8}\drivers\lynxpoint\lynxpointsystem.inf
     dvi:                DevDesc      - Intel(R) QM87 LPC Controller - 8C4F
     dvi:                Section      - Needs_ISAPNP_DRV
     dvi:                Rank         - 0x00ff2001
     dvi:                Signer Score - WHQL
     dvi:                DrvDate      - 04/04/2016
     dvi:                Version      - 10.1.1.18
     dvi:      {Build Driver List - exit(0x00000000)} 20:13:01.699
     ndv:      Searching currently installed INF
     dvi:      {Build Driver List} 20:13:01.699
     dvi:           Searching for hardware ID(s):
     dvi:                pci\ven_8086&dev_8c4f&subsys_05be1028&rev_04
     dvi:                pci\ven_8086&dev_8c4f&subsys_05be1028
     dvi:                pci\ven_8086&dev_8c4f&cc_060100
     dvi:                pci\ven_8086&dev_8c4f&cc_0601
     dvi:           Searching for compatible ID(s):
     dvi:                pci\ven_8086&dev_8c4f&rev_04
     dvi:                pci\ven_8086&dev_8c4f
     dvi:                pci\ven_8086&cc_060100
     dvi:                pci\ven_8086&cc_0601
     dvi:                pci\ven_8086
     dvi:                pci\cc_060100
     dvi:                pci\cc_0601
     dvi:           Created Driver Node:
     dvi:                HardwareID   - PCI\VEN_8086&DEV_8C4F
     dvi:                InfName      -
C:\WINDOWS\System32\DriverStore\FileRepository\lynxpointsystem.inf_amd64_cd1e518d883
ecdfe\lynxpointsystem.inf
     dvi:                DevDesc      - Intel(R) QM87 LPC Controller - 8C4F
     dvi:                Section      - Needs_ISAPNP_DRV
     dvi:                Rank         - 0x00ff2001
     dvi:                Signer Score - WHQL
     dvi:                DrvDate      - 10/03/2016
     dvi:                Version      - 10.1.1.38
     dvi:      {Build Driver List - exit(0x00000000)} 20:13:01.731
     dvi:      {DIF_SELECTBESTCOMPATDRV} 20:13:01.731
     dvi:           Default installer: Enter 20:13:01.735
     dvi:                {Select Best Driver}
     dvi:                     Class GUID of device changed to: {4d36e97d-e325-11ce-
bfc1-08002be10318}.
     dvi:                     Selected Driver:
     dvi:                          Description - Intel(R) QM87 LPC Controller - 8C4F
     dvi:                          InfFile     -
c:\windows\system32\driverstore\filerepository\lynxpointsystem.inf_amd64_cd1e518d883
ecdfe\lynxpointsystem.inf
     dvi:                          Section     - Needs_ISAPNP_DRV
     dvi:                {Select Best Driver - exit(0x00000000)}
     dvi:           Default installer: Exit
     dvi:      {DIF_SELECTBESTCOMPATDRV - exit(0x00000000)} 20:13:01.743
     ndv:      Currently Installed Driver:
     ndv:           Inf Name       - oem1.inf
     ndv:           Driver Date    - 10/03/2016
     ndv:           Driver Version - 10.1.1.38
     ndv: {Update Device Driver - exit(00000103)}
!    ndv: No better matching drivers found for device
```

```
'PCI\VEN_8086&DEV_8C4F&SUBSYS_05BE1028&REV_04\3&11583659&0&F8'.
!    ndv: No devices were updated.
<<<  Section end 2019/09/26 20:13:01.759
<<<  [Exit status: FAILURE(0xC1900101)]
```

Этот анализ показывает, что ошибку обновления Windows можно устранить путем удаления `C:\ProgramData\Microsoft\Crypto\RSA\S-1-5-18\[CN]` файла.

> ⓘ **Примечание.**
>
> В этом примере полное имя файла — `C:\ProgramData\Microsoft\Crypto\RSA\S-1-5-18\be8228fb2d3cb6c6b0ccd9ad51b320b4_a43d512c-69f2-42de-aef9-7a88fabdaa3f`.

Связанные статьи

- Исправьте ошибки клиентский компонент Центра обновления Windows с помощью средства DISM или средства проверки готовности к обновлению системы.

Last updated on 08.04.2025

Процедуры разрешения обновлений Windows 10

15.01.2025Применяется к: Supported versions of Windows Client

Применимо к: Windows 10

> **Примечание**
>
> Это раздел уровня 200 (умеренный).
>
> Для ИТ-специалистов ознакомьтесь с дополнительными сведениями об **ошибках** обновления Windows 10.

В этой статье приведены некоторые распространенные причины и решения, связанные с определенными кодами ошибок обновления. Если обновление Windows 10 завершается ошибкой, можно записать отображаемый код ошибки или найти код ошибки в журнале событий Windows или в файлах журнала установки Windows (например, *setuperr.log*) и просмотреть причину и решения, указанные здесь. Также следует попробовать запустить бесплатное средство SetupDiag , предоставленное корпорацией Майкрософт, которое может автоматически найти причину сбоя обновления.

0xC1900101

Часто наблюдаемый код результата 0xC1900101. Этот код результата можно вызвать на любом этапе процесса обновления, за исключением этапа нижнего уровня. 0xC1900101 является универсальным кодом отката и обычно указывает на то, что несовместимый драйвер присутствует. Несовместимый драйвер может вызвать синие экраны, системные зависания и непредвиденные перезагрузки. Анализ дополнительных файлов журнала часто полезен, например:

- Файл minidump: *$Windows.~bt\Sources\Rollback\setupmem.dmp*
- Журналы событий: *$Windows.~bt\Sources\Rollback*.evtx*
- Журнал установки устройства: *$Windows.~bt\Sources\Rollback\setupapi\setupapi.dev.log*

Журнал установки устройства полезен при откате во время операции sysprep (расширение кода 0x30018).

Чтобы устранить откат, вызванный конфликтами драйверов, попробуйте выполнить настройку с помощью минимального набора драйверов и программ запуска, выполнив чистую загрузку перед началом процесса обновления.

Ознакомьтесь со следующими общими процедурами устранения неполадок, связанными с кодом результатов 0xC1900101:

Развернуть таблицу

Код	Исправление	Причина
0xC1900101 - 0x20004	Удаление антивирусных приложений. Удалите все неиспользуемые устройства SATA. Удалите все неиспользуемые устройства и драйверы. Обновите драйверы и BIOS.	Программа установки Windows столкнулась с ошибкой во время SAFE_OS с операцией INSTALL_RECOVERY_ENVIRONMENT. Эта ошибка вызвана устаревшими драйверами.
0xC1900101 — 0x2000c	Отключите все периферийные устройства, подключенные к системе, за исключением мыши, клавиатуры и дисплея. Обратитесь к поставщику оборудования, чтобы получить обновленные драйверы устройств. Убедитесь, что "Загрузка и установка обновлений (рекомендуется)" принимается в начале процесса обновления.	Программа установки Windows столкнулась с неопределенной ошибкой во время применения Wim на этапе WinPE. Эта ошибка вызвана устаревшими драйверами
0xC1900101 - 0x20017	Убедитесь, что все драйверы обновлены. Откройте файлы Setuperr.log и Setupact.log в каталоге %windir%\Panther, а затем найдите драйверы проблем. Дополнительные сведения см. в разделе Windows Vista, Windows 7, Windows Server 2008 R2, Windows 8.1 и файлов журнала установки Windows 10. Обновите или удалите драйверы проблем.	Водитель вызвал недопустимую операцию. Windows не удалось перенести драйвер, что привело к откату операционной системы. Это сбой загрузки SafeOS, который обычно вызван драйверами или программным обеспечением шифрования дисков, отличных от Майкрософт. Это также может быть вызвано сбоем оборудования.
0xC1900101 — 0x30018	Отключите все периферийные устройства, подключенные к системе, за исключением мыши, клавиатуры и дисплея. Обратитесь к поставщику оборудования, чтобы получить обновленные драйверы устройств. Убедитесь, что "Загрузка и установка обновлений (рекомендуется)" принимается в начале процесса обновления.	Драйвер устройства перестал отвечать на setup.exe во время процесса обновления.
0xC1900101 — 0x3000D	Отключите все периферийные устройства, подключенные к системе, за исключением мыши, клавиатуры и дисплея. Обновите или удалите драйвер отображения.	Сбой установки на этапе FIRST_BOOT при попытке MIGRATE_DATA операции. Это может произойти из-за проблемы с драйвером отображения.
0xC1900101 — 0x4000D	Проверьте дополнительные журналы отката для файла setupmem.dmp или журналов событий для любых непредвиденных перезагрузок или ошибок. Просмотрите журнал отката и определите код остановки. Журнал отката находится в папке *$Windows.~BT\Sources\Rollback* . Ниже показан пример анализа. Этот пример не является репрезентативным для всех случаев: Обнаружена 0x0000007E аварийного сбоя службы сведений о пакете обновления Имя модуля СЛУЖБЫ сведений: Параметр 1 проверки ошибок sp: 0xFFFFFFFFC0000005 Параметр 2 проверки ошибок службы сведений о пакете обновления 2: 0xFFFFF8015BC0036A	Откат произошел из-за проблемы с конфигурацией драйвера. Сбой установки во время второго этапа загрузки при попытке MIGRATE_DATA операции. Это может произойти из-за несовместимых драйверов.

Код	Исправление	Причина
	Параметр 3 для проверки ошибок sp: 0xFFFFD000E5D23728 Параметр 4 для проверки ошибок службы сведений о sp: 0xFFFFD000E5D22F40 Не удается восстановить систему. Сведения о откате sp: отображение окна заставки с восстановлением текста: восстановление предыдущей версии Windows. Как правило, для анализа аварийного сбоя существует файл дампа. Если вы не оснащены для отладки дампа, попробуйте выполнить следующие основные процедуры устранения неполадок: 1. Убедитесь, что у вас достаточно места на диске. 2. Если драйвер определен в сообщении проверки ошибок, отключите драйвер или обратитесь к изготовителю обновлений драйверов. 3. Попробуйте изменить видеоадаптеры. 4. Обратитесь к поставщику оборудования для любых обновлений BIOS. 5. Отключите параметры памяти BIOS, такие как кэширование или тень.	
0xC1900101 - 0x40017	Очистка загрузки в Windows и попытка обновления до Windows 10. Подробные сведения см. в статье Как выполнить «чистую» загрузку в Windows . Убедитесь, что выбран параметр "Скачать и установить обновления (рекомендуется). Компьютеры под управлением Citrix VDA Это сообщение может отображаться после обновления компьютера с Windows 10 версии 1511 до Windows 10 версии 1607. После перезапуска второй системы система создает эту ошибку, а затем откатится к предыдущей версии. Эта проблема также наблюдалась в обновлениях до Windows 8.1 и Windows 8. Эта проблема возникает из-за того, что на компьютере установлен агент citrix Virtual Delivery Agent (VDA). Citrix VDA устанавливает драйверы устройств и драйвер фильтра файловой системы (CtxMcsWbc). Этот драйвер фильтра Citrix запрещает обновление записывать изменения на диск, поэтому обновление не может завершиться и система откатится. Решение Чтобы устранить эту проблему, установите накопительное обновление для Windows 10 версии 1607 и Windows Server 2016: 8 ноября 2016 г. Эту проблему можно обойти двумя способами: Обходное решение 1 1. Используйте приложение установки VDA (VDAWorkstationSetup_7.11) для удаления Citrix VDA. 2. Снова запустите обновление Windows.	Обновление Windows 10 завершилось сбоем после второй перезагрузки. Это вызвано неисправным драйвером. Например, драйверы антивирусной фильтрации или драйверы шифрования.

Код	Исправление	Причина
	3. Переустановите Citrix VDA. Обходное решение 2 Если вы не можете удалить Citrix VDA, выполните следующие действия, чтобы обойти эту проблему: 1. В редакторе реестра перейдите к следующему подразделу: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class{4d36e967-e325-11ce-bfc1-08002be10318}\CtxMcsWbc` 2. Измените значение `Start` записи от **0** до **4**. Это изменение отключает службу кэша Citrix MCS. 3. Перейдите к следующему подразделу: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class{4d36e967-e325-11ce-bfc1-08002be10318}` 4. Удаление `CtxMcsWbc` записи. 5. Перезапустите компьютер и повторите попытку обновления. Отказ от ответственности за сведения, отличные от Майкрософт Продукты, не являющиеся корпорацией Майкрософт, которые рассматриваются в этой статье, производятся компаниями, не зависящими от Корпорации Майкрософт. Корпорация Microsoft не дает никаких гарантий, подразумеваемых и прочих, относительно производительности и надежности этих продуктов.	

0x800xxxxx

Коды результатов, начинающиеся с цифр 0x800, также важны для понимания. Эти коды ошибок указывают на общие ошибки операционной системы и не являются уникальными для процесса обновления Windows. Примеры включают время ожидания, устройства, которые не работают, и процесс неожиданно останавливается.

Ознакомьтесь со следующими общими процедурами устранения неполадок, связанными с кодом результата 0x800xxx:

Развернуть таблицу

Код	Исправление	Причина
80040005 — 0x20007	Эта ошибка имеет несколько возможных причин. Попробуйте выполнить быстрые исправления и, если это не удалось, проанализируйте файлы журналов, чтобы определить проблему и решение.	Неуказанная ошибка произошла с драйвером на этапе SafeOS.
0x80073BC3 — 0x20009 0x80070002 — 0x20009 0x80073B92 — 0x20009	Эти ошибки возникают во время анализа секций и проверки и могут быть вызваны наличием нескольких системных секций. Например, если вы установили новый системный диск, но оставили предыдущий системный диск подключенным, это может вызвать конфликт. Чтобы устранить ошибки, отключите или временно отключите диски, содержащие неиспользуемый системный раздел. После завершения	Запрошенное системное устройство не удается найти, есть нарушение общего доступа или несколько устройств, соответствующих критериям идентификации.

Код	Исправление	Причина
	обновления можно повторно подключить диск. Кроме того, можно удалить неиспользуемую системную секцию.	
800704B8 — 0x3001A	Отключите или удалите антивирусные приложения, отличные от Майкрософт, отключите все ненужные устройства и выполните чистую загрузку.	На первом этапе загрузки произошла расширенная ошибка.
8007042B — 0x4000D	Анализ файлов журнала для определения файла, приложения или драйвера, который не может быть перенесен. Отключение, обновление, удаление или замена устройства или объекта.	Сбой установки во время второго этапа загрузки при попытке MIGRATE_DATA операции. Эта проблема может возникнуть из-за проблем с файловой системой, приложением или драйвером.
8007001F — 0x3000D	Анализ файлов журнала для определения файлов или записей реестра, которые блокируют миграцию данных. Эта ошибка может возникнуть из-за проблемы с профилями пользователей. Это может произойти из-за повреждения записей `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList` реестра в каталоге *\Users* или недопустимых файлов. Примечание. Если предыдущее обновление не выполнено, в каталоге *Windows.old\Users* могут существовать недопустимые профили. Чтобы устранить эту ошибку, убедитесь, что удаленные учетные записи еще не присутствуют в реестре Windows и что файлы в каталоге *\Users* допустимы. Удалите недопустимые файлы или профили пользователей, вызывающие эту ошибку. Определенные файлы и профили, вызывающие ошибку, записываются в файлы журнала установки Windows.	Сбой установки на этапе FIRST_BOOT с ошибкой во время MIGRATE_DATA операции.
8007001F — 0x4000D	Анализ файлов журналов для определения устройства, которое не работает должным образом. Отключите, обновите или замените устройство.	Общий сбой, устройство, подключенное к системе, не работает.
8007042B — 0x4001E	Эта ошибка имеет несколько возможных причин. Попробуйте выполнить быстрые исправления и, если это не удалось, проанализируйте файлы журналов, чтобы определить проблему и решение.	Сбой установки во время второго этапа загрузки при попытке PRE_OOBE операции.

Другие коды результатов

Развернуть таблицу

Код ошибки	Причина	Исправление
0xC1800118	WSUS скачал содержимое, которое оно не может использовать из-за отсутствующих ключей расшифровки.	Инструкции по устранению ошибок 0xC1800118 для получения сведений.
0xC1900200	Setup.exe обнаружил, что компьютер не соответствует минимальным требованиям к системе.	Убедитесь, что система, которую вы пытаетесь обновить, соответствует минимальным требованиям к системе. Дополнительные сведения см . в спецификациях Windows 10.
0x80090011	Во время миграции данных пользователя произошла ошибка драйвера устройства.	Обратитесь к поставщику оборудования и получите все обновленные драйверы устройств. Во время обновления рекомендуется иметь активное подключение к Интернету. Убедитесь, что "Загрузка и установка обновлений (рекомендуется)" принимается в начале процесса обновления.
0xC7700112	Сбой записи данных на системный диск, возможно, из-за сбоя доступа к записи на жестком диске.	Эта проблема устранена в последней версии помощника по обновлению. Убедитесь, что "Загрузка и установка обновлений (рекомендуется)" принимается в начале процесса обновления.
0x80190001	При попытке скачать файлы, необходимые для обновления, возникла непредвиденная ошибка.	Чтобы устранить эту проблему, скачайте и запустите средство создания мультимедиа. См. раздел "Скачать windows 10 ".
0x80246007	Обновление не было успешно загружено.	Попробуйте выполнить обновление операционной системы другими способами. Скачайте и запустите средство создания мультимедиа. См. раздел "Скачать windows 10 ". Попытка выполнить обновление с помощью . ISO или USB. Примечание. Windows 10 Корпоративная недоступны в средстве создания мультимедиа. Дополнительные сведения см. в Центре обслуживания корпоративного лицензирования.
0x80244018	Компьютер подключен через прокси-сервер.	Убедитесь, что в параметрах интернета выбран параметр автоматического обнаружения параметров. (**параметры подключения локальной>сети панель управления> Internet).>**
0xC1900201	Система не передала минимальные требования для установки обновления.	Обратитесь к поставщику оборудования, чтобы получить последние обновления.
0x80240017	Обновление недоступно для этого выпуска Windows.	Административные политики, применяемые вашей организацией, могут препятствовать обновлению. Обратитесь к ИТ-администратору.
0x80070020	Существующий процесс не может получить доступ к файлу, так как он используется другим процессом.	Используйте средство MSCONFIG для выполнения чистой загрузки на компьютере, а затем повторите

Код ошибки	Причина	Исправление
		попытку обновления. Подробные сведения см. в статье Как выполнить «чистую» загрузку в Windows.
0x80070522	У пользователя нет необходимых привилегий или учетных данных для обновления.	Убедитесь, что вы выполнили вход в качестве локального администратора или имеют права локального администратора.
0xC1900107	Операция очистки из предыдущей попытки установки по-прежнему ожидается, и для продолжения обновления требуется перезагрузка системы.	Перезапустите устройство и снова запустите программу установки. Если перезагрузка устройства не устраняет проблему, используйте служебную программу очистки диска для очистки временных файлов и системных файлов. Дополнительные сведения см. в разделе "Очистка дисков" в Windows 10.
0xC1900209	Пользователь решил отменить, так как система не передает проверку совместимости для установки обновления. Setup.exe сообщит об этой ошибке, когда он может обновить компьютер с пользовательскими данными, но не может перенести установленные приложения.	Несовместимое программное обеспечение блокирует процесс обновления. Удалите приложение и повторите попытку обновления. Дополнительные сведения см. в статье о предварительной проверке Windows 10 с помощью SETUP.EXE. Вы также можете скачать пакет средств оценки и развертывания Windows (ADK) для Windows 10 и установить средства совместимости приложений.
0x8007002	Эта ошибка связана с обновлениями с помощью Configuration Manager R2 с пакетом обновления 1 (CU3) (5.00.8238.1403)	Проанализируйте SMSTS.log и убедитесь, что обновление завершается сбоем на этапе "Применить операционную систему": ошибка 80072efe DownloadFileWithRanges() завершилась ошибкой. 80072efe. ApplyOperatingSystem (0x0760) Ошибка 80072efe означает, что подключение к серверу было прекращено ненормально. Чтобы устранить эту проблему, попробуйте проверить развертывание ОС на клиенте в той же виртуальной локальной сети, что и сервер Configuration Manager. Проверьте конфигурацию сети на наличие проблем с случайным подключением к клиентскому серверу, возникающим в удаленной виртуальной локальной локальной сети.
0x80240FFF	Происходит при сбое синхронизации обновлений. Это может произойти при использовании служб Windows Server Update Services самостоятельно или при интеграции с Microsoft Endpoint Configuration Manager. Если вы включите синхронизацию обновлений перед установкой исправлений 3095113, службы WSUS не распознает классификацию обновлений и вместо этого обрабатывает обновление как регулярное обновление.	Это можно предотвратить, установив 3095113 исправлений перед включением синхронизации обновлений. Однако если вы уже выполнили эту проблему, сделайте следующее: 1. Отключите классификацию обновлений. 2. Установите 3095113 исправлений. 3. Удалите ранее синхронизированные обновления. 4. Включите классификацию обновлений. 5. Выполните полную синхронизацию. Подробные сведения о выполнении этих действий см. в статье "Как удалить обновления в WSUS".

Код ошибки	Причина	Исправление
0x8007007E	Происходит при сбое синхронизации обновлений, так как перед включением синхронизации обновлений не установлено исправление 3095113. В частности, операция CopyToCache завершается сбоем на клиентах, которые уже скачали обновление, так как службы центра обновления Windows Server имеют плохие метаданные, связанные с обновлением. Это может произойти при использовании автономных служб Windows Server Update Services или при интеграции WSUS с Microsoft Endpoint Configuration Manager.	Чтобы восстановить службы Windows Server Update Services, выполните следующие действия. Перед установкой исправления необходимо выполнить эти действия на каждом сервере WSUS, который синхронизировал метаданные. Остановите службу Обновл. Windows. • Войдите как пользователь с правами администратора, а затем выполните следующие действия: • Откройте **средства** администрирования из **панель управления**. • Дважды щелкните **Службы**. • Найдите службу Обновл. Windows**, щелкните ее правой** кнопкой мыши и нажмите кнопку "**Остановить**". Когда появится приглашение, введите свои учетные данные. Удалите все файлы и папки в папке *c:\Windows\SoftwareDistribution\DataStore*. Перезапустите службу Центра обновления Windows.

Другие коды ошибок

Развернуть таблицу

Коды ошибок	Причина	Исправление
0x80070003-0x20007	Это сбой во время установки драйвера для этапа SafeOS.	Проверьте драйверы устройств на компьютере и проанализируйте файлы журналов, чтобы определить драйвер проблемы.
0x8007025D — 0x2000C	Эта ошибка возникает, если метаданные ISO-файла повреждены или возникают проблемы со средой хранения, например модуль ОЗУ, содержащий плохие блоки во время установки Windows.	Перезагрузите ISO/Media и повторно презрите обновление Кроме того, повторно создайте установочный носитель средства создания мультимедиа .
0x80070490 — 0x20007	Присутствует несовместимый драйвер устройства.	Проверьте драйверы устройств на компьютере и проанализируйте файлы журналов, чтобы определить драйвер проблемы.
0xC1900101 — 0x2000c	Неуказанная ошибка произошла на этапе SafeOS во время применения WIM. Это может быть вызвано устаревшим драйвером или повреждением диска.	Выполните флажок, чтобы восстановить файловую систему. Дополнительные сведения см. в разделе "Быстрые исправления " в этом руководстве. Обновите драйверы на компьютере и нажмите кнопку "Скачать и установить обновления (рекомендуется)" во время процесса обновления. Отключите устройства, отличные от мыши, клавиатуры и дисплея.

Коды ошибок	Причина	Исправление
0xC1900200 — 0x20008	Компьютер не соответствует минимальным требованиям для скачивания или обновления до Windows 10.	Ознакомьтесь со спецификациями Windows 10 и проверьте, соответствует ли компьютер минимальным требованиям. Просмотрите журналы для сведений о совместимости.
0xC1900200 — 0x20008	Компьютер не соответствует минимальным требованиям для скачивания или обновления до Windows 10. Ознакомьтесь со спецификациями Windows 10 и проверьте, соответствует ли компьютер минимальным требованиям. Просмотрите журналы спецификаций Windows 10.	
0x80070004 — 0x3000D	Это проблема с миграцией данных на первом этапе загрузки. Существует несколько возможных причин.	Анализ файлов журнала для определения проблемы.
0xC1900101 — 0x4001E	Сбой установки на этапе SECOND_BOOT с ошибкой во время PRE_OOBE операции.	Это универсальная ошибка, возникающая во время этапа установки OOBE. Ознакомьтесь с разделом 0xC1900101 этого руководства и ознакомьтесь с общими процедурами устранения неполадок, описанными в этом разделе.
0x80070005 — 0x4000D	Сбой установки на этапе SECOND_BOOT с ошибкой во время MIGRATE_DATA операции. Эта ошибка указывает, что при попытке переноса данных доступ был отклонен.	Анализ файлов журнала, чтобы определить точку данных, доступ к которому запрещен.
0x80070004 — 0x50012	Программа установки Windows не удалось открыть файл.	Анализ файлов журналов для определения точки данных, которая представляет проблемы с доступом.
0xC190020e 0x80070070 — 0x50011 0x80070070 — 0x50012 0x80070070 - 0x60000	Эти ошибки указывают, что на компьютере недостаточно свободного места для установки обновления.	Для обновления компьютера до Windows 10 требуется 16 ГБ свободного жесткого диска для 32-разрядной ОС и 20 ГБ для 64-разрядной ОС. Если недостаточно места, попробуйте освободить место на диске, прежде чем продолжить обновление. **Примечание.** Если устройство разрешает его, для процесса обновления можно использовать внешний USB-диск. Программа установки Windows создаст резервную копию предыдущей версии Windows на USB-внешний диск. Внешний диск должен быть не менее 8 ГБ (рекомендуется 16 ГБ). Внешний диск должен быть отформатирован с помощью NTFS. Диски, отформатированные в FAT32, могут столкнуться с ошибками из-за ограничений размера файла FAT32. USB-накопители предпочтительнее по сравнению с SD-картами, так как драйверы

Коды ошибок	Причина	Исправление
		для SD-карт не переносятся, если устройство не поддерживает подключенный режим ожидания.

Современные ошибки установки

Также см. следующий последовательный список кодов ошибок современной установки (mosetup) с кратким описанием причины.

Развернуть таблицу

Код результата	Message	Description
0XC1900100	MOSETUP_E_VERSION_MISMATCH	Обнаружена непредвиденная версия двоичных файлов платформы установки. Проверьте содержимое пакета.
0XC1900101	MOSETUP_E_SETUP_PLATFORM	Платформа установки обнаружила непреднавиденную ошибку.
0XC1900102	MOSETUP_E_SHUTDOWN_BLOCK	Не удалось создать или уничтожить сообщение блока завершения работы.
0XC1900103	MOSETUP_E_COMPAT_TIMEOUT	Проблемы совместимости не были устранены в течение требуемого периода времени.
0XC1900104	MOSETUP_E_PROCESS_TIMEOUT	Процесс установки не завершился в течение требуемого периода времени.
0XC1900105	MOSETUP_E_TEST_MODE	Процесс установки используется в тестовой среде.
0XC1900106	MOSETUP_E_TERMINATE_PROCESS	Процесс установки был завершен.
0XC1900107	MOSETUP_E_CLEANUP_PENDING	Операция очистки из предыдущей попытки установки по-прежнему ожидается. Требуется перезагрузка системы.
0XC1900108	MOSETUP_E_REPORTING	Произошла ошибка, и значение результата должно быть консолидировано для целей телеметрии.
0XC1900109	MOSETUP_E_COMPAT_TERMINATE	Процесс установки был завершен на этапе

Код результата	Message	Description
		совместимости с действиями.
0XC190010a	MOSETUP_E_UNKNOWN_CMD_LINE	Процесс установки был запущен с неизвестным аргументом командной строки.
0XC190010b	MOSETUP_E_INSTALL_IMAGE_NOT_FOUND	Образ установки не найден.
0XC190010c	MOSETUP_E_AUTOMATION_INVALID	Предоставленные сведения об автоматизации были недопустимыми.
0XC190010d	MOSETUP_E_INVALID_CMD_LINE	Процесс установки был запущен с недопустимым аргументом командной строки.
0XC190010e	MOSETUP_E_EULA_ACCEPT_REQUIRED	Процесс установки требует, чтобы пользователь принял лицензионное соглашение.
0XC1900110	MOSETUP_E_EULA_CANCEL	Пользователь решил отменить лицензионное соглашение.
0XC1900111	MOSETUP_E_ADVERTISE_CANCEL	Пользователь решил отменить рекламу.
0XC1900112	MOSETUP_E_TARGET_DRIVE_NOT_FOUND	Не удалось найти букву целевого диска.
0XC1900113	MOSETUP_E_EULA_DECLINED	Пользователь отказался от условий лицензии.
0XC190011e	MOSETUP_E_FLIGHTING_BVT	Процесс установки был остановлен в целях тестирования.
0XC190011f	MOSETUP_E_PROCESS_CRASHED	Произошел сбой процесса установки.
0XC1900120	MOSETUP_E_EULA_TIMEOUT	Пользователь не принял EULA в течение требуемого периода времени.
0XC1900121	MOSETUP_E_ADVERTISE_TIMEOUT	Пользователь не принял объявление в течение требуемого срока.
0XC1900122	MOSETUP_E_DOWNLOADDISKSPACE_TIMEOUT	Проблемы с дисковой областью загрузки не были устранены в течение требуемого периода времени.
0XC1900123	MOSETUP_E_INSTALLDISKSPACE_TIMEOUT	Проблемы с местом на диске установки не устранены в течение требуемого периода времени.

Код результата	Message	Description
0XC1900124	MOSETUP_E_COMPAT_SYSREQ_TIMEOUT	Минимальные проблемы совместимости требований не были устранены в течение требуемого периода времени.
0XC1900125	MOSETUP_E_COMPAT_DOWNLOADREQ_TIMEOUT	Проблемы совместимости для скачивания не разрешались в течение требуемого периода времени.
0XC1900126	MOSETUP_E_GATHER_OS_STATE_SIGNATURE	Исполняемый файл GatherOsState имеет недопустимую подпись.
0XC1900127	MOSETUP_E_UNINSTALL_ALLOWED_ABORT	Пользователь решил отменить установку, чтобы сохранить параметр "Удалить" активным.
0XC1900128	MOSETUP_E_MISSING_TASK	Установка не может продолжиться, так как требуемая задача отсутствует.
0XC1900129	MOSETUP_E_UPDATEMEDIA_REQUESTED	Для продолжения установки будет запущена более актуальная версия установки.
0XC190012f	MOSETUP_E_FINALIZE_ALREADY_REQUESTED	Установка не может продолжиться, так как операция завершения уже запрошена.
0XC1900130	MOSETUP_E_INSTALL_HASH_MISSING	Установка не может продолжиться, так как хэш экземпляра не найден.
0XC1900131	MOSETUP_E_INSTALL_HASH_MISMATCH	Установка не может продолжаться, так как хэш экземпляра не соответствует.
0XC19001df	MOSETUP_E_DISK_FULL	Установка не может продолжаться, так как система не находится на диске.
0XC19001e0	MOSETUP_E_GATHER_OS_STATE_FAILED	Не удалось выполнить исполняемый файл GatherOsState.
0XC19001e1	MOSETUP_E_PROCESS_SUSPENDED	Процесс установки приостановлен.
0XC19001e2	MOSETUP_E_PREINSTALL_SCRIPT_FAILED	Не удалось выполнить или вернуть ошибку при выполнении скрипта предварительной записи.
0XC19001e3	MOSETUP_E_PRECOMMIT_SCRIPT_FAILED	Не удалось выполнить или вернуть скрипт предварительной

Код результата	Message	Description
		записи.
0XC19001e4	MOSETUP_E_FAILURE_SCRIPT_FAILED	Скрипт сбоя не удалось выполнить или вернуть ошибку.
0XC19001e5	MOSETUP_E_SCRIPT_TIMEOUT	Скрипт превысил ограничение времени ожидания.
0XC1900200	MOSETUP_E_COMPAT_SYSREQ_BLOCK	Система не передает минимальные требования для установки обновления.
0XC1900201	MOSETUP_E_COMPAT_SYSREQ_CANCEL	Пользователь решил отменить, так как система не передает минимальные требования для установки обновления.
0XC1900202	MOSETUP_E_COMPAT_DOWNLOADREQ_BLOCK	Система не передает минимальные требования для скачивания обновления.
0XC1900203	MOSETUP_E_COMPAT_DOWNLOADREQ_CANCEL	Пользователь решил отменить, так как система не передает минимальные требования для скачивания обновления.
0XC1900204	MOSETUP_E_COMPAT_MIGCHOICE_BLOCK	Система не передает требования к требуемому выбору миграции.
0XC1900205	MOSETUP_E_COMPAT_MIGCHOICE_CANCEL	Пользователь выбрал отмену, так как система не передает требования к требуемому выбору миграции.
0XC1900206	MOSETUP_E_COMPAT_DEVICEREQ_BLOCK	Система не передает проверку устройства для установки обновления.
0XC1900207	MOSETUP_E_COMPAT_DEVICEREQ_CANCEL	Пользователь решил отменить, так как система не передает проверку устройства для установки обновления.
0XC1900208	MOSETUP_E_COMPAT_INSTALLREQ_BLOCK	Система не передает проверку compat для установки обновления.
0XC1900209	MOSETUP_E_COMPAT_INSTALLREQ_CANCEL	Пользователь решил отменить, так как система не передает проверку compat для установки обновления.
0XC190020a	MOSETUP_E_COMPAT_RECOVERYREQ_BLOCK	Система не передает минимальные требования для восстановления Windows.

Код результата	Message	Description
0XC190020b	MOSETUP_E_COMPAT_RECOVERYREQ_CANCEL	Пользователь решил отменить, так как система не передает минимальные требования для восстановления Windows.
0XC190020c	MOSETUP_E_DOWNLOADDISKSPACE_BLOCK	Система не передает требования к месту на диске для скачивания полезных данных.
0XC190020d	MOSETUP_E_DOWNLOADDISKSPACE_CANCEL	Пользователь решил отменить, так как устройство не имеет достаточно места на диске для скачивания.
0XC190020e	MOSETUP_E_INSTALLDISKSPACE_BLOCK	Система не передает требования к месту на диске для установки полезных данных.
0XC190020f	MOSETUP_E_INSTALLDISKSPACE_CANCEL	Пользователь решил отменить, так как устройство не имеет достаточно места на диске для установки.
0XC1900210	MOSETUP_E_COMPAT_SCANONLY	Пользователь использовал командную строку setup.exe для выполнения сканирования, а не для установки ОС.
0XC1900211	MOSETUP_E_DOWNLOAD_UNPACK_DISKSPACE_BLOCK	Система не передает требования к местам на диске для скачивания и распаковки мультимедиа.
0XC1900212	MOSETUP_E_DOWNLOAD_UNPACK_DISKSPACE_MULTIARCH_BLOCK	Система не передает требования к местам на диске для скачивания и распаковки мультимедиа с несколькими архитектурами.
0XC1900213	MOSETUP_E_NO_OFFER_FOUND	Не было найдено предложения, соответствующего необходимым критериям.
0XC1900214	MOSETUP_E_UNSUPPORTED_VERSION	Эта версия средства не поддерживается.
0XC1900215	MOSETUP_E_NO_MATCHING_INSTALL_IMAGE	Не удалось найти образ установки для этой системы.
0XC1900216	MOSETUP_E_ROLLBACK_PENDING	Обнаружена ожидающая операция отката ОС.
0XC1900220	MOSETUP_E_COMPAT_REPORT_NOT_DISPLAYED	Отчет о совместимости не может отображаться из-за отсутствия системного компонента.

Код результата	Message	Description
0XC1900400	MOSETUP_E_UA_VERSION_MISMATCH	Обнаружена непредвиденная версия клиента агента обновления.
0XC1900401	MOSETUP_E_UA_NO_PACKAGES_TO_DOWNLOAD	Нет пакетов, которые нужно скачать.
0XC1900402	MOSETUP_E_UA_UPDATE_CANNOT_BE_MERGED	Нет пакетов, которые нужно скачать.
0XC1900403	MOSETUP_E_UA_CORRUPT_PAYLOAD_FILES	Полезные файлы повреждены.
0XC1900404	MOSETUP_E_UA_BOX_NOT_FOUND	Исполняемый файл установки не найден.
0XC1900405	MOSETUP_E_UA_BOX_CRASHED	Процесс установки неожиданно завершился.

Сбор данных

Если вам нужна помощь службы поддержки Microsoft, мы рекомендуем собирать информацию путем выполнения действий, описанных в разделе Сбор информации с помощью TSS для решения проблем, связанных с развертыванием.

Дополнительная информация

- Вопросы и ответы о Windows 10 для ИТ-специалистов
- требования к системе Windows 10 Корпоративная
- Спецификации Windows 10
- Форумы ИТ-специалистов в Windows 10
- Исправление Обновл. Windows ошибок с помощью средства подготовки к обновлению системы или DISM
- Ошибка обновления Windows 7 до Windows 10 (0x800707E7 — 0x3000D))
- Ошибка обновления Windows 10: несоответствие суффикса профиля пользователя, 0x800707E7 — 0x3000D

Отправка ошибок обновления Windows с помощью Центра отзывов

Применяется к: ✅ Windows 11, ✅ Windows 10

> ⓘ **Примечание.**
>
> Эта статья содержит 100 уровней (базовая).
>
> Полный список статей этого раздела см. в статье **Устранение ошибок обновления Windows** .

В этой статье описывается, как отправлять проблемы с обновлением Windows до Корпорации Майкрософт с помощью Центр отзывов о Windows.

О центре отзывов

Приложение "Центр отзывов" позволяет сообщать корпорации Майкрософт о любых проблемах, возникших при использовании Windows. Это также позволяет отправлять в корпорацию Майкрософт предложения по улучшению работы с Windows. Ранее Центр отзывов можно было использовать только в рамках программы предварительной оценки Windows. Теперь любой пользователь может использовать это средство. Приложение "Центр отзывов" можно скачать из Microsoft Store.

Для работы Центра отзывов требуется поддерживаемая в настоящее время версия Windows. Центр отзывов можно использовать для отправки сведений в корпорацию Майкрософт при возникновении проблем при обновлении Windows. При обновлении между поддерживаемой версией Windows Центр отзывов автоматически собирает файлы журналов. Для операционных систем без поддержки до Windows 10, которые не поддерживают Центр отзывов, файлы журналов должны собираться вручную. Затем файлы журнала можно присоединить к элементу отзывов с помощью устройства под управлением поддерживаемой в настоящее время версии Windows , поддерживающей Центр отзывов.

Отправить отзыв

Чтобы отправить отзыв о неудачном обновлении Windows, откройте Центр отзывов.

В Центре отзывов заполните все разделы с максимально возможной детализацией:

1. **Введите свой отзыв**
2. **Выберите категорию**
3. **Найти похожие отзывы** . В этом разделе нет ничего, чтобы заполнить, но важно проверка для аналогичных элементов отзывов. Если найден похожий элемент обратной связи, выберите его и нажмите кнопку **Далее** . Это позволяет корпорации Майкрософт узнать, сколько людей затрагивает та же проблема.
4. **Добавление дополнительных сведений**

Рекомендуемые сведения, которые можно включить в раздел **Добавление дополнительных сведений** :

- Когда произошел сбой?
  - Происходили ли перезагрузки?
  - Сколько раз система перезагружалась?
- Как произошел сбой обновления?
  - Отображались ли какие-либо коды ошибок?
  - Привел ли сбой к появлению синего экрана?
  - Выполняется ли автоматический откат компьютера или он зависает, требуя циклического отката питания компьютера?
- Какое программное обеспечение безопасности установлено?
- Установлены ли на компьютере последние версии драйверов и встроенного ПО?
- Подключены ли какие-либо внешние устройства?

С помощью параметров **Присоединить снимок экрана** и **Вложить файл** можно включить снимки экрана или файлы в элемент обратной связи. Вложения и снимки экрана являются необязательными, но могут быть полезны при диагностике проблемы с обновлением. Например, файлы журналов можно включать в качестве вложений в элемент обратной связи. Расположение файлов журнала обновления Windows описано в статье Файлы журнала программы установки Windows и журналы событий.

Наконец, параметр **Повторное создание проблемы** можно использовать для отправки дополнительных данных и журналов корпорации Майкрософт для оценки.

После завершения всех элементов отзывов нажмите кнопку **Отправить** , чтобы отправить отзыв. Корпорация Майкрософт получает отзыв и начинает анализ проблемы. Отправленные отзывы можно периодически проверять, чтобы узнать, какие решения предоставляются.

Ссылка на отзыв

После отправки отзыва в элемент обратной связи можно добавить дополнительные сведения и элементы. Для этого выполните следующие действия.

1. Откройте Центр отзывов.
2. В верхней части Центра отзывов выберите **Мой отзыв**.
3. Выберите отправленный элемент обратной связи.
4. Выберите **Поделиться**.
5. Скопируйте и используйте отображаемую короткую ссылку.

Last updated on 09.04.2025

Обновл. Windows проблемы, связанные с устранением неполадок

25.04.2025Применяется к: Supported versions of Windows Client

Применимо к: Windows 10

Попробуйте наш виртуальный агент . Это поможет вам быстро определить и устранить распространенные проблемы с обновлением Windows

Если при использовании Обновл. Windows возникают проблемы, выполните следующие действия.

1. Запустите встроенный средство устранения неполадок Обновл. Windows, чтобы устранить распространенные проблемы. Перейдите в **параметры**>, затем в **Обновление и безопасность**>, **Устранение неполадок**> и **Центр обновления Windows**.

2. Установите последнее обновление стека обслуживания, соответствующее вашей версии Windows из каталога центра обновления Майкрософт. Дополнительные сведения об обновлениях стека обслуживания см. в разделе "Обновления стека обслуживания".

3. Убедитесь, что установлены последние обновления Windows, накопительные обновления и накопительные пакеты обновления. Чтобы проверить состояние обновления, ознакомьтесь с соответствующим журналом обновлений для системы:

   - Windows 10 версии 2004 и Windows Server версии 2004
   - Windows 10 версии 1909 и Windows Server версии 1909
   - Windows 10 версии 1903 и Windows Server версии 1903
   - Windows 10 версии 1809 и Windows Server 2019
   - Windows 10 версии 1803
   - Windows 10 версии 1709
   - Windows 10 версии 1703
   - Windows 10 и Windows Server 2016
   - Windows 8.1 и Windows Server 2012 R2
   - Windows Server 2012
   - Windows 7 с пакетом обновления 1 (SP1) и Windows Server 2008 R2 с пакетом обновления 1 (SP1)

Расширенные пользователи могут также для дальнейшего изучения воспользоваться журналом, созданным Центром обновления Windows.

При использовании Обновл. Windows могут возникнуть следующие сценарии.

Почему я предлагаю старое обновление?

Обновление, предлагаемое устройству, зависит от нескольких факторов. Ниже приведены некоторые из наиболее распространенных атрибутов:

- Сборка ОС
- Ветвь ОС
- Языковой стандарт ОС
- Архитектура ОС
- Конфигурация управления обновлениями устройств

Если предлагаемое обновление не является самым текущим, это может быть связано с тем, что ваше устройство управляется сервером WSUS, и вы предлагаете обновления, доступные на этом сервере. Кроме того, если устройство входит в группу развертывания, администратор намеренно замедляет развертывание обновлений. Так как развертывание медленно и измеряется для начала, все устройства не получат обновление в тот же день.

Мое устройство заморожено при сканировании. Почему?

Пользовательский интерфейс параметров взаимодействует со службой Update Orchestrator, которая, в свою очередь, взаимодействует со службой Обновл. Windows. Если эти службы непредвиденно остановятся, может появиться такое поведение. В таких случаях выполните следующие действия.

1. Закройте приложение "Параметры" и снова откройте его.

2. Запустите Services.msc и проверьте, выполняются ли следующие службы:

    - Обновление оркестратора состояния
    - Центр обновления Windows

Обновления компонентов не предлагаются, а другие обновления

Устройства под управлением Windows 10 версий от 1709 до 1803, настроенные для обновления из Центра обновления Windows (включая Центр обновления Windows для бизнеса), могут устанавливать обновления обслуживания и определения, но обновления компонентов им не предоставляются.

Проверка WindowsUpdate.log показывает следующую ошибку:

Выходные данные

```
YYYY/MM/DD HH:mm:ss:SSS PID  TID  Agent           * START * Finding updates
CallerId = Update;taskhostw  Id = 25
YYYY/MM/DD HH:mm:ss:SSS PID  TID  Agent           Online = Yes; Interactive = No;
AllowCachedResults = No; Ignore download priority = No
YYYY/MM/DD HH:mm:ss:SSS PID  TID  Agent           ServiceID = {855E8A7C-ECB4-4CA3-
B045-1DFA50104289} Third party service
YYYY/MM/DD HH:mm:ss:SSS PID  TID  Agent           Search Scope = {Current User}
YYYY/MM/DD HH:mm:ss:SSS PID  TID  Agent           Caller SID for Applicability: S-
1-12-1-2933642503-1247987907-1399130510-4207851353
YYYY/MM/DD HH:mm:ss:SSS PID  TID  Misc            Got 855E8A7C-ECB4-4CA3-B045-
1DFA50104289 redir Client/Server URL:
https://fe3.delivery.mp.microsoft.com/ClientWebService/client.asmx""
YYYY/MM/DD HH:mm:ss:SSS PID  TID  Misc            Token Requested with 0 category
IDs.
YYYY/MM/DD HH:mm:ss:SSS PID  TID  Misc            GetUserTickets: No user tickets
found. Returning WU_E_NO_USERTOKEN.
YYYY/MM/DD HH:mm:ss:SSS PID  TID  Misc            *FAILED* [80070426] Method
failed [AuthTicketHelper::GetDeviceTickets:570]
YYYY/MM/DD HH:mm:ss:SSS PID  TID  Misc            *FAILED* [80070426] Method
failed [AuthTicketHelper::GetDeviceTickets:570]
YYYY/MM/DD HH:mm:ss:SSS PID  TID  Misc            *FAILED* [80070426]
GetDeviceTickets
YYYY/MM/DD HH:mm:ss:SSS PID  TID  Misc            *FAILED* [80070426] Method
failed [AuthTicketHelper::AddTickets:1092]
YYYY/MM/DD HH:mm:ss:SSS PID  TID  Misc            *FAILED* [80070426] Method
failed [CUpdateEndpointProvider::GenerateSecurityTokenWithAuthTickets:1587]
YYYY/MM/DD HH:mm:ss:SSS PID  TID  Misc            *FAILED* [80070426]
GetAgentTokenFromServer
YYYY/MM/DD HH:mm:ss:SSS PID  TID  Misc            *FAILED* [80070426]
GetAgentToken
YYYY/MM/DD HH:mm:ss:SSS PID  TID  Misc            *FAILED* [80070426] EP:Call to
GetEndpointToken
YYYY/MM/DD HH:mm:ss:SSS PID  TID  Misc            *FAILED* [80070426] Failed to
obtain service 855E8A7C-ECB4-4CA3-B045-1DFA50104289 plugin Client/Server auth
token of type 0x00000001
YYYY/MM/DD HH:mm:ss:SSS PID  TID  ProtocolTalker  *FAILED* [80070426] Method
failed [CAgentProtocolTalkerContext::DetermineServiceEndpoint:377]
YYYY/MM/DD HH:mm:ss:SSS PID  TID  ProtocolTalker  *FAILED* [80070426]
Initialization failed for Protocol Talker Context
YYYY/MM/DD HH:mm:ss:SSS PID  TID  Agent           Exit code = 0x80070426
YYYY/MM/DD HH:mm:ss:SSS PID  TID  Agent           * END * Finding updates CallerId
= Update;taskhostw  Id = 25
```

Код ошибки 0x80070426 преобразуется в следующий код:

Выходные данные

```
ERROR_SERVICE_NOT_ACTIVE - # The service has not been started.
```

Помощник по входу в учетную запись Майкрософт (MSA или wlidsvc) — это служба, которая находится под вопросом. Служба полетов DCAT (ServiceId: 855E8A7C-ECB4-4CA3-B045-1DFA50104289) использует MSA для получения глобального идентификатора устройства. Без запуска службы MSA глобальный идентификатор устройства не будет создан и отправлен клиентом, а поиск обновлений компонентов никогда не завершается успешно.

Чтобы устранить эту проблему, сбросить службу MSA на начальный тип по умолчанию "вручную".

Проблемы, связанные с HTTP/Proxy

Обновл. Windows использует WinHttp с запросами частичного диапазона (RFC 7233) для скачивания обновлений и приложений с Обновл. Windows серверов или локальных серверов WSUS. Поэтому прокси-серверы в сети должны поддерживать HTTP-запросы RANGE. Если прокси-сервер был настроен в Internet Explorer (уровне пользователя), но не в WinHTTP (уровне системы), подключения к Обновл. Windows завершаются ошибкой.

Чтобы устранить эту проблему, настройте прокси-сервер в WinHTTP с помощью следующей команды netsh:

Консоль

```
netsh winhttp set proxy ProxyServerName:PortNumber
```

> ⓘ **Примечание**
>
> Вы также можете импортировать параметры прокси-сервера из Internet Explorer с помощью следующей команды: `netsh winhttp import proxy source=ie`

Если скачивание через прокси-сервер завершается ошибкой 0x80d05001 DO_E_HTTP_BLOCKSIZE_MISMATCH или если вы заметили высокую загрузку ЦП во время загрузки обновлений, проверьте конфигурацию прокси-сервера, чтобы разрешить выполнение запросов HTTP RANGE.

Вы можете применить правило, чтобы разрешить HTTP-запросы RANGE для следующих URL-адресов:

- `*.download.windowsupdate.com`
- `*.dl.delivery.mp.microsoft.com`
- `*.delivery.mp.microsoft.com`

Если вы не можете разрешить запросы RANGE, вы будете загружать больше содержимого, чем требуется в обновлениях (так как разностное исправление не будет работать).

Обновление не применимо к компьютеру

Наиболее распространенные причины этой ошибки описаны в следующей таблице:

Развернуть таблицу

Причина	Описание	Решение
Обновление заменено	По мере выпуска обновлений компонента обновленный компонент заменяет старый компонент, который уже находится в системе. При возникновении этой проблемы предыдущее обновление помечается как замененное. Если обновление, которое вы пытаетесь установить, уже имеет более новую версию полезных данных в вашей системе, может появиться это сообщение об ошибке.	Убедитесь, что пакет, который вы устанавливаете, содержит более новые версии двоичных файлов. Кроме того, убедитесь, что пакет заменен другим новым пакетом.
Обновление уже установлено	Если обновление, которое вы пытаетесь установить ранее, было установлено другим обновлением, которое несет ту же полезную нагрузку, может возникнуть это сообщение об ошибке.	Убедитесь, что пакет, который вы пытаетесь установить, не был установлен ранее.
Неправильное обновление для архитектуры	Обновления публикуются архитектурой ЦП. Если обновление, которое вы пытаетесь установить, не соответствует архитектуре ЦП, может возникнуть это сообщение об ошибке.	Убедитесь, что пакет, который вы пытаетесь установить, соответствует используемой версии Windows. Сведения о версии Windows можно найти в разделе "Применимо к" статьи для каждого обновления. Например, на компьютерах под управлением Windows Server 2012 R2

Причина	Описание	Решение
		невозможно установить обновления только для Windows Server 2012 R2. Кроме того, убедитесь, что пакет, который вы устанавливаете, соответствует архитектуре процессора используемой версии Windows. Например, обновление на базе x86 не может быть установлено в операционных системах Windows на базе x64.
Необходимое обновление отсутствует	Для применения некоторых обновлений к системе требуется необходимое обновление. Если у вас отсутствует необходимое обновление, может возникнуть это сообщение об ошибке. Например, 2919355 базы знаний необходимо установить на компьютерах Windows 8.1 и Windows Server 2012 R2 до установки многих обновлений, выпущенных после апреля 2014 года.	Проверьте связанные статьи о пакете в Базе знаний Майкрософт (КБ), чтобы убедиться, что установлены необходимые обновления. Например, при возникновении сообщения об ошибке в Windows 8.1 или Windows Server 2012 R2 может потребоваться установить 2919355 обновления за апрель 2014 г. в качестве предварительных требований и одного или нескольких предварительных обновлений обслуживания (КБ 2919442 и базы знаний 3173424). Чтобы определить, установлены ли эти необходимые обновления, выполните следующую команду PowerShell: `get-hotfix KB3173424,KB2919355, KB2919442`. Если установлены обновления, команда вернет установленную дату в `InstalledOn` разделе выходных данных.

Ошибка 0x800706D9, если служба брандмауэра Защитника Windows отключена

Вы видите, что скачивание обновлений зависло на уровне 0%, особенно в Windows Server 2016, где служба фоновой интеллектуальной передачи (BITS) является диспетчером загрузки по умолчанию.

Ошибка, которая может появиться в журналах Обновл. Windows:

Выходные данные

```
DownloadManager    Error 0x800706d9 occurred while downloading update; notifying
dependent calls.
```

или

Выходные данные

```
[DownloadManager] BITS job {A4AC06DD-D6E6-4420-8720-7407734FDAF2} hit a transient
error, updateId = {D053C08A-6250-4C43-A111-56C5198FE142}.200 <NULL>, error =
0x800706D9
```

или

Выходные данные

```
DownloadManager [0]12F4.1FE8::09/29/2017-13:45:08.530 [agent]DO job {C6E2F6DC-
5B78-4608-B6F1-0678C23614BD} hit a transient error, updateId = 5537BD35-BB74-40B2-
A8C3-B696D3C97CBA.201 <NULL>, error = 0x80D0000A
```

Перейдите в **Services.msc** и убедитесь, что служба **брандмауэра Защитника Windows** включена. Остановка службы, связанной с брандмауэром Windows с расширенной безопасностью, не поддерживается корпорацией Майкрософт. Дополнительные сведения см. в статье об отключении брандмауэра Windows.

Проблемы, возникающие из конфигурации конфликтующих политик

Обновл. Windows предоставляет политику конфигурации широкого диапазона для управления поведением службы Обновл. Windows в управляемой среде. Хотя эти политики позволяют настраивать параметры на детальном уровне, неправильно настроить или задать конфликтующие политики могут привести к непредвиденным поведению.

Дополнительные сведения см. в разделе "Настройка автоматических обновлений с помощью параметров групповой политики или реестра".

Устройство не может получить доступ к файлам обновления

Убедитесь, что устройства могут достичь необходимых конечных точек Обновл. Windows через брандмауэр. Например, для Windows 10 версии 2004 следующие протоколы должны быть доступны следующим конечным точкам:

Развернуть таблицу

Протокол	URL-адрес конечной точки
TLS 1.2	`*.prod.do.dsp.mp.microsoft.com`
HTTP	`emdl.ws.microsoft.com`
HTTP	`*.dl.delivery.mp.microsoft.com`
HTTP	`*.windowsupdate.com`
HTTPS	`*.delivery.mp.microsoft.com`
TLS 1.2	`*.update.microsoft.com`
TLS 1.2	`tsfe.trafficshaping.dsp.mp.microsoft.com`

> **Примечание**
>
> Не следует использовать HTTPS для этих конечных точек, которые указывают HTTP, и наоборот. Подключение завершится ошибкой.

Определенные конечные точки могут отличаться от версий клиента Windows. См. пример конечных точек подключения Windows 10 2004 Enterprise. Аналогичные статьи для других версий клиента Windows доступны в оглавлении рядом.

Обновления не загружают из конечной точки интрасети (WSUS или Configuration Manager)

Клиентские устройства Windows могут получать обновления из различных источников, включая Обновл. Windows в Интернете, сервер Служб обновления Windows Server и другие. Чтобы определить источник Обновл. Windows, которые в настоящее время используются на устройстве, выполните следующие действия.

1. Запустите средство Windows PowerShell с правами администратора.
2. Запустите командлет:

```
PowerShell
$MUSM = New-Object -ComObject "Microsoft.Update.ServiceManager"
```

3. Запустите командлет:

```
PowerShell
```

```
$MUSM.Services
```

Проверьте выходные данные параметров Name и OffersWindowsUPdates, которые можно интерпретировать в соответствии с этой таблицей.

Развернуть таблицу

Выходные данные	Значение
— Имя: Центр обновления Майкрософт -OffersWindowsUpdates: Истина	— Источником обновления является Центр обновления Майкрософт, что означает, что обновления для других продуктов Майкрософт, кроме операционной системы, также могут быть доставлены. — Указывает, что клиент настроен на получение обновлений для всех продуктов Майкрософт (Office и т. д.)
- Имя: DCat Flighting Prod — OffersWindowsUpdates: True	— Начиная с Windows 10 версии 1709 обновления компонентов всегда предоставляются через службу DCAT. — Указывает, что клиент настроен на получение обновлений компонентов из Обновл. Windows.
— Имя: Магазин Windows (DCat Prod) — OffersWindowsUpdates: False	-Источник обновления — это обновления программы предварительной оценки для приложений Магазина. — указывает, что клиент не получит или не настроен на получение этих обновлений.
— имя: служба обновления Windows Server — OffersWindowsUpdates: True	— источник — сервер служб обновления Windows Server. — клиент настроен на получение обновлений от WSUS.
- Имя: Обновл. Windows — OffersWindowsUpdates: True	— источник Обновл. Windows. — Клиент настроен на получение обновлений из Обновл. Windows Online.

У вас есть плохая настройка в среде

В этом примере для каждого набора групповой политики с помощью реестра система настроена на использование WSUS для скачивания обновлений (обратите внимание на вторую строку):

Консоль

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU]
"UseWUServer"=dword:00000001
```

Из журналов Обновл. Windows:

Выходные данные

```
2018-08-06 09:33:31:085  480 1118 Agent ** START **  Agent: Finding updates
[CallerId = OperationalInsight  Id = 49]
2018-08-06 09:33:31:085  480 1118 Agent *********
2018-08-06 09:33:31:085  480 1118 Agent   * Include potentially superseded updates
2018-08-06 09:33:31:085  480 1118 Agent   * Online = No; Ignore download priority
= No
2018-08-06 09:33:31:085  480 1118 Agent   * Criteria = "IsHidden = 0 AND
DeploymentAction=*"
2018-08-06 09:33:31:085  480 1118 Agent   * ServiceID = {00000000-0000-0000-0000-
000000000000} Third party service
2018-08-06 09:33:31:085  480 1118 Agent   * Search Scope = {Machine}
2018-08-06 09:33:32:554  480 1118 Agent   * Found 83 updates and 83 categories in
search; evaluated appl. rules of 517 out of 1473 deployed entities
2018-08-06 09:33:32:554  480 1118 Agent *********
2018-08-06 09:33:32:554  480 1118 Agent **  END  **  Agent: Finding updates
[CallerId = OperationalInsight  Id = 49]
```

В приведенном выше фрагменте журнала мы видим, что `Criteria = "IsHidden = 0 AND DeploymentAction=*"`. "*" означает, что на сервере ничего не указано. Таким образом, проверка происходит, но нет направления для скачивания или установки в агент. Поэтому он просто сканирует обновление и предоставляет результаты.

Как показано в следующих журналах, автоматическое обновление выполняет проверку и не находит утвержденных обновлений. Поэтому он сообщает о отсутствии обновлений для установки или скачивания. Это связано с неправильной конфигурацией. Сторона WSUS должна утвердить обновления для Обновл. Windows, чтобы получить обновления и установить их в указанное время в соответствии с политикой. Так как этот сценарий не включает Configuration Manager, невозможно установить неутвержденные обновления. Вы ожидаете, что агент операционной аналитики выполнит проверку и автоматически активирует загрузку и установку, но это не произойдет с этой конфигурацией.

Выходные данные

```
2018-08-06 10:58:45:992  480 5d8 Agent ** START **  Agent: Finding updates
[CallerId = AutomaticUpdates  Id = 57]
2018-08-06 10:58:45:992  480 5d8 Agent *********
2018-08-06 10:58:45:992  480 5d8 Agent   * Online = Yes; Ignore download priority
= No
2018-08-06 10:58:45:992  480 5d8 Agent   * Criteria = "IsInstalled=0 and
DeploymentAction='Installation' or IsPresent=1 and
DeploymentAction='Uninstallation' or IsInstalled=1 and
DeploymentAction='Installation' and RebootRequired=1 or IsInstalled=0 and
DeploymentAction='Uninstallation' and RebootRequired=1"

2018-08-06 10:58:46:617  480 5d8 PT   + SyncUpdates round trips: 2
```

```
2018-08-06 10:58:47:383  480 5d8 Agent   * Found 0 updates and 83 categories in
search; evaluated appl. rules of 617 out of 1473 deployed entities
2018-08-06 10:58:47:383  480 5d8 Agent Reporting status event with 0 installable,
83 installed,  0 installed pending, 0 failed and 0 downloaded updates
2018-08-06 10:58:47:383  480 5d8 Agent *********
2018-08-06 10:58:47:383  480 5d8 Agent **  END  **  Agent: Finding updates
[CallerId = AutomaticUpdates  Id = 57]
```

Использование высокой пропускной способности в клиенте Windows по Обновл. Windows

Пользователи могут видеть, что Windows потребляет всю пропускную способность в разных офисах в системном контексте. Такое поведение предусмотрено программой. Компоненты, которые могут использовать пропускную способность, расширяются за пределами Обновл. Windows компонентов.

Следующие групповые политики помогут устранить эту ситуацию:

- Блокирование доступа к серверам Центра обновления Windows: Политика: Отключение доступа ко всем функциям Центра обновления Windows (установлено как включено)
- Поиск драйверов: Укажите порядок поиска для источников драйверов устройства (установить на "Не искать в центре обновления Windows")
- Автоматическое обновление Магазина Windows: политика отключает автоматическую загрузку и установку обновлений (установлено для включения)

Другие компоненты, подключающиеся к Интернету:

- Windows Spotlight: Политика настройки Windows Spotlight на экране блокировки (отключено)
- Пользовательский опыт: Политика отключения пользовательских функций Microsoft (задано значение "Включить")
- Фоновый трафик из приложений Windows: политика позволяет приложениям Windows работать в фоновом режиме

Временные ошибки, вызванные тяжелой нагрузкой или перегрузкой сети

Пользователи могут получать следующие ошибки из Обновл. Windows. Эти ошибки являются временными ошибками, возникающими при временной нагрузке службы или

при перебое сетей. Пользователям не нужно предпринимать никаких действий, так как устройство повторит операцию позже.

Развернуть таблицу

Код ошибки	Значение ошибки	Сведения
Поиск распределения нагрузки (WU_S_SEARCH_LOAD_SHEDDING)	0x248001	Операция поиска завершилась успешно, но одна или несколько служб сбрасывали нагрузку.
WU_E_PT_LOAD_SHEDDING	0x8024402d	Сервер сбрасывает нагрузку.

В таких случаях пользователи, которые программно вызываются в API агента центра обновления Windows, чтобы извлечь результат операции поиска, получат orcFailed или orcSucceededWithErrors. Повторная попытка операции позже ожидается успешной.

Сбор данных

Если вам нужна помощь от поддержки Майкрософт, мы рекомендуем собирать сведения, выполнив действия, описанные в статье "Сбор сведений" с помощью TSS для проблем, связанных с развертыванием.

Распространенные ошибки Центра обновления Windows и их устранение

15.01.2025Применяется к: Supported versions of Windows Client

Попробуйте наш виртуальный агент. Это поможет быстро определить и устранить распространенные проблемы Обновл. Windows

В следующей таблице приведены сведения о распространенных ошибках, с которыми вы можете столкнуться с Обновл. Windows, и дает инструкции, которые помогут устранить их.

Область применения: Windows 10, Windows 11

0x8024402F

Развернуть таблицу

Message	Description	Меры по снижению риска
WU_E_PT_ECP_SUCCEEDED_WITH_ERRORS	Обработка внешних .cab файлов завершена с некоторыми ошибками	Эта ошибка может возникать из-за программы веб-фильтрации с помощью Lightspeed Rocket. Добавьте IP-адреса устройств, которые необходимо обновить в списке исключений Lightspeed Rocket.

0x80242006

Развернуть таблицу

Message	Description	Меры по снижению риска

WU_E_UH_INVALIDMETADATA	Не удалось завершить операцию обработчика, так как обновление содержит недопустимые метаданные.	Переименуйте папку распространения программного обеспечения и повторите попытку скачать обновления: Переименуйте следующие папки в *. BAK: *-%systemroot%\system32\catroot2*
		
		Введите следующие команды в командной строке. Нажмите клавишу ВВОД после ввода каждой команды.
		`Ren %systemroot%\SoftwareDistribution\DataStore DataStore.bak`
		`Ren %systemroot%\SoftwareDistribution\Download Download.bak`
		`Ren %systemroot%\system32\catroot2 catroot2.bak`

0x80070BC9

Развернуть таблицу

Message	Description	Меры по снижению риска
ERROR_FAIL_REBOOT_REQUIRED	Запрошенная операция завершилась ошибкой. Перезапустите систему для отката внесенных изменений.	Убедитесь, что у вас нет политик, которые управляют поведением запуска службы установщика Windows. Эта служба должна управляться операционной системой. Тип запуска по умолчанию **службы установщика Windows — вручную.**

0x80200053

Развернуть таблицу

Message	Description	Меры по снижению риска
BG_E_VALIDATION_FAILED	Неприменимо	Убедитесь, что брандмауэры не загружаются. Такая фильтрация может привести к неправильным ответам, полученным клиентом Обновл. Windows.

0x80072EFD или 0x80072EFE или 0x80D02002

Развернуть таблицу

Message	Description	Меры по снижению риска
TIME_OUT_ERRORS	Время ожидания операции	Убедитесь, что нет правил брандмауэра или прокси-серверов, которые блокируют URL-адреса загрузки Майкрософт. Выполните трассировку сетевого монитора, чтобы лучше понять. <См. сценарий устранения неполадок брандмауэра>

0X8007000D

Развернуть таблицу

Message	Description	Меры по снижению риска
ERROR_INVALID_DATA	Указывает, что данные, которые не были загружены или повреждены.	Попытайтесь перезагрузить обновление и запустить установку.

0x8024A10A

Развернуть таблицу

Message	Description	Меры по снижению риска
USO_E_SERVICE_SHUTTING_DOWN	Указывает, что служба Обновл. Windows завершает работу.	Эта ошибка может возникать после длительного периода бездействия. Система не отвечает, что приводит к простою службы и приводит к закрытию службы. Убедитесь, что система остается активной и подключения остаются установленными для завершения установки.

0x80240020

Развернуть таблицу

Message	Description	Меры по снижению риска
WU_E_NO_INTERACTIVE_USER	Операция не завершена, так как интерактивный пользователь не вошел в систему.	Войдите на устройство, чтобы запустить установку и разрешить устройству перезапуститься.

0x80242014

Развернуть таблицу

Message	Description	Меры по снижению риска
WU_E_UH_POSTREBOOTSTILLPENDING	Операция после перезапуска обновления по-прежнему	Для некоторых обновлений Windows требуется перезапустить устройство. Перезапустите устройство, чтобы

Message	Description	Меры по снижению риска
	выполняется.	завершить установку обновления.

0x80246017

Развернуть таблицу

Message	Description	Меры по снижению риска
WU_E_DM_UNAUTHORIZED_LOCAL_USER	Сбой загрузки, так как локальный пользователь был отказано в авторизации для скачивания содержимого.	Убедитесь, что пользователь пытается скачать и установить обновления с достаточными привилегиями для установки обновлений (локальный администратор).

0x8024000B

Развернуть таблицу

Message	Description	Меры по снижению риска
WU_E_CALL_CANCELLED	Операция была отменена.	Операция была отменена пользователем или службой. Вы также можете получить эту ошибку, если не удается отфильтровать результаты.

0x8024000E

Развернуть таблицу

Message	Description	Меры по снижению риска
WU_E_XML_INVALID	Обновл. Windows агент нашел сведения в xml-данных обновления, которые недопустимы.	Некоторые драйверы содержат дополнительные сведения о метаданных в Update.xml, которые Orchestrator может интерпретировать как недопустимые данные. Убедитесь, что на устройстве установлен последний агент Обновл. Windows.

0x8024D009

Развернуть таблицу

Message	Description	Меры по снижению риска
WU_E_SETUP_SKIP_UPDATE	Обновление агента Обновл. Windows было пропущено из-за директивы в файле Wuident.cab.	Эта ошибка может возникнуть, если СЛУЖБЫ WSUS не отправляют самостоятельное обновление клиентам. Дополнительные сведения об устранении проблемы см . в KB920659.

0x80244007

Развернуть таблицу

Message	Description	Меры по снижению риска
WU_E_PT_SOAPCLIENT_SOAPFAULT	Сбой клиента SOAP из-за ошибки SOAP из-за причин `WU_E_PT_SOAP_*`	Эта проблема возникает, так как Windows не может продлить файлы cookie для Обновл. Windows.

Message	Description	Меры по снижению риска
	ошибок.	Дополнительные сведения об устранении проблемы см. в статье об ошибке 0x80244007 при попытке Windows проверить наличие обновлений на сервере WSUS.

0x80070422

Развернуть таблицу

Message	Description	Меры по снижению риска
ERROR_SERVICE_DISABLED	Эта проблема возникает, когда служба Обновл. Windows перестает работать или не работает.	Проверьте, запущена ли служба Обновл. Windows.

0x800f0821

Развернуть таблицу

Message	Description	Меры по снижению риска
CBS_E_ABORT; прерывание клиента, IDABORT, возвращаемое методом ICbsUIHandler, кроме Error()	Превышено время ожидания транзакции CBS.	Операция обслуживания занимает много времени. Срок действия таймера отслеживания стека обслуживания истекает. Расширение времени ожидания приведет к устранению проблемы. Увеличьте ресурсы на устройстве. Если виртуальная машина, увеличьте виртуальный ЦП и память для ускорения операций. Убедитесь, что устройство установило обновление в KB4493473 или более поздней версии.

0x800f0825

Развернуть таблицу

Message	Description	Меры по снижению риска

CBS_E_CANNOT_UNINSTALL; Невозможно удалить пакет.	Обычно эта ошибка возникает из-за повреждения хранилища компонентов, вызванного при частично установленном состоянии компонента.	Восстановите хранилище компонентов с помощью `Dism RestoreHealth` команды или вручную восстановите полезные данные из частично установленного компонента. В командной строке с повышенными привилегиями выполните следующие команды.
		`Dism.exe /Online /Cleanup-Image /Restorehealth`
		`Sfc.exe /Scannow`
		Перезапустите устройство.

0x800F0920

Развернуть таблицу

Message	Description	Меры по снижению риска
CBS_E_HANG_DETECTED; При обработке операции обнаружена ошибка реагирования.	После получения 0x800f0821 после получения 0x800f0821 произошла следующая ошибка.	Операция обслуживания занимает много времени. Срок действия таймера отслеживания стека обслуживания истекает и предполагает, что система перестала отвечать. Расширение времени ожидания приведет к устранению проблемы. Увеличьте ресурсы на устройстве. Если виртуальная машина, увеличьте виртуальный ЦП и память для ускорения операций. Убедитесь, что устройство установило обновление в KB4493473 или более поздней версии.

0x800f081f

Развернуть таблицу

Message	Description	Меры по снижению риска

CBS_E_SOURCE_MISSING; источник для пакета или файла не найден, ResolveSource() неудачно	Повреждение хранилища компонентов	Восстановите хранилище компонентов с помощью `Dism RestoreHealth` команды или вручную восстановите полезные данные из частично установленного компонента. В командной строке с повышенными привилегиями выполните следующие команды:
		`Dism.exe /Online /Cleanup-Image /Restorehealth`
		`Sfc.exe /Scannow`
		Перезапустите устройство.

0x800f0831

Развернуть таблицу

Message	Description	Меры по снижению риска

CBS_E_STORE_CORRUPTION; Хранилище CBS повреждено.	Повреждение в магазине компонентов Windows.	Восстановите хранилище компонентов с `Dism RestoreHealth` помощью или вручную восстановите полезные данные из частично установленного компонента. В командной строке с повышенными привилегиями выполните следующие команды:
		`Dism.exe /Online /Cleanup-Image /Restorehealth`
		`Sfc.exe /Scannow`
		Перезапустите устройство.

0x80070005

Развернуть таблицу

Message	Description	Меры по снижению риска
E_ACCESSDENIED; Общая ошибка отказа в доступе	Изменены разрешения файловой системы или раздела реестра, а стек обслуживания не имеет требуемого уровня доступа.	Эта ошибка обычно означает, что доступ был отклонен. Перейдите в папку *%Windir%\logs\CBS*, откройте последнюю *CBS.log* и выполните поиск `, error` и совпадение с меткой времени. Найдя ошибку, прокрутите страницу вверх и попробуйте определить, что привело к отказу в доступе. Возможно, не удалось получить доступ к файлу или разделу реестра. Определите, какой объект нуждается в правильных разрешениях и меняйте их по мере необходимости.

0x80070570

Развернуть таблицу

Message	Description	Меры по снижению риска

ERROR_FILE_CORRUPT; Файл или каталог поврежден и нечитаем.	Повреждение хранилища компонентов	Восстановите хранилище компонентов с `Dism RestoreHealth` помощью или вручную восстановите полезные данные из частично установленного компонента. В командной строке с повышенными привилегиями выполните следующие команды:
		`Dism.exe /Online /Cleanup-Image /Restorehealth`
		`Sfc.exe /Scannow`
		Перезапустите устройство.

0x80070003

Развернуть таблицу

Message	Description	Меры по снижению риска
ERROR_PATH_NOT_FOUND; Система не может найти указанный путь.	Стек обслуживания не может получить доступ к определенному пути.	Указывает недопустимый путь к исполняемому файлу. Перейдите в папку *%Windir%\logs\CBS*, откройте последнюю *CBS.log* и выполните поиск `, error`. Затем сопоставляйте результаты с меткой времени.

0x80070020

Развернуть таблицу

Message	Description	Меры по снижению риска
ERROR_SHARING_VIOLATION	Многочисленные причины. Требуется анализ журналов CBS.	Эта ошибка возникает из-за драйверов фильтров, отличных от Майкрософт, таких как антивирусная программа. 1. Выполнение чистой загрузки и повторная попытка установки 2. Скачайте монитор процессов sysinternal. 3. Запустите *Procmon.exe*. Он автоматически запустит сбор данных. 4. Снова установите пакет обновления 5. В главном окне монитора процессов в фокусе нажмите клавиши CTRL+E или выберите стекло с увеличением, чтобы остановить захват данных. 6. Выберите **>команду "Сохранить>все события>PML"** и выберите путь для сохранения `.PML` файла. 7. Перейдите в папку *%windir%\logs\cbs*, откройте последний *файл Cbs.log* и выполните поиск ошибки. После поиска строки ошибки немного выше у вас должен быть доступ к файлу во время установки, которая дает ошибку нарушения общего доступа 8. В мониторе процессов отфильтруйте путь и вставьте имя файла (оно должно быть примерно так же, как "path" содержит "имя файла из CBS"). 9. Попробуйте остановить его или удалить процесс, вызывающий ошибку.

0x80073701

Развернуть таблицу

Message	Description	Меры по снижению риска

ERROR_SXS_ASSEMBLY_MISSING; Не удалось найти указанную сборку.	Как правило, повреждение хранилища компонентов возникает, когда компонент находится в частично установленном состоянии.	Восстановите хранилище компонентов с `Dism RestoreHealth command` помощью или вручную восстановите полезные данные из частично установленного компонента. В командной строке с повышенными привилегиями выполните следующие команды.
		`Dism.exe /Online /Cleanup-Image /Restorehealth`
		`Sfc.exe /Scannow`
		Перезапустите устройство.

0x8007371b

Развернуть таблицу

Message	Description	Меры по снижению риска

ERROR_SXS_TRANSACTION_CLOSURE_INCOMPLETE; Один или несколько обязательных элементов транзакции отсутствуют.	Повреждение хранилища компонентов.	Восстановите хранилище компонентов с помощью `Dism RestoreHealth` команды или вручную восстановите полезные данные из частично установленного компонента. В командной строке с повышенными привилегиями выполните следующие команды:
		`Dism.exe /Online /Cleanup-Image /Restorehealth`
		`Sfc.exe /Scannow`
		Перезапустите устройство.

0x80072EFE

Развернуть таблицу

Message	Description	Меры по снижению риска
WININET_E_CONNECTION_ABORTED; Подключение к серверу было закрыто ненормально	BITS не может успешно передать файл.	Обнаружена ошибка BITS или если передаваемый файл не может быть записан в целевую папку на клиенте. Эта ошибка вызвана ошибками подключения при проверке или скачивании обновлений. В командной строке выполните следующую команду: `BITSADMIN /LIST /ALLUSERS /VERBOSE` Найдите код ошибки 0x80072EFE. Вы увидите ссылку на HTTP-код с определенным файлом. С помощью браузера попробуйте скачать его вручную, убедившись, что вы используете параметры прокси-сервера вашей организации. Если скачивание завершается ошибкой, обратитесь к диспетчеру прокси-сервера, чтобы разрешить обмен данными. Кроме того, обратитесь к группе по сети для доступа к этому конкретному URL-адресу.

0x80072F8F

Развернуть таблицу

Message	Description	Меры по снижению риска
WININET_E_DECODING_FAILED; Сбой декодирования содержимого	ПРОТОКОЛ TLS 1.2 настроен неправильно на клиенте.	Эта ошибка обычно означает, что агент Обновл. Windows не смог декодировать полученное содержимое. Установите и настройте TLS 1.2, установив обновление в KB3140245.

0x80072EE2

Развернуть таблицу

Message	Description	Меры по снижению риска

WININET_E_TIMEOUT; Время ожидания операции	Не удалось проверить наличие обновлений из-за проблемы с подключением к Обновл. Windows, Configuration Manager или WSUS.	Эта ошибка обычно означает, что агент Обновл. Windows не удалось подключиться к серверам обновления или собственному источнику, например WSUS, Configuration Manager или Microsoft Intune. Обратитесь к группе сети, чтобы убедиться, что устройство может получить доступ к источникам обновлений. Дополнительные сведения см. в разделе "Устранение неполадок с проверкой обновлений программного обеспечения" в Configuration Manager.
		Если вы используете общедоступные серверы обновления Майкрософт, убедитесь, что устройство может получить доступ к следующим конечным точкам Обновл. Windows:
		`http://windowsupdate.microsoft.com`
		`https://*.windowsupdate.microsoft.com`

Message	Description	Меры по снижению риска

		`https://update.microsoft.com`
		`https://*.update.microsoft.com`
		`https://windowsupdate.com`
		`https://*.windowsupdate.com`
		`https://download.windowsupdate.com`
		`https://*.download.windowsupdate.com`
		`https://download.microsoft.com`
		`https://*.download.windowsupdate.com`
		`https://wustat.windows.com`
		`https://*.wustat.windows.com`
		`https://ntservicepack.microsoft.com`

0x80240022

Развернуть таблицу

Message	Description	Меры по снижению риска
WU_E_ALL_UPDATES_FAILED; Сбой операции для всех обновлений.	Несколько первопричин этой ошибки.	Наиболее распространенная проблема заключается в том, что антивирусное программное обеспечение блокирует доступ к определенным папкам (например, SoftwareDistribution). CBS.log анализ, необходимый для определения защищенного файла или папки.

0x8024401B

Развернуть таблицу

Message	Description	Меры по снижению риска
WU_E_PT_HTTP_STATUS_PROXY_AUTH_REQ; Аналогично состоянию HTTP 407 — требуется проверка подлинности прокси-сервера.	Не удается пройти проверку подлинности через прокси-сервер.	Параметры прокси-сервера Winhttp или WinInet не настроены правильно. Эта ошибка обычно означает, что агент Обновл. Windows не удалось подключиться к серверам обновления или собственному источнику обновления, таким как WSUS, Configuration Manager или Microsoft Intune, из-за ошибки прокси-сервера. Проверьте параметры прокси-сервера на клиенте. Агент Обновл. Windows использует WinHTTP для проверки доступных обновлений. При наличии прокси-сервера между клиентом и источником обновления параметры прокси-сервера необходимо правильно настроить на клиентах, чтобы разрешить им взаимодействовать с помощью полного доменного имени источника. Обратитесь к группам сети и прокси-сервера, чтобы убедиться, что устройство может использовать источник обновления без прокси-сервера, требующего проверки подлинности пользователя.

0x80244022

Развернуть таблицу

Message	Description	Меры по снижению риска
WU_E_PT_HTTP_STATUS_SERVICE_UNAVAILABLE; Аналогично состоянию HTTP 503 — служба временно перегружена.	Не удается подключиться к настроенной	Устранение неполадок сети, необходимых для устранения проблемы с подключением. Обратитесь к группам сети и прокси-сервера, чтобы убедиться, что устройство может использовать источник обновления

Message	Description	Меры по снижению риска
	источнику обновления.	без прокси-сервера, требующего проверки подлинности пользователя.

0x80070490

Развернуть таблицу

Message	Description	Меры по снижению риска
ERROR_NOT_FOUND	Эта ошибка возникает во время установки драйвера в процессе обновления.	Эта проблема возникает, так как в реестре отсутствуют такие сведения, как архитектура для обновляемого драйвера. Вручную добавьте отсутствующее значение inf-файла **Arch** в реестр операций драйверов, выполнив следующие действия. 1. Откройте *regedit* и перейдите к `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\ComponentBasedServicing\DriverOperations\0\2(SequenceID)` 2. Проверьте **значение удостоверения** , чтобы определить отсутствующее значение. 3. Вручную добавьте отсутствующее значение, ссылающееся на сведения в значении **Identity** . Например, Name: Arch; Тип: REG_SZ (строковое значение); Данные: amd64. 4. Продолжайте установку сбоя обновления.

0x800f0922

Развернуть таблицу

Message	Description	Меры по снижению риска
CBS_E_INSTALLERS_FAILED	Не удалось установить накопительное обновление июля в Windows Server 2016	В CBS.log может оказаться, что обновления иногда откатываются, когда маркеры ключа лицензии и продукта не обновляются. Эту проблему можно устранить, добавив разрешения на запись для учетных записей "Пользователь" и "Сетевая служба" в папку *C:\Windows\System32\spp* .

0x80070bc9

Развернуть таблицу

Message	Description	Меры по снижению риска
ERROR_FAIL_REBOOT_REQUIRED	Для типа запуска службы TrustedInstaller задано значение "Вручную" по групповой политике (GPO), что не позволило начать выполнение ожидающих операций.	Служба TrustedInstaller изменяет тип запуска вручную на "Автоматически" при обнаружении обновления, которое необходимо обработать транзакцию после перезапуска. Если значение возвращается вручную перед перезапуском, транзакция не может быть применена. Эта транзакция будет отложена и блокирует все остальные установки обновлений. Чтобы устранить эту проблему, измените политику TrustedInstaller на **автоматическую** и перезагрузите компьютер. Если он не работает, запустите компьютер в WinRE, чтобы вернуть ожидающие действия. Например, `dism /Image:C:\ /Cleanup-Image /RevertPendingActions`. Если она не работает, запустите компьютер в WinRE, переименуйте *\WinSxS\Pending.xml* и удалите ожидающий файл PendingXMLIdentifier из COMPONENTS Hive.

0x800706be

Развернуть таблицу

Message	Description	Меры по снижению риска
Не удалось установить накопительные обновления	Windows Server 2016 Std не удалось установить накопительные пакеты с помощью пакета MSU. Ошибка не возвращается. При установке пакетов с dism.exe он вернул ошибку 0x800706be.	Последнее накопительное обновление не удалось установить и повреждено. Чтобы устранить эту проблему, перейдите к разделу реестра для поврежденного пакета обновления. Измените значение "текущее состояние" на 000020 шестнадцатеричных (32 декабря) - разрешено или 000040 шестнадцатерик (64 декабря) - поэтапно или 000070 шестнадцатеричных (112 дек) - установлено.

Сбор данных

Если вам нужна помощь службы поддержки Microsoft, мы рекомендуем собирать информацию путем выполнения действий, описанных в разделе Сбор информации с помощью TSS для решения проблем, связанных с развертыванием.

Коды ошибок Центра обновления Windows с разбивкой по компонентам

Статья • 03.09.2023 • Применяется к: ✅ Windows 11, ✅ Windows 10

В этом разделе приведены коды ошибок для Центра обновления Windows (Майкрософт).

Ошибки автоматического обновления

Код ошибки	Сообщение	Описание
`0x80243FFF`	`WU_E_AUCLIENT_UNEXPECTED`	Произошла ошибка пользовательского интерфейса, которой не соответствует ни один код `WU_E_AUCLIENT_*`.
`0x8024A000`	`WU_E_AU_NOSERVICE`	Службе автоматического обновления не удалось обработать входящие запросы.
`0x8024A002`	`WU_E_AU_NONLEGACYSERVER`	Старая версия клиента автоматического обновления прекратила работу из-за обновления сервера WSUS.
`0x8024A003`	`WU_E_AU_LEGACYCLIENTDISABLED`	Старая версия клиента автоматического обновления была отключена.
`0x8024A004`	`WU_E_AU_PAUSED`	Службе автоматического обновления не удалось обработать входящие запросы, поскольку она была приостановлена.
`0x8024A005`	`WU_E_AU_NO_REGISTERED_SERVICE`	В `AU` не зарегистрированы неуправляемые службы.
`0x8024AFFF`	`WU_E_AU_UNEXPECTED`	Ошибке автоматического обновления не соответствует ни один код `WU_E_AU*`.

Ошибки пользовательского интерфейса Центра обновления Windows

Код ошибки	Сообщение	Описание
`0x80243001`	`WU_E_INSTALLATION_RESULTS_UNKNOWN_VERSION`	Результаты скачивания и установки не удалось прочитать из реестра из-за нераспознанной версии формата данных.
`0x80243002`	`WU_E_INSTALLATION_RESULTS_INVALID_DATA`	Не удалось прочитать результаты скачивания и установки из реестра из-за недопустимого формата данных.
`0x80243003`	`WU_E_INSTALLATION_RESULTS_NOT_FOUND`	Результаты скачивания и установки недоступны. Возможно, не удалось запустить операцию.
`0x80243004`	`WU_E_TRAYICON_FAILURE`	Произошла ошибка при попытке создания значка в области уведомлений панели задач.
`0x80243FFD`	`WU_E_NON_UI_MODE`	Не удается отобразить пользовательский интерфейс в режиме, отличном от режима пользовательского интерфейса; модули пользовательского интерфейса клиента Центра обновления Windows могут быть не установлены.
`0x80243FFE`	`WU_E_WUCLTUI_UNSUPPORTED_VERSION`	Неподдерживаемая версия экспортированных функций пользовательского интерфейса клиента Центра обновления Windows.
`0x80243FFF`	`WU_E_AUCLIENT_UNEXPECTED`	Произошла ошибка пользовательского интерфейса, которой не соответствует ни один код `WU_E_AUCLIENT_*`.
`0x8024043D`	`WU_E_SERVICEPROP_NOTAVAIL`	Запрошенное свойство службы недоступно.

Ошибки инвентаризации

Код ошибки	Сообщение	Описание
0x80249001	WU_E_INVENTORY_PARSEFAILED	Ошибка синтаксического анализа файла правил.
0x80249002	WU_E_INVENTORY_GET_INVENTORY_TYPE_FAILED	Не удалось получить запрошенный тип инвентаризации от сервера.
0x80249003	WU_E_INVENTORY_RESULT_UPLOAD_FAILED	Не удалось отправить результат инвентаризации на сервер.
0x80249004	WU_E_INVENTORY_UNEXPECTED	Произошла ошибка инвентаризации, которой не соответствует ни один код.
0x80249005	WU_E_INVENTORY_WMI_ERROR	Произошла ошибка инструментария WMI при перечислении экземпляров для определенного класса.

Ошибки обработчика выражений

Код ошибки	Сообщение	Описание
0x8024E001	WU_E_EE_UNKNOWN_EXPRESSION	Не удалось выполнить операцию вычислителя выражений, так как выражение было нераспознано.
0x8024E002	WU_E_EE_INVALID_EXPRESSION	Не удалось завершить операцию вычислителя выражений, так как выражение было недопустимым.
0x8024E003	WU_E_EE_MISSING_METADATA	Не удалось выполнить операцию вычислителя выражений, так как выражение содержит неверное количество узлов метаданных.
0x8024E004	WU_E_EE_INVALID_VERSION	Не удалось выполнить операцию вычислителя выражений, так как версия сериализованных данных выражения недопустима.
0x8024E005	WU_E_EE_NOT_INITIALIZED	Не удалось инициализировать средство оценки выражений.
0x8024E006	WU_E_EE_INVALID_ATTRIBUTEDATA	Не удалось завершить операцию вычислителя выражений из-за недопустимого атрибута.

Код ошибки	Сообщение	Описание
0x8024E007	WU_E_EE_CLUSTER_ERROR	Не удалось выполнить операцию вычислителя выражений, так как не удалось определить состояние кластера компьютера.
0x8024EFFF	WU_E_EE_UNEXPECTED	Произошла ошибка обработчика выражений, которой не соответствует ни один код ошибки WU_E_EE_*.

Ошибки создателя отчетов

Код ошибки	Сообщение	Описание
0x80247001	WU_E_OL_INVALID_SCANFILE	Не удалось завершить операцию, так как пакет проверки был недопустимым.
0x80247002	WU_E_OL_NEWCLIENT_REQUIRED	Не удалось выполнить операцию, так как пакет проверки требует более поздней версии агента клиентский компонент Центра обновления Windows.
0x80247FFF	WU_E_OL_UNEXPECTED	Не удалось выполнить поиск с помощью пакета поиска.
0x8024F001	WU_E_REPORTER_EVENTCACHECORRUPT	Файл кэша событий поврежден.
0x8024F002	WU_E_REPORTER_EVENTNAMESPACEPARSEFAILED	Не удалось проанализировать XML-код в дескрипторе пространства имен событий.
0x8024F003	WU_E_INVALID_EVENT	Не удалось проанализировать XML-код в дескрипторе пространства имен событий.
0x8024F004	WU_E_SERVER_BUSY	Сервер отклонил событие, поскольку был занят.
0x8024FFFF	WU_E_REPORTER_UNEXPECTED	Произошла ошибка создателя отчетов, которой не соответствует ни один код.

Ошибки перенаправителя

Компоненты, которые загружают файл `Wuredir.cab`, а затем анализируют файл `Wuredir.cab`, инициируют следующие ошибки.

Код ошибки	Сообщение	Описание
`0x80245001`	`WU_E_REDIRECTOR_LOAD_XML`	Не удалось загрузить XML-документ перенаправления в класс DOM.
`0x80245002`	`WU_E_REDIRECTOR_S_FALSE`	В XML-документе перенаправителя отсутствуют некоторые необходимые сведения.
`0x80245003`	`WU_E_REDIRECTOR_ID_SMALLER`	Идентификатор redirectorId в загруженном CAB-файле перенаправителя имеет меньшее значение, чем в CAB-файле, находящемся в кэше.
`0x80245FFF`	`WU_E_REDIRECTOR_UNEXPECTED`	Сбой перенаправителя с ошибкой, которой не соответствует ни один код `WU_E_REDIRECTOR_*`.

Ошибки передатчика протокола

Следующие ошибки сопоставляются с `SOAPCLIENT_ERROR` через файл `Atlsoap.h`. Эти ошибки возникают, когда объект `CClientWebService` вызывает метод `GetClientError()`.

Код ошибки	Сообщение	Описание
`0x80244000`	`WU_E_PT_SOAPCLIENT_BASE`	`WU_E_PT_SOAPCLIENT_*` Коды ошибок сопоставляют `SOAPCLIENT_ERROR` с перечислением библиотеки сервера ATL.
`0x80244001`	`WU_E_PT_SOAPCLIENT_INITIALIZE`	То же, что и `SOAPCLIENT_INITIALIZE_ERROR` — сбой инициализации клиента `SOAP`. Возможно, из-за ошибки установки MSXML.
`0x80244002`	`WU_E_PT_SOAPCLIENT_OUTOFMEMORY`	То же, что и `SOAPCLIENT_OUTOFMEMORY` - `SOAP`. Сбой клиента из-за нехватки памяти.
`0x80244003`	`WU_E_PT_SOAPCLIENT_GENERATE`	То же, что и `SOAPCLIENT_GENERATE_ERROR` - `SOAP`. Клиенту не удалось создать запрос.
`0x80244004`	`WU_E_PT_SOAPCLIENT_CONNECT`	То же, что и `SOAPCLIENT_CONNECT_ERROR` - `SOAP`. Клиенту не удалось подключиться к серверу.
`0x80244005`	`WU_E_PT_SOAPCLIENT_SEND`	То же, что и `SOAPCLIENT_SEND_ERROR` - `SOAP`. Клиенту не удалось отправить сообщение из-

Код ошибки	Сообщение	Описание
		за кодов ошибок `WU_E_WINHTTP_*`.
`0x80244006`	`WU_E_PT_SOAPCLIENT_SERVER`	То же, что и `SOAPCLIENT_SERVER_ERROR` - `SOAP`. Сбой клиента из-за ошибки сервера.
`0x80244007`	`WU_E_PT_SOAPCLIENT_SOAPFAULT`	То же, что и `SOAPCLIENT_SOAPFAULT` - `SOAP`. Сбой клиента из-за ошибки SOAP, причиной которой были коды ошибок `WU_E_PT_SOAP_*`.
`0x80244008`	`WU_E_PT_SOAPCLIENT_PARSEFAULT`	То же, что и `SOAPCLIENT_PARSEFAULT_ERROR` - `SOAP`. Клиенту не удалось проанализировать ошибку `SOAP`.
`0x80244009`	`WU_E_PT_SOAPCLIENT_READ`	То же, что и `SOAPCLIENT_READ_ERROR` - `SOAP`. Сбой клиента при чтении ответа с сервера.
`x8024400A`	`WU_E_PT_SOAPCLIENT_PARSE`	То же, что и `SOAPCLIENT_PARSE_ERROR` - `SOAP`. Клиенту не удалось проанализировать ответ с сервера.

Другие ошибки передатчика протокола

Следующие ошибки сопоставляются с `SOAP_ERROR_CODE` из файла `Atlsoap.h`. Источником этих ошибок является участник `m_fault.m_soapErrCode` объекта `CClientWebService`, когда `GetClientError()` возвращает `SOAPCLIENT_SOAPFAULT`.

Код ошибки	Сообщение	Описание
`0x8024400B`	`WU_E_PT_SOAP_VERSION`	То же, что и `SOAP_E_VERSION_MISMATCH` - `SOAP`. Клиент обнаружил неопознанное пространство имен для конверта `SOAP`.
`0x8024400C`	`WU_E_PT_SOAP_MUST_UNDERSTAND`	То же, что и `SOAP_E_MUST_UNDERSTAND` - `SOAP`. Клиенту не удалось распознать заголовок.
`0x8024400D`	`WU_E_PT_SOAP_CLIENT`	То же, что и `SOAP_E_CLIENT` - `SOAP`. Клиент обнаружили неверно сформированное сообщение. Устраните проблему перед повторной отправкой.
`0x8024400E`	`WU_E_PT_SOAP_SERVER`	То же самое: `SOAP_E_SERVER` сообщение `SOAP` не удалось обработать из-за

Код ошибки	Сообщение	Описание
		ошибки сервера; повторно отправьте позже.
0x8024400F	WU_E_PT_WMI_ERROR	Произошла неопределенная ошибка инструментария управления Windows (WMI).
0x80244010	WU_E_PT_EXCEEDED_MAX_SERVER_TRIPS	Превышено максимальное число циклов передачи на сервер.
0x80244011	WU_E_PT_SUS_SERVER_NOT_SET	В реестре отсутствует значение политики WUServer.
0x80244012	WU_E_PT_DOUBLE_INITIALIZATION	Не удалось выполнить инициализацию, так как объект уже инициализирован.
0x80244013	WU_E_PT_INVALID_COMPUTER_NAME	Не удалось определить имя компьютера.
0x80244015	WU_E_PT_REFRESH_CACHE_REQUIRED	Ответ от сервера указывает на то, что сервер изменился или файл cookie является недопустимым. Обновите состояние внутреннего кэша и повторите попытку.
0x80244016	WU_E_PT_HTTP_STATUS_BAD_REQUEST	Аналогично http status 400 — серверу не удалось обработать запрос из-за недопустимого синтаксиса.
0x80244017	WU_E_PT_HTTP_STATUS_DENIED	То же, что и код состояния HTTP 401 — запрошенный ресурс нуждается в аутентификации пользователя.
0x80244018	WU_E_PT_HTTP_STATUS_FORBIDDEN	То же, что и код состояния HTTP 403 — сервер понял запрос, однако отказался его выполнять.
0x80244019	WU_E_PT_HTTP_STATUS_NOT_FOUND	Аналогично http-состоянию 404— серверу не удается найти запрошенный URI (универсальный идентификатор ресурса).
0x8024401A	WU_E_PT_HTTP_STATUS_BAD_METHOD	Аналогично http status 405 — метод HTTP не разрешен.
0x8024401B	WU_E_PT_HTTP_STATUS_PROXY_AUTH_REQ	То же, что и код состояния HTTP 407 — требуется аутентификация прокси-сервера.

Код ошибки	Сообщение	Описание
`0x8024401C`	`WU_E_PT_HTTP_STATUS_REQUEST_TIMEOUT`	То же, что и код состояния HTTP 408 — истекло время ожидания запроса сервером.
`0x8024401D`	`WU_E_PT_HTTP_STATUS_CONFLICT`	Аналогично http-состоянию 409— запрос не был выполнен из-за конфликта с текущим состоянием ресурса.
`0x8024401E`	`WU_E_PT_HTTP_STATUS_GONE`	То же, что и код состояния HTTP 410 — запрошенный ресурс больше не доступен на сервере.
`0x8024401F`	`WU_E_PT_HTTP_STATUS_SERVER_ERROR`	То же, что и код состояния HTTP 500 — запрос не выполнен из-за внутренней ошибки сервера.
`0x80244020`	`WU_E_PT_HTTP_STATUS_NOT_SUPPORTED`	Аналогично http status 500 — сервер не поддерживает функции, необходимые для выполнения запроса.
`0x80244021`	`WU_E_PT_HTTP_STATUS_BAD_GATEWAY`	То же, что и код состояния HTTP 502 — сервер, выполняя роль шлюза или прокси-сервера, получил недопустимый ответ от вышестоящего сервера, к которому он обратился, пытаясь выполнить запрос.
`0x80244022`	`WU_E_PT_HTTP_STATUS_SERVICE_UNAVAIL`	То же, что и код состояния HTTP 503 — служба временно перегружена.
`0x80244023`	`WU_E_PT_HTTP_STATUS_GATEWAY_TIMEOUT`	То же, что и код состояния HTTP 503 — при выполнении запроса было превышено время ожидания шлюза.
`0x80244024`	`WU_E_PT_HTTP_STATUS_VERSION_NOT_SUP`	Аналогично http status 505 — сервер не поддерживает версию протокола HTTP, используемую для запроса.
`0x80244025`	`WU_E_PT_FILE_LOCATIONS_CHANGED`	Не удалось выполнить операцию из-за измененного расположения файла. Обновите внутреннее состояние и повторите отправку.
`0x80244026`	`WU_E_PT_REGISTRATION_NOT_SUPPORTED`	Сбой операции, так как агент клиентский компонент Центра обновления Windows не поддерживает

Код ошибки	Сообщение	Описание
		регистрацию на сервере, отличном от WSUS.
0x80244027	WU_E_PT_NO_AUTH_PLUGINS_REQUESTED	Сервер вернул пустой список сведений проверки подлинности.
0x80244028	WU_E_PT_NO_AUTH_COOKIES_CREATED	Агенту Центра обновления Windows не удалось создать допустимые файлы cookie проверки подлинности.
0x80244029	WU_E_PT_INVALID_CONFIG_PROP	Неправильное значение свойства конфигурации.
0x8024402A	WU_E_PT_CONFIG_PROP_MISSING	Отсутствует значение свойства конфигурации.
0x8024402B	WU_E_PT_HTTP_STATUS_NOT_MAPPED	Не удалось выполнить HTTP-запрос, и причина не соответствует ни одному из WU_E_PT_HTTP_* кодов ошибок.
0x8024402C	WU_E_PT_WINHTTP_NAME_NOT_RESOLVED	То же самое, что и ERROR_WINHTTP_NAME_NOT_RESOLVED — не удается разрешить имя прокси-сервера или целевого сервера.
0x8024402F	WU_E_PT_ECP_SUCCEEDED_WITH_ERRORS	Обработка внешнего CAB-файла была завершена с ошибками.
0x80244030	WU_E_PT_ECP_INIT_FAILED	Инициализация внешнего процессора cab не завершена.
0x80244031	WU_E_PT_ECP_INVALID_FILE_FORMAT	Недопустимый формат файла метаданных.
0x80244032	WU_E_PT_ECP_INVALID_METADATA	Обработчик внешних CAB-файлов обнаружил недопустимые метаданные.
0x80244033	WU_E_PT_ECP_FAILURE_TO_EXTRACT_DIGEST	Не удалось извлечь дайджест файла из внешнего CAB-файла.
0x80244034	WU_E_PT_ECP_FAILURE_TO_DECOMPRESS_CAB_FILE	Не удалось распаковать внешний CAB-файл.
0x80244035	WU_E_PT_ECP_FILE_LOCATION_ERROR	Обработчику внешних CAB-файлов удалось получить расположение файлов.
0x80244FFF	WU_E_PT_UNEXPECTED	Произошла ошибка связи, которой не соответствует ни один код ошибки

Код ошибки	Сообщение	Описание
		`WU_E_PT_*`.
`0x8024502D`	`WU_E_PT_SAME_REDIR_ID`	Агенту Центра обновления Windows не удалось загрузить CAB-файл перенаправителя с новым значением идентификатора redirectorId с сервера во время восстановления.
`0x8024502E`	`WU_E_PT_NO_MANAGED_RECOVER`	Действие восстановления перенаправления не завершено, так как сервер управляется.

Ошибки диспетчера загрузки

Код ошибки	Сообщение	Описание
`0x80246001`	`WU_E_DM_URLNOTAVAILABLE`	Не удалось выполнить операцию диспетчера загрузки, так как у запрошенного файла нет URL-адреса.
`0x80246002`	`WU_E_DM_INCORRECTFILEHASH`	Не удалось завершить операцию диспетчера загрузки, так как дайджест файлов не распознается.
`0x80246003`	`WU_E_DM_UNKNOWNALGORITHM`	Не удалось выполнить операцию диспетчера загрузки, так как метаданные файла запросили нераспознанный хэш-алгоритм.
`0x80246004`	`WU_E_DM_NEEDDOWNLOADREQUEST`	Не удалось выполнить операцию, так как требуется запрос на скачивание от обработчика загрузки.
`0x80246005`	`WU_E_DM_NONETWORK`	Не удалось выполнить операцию диспетчера загрузки, так как сетевое подключение было недоступно.
`0x80246006`	`WU_E_DM_WRONGBITSVERSION`	Не удалось выполнить операцию диспетчера загрузки, так как версия фоновой интеллектуальной службы передачи (BITS) несовместима.
`0x80246007`	`WU_E_DM_NOTDOWNLOADED`	Обновление не загружено.
`0x80246008`	`WU_E_DM_FAILTOCONNECTTOBITS`	Не удалось выполнить операцию диспетчера загрузки, поскольку диспетчеру

Код ошибки	Сообщение	Описание
		загрузки не удалось подключиться к фоновой интеллектуальной службе передачи (BITS).
`0x80246009`	`WU_E_DM_BITSTRANSFERERROR`	Не удалось выполнить операцию диспетчера загрузки из-за неопознанной ошибки передачи с помощью фоновой интеллектуальной службы передачи (BITS).
`0x8024600A`	`WU_E_DM_DOWNLOADLOCATIONCHANGED`	Необходимо перезапустить загрузку, поскольку расположение источника загрузки изменилось.
`0x8024600B`	`WU_E_DM_CONTENTCHANGED`	Необходимо перезапустить загрузку, поскольку содержимое обновления в новой редакции изменилось.
`0x80246FFF`	`WU_E_DM_UNEXPECTED`	Произошла ошибка диспетчера загрузок, которой не соответствует ни один код `WU_E_DM_*`.

Ошибки обработчика обновлений

Код ошибки	Сообщение	Описание
`0x80242000`	`WU_E_UH_REMOTEUNAVAILABLE`	Не удалось выполнить запрос на удаленный обработчик обновлений, так как удаленный процесс недоступен.
`0x80242001`	`WU_E_UH_LOCALONLY`	Не удалось выполнить запрос на удаленный обработчик обновлений, так как обработчик является локальным.
`0x80242002`	`WU_E_UH_UNKNOWNHANDLER`	Не удалось выполнить запрос на обработчик обновления, так как обработчик не удалось распознать.
`0x80242003`	`WU_E_UH_REMOTEALREADYACTIVE`	Не удалось создать удаленный обработчик обновления, так как он уже существует.
`0x80242004`	`WU_E_UH_DOESNOTSUPPORTACTION`	Не удалось выполнить запрос на установку (удаление) обновления обработчиком, так как обновление не поддерживает установку (удаление).

Код ошибки	Сообщение	Описание
0x80242005	WU_E_UH_WRONGHANDLER	Операция не завершена, так как указан неправильный обработчик.
0x80242006	WU_E_UH_INVALIDMETADATA	Не удалось завершить операцию обработчика, так как обновление содержит недопустимые метаданные.
0x80242007	WU_E_UH_INSTALLERHUNG	Не удалось выполнить операцию, так как установщик превысил ограничение по времени.
0x80242008	WU_E_UH_OPERATIONCANCELLED	Операция, выполнявшаяся обработчиком обновлений, была отменена.
0x80242009	WU_E_UH_BADHANDLERXML	Не удалось завершить операцию, так как метаданные, относящиеся к обработчику, недопустимы.
0x8024200A	WU_E_UH_CANREQUIREINPUT	Не удалось выполнить запрос к обработчику на установку обновления, так как для обновления требуется ввод данных пользователем.
0x8024200B	WU_E_UH_INSTALLERFAILURE	Установщику не удалось установить (удалить) одно или несколько обновлений.
0x8024200C	WU_E_UH_FALLBACKTOSELFCONTAINED	Обработчик обновлений должен загрузить автономное содержимое, а не разностно сжатое содержимое для обновления.
0x8024200D	WU_E_UH_NEEDANOTHERDOWNLOAD	Обработчик обновлений не установил обновление, так как его нужно скачать снова.
0x8024200E	WU_E_UH_NOTIFYFAILURE	Обработчику обновления не удалось отправить уведомление о состоянии операции установки (удаления).
0x8024200F	WU_E_UH_INCONSISTENT_FILE_NAMES	Имена файлов, содержащиеся в метаданных обновления и в пакете обновления, не согласованы.
0x80242010	WU_E_UH_FALLBACKERROR	Обработчику обновлений не удалось вернуться к автономному содержимому.

Код ошибки	Сообщение	Описание
0x80242011	WU_E_UH_TOOMANYDOWNLOADREQUESTS	Обработчик обновлений превысил максимальное количество запросов на скачивание.
0x80242012	WU_E_UH_UNEXPECTEDCBSRESPONSE	Обработчик обновлений получил непредвиденный ответ от модели CBS.
0x80242013	WU_E_UH_BADCBSPACKAGEID	Метаданные обновления содержат недопустимый идентификатор пакета CBS.
0x80242014	WU_E_UH_POSTREBOOTSTILLPENDING	Операция после перезагрузки для обновления все еще выполняется.
0x80242015	WU_E_UH_POSTREBOOTRESULTUNKNOWN	Не удалось определить результат операции после перезагрузки для обновления.
0x80242016	WU_E_UH_POSTREBOOTUNEXPECTEDSTATE	Непредвиденное состояние обновления по завершении выполнения операции после перезагрузки.
0x80242017	WU_E_UH_NEW_SERVICING_STACK_REQUIRED	Перед загрузкой или установкой этого обновления необходимо обновить обслуживающий стек ОС.
0x80242FFF	WU_E_UH_UNEXPECTED	Ошибке обработчика обновлений не соответствует ни один код WU_E_UH_*.

Ошибки хранилища данных

Код ошибки	Сообщение	Описание
0x80248000	WU_E_DS_SHUTDOWN	Не удалось выполнить операцию, поскольку агент Центра обновления Windows завершает работу.
0x80248001	WU_E_DS_INUSE	Не удалось выполнить операцию, поскольку хранилище данных использовалось.
0x80248002	WU_E_DS_INVALID	Текущее и ожидаемое состояния хранилища данных не совпадают.
0x80248003	WU_E_DS_TABLEMISSING	В хранилище данных отсутствует таблица.

Код ошибки	Сообщение	Описание
0x80248004	WU_E_DS_TABLEINCORRECT	В хранилище данных имеется таблица, которая содержит непредусмотренные столбцы.
0x80248005	WU_E_DS_INVALIDTABLENAME	Не удалось открыть таблицу, так как она отсутствует в хранилище данных.
0x80248006	WU_E_DS_BADVERSION	Текущая и ожидаемая версии хранилища данных не совпадают.
0x80248007	WU_E_DS_NODATA	Запрошенная информация отсутствует в хранилище данных.
0x80248008	WU_E_DS_MISSINGDATA	В хранилище данных отсутствуют необходимые сведения или имеется пустое значение NULL в столбце таблицы, значение в котором не должно быть пустым.
0x80248009	WU_E_DS_MISSINGREF	В хранилище данных отсутствуют необходимые сведения или имеется ссылка на отсутствующие условия лицензионного соглашения, локализованное свойство или связанную строку.
0x8024800A	WU_E_DS_UNKNOWNHANDLER	Обновление не было обработано, так как его обработчик обновления не удалось распознать.
0x8024800B	WU_E_DS_CANTDELETE	Обновление не было удалено, так как на него по-прежнему ссылаются одна или несколько служб.
0x8024800C	WU_E_DS_LOCKTIMEOUTEXPIRED	Не удалось заблокировать раздел хранилища данных в течение отведенного времени.
0x8024800D	WU_E_DS_NOCATEGORIES	Категория не была добавлена, так как она не содержит родительских категорий и сама по себе не является категорией верхнего уровня.
0x8024800E	WU_E_DS_ROWEXISTS	Строка не была добавлена, так как существующая строка содержит тот же первичный ключ.
0x8024800F	WU_E_DS_STOREFILELOCKED	Не удалось инициализировать хранилище данных, так как оно было заблокировано другим процессом.
0x80248010	WU_E_DS_CANNOTREGISTER	Хранилище данных не может быть зарегистрировано с помощью COM в текущем процессе.

Код ошибки	Сообщение	Описание
`0x80248011`	`WU_E_DS_UNABLETOSTART`	Не удалось создать объект хранилища данных в другом процессе.
`0x80248013`	`WU_E_DS_DUPLICATEUPDATEID`	Сервер отправил клиенту одно и то же обновление с двумя разными кодами версии.
`0x80248014`	`WU_E_DS_UNKNOWNSERVICE`	Операция не завершена, так как служба не хранится в хранилище данных.
`0x80248015`	`WU_E_DS_SERVICEEXPIRED`	Операция не завершена, так как срок действия регистрации службы истек.
`0x80248016`	`WU_E_DS_DECLINENOTALLOWED`	Запрос на скрытие обновления был отклонен, так как оно является обязательным или развернуто с крайним сроком.
`0x80248017`	`WU_E_DS_TABLESESSIONMISMATCH`	Таблица не была закрыта, так как она не связана с сеансом.
`0x80248018`	`WU_E_DS_SESSIONLOCKMISMATCH`	Таблица не была закрыта, так как она не связана с сеансом.
`0x80248019`	`WU_E_DS_NEEDWINDOWSSERVICE`	Запрос на удаление службы клиентский компонент Центра обновления Windows или отмену ее регистрации с помощью автоматического Обновления был отклонен, так как это встроенная служба и (или) Автоматический Обновления не может вернуться к другой службе.
`0x8024801A`	`WU_E_DS_INVALIDOPERATION`	Запрос отклонен, так как операция не разрешена.
`0x8024801B`	`WU_E_DS_SCHEMAMISMATCH`	Схема текущего хранилища данных и схема таблицы в xml-документе резервной копии не совпадают.
`0x8024801C`	`WU_E_DS_RESETREQUIRED`	Для хранилища данных требуется перезагрузка сеанса. Завершите данный сеанс и повторите попытку, открыв новый сеанс.
`0x8024801D`	`WU_E_DS_IMPERSONATED`	Операция хранилища данных не завершена, так как она была запрошена с олицетворенным удостоверением.
`0x80248FFF`	`WU_E_DS_UNEXPECTED`	Произошла ошибка хранилища данных, которой не соответствует ни один код `WU_E_DS_*`.

Ошибки служебных программ драйверов

Перечисленное самонастраивающееся устройство удаляется из спецификаций системы из-за того, что один из кодов оборудования или совместимых кодов соответствует установленному драйверу принтера. Это не неустранимая ошибка, и устройство просто пропущено.

Код ошибки	Сообщение	Описание
`0x8024C001`	`WU_E_DRV_PRUNED`	Драйвер был пропущен.
`0x8024C002`	`WU_E_DRV_NOPROP_OR_LEGACY`	Не удалось найти свойство для драйвера. Возможно, оно не соответствует обязательным требованиям.
`0x8024C003`	`WU_E_DRV_REG_MISMATCH`	Тип реестра, считываемого для драйвера, не соответствует ожидаемому типу.
`0x8024C004`	`WU_E_DRV_NO_METADATA`	В обновлении драйвера отсутствуют метаданные.
`0x8024C005`	`WU_E_DRV_MISSING_ATTRIBUTE`	В обновлении драйвера отсутствует обязательный атрибут.
`0x8024C006`	`WU_E_DRV_SYNC_FAILED`	Ошибка синхронизации драйвера.
`0x8024C007`	`WU_E_DRV_NO_PRINTER_CONTENT`	Отсутствуют сведения, необходимые для синхронизации подходящих принтеров.
`0x8024CFFF`	`WU_E_DRV_UNEXPECTED`	Произошла ошибка драйвера, которой не соответствует ни один код `WU_E_DRV_*`.

Коды ошибок Центра обновления Windows

Код ошибки	Сообщение	Описание
`0x80240001`	`WU_E_NO_SERVICE`	Агенту Центра обновления Windows не удалось предоставить службу.
`0x80240002`	`WU_E_MAX_CAPACITY_REACHED`	Превышена максимальная мощность службы.
`0x80240003`	`WU_E_UNKNOWN_ID`	Не удается найти идентификатор.
`0x80240004`	`WU_E_NOT_INITIALIZED`	Не удалось инициализировать объект .

Код ошибки	Сообщение	Описание
0x80240005	WU_E_RANGEOVERLAP	Обработчик обновлений запросил диапазон байтов, перекрывающий ранее запрошенный диапазон.
0x80240006	WU_E_TOOMANYRANGES	Запрошенное количество диапазонов байтов превышает максимальное значение (2^31 - 1).
0x80240007	WU_E_INVALIDINDEX	Недопустимый индекс в коллекции.
0x80240008	WU_E_ITEMNOTFOUND	Не удалось найти ключ для запрашиваемого элемента.
0x80240009	WU_E_OPERATIONINPROGRESS	Выполнялась другая конфликтующая операция. Некоторые операции, такие как установка, не могут выполняться дважды одновременно.
0x8024000A	WU_E_COULDNOTCANCEL	Отмена операции не разрешена.
0x8024000B	WU_E_CALL_CANCELLED	Операция была отменена.
0x8024000C	WU_E_NOOP	Операция не требовалась.
0x8024000D	WU_E_XML_MISSINGDATA	клиентский компонент Центра обновления Windows агенту не удалось найти необходимые сведения в XML-данных обновления.
0x8024000E	WU_E_XML_INVALID	Агент Центра обновления Windows обнаружил недопустимые сведения в данных XML обновления.
0x8024000F	WU_E_CYCLE_DETECTED	В метаданных обнаружены циклические связи обновления.
0x80240010	WU_E_TOO_DEEP_RELATION	Была выполнена оценка связей обновления со слишком глубоким уровнем вложенности.
0x80240011	WU_E_INVALID_RELATIONSHIP	Обнаружена недопустимая связь обновления.
0x80240012	WU_E_REG_VALUE_INVALID	Считано недопустимое значение реестра.
0x80240013	WU_E_DUPLICATE_ITEM	Операция попыталась добавить повторяющийся элемент в список.
0x80240016	WU_E_INSTALL_NOT_ALLOWED	Операция попыталась установить обновление в то время, как выполнялась

Код ошибки	Сообщение	Описание
		другая установка, либо система ожидала обязательной перезагрузки.
0x80240017	WU_E_NOT_APPLICABLE	Операция не была выполнена, так как отсутствуют применимые обновления.
0x80240018	WU_E_NO_USERTOKEN	Операция не выполнена из-за отсутствия необходимого маркера пользователя.
0x80240019	WU_E_EXCLUSIVE_INSTALL_CONFLICT	Монопольное обновление не может быть установлено вместе с другими обновлениями одновременно.
0x8024001A	WU_E_POLICY_NOT_SET	Значение политики не задано.
0x8024001B	WU_E_SELFUPDATE_IN_PROGRESS	Не удалось выполнить операцию, так как агент клиентский компонент Центра обновления Windows самообновится.
0x8024001D	WU_E_INVALID_UPDATE	Обновление содержит недопустимые метаданные.
0x8024001E	WU_E_SERVICE_STOP	Операция не завершена, так как служба или система была завершена.
0x8024001F	WU_E_NO_CONNECTION	Операция не завершена, так как сетевое подключение было недоступно.
0x80240020	WU_E_NO_INTERACTIVE_USER	Операция не завершена, так как нет вошедшего в систему интерактивного пользователя.
0x80240021	WU_E_TIME_OUT	Операция не завершена, так как истекло время ожидания.
0x80240022	WU_E_ALL_UPDATES_FAILED	Не удалось выполнить операцию для всех обновлений.
0x80240023	WU_E_EULAS_DECLINED	Условия лицензии для всех обновлений были отклонены.
0x80240024	WU_E_NO_UPDATE	Обновления отсутствуют.
0x80240025	WU_E_USER_ACCESS_DISABLED	Доступ к Центру обновления Windows запрещен параметрами групповой политики.
0x80240026	WU_E_INVALID_UPDATE_TYPE	Недопустимый тип обновления.
0x80240027	WU_E_URL_TOO_LONG	Слишком длинный URL-адрес.

Код	Сообщение	Описание
0x80240028	WU_E_UNINSTALL_NOT_ALLOWED	Не удалось удалить обновление, так как запрос не поступил с сервера WSUS.
0x80240029	WU_E_INVALID_PRODUCT_LICENSE	Возможно, поиск пропустил некоторые обновления до появления нелицензированного приложения в системе.
0x8024002A	WU_E_MISSING_HANDLER	Отсутствует компонент, необходимый для обнаружения подходящих обновлений.
0x8024002B	WU_E_LEGACYSERVER	Операция не завершена, так как для нее требуется более новая версия сервера.
0x8024002C	WU_E_BIN_SOURCE_ABSENT	Не удалось установить разностное обновление, так как ему требуется источник.
0x8024002D	WU_E_SOURCE_ABSENT	Не удалось установить полнофайловый пакет обновления, так как для него требуется источник.
0x8024002E	WU_E_WU_DISABLED	Доступ к неуправляемым серверу запрещен.
0x8024002F	WU_E_CALL_CANCELLED_BY_POLICY	Операция не завершена, так как настроена политика DisableWindowsUpdateAccess.
0x80240030	WU_E_INVALID_PROXY_SERVER	Недопустимый формат списка прокси-серверов.
0x80240031	WU_E_INVALID_FILE	Файл имеет неправильный формат.
0x80240032	WU_E_INVALID_CRITERIA	Недопустимая строка условий поиска.
0x80240033	WU_E_EULA_UNAVAILABLE	Не удалось скачать условия лицензии.
0x80240034	WU_E_DOWNLOAD_FAILED	Не удалось скачать обновление.
0x80240035	WU_E_UPDATE_NOT_PROCESSED	Обновление не было обработано.
0x80240036	WU_E_INVALID_OPERATION	Текущее состояние объекта не разрешило операцию.
0x80240037	WU_E_NOT_SUPPORTED	Функциональные возможности операции не поддерживаются.
0x80240038	WU_E_WINHTTP_INVALID_FILE	Загруженный файл имеет непредвиденный тип содержимого.
0x80240039	WU_E_TOO_MANY_RESYNC	Превышено число запросов повторной синхронизации агента от сервера.

Код ошибки	Сообщение	Описание
`0x80240040`	`WU_E_NO_SERVER_CORE_SUPPORT`	`WUA API` Метод не выполняется при установке основных серверных компонентов.
`0x80240041`	`WU_E_SYSPREP_IN_PROGRESS`	Служба недоступна во время выполнения sysprep.
`0x80240042`	`WU_E_UNKNOWN_SERVICE`	Служба обновления больше не зарегистрирована в `AU`.
`0x80240043`	`WU_E_NO_UI_SUPPORT`	`WUA UI`Поддержка отсутствует.
`0x80240FFF`	`WU_E_UNEXPECTED`	Сбой операции с ошибкой, которой не соответствует ни один код.
`0x80070422`		клиентский компонент Центра обновления Windows служба перестала работать или не работает.

Коды успешного выполнения операций Центра обновления Windows

Код ошибки	Сообщение	Описание
`0x00240001`	`WU_S_SERVICE_STOP`	Агент Центра обновления Windows успешно остановлен.
`0x00240002`	`WU_S_SELFUPDATE`	Агент Центра обновления Windows выполнил самостоятельное обновление.
`0x00240003`	`WU_S_UPDATE_ERROR`	Операция успешно выполнена, но при применении обновлений произошли ошибки.
`0x00240004`	`WU_S_MARKED_FOR_DISCONNECT`	Обратный вызов был помечен для отключения позднее, поскольку запрос на отключение операции был получен в процессе выполнения обратного вызова.
`0x00240005`	`WU_S_REBOOT_REQUIRED`	Для завершения установки обновления необходимо перезагрузить систему.
`0x00240006`	`WU_S_ALREADY_INSTALLED`	Устанавливаемое обновление уже установлено в системе.

Код ошибки	Сообщение	Описание
0x00240007	WU_S_ALREADY_UNINSTALLED	Удаляемое обновление не устанавливается в системе.
0x00240008	WU_S_ALREADY_DOWNLOADED	Обновление, которое необходимо скачать, уже загружено.

Незначительные ошибки установщика Windows

Следующие ошибки указывают на то, что часть операции поиска завершается сбоем из-за проблем с установщиком Windows. Другая часть поиска может успешно вернуть обновления. Все дополнительные коды установщика Windows должны использовать один и тот же диапазон кодов ошибок, чтобы вызывающий объект смог сообщить, что они связаны с установщиком Windows.

Код ошибки	Сообщение	Описание
0x80241001	WU_E_MSI_WRONG_VERSION	Некоторые обновления могли не попасть в результаты поиска, поскольку используемая версия установщика Windows ниже 3.1.
0x80241002	WU_E_MSI_NOT_CONFIGURED	Возможно, поиск пропустил некоторые обновления, так как установщик Windows не настроен.
0x80241003	WU_E_MSP_DISABLED	Некоторые обновления могли не попасть в результаты поиска, поскольку исправление установщика Windows отключено политикой.
0x80241004	WU_E_MSI_WRONG_APP_CONTEXT	Не удалось применить обновление, так как приложение устанавливается для каждого пользователя.
0x80241FFF	WU_E_MSP_UNEXPECTED	Некоторые обновления могли не попасть в результаты поиска, поскольку работа установщика Windows завершилась сбоем.

Ошибки обновления и установки агента Центра обновления Windows

Код ошибки	Сообщение	Описание
`0x8024D001`	`WU_E_SETUP_INVALID_INFDATA`	Не удалось обновить агент клиентский компонент Центра обновления Windows, так как INF-файл содержит недопустимые сведения.
`0x8024D002`	`WU_E_SETUP_INVALID_IDENTDATA`	не удалось обновить агент клиентский компонент Центра обновления Windows, так как `wuident.cab` файл содержит недопустимые сведения.
`0x8024D003`	`WU_E_SETUP_ALREADY_INITIALIZED`	клиентский компонент Центра обновления Windows агент не удалось обновить из-за внутренней ошибки, из-за чего инициализация установки выполнялась дважды.
`0x8024D004`	`WU_E_SETUP_NOT_INITIALIZED`	не удалось обновить агент клиентский компонент Центра обновления Windows, так как инициализация установки не завершилась успешно.
`0x8024D005`	`WU_E_SETUP_SOURCE_VERSION_MISMATCH`	Не удалось обновить агент клиентский компонент Центра обновления Windows, так как версии, указанные в INF, не соответствуют фактическим версиям исходного файла.
`0x8024D006`	`WU_E_SETUP_TARGET_VERSION_GREATER`	не удалось обновить агент клиентский компонент Центра обновления Windows, так как файл WUA в целевой системе новее, чем соответствующий исходный файл.
`0x8024D007`	`WU_E_SETUP_REGISTRATION_FAILED`	не удалось обновить агент клиентский компонент Центра обновления Windows, так как `regsvr32.exe` возвращена ошибка.
`0x8024D009`	`WU_E_SETUP_SKIP_UPDATE`	Обновление агента Центра обновления Windows было пропущено из-за директивы в файле `wuident.cab`.
`0x8024D00A`	`WU_E_SETUP_UNSUPPORTED_CONFIGURATION`	не удалось обновить агент клиентский компонент Центра обновления Windows, так как текущая конфигурация системы не поддерживается.

Код ошибки	Сообщение	Описание
0x8024D00B	WU_E_SETUP_BLOCKED_CONFIGURATION	не удалось обновить агент клиентский компонент Центра обновления Windows, так как система настроена на блокировку обновления.
0x8024D00C	WU_E_SETUP_REBOOT_TO_FIX	не удалось обновить агент клиентский компонент Центра обновления Windows, так как требуется перезагрузка системы.
0x8024D00D	WU_E_SETUP_ALREADYRUNNING	Программа установки агента Центра обновления Windows уже запущена.
0x8024D00E	WU_E_SETUP_REBOOTREQUIRED	Чтобы завершить установку пакета программы установки для агента Центра обновления Windows, необходимо выполнить перезагрузку.
0x8024D00F	WU_E_SETUP_HANDLER_EXEC_FAILURE	Не удалось обновить агент клиентский компонент Центра обновления Windows, так как во время выполнения произошел сбой обработчика установки.
0x8024D010	WU_E_SETUP_INVALID_REGISTRY_DATA	не удалось обновить агент клиентский компонент Центра обновления Windows, так как реестр содержит недопустимые сведения.
0x8024D013	WU_E_SETUP_WRONG_SERVER_VERSION	не удалось обновить агент клиентский компонент Центра обновления Windows, так как сервер не содержит сведений об обновлении для этой версии.
0x8024DFFF	WU_E_SETUP_UNEXPECTED	не удалось обновить агент клиентский компонент Центра обновления Windows из-за ошибки, не охваченной другим WU_E_SETUP_* кодом ошибки.

Принцип работы Центра обновления Windows

Статья • 18.03.2023

Область применения

- Windows 10
- Windows 11

Рабочий процесс клиентский компонент Центра обновления Windows имеет четыре основные области функциональности:

Scan

1. Orchestrator запланирует сканирование.
2. Orchestrator проверяет утверждения и политики администратора для скачивания.

Скачать

1. Orchestrator запускает скачивание.
2. клиентский компонент Центра обновления Windows скачивает файлы манифеста и предоставляет их арбитру.
3. Арбитр оценивает манифест и сообщает клиенту клиентский компонент Центра обновления Windows скачать файлы.
4. клиентский компонент Центра обновления Windows клиент загружает файлы во временную папку.
5. Арбитр выполняет этапы скачанных файлов.

Install

1. Orchestrator запускает установку.
2. Арбитр вызывает установщик для установки пакета.

Совершить

1. Orchestrator запускает перезапуск.
2. Арбитр завершает работу перед перезапуском.

Принцип работы обновления

В процессе обновления клиентский компонент Центра обновления Windows Orchestrator работает в фоновом режиме для сканирования, скачивания и установки обновлений. Эти действия выполняются автоматически, в соответствии с вашими параметрами, и автоматически, чтобы не нарушить работу компьютера.

Проверка обновлений

Оркестратор клиентский компонент Центра обновления Windows на компьютере проверяет сервер Центра обновления Майкрософт или конечную точку WSUS на наличие новых обновлений через случайные интервалы. Рандомизация гарантирует, что сервер клиентский компонент Центра обновления Windows не будет перегружен запросами одновременно. Оркестратор обновлений выполняет поиск только обновлений, добавленных с момента последнего поиска обновлений, что позволяет быстро и эффективно находить обновления.

При проверке наличия обновлений клиентский компонент Центра обновления Windows Orchestrator оценивает, подходит ли обновление для вашего устройства. В нем используются рекомендации, определенные издателем обновления, например Microsoft Office, включая корпоративные групповые политики.

Убедитесь, что вы знакомы со следующей терминологией, связанной с клиентский компонент Центра обновления Windows сканирования:

Термин	Определение
Update	Мы используем этот термин для обозначения нескольких разных вещей, но в этом контексте это фактически обновленный код или изменение.
Обновление пакета	Обновление, содержащее 1–N дочерних обновлений; не содержит самих полезных данных.
Дочернее обновление	Конечное обновление, в которое входит другое обновление; содержит полезные данные.

Термин	Определение
Обновление детектора	Специальное обновление, содержащее только правило применимости IsInstalled и не содержит полезных данных. Используется для предварительной оценки.
Обновление категории	Специальный "детектоид", имеющий правило **IsInstalled** , которое всегда является истинным. Используется для группирования обновлений и позволяет устройству фильтровать обновления.
Полная проверка	Сканирование с пустым хранилищем данных.
Разностное сканирование	Проверка с помощью обновлений из предыдущей проверки, уже кэшированных в хранилище данных.
Проверка по сети	Проверка, использующая сеть, и для проверка сервера обновлений.
Автономное сканирование	Проверка, которая не использует сеть, а проверяет локальное хранилище данных. Полезно только в том случае, если проверка в сети выполнялась ранее.
CatScan	Проверка категорий, где вызывающий объект может указать **categoryId** для получения обновлений, опубликованных в этом **categoryId**.
AppCatScan	Проверка категорий, где вызывающий объект может указать **AppCategoryId** для получения приложений, опубликованных в этом **appCategoryId**.
Синхронизация программного обеспечения	Часть проверки, которая проверяет только наличие обновлений программного обеспечения (как приложений, так и операционной системы).
Синхронизация драйверов	Часть проверки, которая проверяет только обновления драйверов. Эта синхронизация является необязательной и выполняется после синхронизации программного обеспечения.
ProductSync	Синхронизация на основе атрибутов, в которой клиент заранее предоставляет список атрибутов устройства, продукта и вызывающего объекта, чтобы позволить службе проверка применимости в облаке.

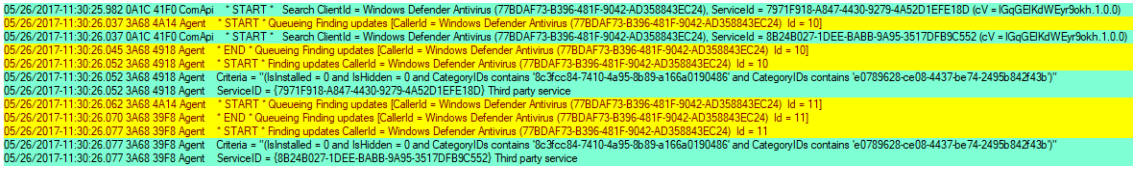
Как работает сканирование клиентский компонент Центра обновления Windows

клиентский компонент Центра обновления Windows выполняет следующие действия при выполнении проверки.

Запускает проверку на наличие обновлений

Когда пользователи начинают сканирование в клиентский компонент Центра обновления Windows с помощью панели Параметры, происходит следующее:

- При проверке сначала создается сообщение "ComApi". Вызывающий объект (Microsoft Defender антивирусная программа) сообщает подсистеме клиентский компонент Центра обновления Windows проверять наличие обновлений.
- Сообщения агента: постановка сканирования в очередь, а затем фактическое начало работы:
    - Обновления идентифицируются по разным идентификаторам ("ID = 10", "ID = 11") и по разным номерам идентификаторов потоков.
    - клиентский компонент Центра обновления Windows использует фильтрацию идентификаторов потока, чтобы сосредоточиться на одной конкретной задаче.



Поведение прокси-сервера

Для клиентский компонент Центра обновления Windows проверяет URL-адреса, используемые для обнаружения обновлений ([MS-WUSP]: Веб-служба SimpleAuth | Документация Майкрософт, [MS-WUSP]: веб-служба клиента | Документация Майкрософт):

- Предпринята попытка использования системного прокси-сервера (задается с помощью `netsh` команды).
- Если wuA не удается связаться со службой из-за определенного прокси-сервера, службы или кода ошибки проверки подлинности, предпринимается попытка прокси-сервера пользователя (как правило, это вошедший в систему пользователь).

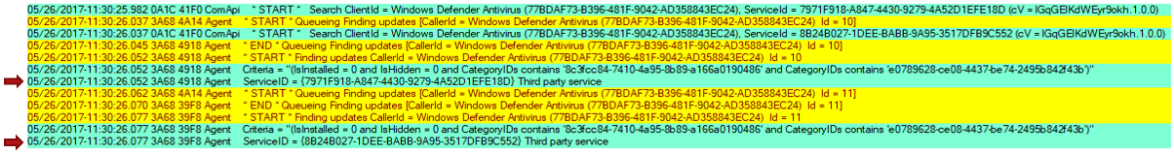
> ⓘ **Примечание**
>
> Для URL-адресов службы обновления WSUS в интрасети мы предоставляем параметр с помощью политики клиентский компонент Центра обновления Windows, чтобы выбрать поведение прокси-сервера.

Для клиентский компонент Центра обновления Windows URL-адресов, которые *не* используются для обнаружения обновлений, например для скачивания или создания отчетов:

- Предпринята попытка прокси-сервера пользователя.
- Если wuA не удается связаться со службой из-за определенного прокси-сервера, службы или кода ошибки проверки подлинности, предпринимается попытка использовать системный прокси-сервер.

Идентифицирует идентификаторы служб

- Идентификаторы служб указывают, какой источник обновлений проверяется.
- Подсистема клиентский компонент Центра обновления Windows обрабатывает каждую службу как отдельную сущность, даже если несколько служб могут содержать одни и те же обновления.



- Общие идентификаторы служб

> **ⓘ Важно!**
>
> ServiceId здесь определяет абстракцию клиента, а не какую-либо конкретную службу в облаке. Не следует делать предположение о том, на какой сервер указывает serviceId. Он полностью контролируется ответами службы поиска служб.

Обслуживание	**ServiceId**
Не указано / по умолчанию	клиентский компонент Центра обновления Windows, Центр обновления Майкрософт или WSUS 00000000-0000-0000-0000-000000000000
Центр обновления Windows	9482F4B4-E343-43B6-B170-9A65BC822C77
Центр обновления Майкрософт	7971f918-a847-4430-9279-4a52d1efe18d
Магазин	855E8A7C-ECB4-4CA3-B045-1DFA50104289

Обслуживание	ServiceId
Тестирование ОС	8B24B027-1DEE-BABB-9A95-3517DFB9C552
WSUS или Configuration Manager	Via ServerSelection::ssManagedServer 3DA21691-E39D-4da6-8A4B-B43877BCB1B7
Автономная служба сканирования	Через IUpdateServiceManager::AddScanPackageService

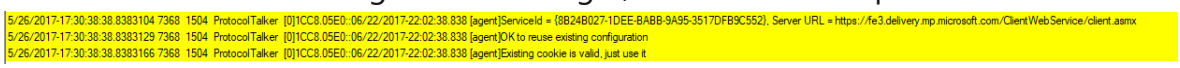
Поиск ошибок сети

Распространенный сбой обновления возникает из-за проблем с сетью. Чтобы найти корень проблемы, выполните следующие действия:

- Найдите сообщения ProtocolTalker, чтобы увидеть сетевой трафик синхронизации клиента и сервера.
- "Ошибки SOAP" могут быть проблемами на стороне клиента или сервера; прочитать сообщение.
- Клиент клиентский компонент Центра обновления Windows использует службу поиска служб для обнаружения конфигураций и конечных точек источников сетевых обновлений Майкрософт: Центра обновления Windows, Центра обновления Майкрософт или flighting.

  > ⓘ **Примечание**
  >
  > Если поиск выполняется в службах WSUS или Configuration Manager, можно игнорировать предупреждающие сообщения для службы указателя служб.

- На сайтах, использующих только СЛУЖБЫ WSUS или Configuration Manager, служба указателя служб может быть заблокирована в брандмауэре. В этом случае запрос завершится ошибкой, и хотя служба не может выполнить проверку клиентский компонент Центра обновления Windows или Центра обновления Майкрософт, она по-прежнему может выполнять проверку на наличие WSUS или Configuration Manager, так как она настроена локально.



Скачивание обновлений

После того как клиентский компонент Центра обновления Windows Orchestrator определит, какие обновления применяются к вашему компьютеру, начнется скачивание обновлений, если выбран параметр для автоматического скачивания обновлений. Он выполняет работу в фоновом режиме, не прерывая обычное использование устройства.

Чтобы другие загрузки не влияли или не замедлялись из-за загрузки обновлений, клиентский компонент Центра обновления Windows использует оптимизацию доставки, которая скачивает обновления и снижает потребление пропускной способности.

Дополнительные сведения см. в статье Настройка оптимизации доставки для Windows 10 обновлений.

Установка обновлений

Если применимо обновление, скачивается "Arbiter" и метаданные. В зависимости от параметров клиентский компонент Центра обновления Windows, когда скачивание завершится, arbiter соберет сведения с устройства и сравнит их с скачанными метаданными, чтобы создать список действий.

В списке действий описаны все файлы, необходимые из клиентский компонент Центра обновления Windows, и то, что с ними должен делать агент установки (например, CBS или программа установки). Список действий предоставляется агенту установки вместе с полезными данными для начала установки.

Фиксация Обновления

Если настроен параметр автоматической установки обновлений, клиентский компонент Центра обновления Windows Orchestrator в большинстве случаев автоматически перезагружает устройство после установки обновлений. Он должен перезапустить устройство, так как оно может быть небезопасным или не полностью обновлено, пока оно не перезапустится. Вы можете использовать групповая политика параметры, управление мобильными устройствами (MDM) или реестр (не рекомендуется), чтобы настроить время перезапуска устройств после установки обновления Windows 10.

Дополнительные сведения см. в разделе Управление перезапусками устройств после обновлений.

Пути обновления Windows

Статья • 29.01.2025 • Применяется к: ✅ Windows 10, ✅ Windows 11

Схемы обновления

В этой статье приводится сводка доступных путей обновления до поддерживаемых в настоящее время версий Windows. Вы можете выполнить обновление до поддерживаемых в настоящее время версий Windows с предыдущих версий Windows, которые также по-прежнему поддерживаются. Пути включают обновление с одного выпуска Windows до более поздней версии той же версии Windows. Также поддерживается переход с одного выпуска Windows на другой выпуск того же выпуска.

> ⓘ **Примечание**
>
> Если вы также переходите на другой выпуск Windows, см. раздел **Обновление выпуска Windows**. В статье **об обновлении выпуска Windows** описаны методы и поддерживаемые пути изменения выпуска Windows. Эти методы требуют ввода лицензии или ключа продукта для нового выпуска Windows перед началом процесса обновления. Для некоторых путей также поддерживается переход на более раннюю версию. Однако приложения и параметры не всегда поддерживаются при понижении версии Windows.

- **Обновление версий Windows**. Вы можете напрямую обновить любую версию Канала общедоступной доступности Windows до более новой поддерживаемой версии канала общедоступной доступности Windows, даже если она включает пропуск версий. Если ваша текущая версия Windows не поддерживается, свяжитесь с представителем службы поддержки для своей учетной записи. Сведения о доступности и услугах см. в разделе Данные о жизненном цикле Windows.

- **Обновление с Windows LTSC до канала общей доступности Windows**. Обновление с Windows LTSC до Канала общей доступности Windows доступно при обновлении до той же или более новой версии сборки. Например, Windows 10 Корпоративная 2016 с долгосрочным обслуживанием можно обновить до Windows 10 Корпоративная 22H2. Обновление поддерживается с помощью процесса обновления на месте с помощью установки Windows. Если требуется сохранить приложения, необходимо использовать ключ продукта.

Если параметр не используется, параметр **Сохранить личные файлы и приложения** неактивен. Командная строка для выполнения обновления:

Командная строка Windows

```
setup.exe /pkey xxxxx-xxxxx-xxxxx-xxxxx-xxxxx
```

где **xxxxx-xxxxx-xxxxx-xxxxx-xxxxx** — это ключ продукта Канала общедоступной доступности Windows. Например, если используется KMS, командная строка для Windows Enterprise будет иметь следующий тип:

Командная строка Windows

```
setup.exe /pkey NPPR9-FWDCX-D2C8J-H872K-2YT43
```

Дополнительные ключи продуктов для использования с KMS см. в разделах Активация клиентов служб управления ключами (KMS) и ключи продуктов: универсальные ключи корпоративной лицензии (GVLK).

> ⓘ **Важно!**
>
> Обновление на месте с Канала общей доступности Windows до Windows LTSC не поддерживается.
>
> Windows 10 LTSC 2015 не блокируют этот путь обновления на месте, даже если он не поддерживается. Эта проблема была исправлена в выпуске Windows 10 LTSC 2016. Windows 10 LTSC 2016 допускает только параметры установки только для данных и чистой установки.

- **Windows N/KN**: номера SKU **Windows N** и **Windows KN** (выпуски без функциональных возможностей, связанных с мультимедиа) следуют тем же путям обновления, что и в следующих таблицах. Если выпуски, предшествующие обновлению и после обновления, имеют разный тип, например Windows 10 Pro N до Windows 11 Pro, персональные данные сохраняются, а приложения и параметры удаляются в процессе обновления.

Поддерживаемые пути обновления Windows

Развернуть таблицу

Выпуск Windows	Домашняя страница Windows	Windows Pro	Windows Pro для образовательных учреждений	Windows для образовательных учреждений	Windows Корпоративная
Домашняя страница Windows	❌	✅	✅	✅	❌
Windows Pro	↓	❌	✅	✅	✅
Windows для образовательных учреждений	❌	❌	❌	❌	↓
Windows Корпоративная	❌	❌	❌	✅	❌

- ✅ = Поддерживается полное обновление, включая персональные данные, параметры и приложения.
- ❌ = Обновление не поддерживается или неприменимо.
- ↓ = понижение версии выпуска; персональные данные сохраняются, приложения и параметры удаляются.

Связанные статьи

- Windows 10 сценарии развертывания.
- Рекомендации по обновлению и миграции Windows.
- Обновление выпуска Windows.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Обновление выпуска Windows

Статья • 04.10.2024 • Применяется к: ✅ Windows 10, ✅ Windows 11

С помощью Windows можно быстро перейти с одного выпуска Windows на другой при условии, что поддерживается путь обновления. Сведения о том, какой выпуск Windows подходит вам, см. в следующих статьях:

- Сравнение выпусков Windows 11 .
- Ознакомьтесь с функциями Windows 11 Pro .
- Windows 10 Pro и Windows 11 Pro .
- Сравнение выпусков Windows 10 .
- Windows для бизнеса .

Полный список всех возможных путей обновления до Windows см. в разделе Пути обновления Windows. Понижение уровня выпуска Windows рассматривается в разделе Срок действия лицензии этой статьи.

В следующей таблице показаны методы и пути, доступные для изменения выпуска Windows, работающего на компьютере.

Развернуть таблицу

Обновление выпуска	MDM	Подготовка пакет	Команда-средство line	Ввод вручную ключ продукта
Home > Pro	❌	❌	❌	☑
Home > Pro для рабочих станций	❌	❌	❌	☑
Home > Pro Education	☑	☑	☑	☑
Домашнее > образование	☑	☑	☑	☑
Pro > Pro для рабочих станций	✅	✅	✅	✅
Pro > Pro Education	✅	✅	✅	✅
Pro > Education	☑	☑	☑	☑
Pro > Enterprise	✅	✅	✅	✅
Pro для рабочих станций > Pro для образовательных учреждений	✅	✅	✅	✅
Pro для рабочих станций для > образовательных учреждений	☑	☑	☑	☑
Pro для рабочих станций > Enterprise	✅	✅	✅	✅
Pro Education > Education	☑	☑	☑	☑

Обновление выпуска	MDM	Подготовка пакет	Команда-средство line	Ввод вручную ключ продукта
Корпоративное > образование	☑	☑	☑	☑

- ✅ = Поддерживается, перезагрузка не требуется.
- ☑ = Поддерживается, но требуется перезагрузка.
- ❌ = Не поддерживается.
- MDM = современное управление устройствами.

> **Примечание**
>
> - Для каждого выпуска для настольных систем, указанного в таблице, также имеются варианты N и KN SKU. Эти выпуски не содержат функциональных возможностей для работы с мультимедиа. Устройства с установленными выпусками N и KN SKU можно обновить до соответствующих выпусков N и KN SKU, используя те же методы.
>
> - Обновления выпусков через Microsoft Store для бизнеса больше не доступны с прекращением использования Microsoft Store для бизнеса. Дополнительные сведения см. в разделе Microsoft Store для бизнеса и 31 марта 2023 г.

> **Совет**
>
> Обновление выпуска также возможно с помощью политики обновления выпуска в Microsoft Configuration Manager. Дополнительные сведения см. в статье **Обновление устройств Windows до нового выпуска с помощью Configuration Manager**.

Обновление с помощью современного управления устройствами (MDM)

Чтобы обновить классические выпуски Windows с помощью MDM, введите ключ продукта для обновленного выпуска в параметре политики **UpgradeEditionWithProductKey** поставщика CSP **WindowsLicensing** . Дополнительные сведения см. в статье WindowsLicensing CSP.

Сведения об обновлении выпусков Windows с помощью Microsoft Intune, включая выход из S-режима, см. в статье Обновление выпусков Windows 10/11 или выход из S-режима на устройствах с помощью Microsoft Intune.

Обновление с использованием пакета подготовки

Используйте Designer конфигурации Windows, чтобы создать пакет подготовки для обновления классического выпуска Windows. Конфигурация Windows Designer доступна как часть комплекта средств оценки и развертывания Windows (Windows ADK) или как автономное приложение Microsoft Store. Скачайте Designer конфигурации Windows из одного из следующих расположений:

- Скачайте и установите Windows ADK. При установке ADK выберите **Конфигурация Designer**. После установки Designer конфигурации Windows можно найти в меню Пуск в разделе **Windows Kits**>**Windows Imaging and Configuration Designer**.
- Designer конфигурации Windows — приложение Microsoft Store. После установки Designer конфигурации Windows можно найти в меню Пуск как **Designer Конфигурация Windows**.

  Скачивание Designer конфигурации Windows из Microsoft Store

Чтобы создать пакет подготовки для обновления классических выпусков Windows, выполните следующие действия.

1. Откройте конструктор конфигураций Windows.
2. Выберите **Расширенная подготовка**.
3. В открывавшемся окне **Новый проект** :
   a. В **разделе Введите сведения о проекте** присвойте проекту имя и нажмите кнопку **Далее** .
   b. В разделе **Выбор параметров для просмотра и настройки** выберите **Все классические выпуски Windows** , а затем нажмите кнопку **Далее** .
   c. В разделе **Импорт пакета подготовки (необязательно)** нажмите кнопку **Готово** .
4. В разделе **Доступные настройки** разверните узел Параметры >**среды выполненияEditionUpgrade** и выберите **ChangeProductKey**.
5. В области **EditionUpgrade/ChangeProductKey** рядом с **элементом ChangeProductKey** введите ключ продукта для обновленного выпуска.
6. В меню **Файл** выберите **Сохранить**.
7. В меню **Экспорт** выберите **Пакет подготовки**.
8. Выполните шаги мастера **сборки** , чтобы создать пакет подготовки, чтобы сохранить пакет подготовки в известном расположении.

Дополнительные сведения о Designer конфигурации Windows см. в следующих статьях:

- Создание пакета подготовки
- Применение пакета подготовки

Обновление с помощью программы командной строки

Средство `changepk.exe` командной строки можно использовать для обновления устройств до поддерживаемого выпуска Windows:

Командная строка Windows

```
changepk.exe /ProductKey <product_key>`
```

Обновления также можно выполнить с помощью `slmgr.vbs` ключа установки клиента KMS и . Пример:

Командная строка Windows

```
cscript.exe c:\windows\system32\slmgr.vbs /ipk <product_key>
```

Обновление путем ввода ключа продукта вручную

Если обновляется только несколько устройств, ключ продукта для обновленного выпуска можно ввести вручную. Чтобы вручную ввести ключ продукта, выполните следующие действия:

1. Щелкните правой кнопкой мыши меню **Пуск** и выберите **Выполнить**.
2. В окне **Выполнить** рядом с **полем Открыть** введите

   `ms-settings:activation`

   и нажмите **кнопку ОК**.
3. Выберите **Изменить ключ продукта**.
4. Введите ключ продукта.
5. Следуйте инструкциям на экране.

Кроме того, выберите следующую ссылку, чтобы автоматически открыть приложение **"Параметры"** на странице активации:

Активация

Обновление путем приобретения лицензии в Microsoft Store

Если у вас нет ключа продукта, вы можете обновить выпуск Windows с помощью Microsoft Store. Чтобы выполнить обновление через Microsoft Store, выполните следующие действия.

1. Щелкните правой кнопкой мыши меню **Пуск** и выберите **Выполнить**.
2. В окне **Выполнить** рядом с **полем Открыть** введите

   `ms-windows-store://windowsupgrade/`

   и нажмите **кнопку OK**.
3. Следуйте инструкциям на экране.

Кроме того, выберите следующую ссылку, чтобы автоматически открыть Microsoft Store на странице обновления выпуска Windows:

Обновление выпуска Windows

Окончание срока действия лицензии

Клиентам с корпоративной лицензией, срок действия лицензии которых истек, необходимо изменить выпуск Windows на выпуск с активной лицензией. Понижение уровня выпуска Windows можно использовать те же методы, которые использовались для обновления выпуска. Если путь более ранней версии поддерживается, приложения и параметры можно перенести из текущего выпуска. Если путь не поддерживается, требуется чистая установка.

Следующие сценарии не поддерживаются:

- Понижение версии Windows до pervious путем ввода другого ключа продукта, например с Windows 11 Pro до Windows 10 Pro.
- Переход с более поздней версии на более раннюю версию того же выпуска Windows, например с Windows 11 Pro 22H2 до Windows 11 Pro 22H1, если не используется откат.

> ⓘ **Примечание**
>
> Если вы используете активацию подписки Windows и срок действия лицензии истекает, устройства автоматически отменить изменения в исходный выпуск по истечении льготного периода.

Поддерживаемые пути более ранней версии Windows

Развернуть таблицу

Выпуск	Домашняя	Pro	Pro для Рабочие станции	Pro Education	Education	Корпоративная LTSC	Корпоративная
Домашняя	-	❌	❌	❌	❌	❌	❌
Профессионал	❌	-	❌	❌	❌	❌	❌
Pro для рабочих станций	❌	❌	-	❌	❌	❌	❌
Pro для образовательных учреждений	❌	❌	❌	-	❌	❌	❌
Education	❌	✅	✅	✅	-	❌	-
Корпоративная LTSC	❌	❌	❌	❌	❌	-	❌
Корпоративная	❌	✅	✅	✅	-	❌	-

- ✅ = Поддерживаемый путь к более ранней версии.
- ❌ = не поддерживается или не поддерживается понижение версии.
- - = не считается понижением версии или обновлением.

> ⓘ **Примечание**
>
> Номера SKU Windows **N** и Windows **KN** следуют тем же правилам, что и в таблице.

Таблица может не представлять более сложные сценарии. Например, вы можете выполнить обновление с Pro до Pro для рабочей станции на компьютере с внедренным ключом Pro с помощью лицензионного ключа Pro для рабочей станции. Затем вы можете перейти на более раннюю версию компьютера до Pro с помощью встроенного по встроенному ПО. Такое понижение схемы допустимо, только потому что на компьютере предварительно установлена версия Pro.

Пример сценария: понижение уровня enterprise

- Исходный выпуск: **Профессиональная OEM**
- Выпуск обновления: **Корпоративная**
- Допустимые схемы понижения версии: **Pro, Pro для рабочих станций, Pro для образовательных учреждений, для образовательных учреждений**

Вы можете перейти напрямую от выпуска Корпоративная к любому действительному выпуску. В этом примере для понижения версии до Pro для рабочих станций, Pro для образовательных учреждений или для образовательных учреждений требуется дополнительный ключ активации, чтобы заменить встроенный ключ выпуска Pro. Во всех

случаях необходимо соблюдать условия лицензии Майкрософт. Если вы являетесь клиентом корпоративной лицензии, обратитесь к справочному руководству по корпоративному лицензированию Майкрософт.

Связанные статьи

- Пути обновления Windows
- Volume Licensing Service Center
- Активация подписки Windows

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Развертывание Windows с помощью Microsoft 365

Статья • 27.02.2025 • Применяется к: ✅ Windows 11, ✅ Windows 10

В этой статье представлен краткий обзор Microsoft 365 и описано, как использовать бесплатную 90-дневную пробную учетную запись для ознакомления с некоторыми преимуществами Microsoft 365.

Microsoft 365 — это предложение корпорации Майкрософт, сочетающее Windows с Office 365, а также Enterprise Mobility and Security (EMS). Общие сведения см. на Microsoft 365 корпоративный плакате.

Для развертывания Windows Microsoft 365 включает помощник по развертыванию, который описывает весь процесс развертывания Windows. Мастер поддерживает несколько методов развертывания Windows, в том числе:

- Windows Autopilot.
- Обновление на месте.
- Развертывание обновления Windows с помощью Intune.
- Развертывание обновления Windows с помощью Microsoft Configuration Manager.
- Развертывание обновления компьютера с помощью Microsoft Configuration Manager.

Бесплатная пробная учетная запись

Если существует учетная запись подписки на службы Майкрософт и есть доступ к центру Microsoft 365 Admin:

1. Войдите в центр Microsoft 365 Admin.
2. Перейдите в **раздел Выставление счетов** и **приобретение служб**.
3. В разделе Корпоративные наборы предложений служб найдите плитки Microsoft 365 E3 и Microsoft 365 E5.
4. Выберите один из доступных вариантов **начать бесплатную пробную версию** .

Если подписки на службы Майкрософт нет, помощника по развертыванию Microsoft 365 и других ресурсов можно попробовать бесплатно. Просто выполните следующие действия.

1. Получите бесплатную пробную версию Microsoft 365.

2. Обратитесь к помощнику по развертыванию Microsoft 365.

> **Примечание**
>
> При первом запуске руководства по настройке появляется руководство **по подготовке среды** . В этом руководстве описаны основные сведения, такие как проверка домена и метод добавления пользователей. В конце руководства **По подготовке среды** есть кнопка **Готово к продолжению** , которая возвращается к выбранному исходному руководству.

плакат Microsoft 365 корпоративный

Выберите Microsoft 365 корпоративный плакат, чтобы просмотреть последнюю версию Microsoft 365 корпоративный плаката.

Связанные статьи

- Сценарии развертывания Windows.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Начало работы с Центром обновления Windows

Статья • 18.03.2023

> Применимо к: Windows 10

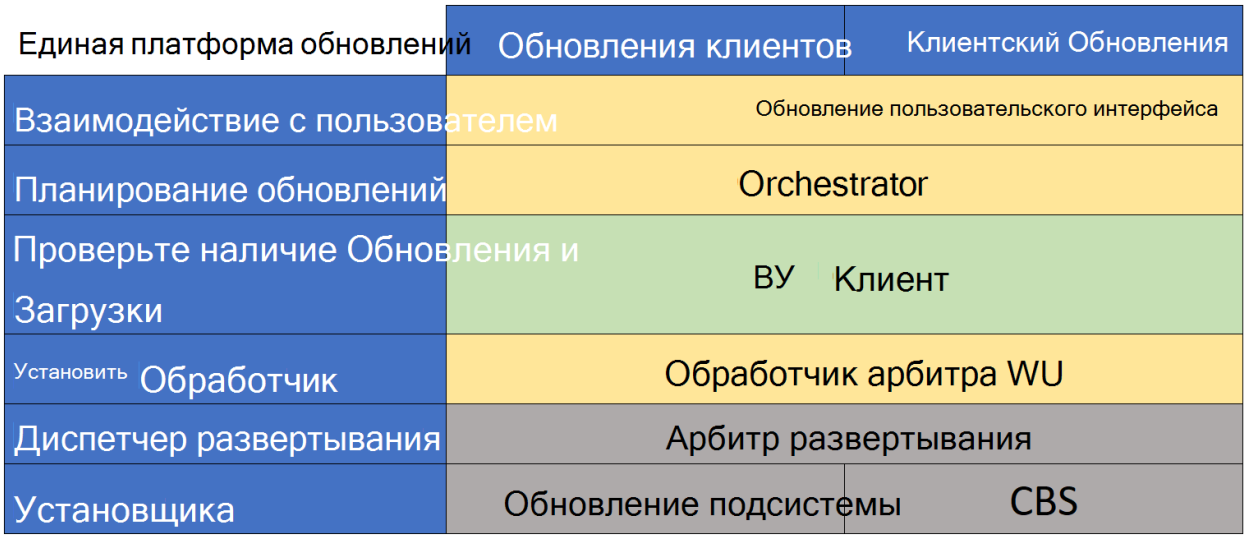
С выпуском Windows 10 мы переместили модель обновления на единую платформу обновлений. Единая платформа обновлений (UUP) — это единая модель публикации, размещения, сканирования и скачивания для всех типов обновлений ОС, клиентских устройств для всех операционных систем под управлением Windows, от ежемесячных обновлений качества до новых обновлений компонентов.

Используйте следующие сведения, чтобы приступить к работе с клиентский компонент Центра обновления Windows.

- Общие сведения об архитектуре UUP
- Узнайте, как работает клиентский компонент Центра обновления Windows
- Поиск файлов журнала клиентский компонент Центра обновления Windows
- Узнайте, как устранять неполадки клиентский компонент Центра обновления Windows
- Просмотрите распространенные ошибки клиентский компонент Центра обновления Windows и проверка справочник по коду ошибок
- Ознакомьтесь с другими ресурсами, которые помогут вам использовать клиентский компонент Центра обновления Windows
- Ознакомьтесь с разделом блога Windows IT Pro блога Майкрософт.

Архитектура единой платформы обновлений (UUP)

Чтобы понять изменения в архитектуре клиентский компонент Центра обновления Windows, которую представляет UUP, начнем с некоторых новых ключевых терминов.



- **Обновление пользовательского интерфейса** — пользовательский интерфейс для запуска клиентский компонент Центра обновления Windows проверка и журнала. Доступно в **разделе Параметры —> Обновление & безопасности — > клиентский компонент Центра обновления Windows**.

- **Update Session Orchestrator (USO)** — компонент ОС Windows, который управляет последовательностью скачивания и установки обновлений различных типов из клиентский компонент Центра обновления Windows.

  Типы обновлений-

  - Обновления компонентов ОС
  - Обновления системы безопасности ОС
  - Драйверы устройств
  - Обновления определений Defender

  > ⓘ **Примечание**
  >
  > Другие типы обновлений, такие как обновления классических приложений Office, устанавливаются, если пользователь выбирает Центр обновления Майкрософт.
  >
  > Приложения Магазина не устанавливаются USO, сегодня они являются отдельными.

- **клиентский компонент Центра обновления Windows Client/UpdateAgent** — компонент, работающий на компьютере. По сути, это библиотека DLL, которая загружается на устройство при необходимости обновления. Он отображает интерфейсы API, необходимые для выполнения обновления, в том числе те,

которые необходимы для создания списка полезных данных для скачивания, а также запуска операций этапа и фиксации. Он предоставляет единый интерфейс, который абстрагирует базовые технологии обновления от вызывающего объекта.

- **клиентский компонент Центра обновления Windows дескриптор arbiter** — код, включенный в двоичный файл UpdateAgent. Арбитр собирает сведения об устройстве и использует CompDB для вывода списка действий. Он отвечает за определение окончательного "состояния композиции" устройства и того, какие полезные данные (например, диски ESD или пакеты) необходимы для обновления устройства.

- **Администратор развертывания** — диспетчер развертывания, который вызывает различные установщики. Например, CBS.

К дополнительным компонентам относятся:

- **CompDB** — универсальный термин для обозначения XML-кода, описывающий сведения о композиции целевой сборки, доступных пакетах diff и условных правилах.
- **Список действий** — полезные данные и дополнительные сведения, необходимые для выполнения обновления. Список действий используется UpdateAgent, а также другими установщиками для определения полезных данных для скачивания. Он также потребляется агентом установки, чтобы определить, какие действия необходимо предпринять, например установку или удаление пакетов.

Файлы журнала Центра обновления Windows

Статья • 08.12.2023 • Применяется к: ✅ Windows 11, ✅ Windows 10

В следующей таблице описаны файлы журналов, созданные клиентский компонент Центра обновления Windows.

Развернуть таблицу

Файл журнала	Расположение	Описание	Варианты использования
Windowsupdate.log	C:\Windows\Logs\WindowsUpdate	Начиная с Windows 8.1 и продолжая Windows 10, клиентский компонент Центра обновления Windows клиент использует трассировку событий Windows (ETW) для создания журналов диагностики.	Если при запуске клиентский компонент Центра обновления Windows появляется сообщение об ошибке, можно использовать сведения, включенные в файл журнала Windowsupdate.log, для устранения проблемы.
UpdateSessionOrchestration.etl	C:\ProgramData\USOShared\Logs	Начиная с Windows 10 Служба оркестратора обновлений отвечает за последовательность скачивания и установки обновлений различных типов из клиентский компонент Центра обновления Windows. События регистрируются в этих ETL-файлах.	• Если вы видите, что обновления доступны, но скачивание не запускается. • Когда обновления скачиваются, но установка не активируется. • При установке обновлений, но перезагрузка не активируется.
NotificationUxBroker.etl	C:\ProgramData\USOShared\Logs	Начиная Windows 10, всплывающее	Если вы хотите проверка, было ли

Файл журнала	Расположение	Описание	Варианты использования
		уведомление или баннер активируются NotificationUxBroker.exe.	активировано уведомление.
Cbs.log	%systemroot%\Logs\CBS	Этот журнал содержит аналитические сведения об установке обновлений в стеке обслуживания.	Устранение неполадок, связанных с установкой клиентский компонент Центра обновления Windows.

Создание WindowsUpdate.log

Сведения о слиянии и преобразовании файлов трассировки клиентский компонент Центра обновления Windows (ETL-файлов) в один удобочитаемый WindowsUpdate.log файл см. в статье Get-WindowsUpdateLog.

> ⓘ **Примечание**
>
> При выполнении командлета **Get-WindowsUpdateLog** создается копия WindowsUpdate.log файла в виде статического файла журнала. Он не обновляется как старый WindowsUpdate.log, если вы не запустите **Get-WindowsUpdateLog** снова.

компоненты журнала клиентский компонент Центра обновления Windows

Подсистема клиентский компонент Центра обновления Windows имеет разные имена компонентов. Ниже приведены некоторые из наиболее распространенных компонентов, которые отображаются в файле WindowsUpdate.log.

- АГЕНТ — агент клиентский компонент Центра обновления Windows
- AU — эта задача выполняется автоматическим Обновления
- AUCLNT — взаимодействие между au и вошедшего в систему пользователя
- CDM- диспетчер устройств
- CMPRESS — агент сжатия
- КЛИЕНТСКИЙ КОМПОНЕНТ ЦЕНТРА ОБНОВЛЕНИЯ WINDOWS API COMAPI
- DRIVER — сведения о драйвере устройства
- DTASTOR — обрабатывает транзакции базы данных.
- EEHNDLER — обработчик выражений, используемый для оценки применимости обновлений.
- HANDLER — управляет установщиками обновлений.
- MISC — общие сведения об услугах

- OFFLSNC — обнаруживает доступные обновления без сетевого подключения.
- PARSER — синтаксический анализ сведений о выражении
- PT — синхронизирует сведения об обновлениях с локальным хранилищем данных.
- REPORT — собирает сведения о отчетах.
- SERVICE — запуск и завершение работы службы автоматического Обновления
- SETUP — устанавливает новые версии клиента клиентский компонент Центра обновления Windows, если он доступен.
- ФУНКЦИЯ SHUTDWN — установка при завершении работы
- WUREDIR — файлы перенаправления клиентский компонент Центра обновления Windows
- WUWEB — элемент управления ActiveX клиентский компонент Центра обновления Windows
- ProtocolTalker — синхронизация клиента и сервера
- DownloadManager — создает и отслеживает загрузки полезных данных
- Обработчик, установка — обработчики установщика (CBS и т. д.)
- EEHandler — оценка правил применимости обновлений
- Хранилище данных — локальное кэширование данных обновления
- IdleTimer — отслеживание активных вызовов, остановка службы

> ⓘ **Примечание**
>
> Многие сообщения журнала компонентов неоценимы, если вы ищете проблемы в этой конкретной области. Однако они могут быть бесполезными, если вы не будете фильтровать, чтобы исключить ненужные компоненты, чтобы вы могли сосредоточиться на том, что важно.

структура журнала клиентский компонент Центра обновления Windows

Структура журнала обновления Windows разделена на четыре main удостоверения:

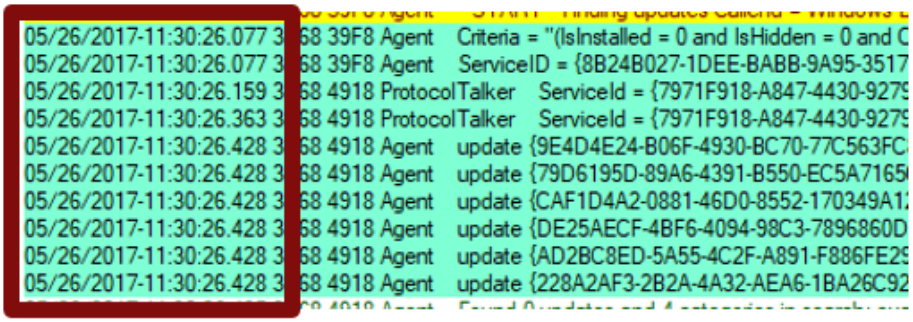
- Метки времени
- Идентификатор процесса и идентификатор потока
- Имя компонента
- Обновление идентификаторов
  - Идентификатор обновления и номер редакции
  - Идентификатор редакции
  - Локальный идентификатор
  - Несогласованная терминология

Структура WindowsUpdate.log рассматривается в следующих разделах.

Метки времени

Метка времени указывает время, в течение которого выполняется ведение журнала.

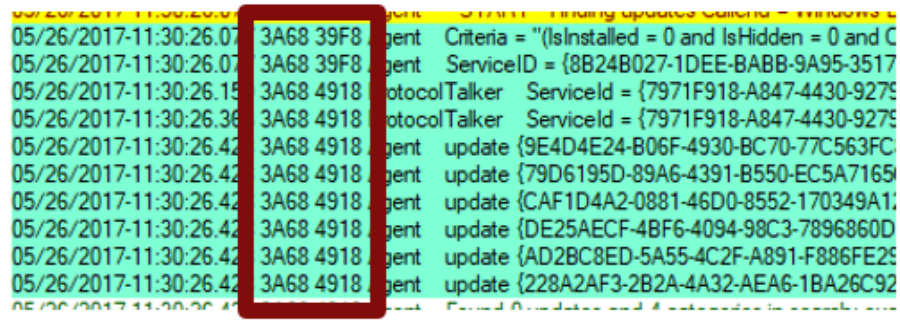
- Сообщения обычно находятся в хронологическом порядке, но могут возникать исключения.
- Пауза во время синхронизации может указывать на проблему с сетью, даже если проверка выполнена успешно.
- Длительная пауза ближе к концу сканирования может указывать на проблему цепочки замены.



Идентификатор процесса и идентификатор потока

Идентификаторы процессов и потоков являются случайными, и они могут отличаться от журнала к журналу и даже от сеанса службы к сеансу службы в одном журнале.

- Первые четыре цифры в шестнадцатеричном формате являются идентификатором процесса.
- Следующие четыре цифры в шестнадцатеричном формате являются идентификатором потока.
- Каждый компонент, например USO, обработчик клиентский компонент Центра обновления Windows, вызывающие COM API и обработчики установщика клиентский компонент Центра обновления Windows, имеет собственный идентификатор процесса.

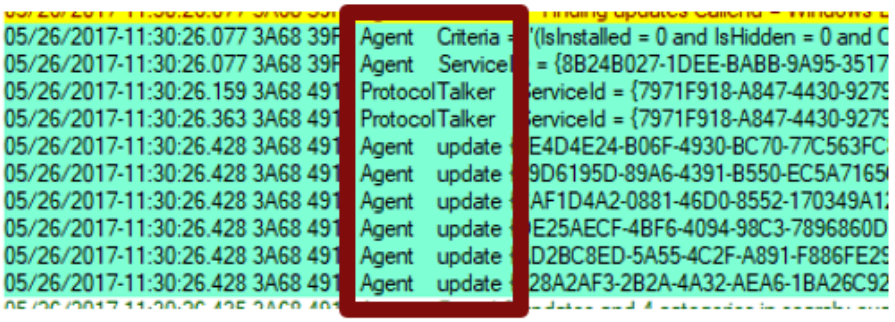


Имя компонента

Найдите и определите компоненты, связанные с идентификаторами. Разные части подсистемы клиентский компонент Центра обновления Windows имеют разные имена компонентов. Ниже перечислены некоторые из них.

- ProtocolTalker — синхронизация клиента и сервера
- DownloadManager — создает и отслеживает загрузки полезных данных
- Обработчик, установка — обработчики установщика (CBS и т. д.)
- EEHandler — оценка правил применимости обновлений
- Хранилище данных — локальное кэширование данных обновления

- IdleTimer — отслеживание активных вызовов, остановка службы



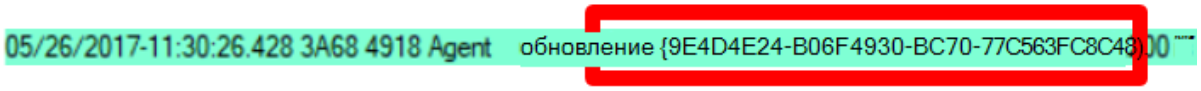
Обновление идентификаторов

Ниже перечислены идентификаторы обновлений.

Идентификатор обновления и номер редакции

Существуют разные идентификаторы для одного и того же обновления в разных контекстах. Важно знать схемы идентификаторов.

- Идентификатор обновления: guid (указанный на предыдущем снимке экрана), назначенный данному обновлению во время публикации.
- Номер редакции: число увеличивается каждый раз, когда данное обновление (с заданным идентификатором обновления) изменяется и повторно публикуется в службе.
- Номера редакций повторно используются из одного обновления в другое (не уникальный идентификатор).
- Идентификатор обновления и номер редакции часто отображаются вместе как "{GUID}.revision".



Идентификатор редакции

- Идентификатор редакции (не путайте это значение с номером редакции) — это серийный номер, выданный при первоначальной публикации или изменении обновления в данной службе.
- Существующее исправленное обновление сохраняет тот же идентификатор обновления (GUID), его номер редакции увеличивается (например, с 100 до 101), но получает новый идентификатор редакции, не связанный с предыдущим идентификатором.
- Идентификаторы редакций уникальны для заданного источника обновлений, но не в нескольких источниках.
- Одна и та же редакция обновления может иметь разные идентификаторы редакций в клиентский компонент Центра обновления Windows и WSUS.
- Один и тот же идентификатор редакции может представлять различные обновления в клиентский компонент Центра обновления Windows и WSUS.

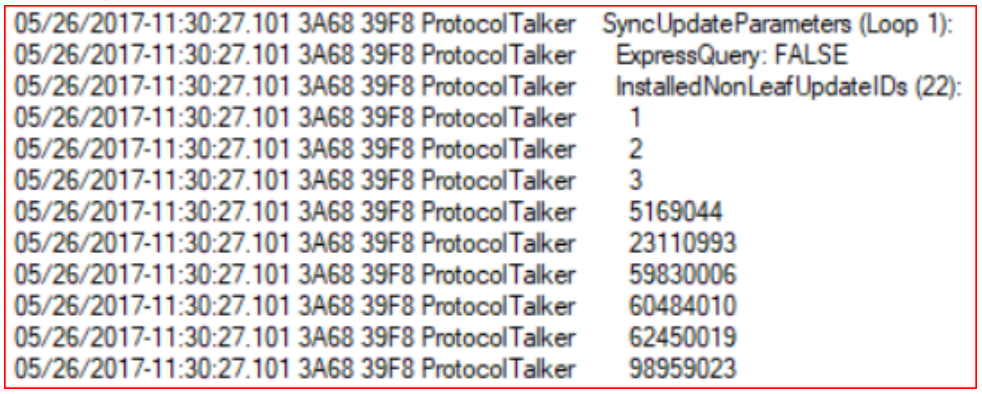
Локальный идентификатор

- Локальный идентификатор — это серийный номер, выданный клиентом клиентский компонент Центра обновления Windows при получении обновления от службы.
- Обычно встречается в журналах отладки, особенно с использованием локального кэша для сведений об обновлении (хранилище данных)
- Разные клиентские компьютеры назначают разные локальные идентификаторы для одного и того же обновления.
- Локальные идентификаторы, которые использует клиент, можно найти, получив файл %WINDIR%\SoftwareDistribution\Datastore\Datastore.edb.

Несогласованная терминология

- Иногда в журналах термины используются несогласованно. Например, список InstalledNonLeafUpdateIDs фактически содержит идентификаторы редакций, а не идентификаторы обновлений.

- Распознать идентификаторы по форме и контексту:
  - Идентификаторы guid — это идентификаторы обновлений
  - Небольшие целые числа, которые отображаются рядом с идентификатором обновления, являются номерами редакций.
  - Большие целые числа обычно являются идентификаторами редакций.
  - Небольшие целые числа (особенно в хранилище данных) могут быть локальными идентификаторами



Анализ файлов журнала программы установки Windows с помощью средства setupDiag

SetupDiag — это средство диагностики, которое можно использовать для анализа журналов, связанных с установкой windows Обновления. Подробные сведения см. в разделе SetupDiag.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Обновления стека обслуживания

Статья • 23.01.2025 • Применяется к: ✅ Windows 11, ✅ Windows 10, ✅ Windows Server

Что такое обновление стека обслуживания?

Обновления стека обслуживания предоставляют исправления для стека обслуживания, компонента, который устанавливает обновления Windows. Кроме того, он содержит стек обслуживания на основе компонентов (CBS), который является ключевым базовым компонентом для нескольких элементов развертывания Windows, таких как:

- Обслуживание образов развертывания и управление ими (DISM)
- Средство проверки системных файлов (SFC)
- Изменение функций или ролей Windows
- Восстановление компонентов

CBS — это небольшой компонент, который обычно не выпускает обновления каждый месяц.

В чем разница между обновлением стека обслуживания и накопительным обновлением?

Клиент Windows и Windows Server используют механизм накопительного обновления, в котором множество исправлений для повышения качества и безопасности Windows упаковываются в одно обновление. Каждое накопительное обновление включает изменения и исправления из всех предыдущих обновлений. Обновление стека обслуживания повышает надежность процесса обновления, чтобы устранить потенциальные проблемы при установке последнего ежемесячного обновления для системы безопасности и обновлений компонентов.

Начиная с февраля 2021 г. накопительное обновление включает последние обновления стека обслуживания, предоставляя единую совокупную полезную нагрузку для клиентский компонент Центра обновления Windows, Windows Server Update Services (WSUS) и каталога Центра обновления Майкрософт. Это совокупное ежемесячное накопительное обновление доступно в Windows 10 версии 2004 и более поздних, начиная с KB4601382. Если вы используете средство управления конечными точками при поддержке WSUS, например Configuration Manager, вам достаточно выбрать и развернуть ежемесячное накопительное обновление.

Последние обновления стека обслуживания автоматически применяются правильно. Заметки о выпуске и сведения о файлах накопительных обновлений, включая заметки и сведения, связанные с стеком обслуживания, приведены в одной статье базы знаний.

Когда они выпускаются?

Изменения в стеке обслуживания разрабатываются и выпускаются в рамках ежемесячного накопительного обновления в зависимости от новых проблем или уязвимостей. В редких случаях для решения проблемы, влияющей на установку ежемесячного накопительного обновления, может потребоваться выпуск обновления стека обслуживания предварительных требований. Обновления стека обслуживания вне диапазона классифицируются как безопасность с оценкой серьезности критической.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Накопительные обновления контрольных точек и использование каталога Центра обновления Майкрософт

Статья • 01.02.2025 •

Применяется к: ✅ Windows 11, version 24H2 and later, ✅ Windows Server 2025 and later

Начиная с Windows 11 версии 24H2 ежемесячные обновления для системы безопасности и необязательные обновления предварительной версии, не связанные с безопасностью, могут предшествовать накопительному обновлению контрольных точек. Устройства, обновляемые с каналов выпуска клиентский компонент Центра обновления Windows (WU) и Windows Server Update Services (WSUS), могут продолжать легко устанавливать последнее ежемесячное обновление для системы безопасности или дополнительный выпуск предварительной версии, не связанные с безопасностью, независимо от наличия каких-либо предыдущих накопительных обновлений контрольных точек, поэтому **Процессы обновления с использованием wu и WSUS остаются неизменными**. В этой статье описывается, как пользователи каталога Центра обновления Майкрософт могут легко обновлять свои устройства (или образы) с помощью накопительных обновлений контрольных точек.

Накопительные обновления контрольных точек

Windows 11 обновления качества используют технологию обслуживания и создаются совокупно с момента выпуска новой ОС Windows до производства (RTM). Эти ежемесячные обновления включают все изменения, начиная с RTM, в виде двоичных дифференциалов, вычисляемых из начальной версии этих двоичных файлов.

В Windows 11 версии 24H2 корпорация Майкрософт представила новую концепцию накопительных обновлений контрольных точек. Это изменение позволяет получать функции и улучшения безопасности с помощью последнего накопительного обновления через небольшие добавочные дифференциалы, содержащие только изменения с момента предыдущего накопительного обновления контрольных точек. Это изменение означает, что вы можете сэкономить время, пропускную способность и место на жестком диске.

В дальнейшем корпорация Майкрософт может периодически выпускать накопительные обновления в качестве контрольных точек. Последующие обновления будут состоять из следующих:

- Файлы пакета обновления, связанные с контрольными точками, и
- Новые файлы пакетов обновления, содержащие добавочные двоичные различия по отношению к версии двоичных файлов в последней контрольной точке.

Этот процесс может повторяться несколько раз, создавая тем самым несколько контрольных точек в течение жизненного цикла конкретного выпуска Windows. Стек обслуживания Windows 11 версии 24H2 может объединять все контрольные точки и скачивать и устанавливать только содержимое, отсутствующее на устройстве.

Если какие-либо накопительные обновления контрольных точек предшествуют целевому обновлению, устройство или образ должны принять все предыдущие накопительные обновления контрольных точек, прежде чем они смогут принять целевое обновление. Другими словами, последнее накопительное обновление после контрольной точки можно применить к образам или устройствам, которые находятся на этой контрольной точке или в последующем последнем накопительном обновлении. Для обновлений, полученных из WU и WSUS, этот процесс выполняется легко. Вы можете продолжать использовать те же средства и процессы, которые используются в настоящее время для утверждения и развертывания обновлений. Мы ожидаем, что процесс обновления с помощью накопительного обновления контрольных точек позволит эффективно принимать будущие накопительные обновления контрольных точек.

Применимость

Накопительное обновление контрольных точек — это еще одно ежемесячное обновление для системы безопасности, информирующее о том, как создаются последующие обновления. Когда пользователи должны принимать эти обновления, нет никаких изменений в политике или новых требований, хотя рекомендуется принимать ежемесячные обновления для системы безопасности при первой возможности, чтобы обеспечить защиту и производительность ваших устройств.

Обновление установочного носителя Windows

Эта функция не вносит никаких изменений в применимость ежемесячных обновлений для системы безопасности. Как и ранее, эти обновления применяются к ос main (install.wim) и WinPE (boot.wim), но не к WinRE (winre.wim).

WinRE обслуживается путем применения обновления стека обслуживания из накопительного обновления (последнее накопительное обновление не применяется) и динамического обновления SafeOS. Вот как это было в течение некоторого времени, и нет никаких последних изменений в обслуживании WinRE и, конечно, никаких изменений из-за функции накопительных обновлений контрольных точек. Мы понимаем, что не все, возможно, имели общее представление об этом, но применение обновления стека обслуживания, а затем динамическое обновление SafeOS является единственным способом обеспечить обслуживание WinRE. Дополнительные сведения см. в разделе Обновление установочного носителя Windows с помощью динамического обновления.

Обновление из каталога Центра обновления Майкрософт

При установке определенного ежемесячного обновления для системы безопасности или дополнительного обновления предварительной версии, не относящихся к безопасности, пользователи каталога Центра обновления Майкрософт могут определять и скачивать предыдущие накопительные обновления контрольных точек и применять их последовательно в определенных ситуациях или за один раз с помощью службы обслуживания образов развертывания и управления ими (DISM).

Поиск предыдущих накопительных обновлений контрольных точек

Для данного обновления пользователи могут найти статью базы знаний и найти все предыдущие контрольные точки(если таковые имеются) в канале выпуска **каталога** . Например, ежемесячное обновление для системы безопасности 2024-12 (KB5048667) содержит одно предыдущее накопительное обновление контрольных точек за 10 декабря 2024 г. по KB5048667 г. (сборка ОС 26100.2605):

> **Установка каждого файла MSU по отдельности по порядку**
>
> Скачайте и установите каждый файл MSU по отдельности с помощью DISM или клиентский компонент Центра обновления Windows автономного установщика в следующем порядке:

- windows11.0-kb5043080-x64_953449672073f8fb99badb4cc6d5d7849b9c83e8.msu
- windows11.0-kb5048667-x64_d4ad0ca69de9a02bc356757581e0e0d6960c9f93.msu

Кроме того, пользователи могут выполнить поиск по номеру базы знаний в каталоге Центра обновления Майкрософт и нажать кнопку **Скачать** для выбранной архитектуры. Во всплывающем окне загрузки отображаются все предыдущие контрольные точки для обновления, чтобы пользователи могли удобно скачать все `.msu` файлы и применить их к своему образу или устройству. Например, в каталоге Центра обновления Майкрософт отображается накопительное обновление 2024-12 (KB5048667) с одним предыдущим накопительным обновлением контрольной точки , KB5043080.

Обновление с помощью накопительных обновлений контрольных точек

Устройство имеет последнее накопительное обновление контрольной точки и не нуждается в настройке:

Устройства или образы, на которых установлено последнее накопительное обновление контрольных точек и не требуются функции по запросу (FoD) или настройка языкового пакета, можно обновить до последнего целевого накопительного обновления, не изменив существующий процесс. Вы можете скопировать целевой `.msu` файл из каталога Центра обновления Майкрософт и установить его, например с помощью параметров командной строки для обслуживания пакета операционной системы DISM (.cabили .msu).

Примеры подходящих устройств:

Развернуть таблицу

Устройство включено	Требуется установить
• Накопительное обновление контрольных точек, 2024-09 (KB5043080)	• Последующее ежемесячное обновление для системы безопасности, например 2024-11 (KB5046617) или • Последующий дополнительный выпуск, отличный от безопасности, например 2024-11 (KB5046740)

Устройство включено	Требуется установить
• Последующий дополнительный предварительный выпуск без безопасности, например 2024-09 (KB5043178), или • Последующее ежемесячное обновление для системы безопасности, например 2024-10 (KB5044284)	• Последующее ежемесячное обновление для системы безопасности, например 2025-01 (KB5050009), или • Последующий дополнительный выпуск, отличный от безопасности, например 2024-11 (KB5046740)

Для устройства требуется настройка FoD или языкового пакета:

Для установки FoD-файлов или языковых пакетов требуется полная последняя полезная нагрузка накопительного обновления, которую теперь можно разделить между файлами, связанными с каждым предыдущим накопительным обновлением контрольных точек. Таким образом, при настройке FoD или языковых пакетов для автономного носителя необходимо установить все предыдущие накопительные обновления контрольных точек и целевое накопительное обновление независимо от того, было ли установлено на устройстве какое-либо из предыдущих контрольных точек накопительное обновление. Это необходимо сделать с помощью DISM.

1. Скопируйте MSU-файлы последнего накопительного обновления (целевого) и всех предыдущих накопительных обновлений контрольных точек в локальную папку. Убедитесь, что отсутствуют другие MSU-файлы.
2. Подключите файл install.wim.
3. Запустите `DISM /add-package` с последним `.msu` файлом в качестве единственного целевого объекта.
4. Выполните команду `/Cleanup-Image /StartComponentCleanup`.
5. Отключить.
6. Выполните команду `DISM /export-image` , чтобы оптимизировать размер изображения, если это важно для вас.

Устройство не имеет последнего накопительного обновления контрольных точек и не нуждается в настройке:

Устройства, которые не установлены на последнем накопительном обновлении контрольных точек и не нуждаются в настройке FoD или языкового пакета, могут установить все необходимые накопительные обновления по одному в правильной последовательности. Кроме того, их можно обновить с помощью DISM, чтобы установить все накопительные обновления за один раз. Дополнительные сведения см. в разделе Накопительные обновления с помощью контрольных точек . Если доступно в общей сложности четыре накопительных обновления контрольных

точек и на устройстве уже установлено первое, DISM применяет оставшиеся три накопительных обновления контрольных точек в правильном порядке, за которым следует целевое накопительное обновление.

Связанные статьи

- Обновления стека обслуживания
- Функции по запросу
- Скачивание обновлений, включающих драйверы и исправления, из каталога Центра обновления Майкрософт
- Обновление установочного носителя Windows с помощью динамического обновления

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Поставщик CSP политики — обновление

Политики обновления CSP перечислены ниже в зависимости от области групповой политики:

- Управление обновлениями, предлагаемыми из клиентский компонент Центра обновления Windows
  - AllowNonMicrosoftSignedUpdate
  - AllowOptionalContent
  - AutomaticMaintenanceWakeUp
  - BranchReadinessLevel
  - DeferFeatureUpdatesPeriodInDays
  - DeferQualityUpdatesPeriodInDays
  - DisableWUfBSafeguards
  - ExcludeWUDriversInQualityUpdate
  - ManagePreviewBuilds
  - PauseFeatureUpdates
  - PauseFeatureUpdatesStartTime
  - PauseQualityUpdates
  - PauseQualityUpdatesStartTime
  - ProductVersion
  - TargetReleaseVersion
- Управление обновлениями, предлагаемыми из службы обновлений Windows Server
  - AllowUpdateService
  - DetectionFrequency
  - DoNotEnforceEnterpriseTLSCertPinningForUpdateDetection
  - FillEmptyContentUrls
  - SetPolicyDrivenUpdateSourceForDriverUpdates
  - SetPolicyDrivenUpdateSourceForFeatureUpdates
  - SetPolicyDrivenUpdateSourceForOtherUpdates
  - SetPolicyDrivenUpdateSourceForQualityUpdates
  - SetProxyBehaviorForUpdateDetection
  - UpdateServiceUrl
  - UpdateServiceUrlAlternate
- Управление взаимодействием с конечными пользователями
  - ActiveHoursEnd
  - ActiveHoursMaxRange
  - ActiveHoursStart
  - AllowAutoUpdate
  - AllowAutoWindowsUpdateDownloadOverMeteredNetwork
  - AllowMUUpdateService

- AllowTemporaryEnterpriseFeatureControl
- ConfigureDeadlineForFeatureUpdates
- ConfigureDeadlineForQualityUpdates
- ConfigureDeadlineGracePeriod
- ConfigureDeadlineGracePeriodForFeatureUpdates
- ConfigureDeadlineNoAutoRebootForFeatureUpdates
- ConfigureDeadlineNoAutoRebootForQualityUpdates
- ConfigureFeatureUpdateUninstallPeriod
- NoUpdateNotificationsDuringActiveHours
- ScheduledInstallDay
- ScheduledInstallEveryWeek
- ScheduledInstallFirstWeek
- ScheduledInstallFourthWeek
- ScheduledInstallSecondWeek
- ScheduledInstallThirdWeek
- ScheduledInstallTime
- SetDisablePauseUXAccess
- SetDisableUXWUAccess
- SetEDURestart
- UpdateNotificationLevel

- Устаревшие политики
  - AlwaysAutoRebootAtScheduledTimeMinutes
  - AutoRestartDeadlinePeriodInDays
  - AutoRestartDeadlinePeriodInDaysForFeatureUpdates
  - AutoRestartNotificationSchedule
  - AutoRestartRequiredNotificationDismissal
  - DeferUpdatePeriod
  - DeferUpgradePeriod
  - DisableDualScan
  - EngagedRestartDeadline
  - EngagedRestartDeadlineForFeatureUpdates
  - EngagedRestartSnoozeSchedule
  - EngagedRestartSnoozeScheduleForFeatureUpdates
  - EngagedRestartTransitionSchedule
  - EngagedRestartTransitionScheduleForFeatureUpdates
  - IgnoreMOAppDownloadLimit
  - IgnoreMOUpdateDownloadLimit
  - PauseDeferrals
  - PhoneUpdateRestrictions
  - RequireDeferUpgrade
  - RequireUpdateApproval

- ScheduleImminentRestartWarning
- ScheduleRestartWarning
- SetAutoRestartNotificationDisable

Управление обновлениями, предлагаемыми из клиентский компонент Центра обновления Windows

AllowNonMicrosoftSignedUpdate

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования ✅ IIoT Enterprise или IoT Enterprise LTSC	✅Windows 10, версия 1507 [10.0.10240] и более поздние

Device

```
./Device/Vendor/MSFT/Policy/Config/Update/AllowNonMicrosoftSignedUpdate
```

Позволяет ИТ-администратору управлять тем, принимает ли функция автоматического обновления те обновления, которые подписаны другими разработчиками помимо корпорации Майкрософт, когда обновление обнаруживается в расположении UpdateServiceUrl. Эта политика поддерживает использование WSUS для распространения стороннего программного обеспечения и исправлений. Эта политика относится к публикациям в классических и локальных средах посредством WSUS для сторонних обновлений (двоичные файлы и обновления, не размещающиеся в Центре обновления Майкрософт) и позволяет ИТ-отделу указывать, принимает ли служба автоматических обновлений те обновления, которые подписаны организациями, отличными от Майкрософт, при обнаружении обновления в расположении службы обновлений Майкрософт в интрасети.

Описание свойств инфраструктуры:

Развернуть таблицу

Имя свойства	Значение свойства
Формат	`int`
Тип доступа	Добавить, удалить, получить, заменить
Значение по умолчанию	1

Допустимые значения:

Развернуть таблицу

Значение	Описание
0	Не разрешено или не настроено. Обновления из службы обновления Майкрософт в интрасети должны быть подписаны корпорацией Майкрософт.
1 (по умолчанию)	Разрешено. Принимает обновления, полученные через расположение службы обновлений Майкрософт в интрасети, если они подписаны сертификатом, найденным в хранилище сертификатов "Доверенные издатели" локального компьютера.

AllowOptionalContent

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования ✅ IIoT Enterprise или IoT Enterprise LTSC	✅Windows 10 версии 21H2 [10.0.19044.3757] и более поздних версий

Device

```
./Device/Vendor/MSFT/Policy/Config/Update/AllowOptionalContent
```

Эта политика позволяет устройствам получать необязательные обновления (в том числе постепенное развертывание функций (CFR). Дополнительные сведения см. на странице aka.ms/AllowOptionalContent).

При настройке политики.

- Если выбран параметр "Автоматически получать необязательные обновления (включая cfR)", устройство автоматически получит последние необязательные обновления в соответствии с настроенными отсрочками обновлений качества. Сюда входят необязательные накопительные обновления и постепенное развертывание компонентов (CFR).
- Если выбран параметр "Автоматически получать необязательные обновления", устройство будет получать только необязательные накопительные обновления автоматически в соответствии с отсрочками обновлений качества.
- Если выбран параметр "Пользователи могут выбрать необязательные обновления для получения", пользователи могут выбрать, какие необязательные обновления следует получить, перейдя в раздел Параметры > клиентский компонент Центра обновления Windows > Дополнительные параметры > Необязательные обновления. Пользователи также могут включить переключатель "Получить последние обновления, как только они будут доступны", чтобы автоматически получать необязательные обновления и постепенное развертывание функций.

Описание свойств инфраструктуры:

Развернуть таблицу

Имя свойства	Значение свойства
Формат	`int`
Тип доступа	Добавить, удалить, получить, заменить
Значение по умолчанию	0

Допустимые значения:

Развернуть таблицу

Значение	Описание
0 (по умолчанию)	Не получайте необязательные обновления.
1	Автоматически получать необязательные обновления (включая cfr).
2	Автоматически получать необязательные обновления.
3	Пользователи могут выбрать необязательные обновления для получения.

Сопоставление групповой политики:

Развернуть таблицу

Имя	Значение
Имя	AllowOptionalContent
Понятное имя	Включение необязательных обновлений
Location	Конфигурация компьютера
Путь	Компоненты > Windows клиентский компонент Центра обновления Windows > Управление обновлениями, предлагаемыми из клиентский компонент Центра обновления Windows
Имя раздела реестра	Software\Policies\Microsoft\Windows\WindowsUpdate
Имя значения реестра	SetAllowOptionalContent
Имя файла ADMX	WindowsUpdate.admx

AutomaticMaintenanceWakeUp

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования ✅ IIoT Enterprise или IoT Enterprise LTSC	✅Windows 10, версия 1903 [10.0.18362] и более поздние

Device

```
./Device/Vendor/MSFT/Policy/Config/Update/AutomaticMaintenanceWakeUp
```

Этот параметр политики позволяет настроить политику пробуждения автоматического обслуживания.

Политика пробуждения обслуживания указывает, должно ли автоматическое обслуживание отправлять запрос на пробуждение ос для ежедневного запланированного

обслуживания. Обратите внимание, что если политика пробуждения питания ОС явно отключена, этот параметр не действует.

- Если этот параметр политики включен, автоматическое обслуживание попытается задать политику пробуждения ОС и при необходимости отправить запрос на пробуждение в течение ежедневного запланированного времени.
- Если этот параметр политики отключен или не настроен, применяется параметр пробуждения, указанный в разделе Безопасность и обслуживание и автоматическое обслуживание панель управления.

Описание свойств инфраструктуры:

Развернуть таблицу

Имя свойства	Значение свойства
Формат	`int`
Тип доступа	Добавить, удалить, получить, заменить
Значение по умолчанию	1

Допустимые значения:

Развернуть таблицу

Значение	Описание
0	Отключено.
1 (по умолчанию)	Включено.

Сопоставление групповой политики:

Развернуть таблицу

Имя	Значение
Имя	WakeUpPolicy
Понятное имя	Политика пробуждения автоматического обслуживания
Location	Конфигурация компьютера
Путь	Планировщик обслуживания компонентов > Windows
Имя раздела реестра	Software\Policies\Microsoft\Windows\Task Scheduler\Maintenance

Имя	Значение
Имя значения реестра	Пробуждения
Имя файла ADMX	msched.admx

BranchReadinessLevel

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования ✅ IIoT Enterprise или IoT Enterprise LTSC	✅Windows 10, версия 1607 [10.0.14393] и более поздние

Device

```
./Device/Vendor/MSFT/Policy/Config/Update/BranchReadinessLevel
```

Включите эту политику, чтобы указать, когда следует получать Обновления компонентов.

Отложить Обновления | Это позволяет устройствам отложить принятие следующего обновления компонентов, доступного для текущего продукта (или нового продукта, если указано в политике Выбор версии целевого обновления компонентов). Обновление компонентов можно отложить на 14 дней для всех каналов предварительной версии и до 365 дней для канала общей доступности. Дополнительные сведения о текущих выпусках см. в разделе aka.ms/WindowsTargetVersioninfo.

Приостановка Обновления | Чтобы предотвратить предложение Обновления компонентов на устройстве, можно временно приостановить Обновления компонентов. Эта пауза будет действовать в течение 35 дней с указанной даты начала или до тех пор, пока поле не будет очищено. Обратите внимание, что Обновления качества по-прежнему будет предлагаться, даже если Обновления функций приостановлены.

Описание свойств инфраструктуры:

Развернуть таблицу

Имя свойства	Значение свойства
Формат	`int`
Тип доступа	Добавить, удалить, получить, заменить
Значение по умолчанию	16

Допустимые значения:

Развернуть таблицу

Значение	Описание
2	{0x2} — сборка программы предварительной оценки Windows — Fast (добавлена в Windows 10, версия 1709).
4	{0x4} — сборка программы предварительной оценки Windows — slow (добавлена в Windows 10 версии 1709).
8	{0x8} — выпуск сборки программы предварительной оценки Windows (добавлена в Windows 10, версия 1709).
16 (по умолчанию)	{0x10} — полугодовой канал (целевой). Устройство получает все применимые обновления компонентов из semi-annual Channel (Targeted).
32	2 {0x20} — полугодовой канал. Устройство получает обновления компонентов из semi-annual Channel. (* Применимо только к выпускам до 1903 года, для всех выпусков 1903 года и после semi-annual Channel и Semi-annual Channel (Targeted) в один semi-annual Channel со значением 16).
64	{0x40} — выпуск предварительной версии только Обновления качества.
128	{0x80} — Канал Canary.

Сопоставление групповой политики:

Развернуть таблицу

Имя	Значение
Имя	DeferFeatureUpdates
Понятное имя	Выбор момента получения предварительных сборок и Обновления компонентов
Location	Конфигурация компьютера
Путь	Компоненты > Windows клиентский компонент Центра обновления Windows > Управление обновлениями, предлагаемыми из клиентский компонент Центра

Имя	Значение
	обновления Windows
Имя раздела реестра	Software\Policies\Microsoft\Windows\WindowsUpdate
Имя файла ADMX	WindowsUpdate.admx

DeferFeatureUpdatesPeriodInDays

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования ✅ IIoT Enterprise или IoT Enterprise LTSC	✅Windows 10, версия 1607 [10.0.14393] и более поздние

Device

```
./Device/Vendor/MSFT/Policy/Config/Update/DeferFeatureUpdatesPeriodInDays
```

Включите эту политику, чтобы указать, когда следует получать Обновления компонентов.

Отложить Обновления | Это позволяет устройствам отложить принятие следующего обновления компонентов, доступного для текущего продукта (или нового продукта, если указано в политике Выбор версии целевого обновления компонентов). Обновление компонентов можно отложить на 14 дней для всех каналов предварительной версии и до 365 дней для канала общей доступности. Дополнительные сведения о текущих выпусках см. в разделе aka.ms/WindowsTargetVersioninfo.

Приостановка Обновления | Чтобы предотвратить предложение Обновления компонентов на устройстве, можно временно приостановить Обновления компонентов. Эта пауза будет действовать в течение 35 дней с указанной даты начала или до тех пор, пока поле не будет очищено. Обратите внимание, что Обновления качества по-прежнему будет предлагаться, даже если Обновления функций приостановлены.

Описание свойств инфраструктуры:

Развернуть таблицу

Имя свойства	Значение свойства
Формат	`int`
Тип доступа	Добавить, удалить, получить, заменить
Допустимые значения	Диапазон: `[0-365]`
Значение по умолчанию	0

Сопоставление групповой политики:

Развернуть таблицу

Имя	Значение
Имя	DeferFeatureUpdates
Понятное имя	Выбор момента получения предварительных сборок и Обновления компонентов
Имя элемента	Через сколько дней после выпуска обновления компонентов вы хотите отложить обновление, прежде чем оно будет предложено устройству?
Location	Конфигурация компьютера
Путь	Компоненты > Windows клиентский компонент Центра обновления Windows > Управление обновлениями, предлагаемыми из клиентский компонент Центра обновления Windows
Имя раздела реестра	Software\Policies\Microsoft\Windows\WindowsUpdate
Имя файла ADMX	WindowsUpdate.admx

DeferQualityUpdatesPeriodInDays

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования	✅Windows 10, версия 1607 [10.0.14393] и более поздние

Область применения	Выпуски	Применимая ОС
	✅ IIoT Enterprise или IoT Enterprise LTSC	

Device

```
./Device/Vendor/MSFT/Policy/Config/Update/DeferQualityUpdatesPeriodInDays
```

Включите эту политику, чтобы указать, когда следует получать обновления качества.

Вы можете отложить получение обновлений качества до 30 дней.

Чтобы предотвратить получение обновлений качества в запланированное время, можно временно приостановить обновления качества. Пауза будет действовать в течение 35 дней или до тех пор, пока вы не очистите поле даты начала.

Чтобы возобновить получение приостановленных Обновления качества, очистите поле даты начала.

Если вы отключите или не настроите эту политику, клиентский компонент Центра обновления Windows не изменит ее поведение.

Описание свойств инфраструктуры:

Развернуть таблицу

Имя свойства	Значение свойства
Формат	`int`
Тип доступа	Добавить, удалить, получить, заменить
Допустимые значения	Диапазон: `[0-30]`
Значение по умолчанию	0

Сопоставление групповой политики:

Развернуть таблицу

Имя	Значение
Имя	DeferQualityUpdates
Понятное	Выбор момента получения Обновления качества

Имя	Значение
имя	
Имя элемента	После выпуска обновления качества отложите его получение на это много дней.
Location	Конфигурация компьютера
Путь	Компоненты > Windows клиентский компонент Центра обновления Windows > Управление обновлениями, предлагаемыми из клиентский компонент Центра обновления Windows
Имя раздела реестра	Software\Policies\Microsoft\Windows\WindowsUpdate
Имя файла ADMX	WindowsUpdate.admx

DisableWUfBSafeguards

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования ✅ IIoT Enterprise или IoT Enterprise LTSC	✅Windows 10, версия 1809 с KB4577069 [10.0.17763.1490] и более поздних версий ✅Windows 10 версии 1903 с KB4577062 [10.0.18362.1110] и более поздних версий ✅Windows 10 версии 1909 с KB4577062 [10.0.18363.1110] и более поздних версий ✅Windows 10 версии 2004 с KB4577063 [10.0.19041.546] и более поздних версий ✅Windows 11, версия 21H2 [10.0.22000] и более поздние

Device

```
./Device/Vendor/MSFT/Policy/Config/Update/DisableWUfBSafeguards
```

Этот параметр политики указывает, что устройство клиентский компонент Центра обновления Windows для бизнеса должно пропускать меры безопасности.

Защитные удержания предотвращают предложение новой версии ОС устройству с известной проблемой совместимости. Предложение будет продолжено после того, как

будет выдано исправление и проверено на удерживаемом устройстве. Цель мер безопасности — защитить устройство и пользователя от неудачного или плохого обновления. Защита от удержания по умолчанию предоставляется всем устройствам, пытающимся обновиться до новой версии Windows 10 обновления компонентов через клиентский компонент Центра обновления Windows.

ПРИ необходимости ИТ-администраторы могут отказаться от защиты устройств с помощью этого параметра политики или с помощью групповая политика **Отключить меры безопасности для Обновления компонентов**.

> ⓘ **Примечание.**
>
> Отказ от мер безопасности может поставить устройства под угрозу из-за известных проблем с производительностью. Мы рекомендуем отказаться только в ИТ-среде для целей проверки. Кроме того, вы можете использовать канал предварительной версии программы предварительной оценки Windows для бизнеса, чтобы проверить предстоящую версию обновления компонентов Windows 10 без применения мер безопасности.
>
> После перехода на новую версию Windows 10 политика защиты будет отменить изменения значение "Не настроено" на устройстве, даже если она была включена ранее. Это гарантирует, что администратор сознательно отключает защиту майкрософт по умолчанию от известных проблем для каждого нового обновления компонентов.
>
> Отключение мер безопасности не гарантирует, что устройство сможет успешно обновиться. Обновление по-прежнему может завершиться ошибкой на устройстве и, скорее всего, приведет к плохому опыту после обновления, так как вы обходите защиту, предоставленную корпорацией Майкрософт, относящуюся к известным проблемам.

Описание свойств инфраструктуры:

Развернуть таблицу

Имя свойства	Значение свойства
Формат	`int`
Тип доступа	Добавить, удалить, получить, заменить
Значение по умолчанию	0

Допустимые значения:

Развернуть таблицу

Значение	Описание
0 (по умолчанию)	Меры безопасности включены, и устройства могут быть заблокированы для обновления до тех пор, пока не будет снята защита.
1	Меры безопасности не включены, и обновления будут развернуты без блокировки мер безопасности.

ExcludeWUDriversInQualityUpdate

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования ✅ IIoT Enterprise или IoT Enterprise LTSC	✅Windows 10, версия 1607 [10.0.14393] и более поздние

Device

```
./Device/Vendor/MSFT/Policy/Config/Update/ExcludeWUDriversInQualityUpdate
```

Включите эту политику, чтобы не включать драйверы в исправления Windows.

Если эта политика отключена или не настроена, клиентский компонент Центра обновления Windows будут включать обновления с классификацией драйверов.

Описание свойств инфраструктуры:

Развернуть таблицу

Имя свойства	Значение свойства
Формат	`int`
Тип доступа	Добавить, удалить, получить, заменить
Значение по умолчанию	0

Допустимые значения:

Развернуть таблицу

Значение	Описание
0 (по умолчанию)	Разрешить драйверы клиентский компонент Центра обновления Windows.
1	Исключите драйверы клиентский компонент Центра обновления Windows.

Сопоставление групповой политики:

Развернуть таблицу

Имя	Значение
Имя	ExcludeWUDriversInQualityUpdate
Понятное имя	Исключать драйверы из обновлений Windows
Location	Конфигурация компьютера
Путь	Компоненты > Windows клиентский компонент Центра обновления Windows > Управление обновлениями, предлагаемыми из клиентский компонент Центра обновления Windows
Имя раздела реестра	Software\Policies\Microsoft\Windows\WindowsUpdate
Имя значения реестра	ExcludeWUDriversInQualityUpdate
Имя файла ADMX	WindowsUpdate.admx

ManagePreviewBuilds

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования	✅Windows 10, версия 1709 [10.0.16299] и более поздние

Область применения	Выпуски	Применимая ОС
	✅ IIoT Enterprise или IoT Enterprise LTSC	

Device

```
./Device/Vendor/MSFT/Policy/Config/Update/ManagePreviewBuilds
```

Включите эту политику, чтобы управлять обновлениями, которые вы получаете до выпуска обновления в мире.

Канал разработки.

Идеально подходит для технически подкованных пользователей. Участники программы предварительной оценки в Канале разработки будут получать сборки из нашей активной ветви разработки, которая находится в самом раннем цикле разработки. Эти сборки не соответствуют конкретному выпуску Windows 10.

Бета-канал.

Идеально подходит для обозревателей функций, которые хотят увидеть предстоящие Windows 10 функции. Ваш отзыв будет особенно важен здесь, так как он поможет нашим инженерам убедиться, что ключевые проблемы будут устранены перед крупным выпуском.

Канал предварительной версии выпуска (по умолчанию) участники программы предварительной оценки в канале предварительной версии выпуска будут иметь доступ к предстоящему выпуску Windows 10, прежде чем он будет выпущен в мире. Эти сборки поддерживаются корпорацией Майкрософт. Канал предварительной версии выпуска — это место, где мы рекомендуем компаниям предварительной версии и проверить предстоящие Windows 10 выпуски перед широким развертыванием в организации.

Канал предварительной версии выпуска, только качество Обновления.

Идеально подходит для тех, кто хочет проверить функции и исправления, доступные в ближайшее время до текущей версии. Обратите внимание, что выпущенные обновления компонентов будут по-прежнему предлагаться в соответствии с настроенными политиками при выборе этого параметра.

> ⓘ **Примечание.**
>
> Для регистрации предварительной версии сборки требуется параметр уровня телеметрии 2 или выше, а домен зарегистрирован на insider.windows.com.

Дополнительные сведения о предварительных сборках см. в разделе: https://aka.ms/wipforbiz

Если вы отключите или не настроите эту политику, клиентский компонент Центра обновления Windows не будет предлагать вам никаких предварительных обновлений, и вы получите такое содержимое после выпуска в мире. Отключение этой политики приведет к тому, что все устройства, которые сейчас находятся в предварительной сборке, откажутся и останутся на последнем обновлении компонентов после выпуска.

Описание свойств инфраструктуры:

Развернуть таблицу

Имя свойства	Значение свойства
Формат	`int`
Тип доступа	Добавить, удалить, получить, заменить
Значение по умолчанию	3

Допустимые значения:

Развернуть таблицу

Значение	Описание
0	Отключите предварительные сборки.
1	Отключите предварительные сборки, когда следующий выпуск будет общедоступным.
2	Включите предварительные сборки.
3 (по умолчанию)	Предварительный просмотр сборок остается для выбора пользователем.

Сопоставление групповой политики:

Развернуть таблицу

Имя	Значение
Имя	ManagePreviewBuilds
Понятное имя	Управление предварительными сборками

Имя	Значение
Location	Конфигурация компьютера
Путь	Компоненты > Windows клиентский компонент Центра обновления Windows > Управление обновлениями, предлагаемыми из клиентский компонент Центра обновления Windows
Имя раздела реестра	Software\Policies\Microsoft\Windows\WindowsUpdate
Имя файла ADMX	WindowsUpdate.admx

PauseFeatureUpdates

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования ✅ IIoT Enterprise или IoT Enterprise LTSC	✅Windows 10, версия 1607 [10.0.14393] и более поздние

Device

```
./Device/Vendor/MSFT/Policy/Config/Update/PauseFeatureUpdates
```

Включите эту политику, чтобы указать, когда следует получать Обновления компонентов.

Отложить Обновления | Это позволяет устройствам отложить принятие следующего обновления компонентов, доступного для текущего продукта (или нового продукта, если указано в политике Выбор версии целевого обновления компонентов). Обновление компонентов можно отложить на 14 дней для всех каналов предварительной версии и до 365 дней для канала общей доступности. Дополнительные сведения о текущих выпусках см. в разделе aka.ms/WindowsTargetVersioninfo.

Приостановка Обновления | Чтобы предотвратить предложение Обновления компонентов на устройстве, можно временно приостановить Обновления компонентов. Эта пауза будет действовать в течение 35 дней с указанной даты начала или до тех пор,

пока поле не будет очищено. Обратите внимание, что Обновления качества по-прежнему будет предлагаться, даже если Обновления функций приостановлены.

> ⓘ **Примечание.**
>
> Мы рекомендуем использовать политику Update/PauseFeatureUpdatesStartTime, если вы используете Windows 10 версии 1703 или более поздней.

Описание свойств инфраструктуры:

Развернуть таблицу

Имя свойства	Значение свойства
Формат	`int`
Тип доступа	Добавить, удалить, получить, заменить
Значение по умолчанию	0

Допустимые значения:

Развернуть таблицу

Значение	Описание
0 (по умолчанию)	Обновления функций не приостанавливаются.
1	Обновления функций приостанавливаются на 60 дней или до тех пор, пока значение не будет возвращено в значение 0, в зависимости от того, что наступит раньше.

Сопоставление групповой политики:

Развернуть таблицу

Имя	Значение
Имя	DeferFeatureUpdates
Понятное имя	Выбор момента получения предварительных сборок и Обновления компонентов
Location	Конфигурация компьютера

Имя	Значение
Путь	Компоненты > Windows клиентский компонент Центра обновления Windows > Управление обновлениями, предлагаемыми из клиентский компонент Центра обновления Windows
Имя раздела реестра	Software\Policies\Microsoft\Windows\WindowsUpdate
Имя файла ADMX	WindowsUpdate.admx

PauseFeatureUpdatesStartTime

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования ✅ IIoT Enterprise или IoT Enterprise LTSC	✅Windows 10, версия 1703 [10.0.15063] и более поздние

Device

```
./Device/Vendor/MSFT/Policy/Config/Update/PauseFeatureUpdatesStartTime
```

Указывает дату и время, когда ИТ-администратор хочет начать приостановку Обновления компонента. Тип значения — string (гггг-мм-дд, например 2018-10-28).

Описание свойств инфраструктуры:

Развернуть таблицу

Имя свойства	Значение свойства
Формат	`chr` (строка)
Тип доступа	Добавить, удалить, получить, заменить

Сопоставление групповой политики:

Развернуть таблицу

Имя	Значение
Имя	DeferFeatureUpdates
Понятное имя	Выбор момента получения предварительных сборок и Обновления компонентов
Имя элемента	Приостановите предварительные сборки или Обновления запуска компонентов.
Location	Конфигурация компьютера
Путь	Компоненты > Windows клиентский компонент Центра обновления Windows > Управление обновлениями, предлагаемыми из клиентский компонент Центра обновления Windows
Имя раздела реестра	Software\Policies\Microsoft\Windows\WindowsUpdate
Имя файла ADMX	WindowsUpdate.admx

PauseQualityUpdates

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования ✅ IIoT Enterprise или IoT Enterprise LTSC	✅Windows 10, версия 1607 [10.0.14393] и более поздние

Device

```
./Device/Vendor/MSFT/Policy/Config/Update/PauseQualityUpdates
```

Включите эту политику, чтобы указать, когда следует получать обновления качества.

Вы можете отложить получение обновлений качества до 30 дней.

Чтобы предотвратить получение обновлений качества в запланированное время, можно временно приостановить обновления качества. Пауза будет действовать в течение 35

дней или до тех пор, пока вы не очистите поле даты начала.

Чтобы возобновить получение приостановленных Обновления качества, очистите поле даты начала.

Если вы отключите или не настроите эту политику, клиентский компонент Центра обновления Windows не изменит ее поведение.

> ⓘ **Примечание.**
>
> Если вы используете Windows 10 версии 1703 или более поздней, рекомендуется использовать политику Update/PauseQualityUpdatesStartTime.

Описание свойств инфраструктуры:

Развернуть таблицу

Имя свойства	Значение свойства
Формат	`int`
Тип доступа	Добавить, удалить, получить, заменить
Значение по умолчанию	0

Допустимые значения:

Развернуть таблицу

Значение	Описание
0 (по умолчанию)	Обновления качества не приостанавливаются.
1	Обновления качества приостанавливаются на 35 дней или до тех пор, пока значение не будет возвращено в значение 0, в зависимости от того, что наступит раньше.

Сопоставление групповой политики:

Развернуть таблицу

Имя	Значение
Имя	DeferQualityUpdates

Имя	Значение
Понятное имя	Выбор момента получения Обновления качества
Location	Конфигурация компьютера
Путь	Компоненты > Windows клиентский компонент Центра обновления Windows > Управление обновлениями, предлагаемыми из клиентский компонент Центра обновления Windows
Имя раздела реестра	Software\Policies\Microsoft\Windows\WindowsUpdate
Имя файла ADMX	WindowsUpdate.admx

PauseQualityUpdatesStartTime

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования ✅ IIoT Enterprise или IoT Enterprise LTSC	✅Windows 10, версия 1703 [10.0.15063] и более поздние

Device

```
./Device/Vendor/MSFT/Policy/Config/Update/PauseQualityUpdatesStartTime
```

Указывает дату и время, когда ИТ-администратор хочет начать приостановку Обновления качества. Тип значения — string (гггг-мм-дд, например 2018-10-28).

> ⓘ **Примечание.**
>
> Если эта политика настроена, Обновления качества будет приостановлена на 35 дней с указанной даты начала.

Описание свойств инфраструктуры:

Развернуть таблицу

Имя свойства	Значение свойства
Формат	`chr` (строка)
Тип доступа	Добавить, удалить, получить, заменить

Сопоставление групповой политики:

Развернуть таблицу

Имя	Значение
Имя	DeferQualityUpdates
Понятное имя	Выбор момента получения Обновления качества
Имя элемента	Приостановите запуск Обновления качества.
Location	Конфигурация компьютера
Путь	Компоненты > Windows клиентский компонент Центра обновления Windows > Управление обновлениями, предлагаемыми из клиентский компонент Центра обновления Windows
Имя раздела реестра	Software\Policies\Microsoft\Windows\WindowsUpdate
Имя файла ADMX	WindowsUpdate.admx

ProductVersion

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования ✅ IIoT Enterprise или IoT Enterprise LTSC	✅Windows 10 версии 2004 с KB5005101 [10.0.19041.1202] и более поздних версий ✅Windows 10 версии 20H2 с KB5005101 [10.0.19042.1202] и более поздних версий ✅Windows 10 версии 21H1 с KB5005101 [10.0.19043.1202] и более поздних версий

Область применения	Выпуски	Применимая ОС
		✅Windows 11, версия 21H2 [10.0.22000] и более поздние

Device
`./Device/Vendor/MSFT/Policy/Config/Update/ProductVersion`

Введите продукт и версию, как указано на странице целевой версии клиентский компонент Центра обновления Windows:

aka.ms/WindowsTargetVersioninfo.

Устройство запросит клиентский компонент Центра обновления Windows продукт и версию при последующих проверках.

Ввод целевого продукта и нажатие кнопки "OK" или "Применить" означает, что я принимаю условия лицензионного соглашения на использование программного обеспечения Майкрософт, указанные в aka.ms/WindowsTargetVersioninfo. Если организация лицензирует программное обеспечение, я имею право привязать организацию.

Если вы введете недопустимое значение, вы останетесь в текущей версии до тех пор, пока не исправите значения в поддерживаемый продукт и версию.

Поддерживаемый тип значения — это строка, содержащая продукт Windows. Например, "Windows 11", "11" или "Windows 10". Используя эту политику клиентский компонент Центра обновления Windows для бизнеса для обновления устройств до нового продукта (например, Windows 11), вы соглашаетесь с тем, что при применении этой операционной системы к устройству:

1. Соответствующая лицензия Windows была приобретена в рамках корпоративного лицензирования, или
2. Вы имеете право на привязку организации и принимаете от ее имени соответствующие условия лицензионного соглашения на использование программного обеспечения Майкрософт.

> ⓘ **Примечание.**
>
> Если продукт не указан, устройство будет продолжать получать более новые версии продукта Windows, на который оно сейчас работает.

Описание свойств инфраструктуры:

Развернуть таблицу

Имя свойства	Значение свойства
Формат	`chr` (строка)
Тип доступа	Добавить, удалить, получить, заменить

Сопоставление групповой политики:

Развернуть таблицу

Имя	Значение
Имя	TargetReleaseVersion
Понятное имя	Выберите целевую версию обновления компонентов.
Имя элемента	Для какой версии продукта Windows вы хотите получать обновления компонентов? например, Windows 10.
Location	Конфигурация компьютера
Путь	Компоненты > Windows клиентский компонент Центра обновления Windows > Управление обновлениями, предлагаемыми из клиентский компонент Центра обновления Windows
Имя раздела реестра	Software\Policies\Microsoft\Windows\WindowsUpdate
Имя файла ADMX	WindowsUpdate.admx

TargetReleaseVersion

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования	✅Windows 10 версии 1803 с KB4556807 [10.0.17134.1488] и более поздних версий ✅Windows 10, версия 1809 с KB4551853 [10.0.17763.1217] и более поздних версий

Область применения	Выпуски	Применимая ОС
	✅ IIoT Enterprise или IoT Enterprise LTSC	✅Windows 10 версии 1903 с KB4556799 [10.0.18362.836] и более поздних версий ✅Windows 10 версии 1909 с KB4556799 [10.0.18363.836] и более поздних версий ✅Windows 10, версия 2004 [10.0.19041] и более поздние

Device

`./Device/Vendor/MSFT/Policy/Config/Update/TargetReleaseVersion`

Введите продукт и версию, как указано на странице целевой версии клиентский компонент Центра обновления Windows:

aka.ms/WindowsTargetVersioninfo.

Устройство запросит клиентский компонент Центра обновления Windows продукт и версию при последующих проверках.

Ввод целевого продукта и нажатие кнопки "OK" или "Применить" означает, что я принимаю условия лицензионного соглашения на использование программного обеспечения Майкрософт, указанные в aka.ms/WindowsTargetVersioninfo. Если организация лицензирует программное обеспечение, я имею право привязать организацию.

Если вы введете недопустимое значение, вы останетесь в текущей версии до тех пор, пока не исправите значения в поддерживаемый продукт и версию.

Поддерживаемый тип значения — это строка, содержащая номер версии Windows. Например, `1809`, `1903`, и т. д.

> ⓘ **Примечание.**
>
> Чтобы он работал, необходимо настроить поставщик служб CSP ProductVersion вместе с поставщиком CSP TargetReleaseVersion.

Описание свойств инфраструктуры:

⛶ **Развернуть таблицу**

Имя свойства	Значение свойства
Формат	`chr` (строка)
Тип доступа	Добавить, удалить, получить, заменить

Сопоставление групповой политики:

Развернуть таблицу

Имя	Значение
Имя	TargetReleaseVersion
Понятное имя	Выберите целевую версию обновления компонентов.
Имя элемента	Целевая версия для Обновления компонентов.
Location	Конфигурация компьютера
Путь	Компоненты > Windows клиентский компонент Центра обновления Windows > Управление обновлениями, предлагаемыми из клиентский компонент Центра обновления Windows
Имя раздела реестра	Software\Policies\Microsoft\Windows\WindowsUpdate
Имя файла ADMX	WindowsUpdate.admx

Управление обновлениями, предлагаемыми из службы обновлений Windows Server

AllowUpdateService

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования	✅Windows 10, версия 1507 [10.0.10240] и более поздние

Область применения	Выпуски	Применимая ОС
	✅ IIoT Enterprise или IoT Enterprise LTSC	

Device

```
./Device/Vendor/MSFT/Policy/Config/Update/AllowUpdateService
```

Определяет, разрешено ли устройству использовать Центр обновления Майкрософт, службы Windows Server Update Services (WSUS) или Microsoft Store. Даже если Центр обновления Windows настроен для получения обновлений из службы обновления в интрасети, он будет периодически получать сведения из общедоступной службы обновления Windows для обеспечения подключений в будущем к Центру обновления Windows и другим службам, таким как Центр обновления Майкрософт или Microsoft Store. Включение этой политики отключит эту функцию и может привести к прекращению работы подключения к общедоступным службам, таким как Microsoft Store.

> ⓘ **Примечание.**
>
> Эта политика применяется только в том случае, если рабочий стол или устройство настроены для подключения к службе обновления интрасети с помощью политики Укажите расположение службы обновлений Майкрософт в интрасети.

Описание свойств инфраструктуры:

Развернуть таблицу

Имя свойства	Значение свойства
Формат	`int`
Тип доступа	Добавить, удалить, получить, заменить
Значение по умолчанию	1

Допустимые значения:

Развернуть таблицу

Значение	Описание
0	Не допускается.

Значение	Описание
1 (по умолчанию)	Разрешено.

Сопоставление групповой политики:

Развернуть таблицу

Имя	Значение
Имя	CorpWuURL
Понятное имя	Указать размещение службы обновлений Майкрософт в интрасети
Location	Конфигурация компьютера
Путь	Компоненты > Windows клиентский компонент Центра обновления Windows > Управление обновлениями, предлагаемыми из Windows Server Update Service
Имя раздела реестра	Software\Policies\Microsoft\Windows\WindowsUpdate
Имя файла ADMX	WindowsUpdate.admx

DetectionFrequency

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования ✅ IIoT Enterprise или IoT Enterprise LTSC	✅Windows 10, версия 1703 [10.0.15063] и более поздние

Device

```
./Device/Vendor/MSFT/Policy/Config/Update/DetectionFrequency
```

Указывает промежуток времени в часах между поисками доступных обновлений. Точное время ожидания — это сумма конкретного значения и случайный вариант в 0–4 часа.

Если для состояния задано значение Включено, Windows будет проверка доступных обновлений через указанный интервал.

Если для состояния задано значение Отключено или Не настроено, Windows будет проверка доступных обновлений через интервал по умолчанию, равный 22 часам.

> ⓘ **Примечание.**
>
> Для того чтобы эта политика действовала, должен быть включен параметр "Указать размещение службы обновлений Майкрософт в интрасети".

> ⓘ **Примечание.**
>
> Если политика "Настройка автоматического обновления" выключена, эта политика не оказывает влияния.

> ⓘ **Примечание.**
>
> Эта политика не поддерживается в Windows RT. Установка этой политики не повлияет на компьютеры Windows RT.

Эта политика должна быть включена только в том случае, если UpdateServiceUrl настроен так, чтобы устройство указывало на сервер WSUS, а не Центр обновления Майкрософт.

> ⓘ **Примечание.**
>
> Существует случайный вариант от 0 до 4 часов, применяемый к частоте сканирования, который нельзя настроить.

Описание свойств инфраструктуры:

Развернуть таблицу

Имя свойства	Значение свойства
Формат	`int`
Тип доступа	Добавить, удалить, получить, заменить
Допустимые значения	Диапазон: `[1-22]`

Имя свойства	Значение свойства
Значение по умолчанию	22

Сопоставление групповой политики:

Развернуть таблицу

Имя	Значение
Имя	DetectionFrequency_Title
Понятное имя	Частота поиска автоматических обновлений
Имя элемента	interval (часы)
Location	Конфигурация компьютера
Путь	Компоненты > Windows клиентский компонент Центра обновления Windows > Управление обновлениями, предлагаемыми из Windows Server Update Service
Имя раздела реестра	Software\Policies\Microsoft\Windows\WindowsUpdate\AU
Имя файла ADMX	WindowsUpdate.admx

DoNotEnforceEnterpriseTLSCertPinningForUpdateDetection

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования ✅ IIoT Enterprise или IoT Enterprise LTSC	✅Windows 10 версии 1507 с KB4598231 [10.0.10240.18818] и более поздних версий ✅Windows 10 версии 1607 с KB4598243 [10.0.14393.4169] и более поздних версий ✅Windows 10 версии 1703 с KB4520010 [10.0.15063.2108] и более поздних версий ✅Windows 10 версии 1709 с KB4580328 [10.0.16299.2166] и более поздних версий ✅Windows 10 версии 1803 с KB4598245 [10.0.17134.1967] и более поздних версий ✅Windows 10, версия 1809 с KB4598230 [10.0.17763.1697] и более поздних версий

Область применения	Выпуски	Применимая ОС
		✅Windows 10, версия 1903 [10.0.18362.1316] и более поздние ✅Windows 10 версии 1909 с KB4598229 [10.0.18363.1316] и более поздних версий ✅Windows 10 версии 2004 с KB4598242 [10.0.19041.746] и более поздних версий ✅Windows 10, версия 20H2 с KB4598242 [10.0.19042.746] и более поздние версии ✅Windows 11, версия 21H2 [10.0.22000] и более поздние

Device

```
./Device/Vendor/MSFT/Policy/Config/Update/DoNotEnforceEnterpriseTLSCertPinningForUpdateDetection
```

Примечание.

По умолчанию закрепление сертификатов для клиентский компонент Центра обновления Windows клиента не применяется. Чтобы обеспечить наивысший уровень безопасности, рекомендуется использовать закрепление tls-сертификата WSUS на всех устройствах.

Описание свойств инфраструктуры:

Развернуть таблицу

Имя свойства	Значение свойства
Формат	`int`
Тип доступа	Добавить, удалить, получить, заменить
Значение по умолчанию	0

Допустимые значения:

Развернуть таблицу

Значение	Описание
0 (по умолчанию)	Служба отключена.

Значение	Описание
1	Включено.

Сопоставление групповой политики:

Развернуть таблицу

Имя	Значение
Имя	CorpWuURL
Понятное имя	Указать размещение службы обновлений Майкрософт в интрасети
Имя элемента	Не применяйте закрепление сертификата TLS для клиентский компонент Центра обновления Windows клиента для обнаружения обновлений.
Location	Конфигурация компьютера
Путь	Компоненты > Windows клиентский компонент Центра обновления Windows > Управление обновлениями, предлагаемыми из Windows Server Update Service
Имя раздела реестра	Software\Policies\Microsoft\Windows\WindowsUpdate
Имя файла ADMX	WindowsUpdate.admx

FillEmptyContentUrls

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования ✅ IIoT Enterprise или IoT Enterprise LTSC	✅Windows 10, версия 1607 [10.0.14393] и более поздние

Device

```
./Device/Vendor/MSFT/Policy/Config/Update/FillEmptyContentUrls
```

Позволяет агенту клиентский компонент Центра обновления Windows определять URL-адрес загрузки, если он отсутствует в метаданных. Этот сценарий будет происходить, когда служба обновления интрасети хранит файлы метаданных, но содержимое загрузки хранится в кэше файлов ISV (указывается в качестве альтернативного URL-адреса загрузки).

> ⓘ **Примечание.**
>
> Этот параметр следует использовать только в сочетании с альтернативным URL-адресом для скачивания и настроен для использования кэша файлов ISV. Этот параметр используется, если служба обновления интрасети не предоставляет URL-адреса загрузки в метаданных обновления для файлов, доступных на альтернативном сервере загрузки.

Описание свойств инфраструктуры:

Развернуть таблицу

Имя свойства	Значение свойства
Формат	`int`
Тип доступа	Добавить, удалить, получить, заменить
Значение по умолчанию	0

Допустимые значения:

Развернуть таблицу

Значение	Описание
0 (по умолчанию)	Служба отключена.
1	Включено.

Сопоставление групповой политики:

Развернуть таблицу

Имя	Значение
Имя	CorpWuURL

Имя	Значение
Понятное имя	Указать размещение службы обновлений Майкрософт в интрасети
Имя элемента	Скачивайте файлы без URL-адреса в метаданных, если задан альтернативный сервер загрузки.
Location	Конфигурация компьютера
Путь	Компоненты > Windows клиентский компонент Центра обновления Windows > Управление обновлениями, предлагаемыми из Windows Server Update Service
Имя раздела реестра	Software\Policies\Microsoft\Windows\WindowsUpdate
Имя файла ADMX	WindowsUpdate.admx

SetPolicyDrivenUpdateSourceForDriverUpdates

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования ✅ IIoT Enterprise или IoT Enterprise LTSC	✅ [10.0.20348.371] и более поздних версий ✅Windows 10 версии 2004 с KB5005101 [10.0.19041.1202] и более поздних версий ✅Windows 10 версии 20H2 с KB5005101 [10.0.19042.1202] и более поздних версий ✅Windows 10 версии 21H1 с KB5005101 [10.0.19043.1202] и более поздних версий ✅Windows 10 версии 21H2 [10.0.19044.1288] и более поздних версий ✅Windows 10 версии 22H2 [10.0.19045.2130] и более поздних ✅Windows 11, версия 21H2 [10.0.22000] и более поздние

Device

```
./Device/Vendor/MSFT/Policy/Config/Update/SetPolicyDrivenUpdateSourceForDriverUpdates
```

Настройте эту политику, чтобы указать, следует ли получать **Обновления драйвера Windows** из конечной точки клиентский компонент Центра обновления Windows,

управляемой политиками клиентский компонент Центра обновления Windows для бизнеса или с помощью настроенных вами политик. Windows Server сервер службы обновления (WSUS). Если вы настроите эту политику, также настройте политики источника сканирования для других типов обновлений:

- SetPolicyDrivenUpdateSourceForFeatureUpdates
- SetPolicyDrivenUpdateSourceForQualityUpdates
- SetPolicyDrivenUpdateSourceForOtherUpdates

> ⓘ **Примечание.**
>
> Если вы неправильно настроили Update/UpdateServiceUrl для указания на сервер WSUS, эта политика не будет действовать.

Описание свойств инфраструктуры:

Развернуть таблицу

Имя свойства	Значение свойства
Формат	`int`
Тип доступа	Добавить, удалить, получить, заменить
Значение по умолчанию	1

Допустимые значения:

Развернуть таблицу

Значение	Описание
0	Обнаружение, скачивание и развертывание Обновления драйвера из клиентский компонент Центра обновления Windows.
1 (по умолчанию)	Обнаружение, скачивание и развертывание Обновления драйвера из Windows Server Update Services (WSUS).

Сопоставление групповой политики:

Развернуть таблицу

Имя	Значение
Имя	CorpWuURL

Имя	Значение
Понятное имя	Указать размещение службы обновлений Майкрософт в интрасети
Location	Конфигурация компьютера
Путь	Компоненты > Windows клиентский компонент Центра обновления Windows > Управление обновлениями, предлагаемыми из Windows Server Update Service
Имя раздела реестра	Software\Policies\Microsoft\Windows\WindowsUpdate
Имя файла ADMX	WindowsUpdate.admx

SetPolicyDrivenUpdateSourceForFeatureUpdates

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования ✅ IIoT Enterprise или IoT Enterprise LTSC	✅ [10.0.20348.371] и более поздних версий ✅Windows 10 версии 2004 с KB5005101 [10.0.19041.1202] и более поздних версий ✅Windows 10 версии 20H2 с KB5005101 [10.0.19042.1202] и более поздних версий ✅Windows 10 версии 21H1 с KB5005101 [10.0.19043.1202] и более поздних версий ✅Windows 10 версии 21H2 [10.0.19044.1288] и более поздних версий ✅Windows 10 версии 22H2 [10.0.19045.2130] и более поздних ✅Windows 11, версия 21H2 [10.0.22000] и более поздние

Device

```
./Device/Vendor/MSFT/Policy/Config/Update/SetPolicyDrivenUpdateSourceForFeatureUpdates
```

Настройте эту политику, чтобы указать, следует ли получать **Обновления компонентов Windows** из конечной точки клиентский компонент Центра обновления Windows, управляемой политиками клиентский компонент Центра обновления Windows для бизнеса или с помощью настроенных вами политик. Windows Server сервер службы

обновления (WSUS). Если вы настроите эту политику, также настройте политики источника сканирования для других типов обновлений:

- SetPolicyDrivenUpdateSourceForQualityUpdates
- SetPolicyDrivenUpdateSourceForDriverUpdates
- SetPolicyDrivenUpdateSourceForOtherUpdates

> ⓘ **Примечание.**
>
> - Если вы неправильно настроили Update/UpdateServiceUrl для указания на сервер WSUS, эта политика не будет действовать.
> - Если вы также используете политику **Укажите параметры для установки дополнительных компонентов и восстановления компонентов** (ADMX_Servicing), чтобы включить содержимое для FoD и языковых пакетов, см. статью Как сделать функции по запросу и языковые пакеты доступными при использовании WSUS или Configuration Manager для проверки конфигурации политики.

Описание свойств инфраструктуры:

⛶ **Развернуть таблицу**

Имя свойства	Значение свойства
Формат	`int`
Тип доступа	Добавить, удалить, получить, заменить
Значение по умолчанию	1

Допустимые значения:

⛶ **Развернуть таблицу**

Значение	Описание
0	Обнаружение, скачивание и развертывание Обновления компонентов из клиентский компонент Центра обновления Windows.
1 (по умолчанию)	Обнаружение, скачивание и развертывание Обновления компонентов из Windows Server Update Services (WSUS).

Сопоставление групповой политики:

Развернуть таблицу

Имя	Значение
Имя	CorpWuURL
Понятное имя	Указать размещение службы обновлений Майкрософт в интрасети
Location	Конфигурация компьютера
Путь	Компоненты > Windows клиентский компонент Центра обновления Windows > Управление обновлениями, предлагаемыми из Windows Server Update Service
Имя раздела реестра	Software\Policies\Microsoft\Windows\WindowsUpdate
Имя файла ADMX	WindowsUpdate.admx

SetPolicyDrivenUpdateSourceForOtherUpdates

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования ✅ IIoT Enterprise или IoT Enterprise LTSC	✅ [10.0.20348.371] и более поздних версий ✅Windows 10 версии 2004 с KB5005101 [10.0.19041.1202] и более поздних версий ✅Windows 10 версии 20H2 с KB5005101 [10.0.19042.1202] и более поздних версий ✅Windows 10 версии 21H1 с KB5005101 [10.0.19043.1202] и более поздних версий ✅Windows 10 версии 21H2 [10.0.19044.1288] и более поздних версий ✅Windows 10 версии 22H2 [10.0.19045.2130] и более поздних ✅Windows 11, версия 21H2 [10.0.22000] и более поздние

Device

```
./Device/Vendor/MSFT/Policy/Config/Update/SetPolicyDrivenUpdateSourceForOtherUpdates
```

Настройте эту политику, чтобы указать, следует ли получать **другие Обновления** из конечной точки клиентский компонент Центра обновления Windows, управляемой

политиками клиентский компонент Центра обновления Windows для бизнеса или с помощью настроенного Windows Server Сервер службы обновления (WSUS). Если вы настроите эту политику, также настройте политики источника сканирования для других типов обновлений:

- SetPolicyDrivenUpdateSourceForFeatureUpdates
- SetPolicyDrivenUpdateSourceForQualityUpdates
- SetPolicyDrivenUpdateSourceForDriverUpdates

> **Примечание.**
>
> Если вы неправильно настроили Update/UpdateServiceUrl для указания на сервер WSUS, эта политика не будет действовать.

Описание свойств инфраструктуры:

Развернуть таблицу

Имя свойства	Значение свойства
Формат	`int`
Тип доступа	Добавить, удалить, получить, заменить
Значение по умолчанию	1

Допустимые значения:

Развернуть таблицу

Значение	Описание
0	Обнаружение, скачивание и развертывание других Обновления из клиентский компонент Центра обновления Windows.
1 (по умолчанию)	Обнаружение, скачивание и развертывание других Обновления из Windows Server Update Services (WSUS).

Сопоставление групповой политики:

Развернуть таблицу

Имя	Значение
Имя	CorpWuURL

Имя	Значение
Понятное имя	Указать размещение службы обновлений Майкрософт в интрасети
Location	Конфигурация компьютера
Путь	Компоненты > Windows клиентский компонент Центра обновления Windows > Управление обновлениями, предлагаемыми из Windows Server Update Service
Имя раздела реестра	Software\Policies\Microsoft\Windows\WindowsUpdate
Имя файла ADMX	WindowsUpdate.admx

SetPolicyDrivenUpdateSourceForQualityUpdates

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования ✅ IIoT Enterprise или IoT Enterprise LTSC	✅ [10.0.20348.371] и более поздних версий ✅Windows 10 версии 2004 с KB5005101 [10.0.19041.1202] и более поздних версий ✅Windows 10 версии 20H2 с KB5005101 [10.0.19042.1202] и более поздних версий ✅Windows 10 версии 21H1 с KB5005101 [10.0.19043.1202] и более поздних версий ✅Windows 10 версии 21H2 [10.0.19044.1288] и более поздних версий ✅Windows 10 версии 22H2 [10.0.19045.2130] и более поздних ✅Windows 11, версия 21H2 [10.0.22000] и более поздние

Device

```
./Device/Vendor/MSFT/Policy/Config/Update/SetPolicyDrivenUpdateSourceForQualityUpdates
```

Настройте эту политику, чтобы указать, следует ли получать **Обновления качества Windows** из конечной точки клиентский компонент Центра обновления Windows, управляемой политиками клиентский компонент Центра обновления Windows для бизнеса или с помощью настроенных вами политик. Windows Server сервер службы

обновления (WSUS). Если вы настроите эту политику, также настройте политики источника сканирования для других типов обновлений:

- SetPolicyDrivenUpdateSourceForFeatureUpdates
- SetPolicyDrivenUpdateSourceForDriverUpdates
- SetPolicyDrivenUpdateSourceForOtherUpdates

> ⓘ **Примечание.**
>
> - Если вы неправильно настроили Update/UpdateServiceUrl для указания на сервер WSUS, эта политика не будет действовать.
> - Если вы также используете политику **Укажите параметры для установки дополнительных компонентов и восстановления компонентов** (ADMX_Servicing), чтобы включить содержимое для FoD и языковых пакетов, см. статью Как сделать функции по запросу и языковые пакеты доступными при использовании WSUS или Configuration Manager для проверки конфигурации политики.

Описание свойств инфраструктуры:

⛶ **Развернуть таблицу**

Имя свойства	**Значение свойства**
Формат	`int`
Тип доступа	Добавить, удалить, получить, заменить
Значение по умолчанию	1

Допустимые значения:

⛶ **Развернуть таблицу**

Значение	**Описание**
0	Обнаружение, скачивание и развертывание Обновления качества из клиентский компонент Центра обновления Windows.
1 (по умолчанию)	Обнаружение, скачивание и развертывание Обновления качества из Windows Server Update Services (WSUS).

Сопоставление групповой политики:

Развернуть таблицу

Имя	Значение
Имя	CorpWuURL
Понятное имя	Указать размещение службы обновлений Майкрософт в интрасети
Location	Конфигурация компьютера
Путь	Компоненты > Windows клиентский компонент Центра обновления Windows > Управление обновлениями, предлагаемыми из Windows Server Update Service
Имя раздела реестра	Software\Policies\Microsoft\Windows\WindowsUpdate
Имя файла ADMX	WindowsUpdate.admx

SetProxyBehaviorForUpdateDetection

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования ✅ IIoT Enterprise или IoT Enterprise LTSC	✅Windows 10 версии 1507 с KB4577049 [10.0.10240.18696] и более поздних версий ✅Windows 10 версии 1607 с KB4577015 [10.0.14393.3930] и более поздних версий ✅Windows 10 версии 1703 [10.0.15063.2500] и более поздних версий ✅Windows 10 версии 1709 с KB4577041 [10.0.16299.2107] и более поздних версий ✅Windows 10 версии 1803 с KB4577032 [10.0.17134.1726] и более поздних версий ✅Windows 10, версия 1809 с KB4570333 [10.0.17763.1457] и более поздних версий ✅Windows 10 версии 1903 с KB4574727 [10.0.18362.1082] и более поздних версий ✅Windows 10 версии 1909 с KB4574727 [10.0.18363.1082] и более поздних версий ✅Windows 10 версии 2004 с KB4571756 [10.0.19041.508] и более поздних версий ✅Windows 11, версия 21H2 [10.0.22000] и более поздние

Device
`./Device/Vendor/MSFT/Policy/Config/Update/SetProxyBehaviorForUpdateDetection`

По умолчанию HTTP-серверы WSUS проверяют только в том случае, если настроен системный прокси-сервер. Этот параметр политики позволяет настроить прокси-сервер пользователя в качестве резервного средства для обнаружения обновлений при использовании сервера интрасети на основе HTTP, несмотря на обнаруженные уязвимости.

Этот параметр политики не влияет на тех клиентов, которые, согласно рекомендациям Майкрософт, защитили свой сервер WSUS с помощью протокола TLS/SSL, используя таким образом серверы интрасети на основе HTTPS для обеспечения безопасности систем. При этом, если требуется прокси-сервер, рекомендуется настроить системный прокси-сервер для обеспечения наивысшего уровня безопасности.

> ⓘ **Примечание.**
>
> Настройка этого параметра политики в значение 1 создает для вашей среды потенциальный риск безопасности и делает сканирование небезопасным.

Описание свойств инфраструктуры:

Развернуть таблицу

Имя свойства	Значение свойства
Формат	`int`
Тип доступа	Добавить, удалить, получить, заменить
Значение по умолчанию	0

Допустимые значения:

Развернуть таблицу

Значение	Описание
0 (по умолчанию)	Используйте системный прокси-сервер только для обнаружения обновлений (по умолчанию).
1	Разрешите использование прокси-сервера пользователя в качестве резервного при сбое обнаружения с помощью системного прокси-сервера.

Сопоставление групповой политики:

Развернуть таблицу

Имя	Значение
Имя	CorpWuURL
Понятное имя	Указать размещение службы обновлений Майкрософт в интрасети
Имя элемента	Выберите поведение прокси-сервера для клиентский компонент Центра обновления Windows клиента для обнаружения обновлений.
Location	Конфигурация компьютера
Путь	Компоненты > Windows клиентский компонент Центра обновления Windows > Управление обновлениями, предлагаемыми из Windows Server Update Service
Имя раздела реестра	Software\Policies\Microsoft\Windows\WindowsUpdate
Имя файла ADMX	WindowsUpdate.admx

UpdateServiceUrl

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования ✅ IIoT Enterprise или IoT Enterprise LTSC	✅Windows 10, версия 1507 [10.0.10240] и более поздние

Device

```
./Device/Vendor/MSFT/Policy/Config/Update/UpdateServiceUrl
```

Разрешает устройству проверять наличие обновлений с сервера WSUS, а не из Центра обновления Майкрософт. Это полезно для локальных MDM, которым необходимо обновить устройства, которые не могут подключиться к Интернету.

В следующем списке показаны поддерживаемые значения:

- Не настроено. Устройство проверяет наличие обновлений из Центра обновления Майкрософт.
- Задайте URL-адрес, например `http://abcd-srv:8530`: устройство проверяет наличие обновлений с сервера WSUS по указанному URL-адресу.

Описание свойств инфраструктуры:

Развернуть таблицу

Имя свойства	Значение свойства
Формат	`chr` (строка)
Тип доступа	Добавить, удалить, получить, заменить
Значение по умолчанию	CorpWSUS

Сопоставление групповой политики:

Развернуть таблицу

Имя	Значение
Имя	CorpWuURL
Понятное имя	Указать размещение службы обновлений Майкрософт в интрасети
Имя элемента	Настройте службу обновлений интрасети для обнаружения обновлений.
Location	Конфигурация компьютера
Путь	Компоненты > Windows клиентский компонент Центра обновления Windows > Управление обновлениями, предлагаемыми из Windows Server Update Service
Имя раздела реестра	Software\Policies\Microsoft\Windows\WindowsUpdate
Имя файла ADMX	WindowsUpdate.admx

Пример:

XML

```
<Replace>
    <CmdID>$CmdID$</CmdID>
    <Item>
```

```
        <Meta>
            <Format>chr</Format>
            <Type>text/plain</Type>
        </Meta>
        <Target>
            <LocURI>./Vendor/MSFT/Policy/Config/Update/UpdateServiceUrl</LocURI>
        </Target>
        <Data>http://abcd-srv:8530</Data>
    </Item>
</Replace>
```

UpdateServiceUrlAlternate

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования ✅ IIoT Enterprise или IoT Enterprise LTSC	✅Windows 10, версия 1607 [10.0.14393] и более поздние

Device

```
./Device/Vendor/MSFT/Policy/Config/Update/UpdateServiceUrlAlternate
```

Указывает альтернативный сервер в интрасети, на котором размещены обновления из Центра обновления Майкрософт. Затем можно использовать эту службу обновления для автоматического обновления компьютеров в вашей сети. Этот параметр позволяет указать сервер в вашей сети, который будет функционировать в качестве внутренней службы обновления. Клиент автоматического обновления будет искать обновления, которые применяются к компьютерам в вашей сети, в этой службе. Чтобы использовать этот параметр, необходимо установить два значения имен серверов: сервер, с которого клиент автоматических обновлений обнаруживает и скачивает обновления, и сервер, на который обновленные рабочие станции отправляют статистику. Оба значения могут соответствовать одному серверу. Можно указать дополнительное значение имени сервера, чтобы настроить агент Центра обновления Windows и скачивать обновления с альтернативного сервера скачивания вместо сервера WSUS. Тип значения — строка, а значение по умолчанию — пустая строка, . Если параметр не настроен и автоматическое Обновления не отключено политикой или пользовательскими предпочтениями, клиент автоматического Обновления подключается непосредственно к сайту клиентский компонент Центра обновления Windows в Интернете.

> ⓘ **Примечание.**
>
> Если настройка автоматического Обновления групповая политика отключена, эта политика не действует. Если групповая политика альтернативного сервера загрузки не задан, он будет по умолчанию использовать сервер WSUS для скачивания обновлений. Эта политика не поддерживается в Windows RT. Установка этой политики не повлияет на компьютеры Windows RT.

Описание свойств инфраструктуры:

Развернуть таблицу

Имя свойства	Значение свойства
Формат	`chr` (строка)
Тип доступа	Добавить, удалить, получить, заменить

Сопоставление групповой политики:

Развернуть таблицу

Имя	Значение
Имя	CorpWuURL
Понятное имя	Указать размещение службы обновлений Майкрософт в интрасети
Имя элемента	Задайте альтернативный сервер загрузки.
Location	Конфигурация компьютера
Путь	Компоненты > Windows клиентский компонент Центра обновления Windows > Управление обновлениями, предлагаемыми из Windows Server Update Service
Имя раздела реестра	Software\Policies\Microsoft\Windows\WindowsUpdate
Имя файла ADMX	WindowsUpdate.admx

Управление взаимодействием с конечными пользователями

ActiveHoursEnd

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования ✅ IIoT Enterprise или IoT Enterprise LTSC	✅Windows 10, версия 1607 [10.0.14393] и более поздние

Device

```
./Device/Vendor/MSFT/Policy/Config/Update/ActiveHoursEnd
```

- Если эта политика включена, компьютер не будет автоматически перезагружать после обновления в часы активности. Компьютер будет пытаться перезапустить в нерабочее время.

Обратите внимание, что компьютер необходимо перезапустить, чтобы некоторые обновления вступили в силу.

- Если эта политика отключена или не настроена, а другие групповые политики перезагрузки отсутствуют, будет действовать выбранное пользователем время активности.

Если включена какая-либо из следующих двух политик, эта политика не будет действовать.

1. Нет автоматического перезапуска с вошедшего в систему пользователей для запланированных автоматических установок обновлений.

2. Всегда автоматически перезапускается по расписанию.

Обратите внимание, что максимальный диапазон активных часов по умолчанию составляет 18 часов от времени начала активных часов, если иное не настроено с помощью политики Укажите диапазон активных часов для автоматического перезапуска.

Описание свойств инфраструктуры:

Развернуть таблицу

Имя свойства	Значение свойства
Формат	`int`
Тип доступа	Добавить, удалить, получить, заменить
Допустимые значения	Диапазон: `[0-23]`
Значение по умолчанию	17

Сопоставление групповой политики:

Развернуть таблицу

Имя	Значение
Имя	ActiveHours
Понятное имя	Отключить автоматический перезапуск при обновлении в период активности
Имя элемента	Конец.
Location	Конфигурация компьютера
Путь	Компоненты > Windows клиентский компонент Центра обновления Windows > управление взаимодействием с конечными пользователями
Имя раздела реестра	Software\Policies\Microsoft\Windows\WindowsUpdate
Имя файла ADMX	WindowsUpdate.admx

ActiveHoursMaxRange

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования ✅ IIoT Enterprise или IoT Enterprise LTSC	✅Windows 10, версия 1703 [10.0.15063] и более поздние

Device

```
./Device/Vendor/MSFT/Policy/Config/Update/ActiveHoursMaxRange
```

Включите эту политику, чтобы указать максимальное количество часов с момента начала, в течение которых пользователи могут задавать свои часы активности.

Диапазон максимальных активных часов может быть установлен в диапазоне от 8 до 18 часов.

Если вы отключите или не настроите эту политику, будет использоваться диапазон максимальных активных часов по умолчанию.

Описание свойств инфраструктуры:

Развернуть таблицу

Имя свойства	**Значение свойства**
Формат	`int`
Тип доступа	Добавить, удалить, получить, заменить
Допустимые значения	Диапазон: `[8-18]`
Значение по умолчанию	18

Сопоставление групповой политики:

Развернуть таблицу

Имя	**Значение**
Имя	ActiveHoursMaxRange
Понятное имя	Указание диапазона активных часов для автоматического перезапуска
Имя элемента	Максимальный диапазон.
Location	Конфигурация компьютера
Путь	Компоненты > Windows клиентский компонент Центра обновления Windows > управление взаимодействием с конечными пользователями
Имя раздела реестра	Software\Policies\Microsoft\Windows\WindowsUpdate

Имя	Значение
Имя файла ADMX	WindowsUpdate.admx

ActiveHoursStart

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования ✅ IIoT Enterprise или IoT Enterprise LTSC	✅Windows 10, версия 1607 [10.0.14393] и более поздние

Device

```
./Device/Vendor/MSFT/Policy/Config/Update/ActiveHoursStart
```

- Если эта политика включена, компьютер не будет автоматически перезагружать после обновления в часы активности. Компьютер будет пытаться перезапустить в нерабочее время.

Обратите внимание, что компьютер необходимо перезапустить, чтобы некоторые обновления вступили в силу.

- Если эта политика отключена или не настроена, а другие групповые политики перезагрузки отсутствуют, будет действовать выбранное пользователем время активности.

Если включена какая-либо из следующих двух политик, эта политика не будет действовать.

1. Нет автоматического перезапуска с вошедшего в систему пользователей для запланированных автоматических установок обновлений.

2. Всегда автоматически перезапускается по расписанию.

Обратите внимание, что максимальный диапазон активных часов по умолчанию составляет 18 часов от времени начала активных часов, если иное не настроено с помощью политики Укажите диапазон активных часов для автоматического перезапуска.

Описание свойств инфраструктуры:

Развернуть таблицу

Имя свойства	Значение свойства
Формат	`int`
Тип доступа	Добавить, удалить, получить, заменить
Допустимые значения	Диапазон: `[0-23]`
Значение по умолчанию	8

Сопоставление групповой политики:

Развернуть таблицу

Имя	Значение
Имя	ActiveHours
Понятное имя	Отключить автоматический перезапуск при обновлении в период активности
Имя элемента	кнопку "Пуск".
Location	Конфигурация компьютера
Путь	Компоненты > Windows клиентский компонент Центра обновления Windows > управление взаимодействием с конечными пользователями
Имя раздела реестра	Software\Policies\Microsoft\Windows\WindowsUpdate
Имя файла ADMX	WindowsUpdate.admx

AllowAutoUpdate

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise	✅Windows 10, версия 1507 [10.0.10240] и более поздние

Область применения	Выпуски	Применимая ОС
	✅ для образования ✅ IIoT Enterprise или IoT Enterprise LTSC	

Device

```
./Device/Vendor/MSFT/Policy/Config/Update/AllowAutoUpdate
```

Позволяет ИТ-администратору управлять поведением автоматического обновления, чтобы искать, скачивать и устанавливать обновления. Важно. Этот параметр следует использовать только для систем с соответствием нормативным требованиям, так как вы также не будете получать обновления для системы безопасности. Если политика не настроена, конечные пользователи получают поведение по умолчанию (автоматическая установка и перезапуск).

Описание свойств инфраструктуры:

Развернуть таблицу

Имя свойства	Значение свойства
Формат	`int`
Тип доступа	Добавить, удалить, получить, заменить
Значение по умолчанию	2

Допустимые значения:

Развернуть таблицу

Значение	Описание
0	Уведомлять пользователя перед скачиванием обновления. Эта политика используется организацией, которая хочет разрешить конечным пользователям управлять использованием данных. С помощью этого параметра пользователи будут уведомлены о наличии обновлений для устройства, которые готовы к скачиванию. Пользователи могут скачивать и устанавливать обновления из панели управления Центра обновления Windows.
1	Автоматическая установка обновления с последующим уведомлением пользователя о необходимости запланировать перезапуск устройства. Обновления автоматически скачиваются в сетях без лимита и устанавливаются во время автоматического обслуживания, если устройство не используется и не работает от аккумулятора. Если

Значение	Описание
	в режиме автоматического обслуживания не удается установить обновления в течение двух дней, Центр обновления Windows установит обновления немедленно. Если для установки требуется перезапуск, пользователю будет предложено запланировать время перезапуска. Если после установки обновления пользователь не запланировал перезагрузку, устройство попытается перезапустить автоматически. Пользователь будет уведомлен о запланированном перезапуске и может перепланировать его, если предложенное время неудобно. Включение конечным пользователем управления временем запуска снижает риск случайной потери данных, вызванной приложениями, которые не завершаются должным образом при перезапуске.
2 (по умолчанию)	Автоматическая установка и перезапуск. Обновления автоматически скачиваются в сетях без лимита и устанавливаются во время автоматического обслуживания, если устройство не используется и не работает от аккумулятора. Если в режиме автоматического обслуживания не удается установить обновления в течение двух дней, Центр обновления Windows установит обновления немедленно. Если требуется перезапуск, устройство автоматически перезапускается вне периода активного использования устройства. Это поведение по умолчанию для неуправляемых устройств. Устройства обновляются быстро, но это повышает риск случайной потери данных, вызванной приложением, которое не завершает работу должным образом при перезапуске.
3	Автоматическая установка и перезапуск в указанное время. ИТ-специалист указывает день и время установки. Если не указать день и время, установка будет по умолчанию выполняться каждый день в 3:00. Автоматическая установка происходит в это время, а перезапуск устройства происходит после 15-минутного обратного отсчета. Если пользователь вошел в систему, когда Windows готова к перезапуску, он может прервать 15-минутный обратный отсчет, чтобы отложить перезапуск.
4	Автоматическая установка и перезапуск без участия конечного пользователя. Обновления автоматически скачиваются в сетях без лимита и устанавливаются во время автоматического обслуживания, если устройство не используется и не работает от аккумулятора. Если в режиме автоматического обслуживания не удается установить обновления в течение двух дней, Центр обновления Windows установит обновления немедленно. Если требуется перезапуск, устройство автоматически перезапускается вне периода активного использования устройства. Этот параметр также устанавливает для панели управления пользователя режим только для чтения.
5	Отключить автоматические обновления.

Сопоставление групповой политики:

Развернуть таблицу

Имя	Значение
Имя	AutoUpdateCfg

Имя	Значение
Понятное имя	Настройка автоматического обновления
Имя элемента	Настройте автоматическое обновление.
Location	Конфигурация компьютера
Путь	Компоненты > Windows клиентский компонент Центра обновления Windows > управление взаимодействием с конечными пользователями
Имя раздела реестра	Software\Policies\Microsoft\Windows\WindowsUpdate\AU
Имя файла ADMX	WindowsUpdate.admx

AllowAutoWindowsUpdateDownloadOverMeteredNetwork

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования ✅ IIoT Enterprise или IoT Enterprise LTSC	✅Windows 10, версия 1709 [10.0.16299] и более поздние

Device

```
./Device/Vendor/MSFT/Policy/Config/Update/AllowAutoWindowsUpdateDownloadOverMeteredNetwork
```

Включение этой политики автоматически скачивает обновления даже через лимитные подключения к данным (может взиматься плата).

Значительное число устройств в основном используют передачу данных сотовой связи и не имеют Wi-Fi доступа, что приводит к уменьшению числа устройств, получающих обновления. Так как большое количество устройств имеет большие планы данных или неограниченное количество данных, эта политика может разблокировать получение обновлений устройствами.

Эта политика доступна с помощью параметра Обновить в пользовательском интерфейсе или групповая политика.

Описание свойств инфраструктуры:

Развернуть таблицу

Имя свойства	Значение свойства
Формат	`int`
Тип доступа	Добавить, удалить, получить, заменить
Значение по умолчанию	0

Допустимые значения:

Развернуть таблицу

Значение	Описание
0 (по умолчанию)	Не допускается.
1	Разрешено.

Сопоставление групповой политики:

Развернуть таблицу

Имя	Значение
Имя	AllowAutoWindowsUpdateDownloadOverMeteredNetwork
Понятное имя	Разрешить автоматическую загрузку обновлений через лимитные подключения
Location	Конфигурация компьютера
Путь	Компоненты > Windows клиентский компонент Центра обновления Windows > управление взаимодействием с конечными пользователями
Имя раздела реестра	Software\Policies\Microsoft\Windows\WindowsUpdate
Имя значения реестра	AllowAutoWindowsUpdateDownloadOverMeteredNetwork

Имя	Значение
Имя файла ADMX	WindowsUpdate.admx

AllowMUUpdateService

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования ✅ IIoT Enterprise или IoT Enterprise LTSC	✅Windows 10, версия 1607 [10.0.14393] и более поздние

Device

```
./Device/Vendor/MSFT/Policy/Config/Update/AllowMUUpdateService
```

Позволяет ИТ-администратору управлять тем, следует ли проверять обновлений для приложений в Центре обновления Майкрософт.

Примечание.

- Список других продуктов Майкрософт, которые могут быть обновлены, см. в разделе Обновление других продуктов Майкрософт.
- Если задать для этой политики значение 0 или Не настроено, не отменить изменения конфигурацию для автоматического получения обновлений из Центра обновления Майкрософт. Чтобы отменить изменения конфигурацию, можно выполнить приведенные ниже команды PowerShell, чтобы удалить службу Центра обновления Майкрософт:

PowerShell

```
$MUSM = New-Object -ComObject "Microsoft.Update.ServiceManager"
$MUSM.RemoveService("7971f918-a847-4430-9279-4a52d1efe18d")
```

Описание свойств инфраструктуры:

Развернуть таблицу

Имя свойства	Значение свойства
Формат	`int`
Тип доступа	Добавить, удалить, получить, заменить
Значение по умолчанию	0

Допустимые значения:

Развернуть таблицу

Значение	Описание
0 (по умолчанию)	Не разрешено или не настроено.
1	Разрешено. Принимает обновления, полученные из Центра обновления Майкрософт.

Сопоставление групповой политики:

Развернуть таблицу

Имя	Значение
Имя	AutoUpdateCfg
Понятное имя	Настройка автоматического обновления
Имя элемента	Установите обновления для других продуктов Майкрософт.
Location	Конфигурация компьютера
Путь	Компоненты > Windows клиентский компонент Центра обновления Windows > управление взаимодействием с конечными пользователями
Имя раздела реестра	Software\Policies\Microsoft\Windows\WindowsUpdate\AU
Имя файла ADMX	WindowsUpdate.admx

AllowTemporaryEnterpriseFeatureControl

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования ✅ IIoT Enterprise или IoT Enterprise LTSC	✅Windows 11 версии 22H2 с KB5022913 [10.0.22621.1344] и более поздних версий

Device

`./Device/Vendor/MSFT/Policy/Config/Update/AllowTemporaryEnterpriseFeatureControl`

Функции, появившиеся в рамках обслуживания (за пределами ежегодного обновления компонентов), по умолчанию отключены для устройств, на которых управляются обновления Windows*.

- Если для этой политики настроено значение "Включено", все функции, доступные в последнем ежемесячном обновлении качества, будут включены.
- Если для этой политики задано значение "Не настроено" или "Отключено", функции, поставляемые через ежемесячное обновление качества (обслуживание), останутся отключенными до тех пор, пока не будет установлено обновление компонентов, включающее эти компоненты.

*Управляемые устройства с обновлением Windows — это устройства, на которых обновления Windows управляются с помощью политики; через облако с помощью клиентский компонент Центра обновления Windows для бизнеса или локально с Windows Server Update Services (WSUS).

> **Примечание.**
>
> В Intune этот параметр называется **Разрешить временное управление функциями предприятия** и доступен в каталоге параметров. По умолчанию для устройств, управляемых Windows-Update, отключены все функции, представленные в службе обслуживания, которые находятся за коммерческим элементом управления. Если задано значение Разрешено, эти функции включаются и включаются. Дополнительные сведения см. в разделе Блог: Коммерческий контроль для непрерывных инноваций.

Описание свойств инфраструктуры:

Развернуть таблицу

Имя свойства	Значение свойства
Формат	`int`
Тип доступа	Добавить, удалить, получить, заменить
Значение по умолчанию	0

Допустимые значения:

Развернуть таблицу

Значение	Описание
0 (по умолчанию)	Не допускается.
1	Разрешено.

Сопоставление групповой политики:

Развернуть таблицу

Имя	Значение
Имя	AllowTemporaryEnterpriseFeatureControl
Понятное имя	Включение функций, представленных через обслуживание, которые отключены по умолчанию
Location	Конфигурация компьютера
Путь	Компоненты > Windows клиентский компонент Центра обновления Windows > управление взаимодействием с конечными пользователями
Имя раздела реестра	Software\Policies\Microsoft\Windows\WindowsUpdate
Имя значения реестра	AllowTemporaryEnterpriseFeatureControl
Имя файла ADMX	WindowsUpdate.admx

ConfigureDeadlineForFeatureUpdates

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования ✅ IIoT Enterprise или IoT Enterprise LTSC	✅Windows 10, версия 1903 [10.0.18362] и более поздние

Device

```
./Device/Vendor/MSFT/Policy/Config/Update/ConfigureDeadlineForFeatureUpdates
```

Количество дней до автоматической установки обновлений компонентов на устройствах независимо от времени активности. До истечения крайнего срока пользователи смогут запланировать перезапуски, а автоматические перезапуски могут происходить в нерабочее время. Если задано значение 0, обновления будут скачивать и устанавливаться немедленно, но могут не завершиться в течение дня из-за доступности устройства и сетевого подключения.

> ⓘ **Примечание.**
>
> - После истечения крайнего срока перезапуски будут происходить независимо от времени активности, и пользователи не смогут перенести расписание.
> - При использовании этой политики параметры скачивания, установки и перезагрузки из раздела Update/AllowAutoUpdate игнорируются.

Описание свойств инфраструктуры:

Развернуть таблицу

Имя свойства	Значение свойства
Формат	`int`
Тип доступа	Добавить, удалить, получить, заменить
Допустимые значения	Диапазон: `[0-30]`
Значение по умолчанию	2

Сопоставление групповой политики:

Развернуть таблицу

Имя	Значение
Имя	ComplianceDeadlineForFU
Понятное имя	Указание крайнего срока автоматического обновления и перезапуска для обновления компонентов
Имя элемента	Крайний срок (дни)
Location	Конфигурация компьютера
Путь	Компоненты > Windows клиентский компонент Центра обновления Windows > управление взаимодействием с конечными пользователями
Имя раздела реестра	Software\Policies\Microsoft\Windows\WindowsUpdate
Имя файла ADMX	WindowsUpdate.admx

ConfigureDeadlineForQualityUpdates

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования ✅ IIoT Enterprise или IoT Enterprise LTSC	✅Windows 10, версия 1903 [10.0.18362] и более поздние

Device

```
./Device/Vendor/MSFT/Policy/Config/Update/ConfigureDeadlineForQualityUpdates
```

Количество дней до автоматической установки обновлений качества на устройствах независимо от времени активности. До истечения крайнего срока пользователи смогут запланировать перезапуски, а автоматические перезапуски могут происходить в нерабочее время. Если задано значение 0, обновления будут скачивать и устанавливаться немедленно, но могут не завершиться в течение дня из-за доступности устройства и сетевого подключения.

> ⓘ **Примечание.**
>
> - После истечения крайнего срока перезапуски будут происходить независимо от времени активности, и пользователи не смогут перенести расписание.
> - При использовании этой политики параметры скачивания, установки и перезагрузки из раздела Update/AllowAutoUpdate игнорируются.

Описание свойств инфраструктуры:

Развернуть таблицу

Имя свойства	Значение свойства
Формат	`int`
Тип доступа	Добавить, удалить, получить, заменить
Допустимые значения	Диапазон: `[0-30]`
Значение по умолчанию	7

Сопоставление групповой политики:

Развернуть таблицу

Имя	Значение
Имя	ComplianceDeadline
Понятное имя	Указание крайнего срока автоматического обновления и перезапуска для обновления качества
Имя элемента	Крайний срок (дни)
Location	Конфигурация компьютера
Путь	Компоненты > Windows клиентский компонент Центра обновления Windows > управление взаимодействием с конечными пользователями
Имя раздела реестра	Software\Policies\Microsoft\Windows\WindowsUpdate
Имя файла ADMX	WindowsUpdate.admx

ConfigureDeadlineGracePeriod

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования ✅ IIoT Enterprise или IoT Enterprise LTSC	✅Windows 10, версия 1903 [10.0.18362] и более поздние

Device

```
./Device/Vendor/MSFT/Policy/Config/Update/ConfigureDeadlineGracePeriod
```

Минимальное количество дней с момента установки обновлений до автоматического перезапуска для обновлений качества. Эта политика вступает в силу только при настройке Update/ConfigureDeadlineForQualityUpdates. Если параметр Update/ConfigureDeadlineForQualityUpdates настроен, но эта политика не задана, то значение по умолчанию 2 дня вступит в силу.

Описание свойств инфраструктуры:

Развернуть таблицу

Имя свойства	Значение свойства
Формат	`int`
Тип доступа	Добавить, удалить, получить, заменить
Допустимые значения	Диапазон: `[0-7]`
Значение по умолчанию	2

Сопоставление групповой политики:

Развернуть таблицу

Имя	Значение
Имя	ComplianceDeadline
Понятное	Указание крайнего срока автоматического обновления и перезапуска для

Имя	Значение
имя	обновления качества
Имя элемента	Льготный период (в днях)
Location	Конфигурация компьютера
Путь	Компоненты > Windows клиентский компонент Центра обновления Windows > управление взаимодействием с конечными пользователями
Имя раздела реестра	Software\Policies\Microsoft\Windows\WindowsUpdate
Имя файла ADMX	WindowsUpdate.admx

ConfigureDeadlineGracePeriodForFeatureUpdates

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования ✅ IIoT Enterprise или IoT Enterprise LTSC	✅Windows 10, версия 1809 с KB5000854 [10.0.17763.1852] и более поздних версий ✅Windows 10 версии 1909 с KB5000850 [10.0.18363.1474] и более поздних версий ✅Windows 10 версии 2004 с KB5000842 [10.0.19041.906] и более поздних версий ✅Windows 10 версии 20H2 с KB5000842 [10.0.19042.906] и более поздних версий ✅Windows 11, версия 21H2 [10.0.22000] и более поздние

Device

```
./Device/Vendor/MSFT/Policy/Config/Update/ConfigureDeadlineGracePeriodForFeatureUpdates
```

Минимальное количество дней с момента установки обновления до автоматического перезапуска обновлений компонентов. Эта политика вступает в силу только при настройке Update/ConfigureDeadlineForFeatureUpdates. Если параметр Update/ConfigureDeadlineForFeatureUpdates настроен, но эта политика не задана, будет использоваться значение, настроенное параметром Update/ConfigureDeadlineGracePeriod.

Если параметр Update/ConfigureDeadlineGracePeriod также не настроен, в силу вступают значения по умолчанию 7 дней.

Описание свойств инфраструктуры:

Развернуть таблицу

Имя свойства	Значение свойства
Формат	`int`
Тип доступа	Добавить, удалить, получить, заменить
Допустимые значения	Диапазон: `[0-7]`
Значение по умолчанию	7

Сопоставление групповой политики:

Развернуть таблицу

Имя	Значение
Имя	ComplianceDeadlineForFU
Понятное имя	Указание крайнего срока автоматического обновления и перезапуска для обновления компонентов
Имя элемента	Льготный период (в днях)
Location	Конфигурация компьютера
Путь	Компоненты > Windows клиентский компонент Центра обновления Windows > управление взаимодействием с конечными пользователями
Имя раздела реестра	Software\Policies\Microsoft\Windows\WindowsUpdate
Имя файла ADMX	WindowsUpdate.admx

ConfigureDeadlineNoAutoRebootForFeatureUpdates

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования ✅ IIoT Enterprise или IoT Enterprise LTSC	✅Windows 11, версия 22H2 [10.0.22621] и более поздние

Device

```
./Device/Vendor/MSFT/Policy/Config/Update/ConfigureDeadlineNoAutoRebootForFeatureUpdates
```

Эта политика позволяет указать количество дней до автоматической установки обновлений компонентов на устройствах и льготный период, по истечении которого автоматически происходит необходимый перезапуск.

Установите крайние сроки обновления компонентов и исправлений в соответствии с вашими целями соответствия. Обновления будут загружены и установлены, как только они будут предложены, а автоматический перезапуск будет предпринят в нерабочее время. После истечения крайнего срока перезапуски будут выполняться независимо от времени активности, и пользователи не смогут перенести расписание. Если крайний срок установлен в 0 дней, обновление будет установлено сразу после предложения, но может не завершиться в течение дня из-за доступности устройства и сетевого подключения.

Задайте льготный период для обновлений компонентов, чтобы гарантировать пользователям минимальное время для управления перезапусками после установки обновлений. Пользователи смогут планировать перезапуски в течение льготного периода, а Windows по-прежнему может автоматически перезапускаться в нерабочее время, если пользователи не планируют перезапуски. Льготный период может не входить в силу, если у пользователей уже есть больше дней, установленных в качестве льготного периода для управления перезапуском на основе конфигураций крайних сроков.

Вы можете настроить устройство для задержки перезапуска до истечения крайнего срока и льготного периода.

Если эта политика отключена или не настроена, устройства будут получать обновления и перезапускаться в соответствии с расписанием по умолчанию.

Эта политика переопределит следующие политики:

1. Укажите крайний срок перед автоматическим перезапуском для установки обновлений

2. Укажите задействованный переход перезапуска и расписание уведомлений для обновлений.

3. Всегда автоматически перезагружаться в запланированное время

4. Настройка автоматического Обновления.

Описание свойств инфраструктуры:

Развернуть таблицу

Имя свойства	Значение свойства
Формат	`int`
Тип доступа	Добавить, удалить, получить, заменить
Значение по умолчанию	0

Допустимые значения:

Развернуть таблицу

Значение	Описание
0 (по умолчанию)	Служба отключена.
1	Включено.

Сопоставление групповой политики:

Развернуть таблицу

Имя	Значение
Имя	ComplianceDeadlineForFU
Понятное имя	Указание крайнего срока автоматического обновления и перезапуска для обновления компонентов
Имя элемента	Не перезапускайте автоматически до окончания льготного периода.
Location	Конфигурация компьютера
Путь	Компоненты > Windows клиентский компонент Центра обновления Windows > управление взаимодействием с конечными пользователями

Имя	Значение
Имя раздела реестра	Software\Policies\Microsoft\Windows\WindowsUpdate
Имя файла ADMX	WindowsUpdate.admx

ConfigureDeadlineNoAutoRebootForQualityUpdates

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования ✅ IIoT Enterprise или IoT Enterprise LTSC	✅Windows 11, версия 22H2 [10.0.22621] и более поздние

Device

```
./Device/Vendor/MSFT/Policy/Config/Update/ConfigureDeadlineNoAutoRebootForQualityUpdates
```

Эта политика позволяет указать количество дней до автоматической установки обновлений качества на устройствах и льготный период, по истечении которого автоматически происходит необходимый перезапуск.

Установите крайние сроки для обновлений качества в соответствии с вашими целями соответствия. Обновления будут загружены и установлены, как только они будут предложены, а автоматический перезапуск будет предпринят в нерабочее время. После истечения крайнего срока перезапуски будут выполняться независимо от времени активности, и пользователи не смогут перенести расписание. Если крайний срок установлен в 0 дней, обновление будет установлено сразу после предложения, но может не завершиться в течение дня из-за доступности устройства и сетевого подключения.

Задайте льготный период для исправлений, чтобы гарантировать пользователям минимальное время для управления перезапусками после установки обновлений. Пользователи смогут планировать перезапуски в течение льготного периода, а Windows по-прежнему может автоматически перезапускаться в нерабочее время, если пользователи не планируют перезапуски. Льготный период может не входить в силу, если

у пользователей уже есть больше дней, установленных в качестве льготного периода для управления перезапуском на основе конфигураций крайних сроков.

Вы можете настроить устройство для задержки перезапуска до истечения крайнего срока и льготного периода.

Если эта политика отключена или не настроена, устройства будут получать обновления и перезапускаться в соответствии с расписанием по умолчанию.

Эта политика переопределит следующие политики:

1. Укажите крайний срок перед автоматическим перезапуском для установки обновлений
2. Укажите задействованный переход перезапуска и расписание уведомлений для обновлений.
3. Всегда автоматически перезагружаться в запланированное время
4. Настройка автоматического Обновления.

Описание свойств инфраструктуры:

Развернуть таблицу

Имя свойства	Значение свойства
Формат	`int`
Тип доступа	Добавить, удалить, получить, заменить
Значение по умолчанию	0

Допустимые значения:

Развернуть таблицу

Значение	Описание
0 (по умолчанию)	Служба отключена.
1	Включено.

Сопоставление групповой политики:

Развернуть таблицу

Имя	Значение
Имя	ComplianceDeadline
Понятное имя	Указание крайнего срока автоматического обновления и перезапуска для обновления качества
Имя элемента	Не перезапускайте автоматически до окончания льготного периода.
Location	Конфигурация компьютера
Путь	Компоненты > Windows клиентский компонент Центра обновления Windows > управление взаимодействием с конечными пользователями
Имя раздела реестра	Software\Policies\Microsoft\Windows\WindowsUpdate
Имя файла ADMX	WindowsUpdate.admx

ConfigureFeatureUpdateUninstallPeriod

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования ✅ IIoT Enterprise или IoT Enterprise LTSC	✅Windows 10, версия 1803 [10.0.17134] и более поздние

Device

```
./Device/Vendor/MSFT/Policy/Config/Update/ConfigureFeatureUpdateUninstallPeriod
```

Разрешить предприятиям или ИТ-администраторам настроить период удаления обновлений компонентов.

Описание свойств инфраструктуры:

Развернуть таблицу

Имя свойства	Значение свойства
Формат	`int`
Тип доступа	Добавить, удалить, получить, заменить
Допустимые значения	Диапазон: `[2-60]`
Значение по умолчанию	10

NoUpdateNotificationsDuringActiveHours

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования ✅ IIoT Enterprise или IoT Enterprise LTSC	✅Windows 11, версия 22H2 [10.0.22621] и более поздние

Device

```
./Device/Vendor/MSFT/Policy/Config/Update/NoUpdateNotificationsDuringActiveHours
```

0 (по умолчанию) — используйте клиентский компонент Центра обновления Windows уведомления по умолчанию 1— отключить все уведомления, за исключением предупреждений о перезапуске 2 — отключить все уведомления, включая предупреждения о перезапуске.

Эта политика позволяет определить, какие клиентский компонент Центра обновления Windows уведомления видят пользователи. Эта политика не определяет, как и когда загружаются и устанавливаются обновления.

Важно, если вы решили не получать уведомления об обновлениях, а также определить другую групповую политику, чтобы устройства не получали обновления автоматически, ни вы, ни пользователи устройств не знали о критически важных обновлениях безопасности, качества или компонентов, и ваши устройства могут быть подвержены риску.

Если выбрать "Применить только в часы активности" в сочетании с вариантом 1 или 2, уведомления будут отключены только в часы активности. Вы можете задать часы активности, задав параметр "Отключить автоматический перезапуск для обновлений в

активное время" или разрешить устройству устанавливать часы активности в зависимости от поведения пользователя. Чтобы обеспечить безопасность устройства, по-прежнему будет отображаться уведомление, если этот параметр выбран после достижения крайнего срока "Указать крайние сроки для автоматического обновления и перезапуска", если он настроен, независимо от времени активности.

> ⓘ **Примечание.**
>
> Эту политику можно использовать в сочетании с политиками Update/ActiveHoursStart и Update/ActiveHoursEnd, чтобы гарантировать, что конечный пользователь не видит уведомлений об обновлениях в часы активности до достижения крайнего срока. Если период активного часа не настроен, это будет применяться к окну интеллектуального активного времени, рассчитанного на устройстве.

Описание свойств инфраструктуры:

⛶ **Развернуть таблицу**

Имя свойства	**Значение свойства**
Формат	`int`
Тип доступа	Добавить, удалить, получить, заменить
Значение по умолчанию	0

Допустимые значения:

⛶ **Развернуть таблицу**

Значение	**Описание**
0 (по умолчанию)	Служба отключена.
1	Включено.

Сопоставление групповой политики:

⛶ **Развернуть таблицу**

Имя	**Значение**
Имя	UpdateNotificationLevel

Имя	Значение
Понятное имя	Параметры отображения уведомлений об обновлении
Имя элемента	Применяется только в часы активности.
Location	Конфигурация компьютера
Путь	Компоненты > Windows клиентский компонент Центра обновления Windows > управление взаимодействием с конечными пользователями
Имя раздела реестра	Software\Policies\Microsoft\Windows\WindowsUpdate
Имя файла ADMX	WindowsUpdate.admx

ScheduledInstallDay

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования ✅ IIoT Enterprise или IoT Enterprise LTSC	✅Windows 10, версия 1507 [10.0.10240] и более поздние

Device

```
./Device/Vendor/MSFT/Policy/Config/Update/ScheduledInstallDay
```

Позволяет ИТ-администратору планировать день установки обновления. Тип данных — целое число.

> ⓘ **Примечание.**
>
> Эта политика вступит в силу, только если параметр Update/AllowAutoUpdate настроен на вариант 3 или 4 для запланированной установки.

Описание свойств инфраструктуры:

Развернуть таблицу

Имя свойства	Значение свойства
Формат	`int`
Тип доступа	Добавить, удалить, получить, заменить
Значение по умолчанию	0

Допустимые значения:

Развернуть таблицу

Значение	Описание
0 (по умолчанию)	Каждый день.
1	Воскресенье.
2	Понедельник.
3	Вторник.
4	Среда.
5	Четверг.
6	Пятница.
7	Суббота.

Сопоставление групповой политики:

Развернуть таблицу

Имя	Значение
Имя	AutoUpdateCfg
Понятное имя	Настройка автоматического обновления
Имя элемента	Запланированный день установки.
Location	Конфигурация компьютера
Путь	Компоненты > Windows клиентский компонент Центра обновления Windows > управление взаимодействием с конечными пользователями

Имя	Значение
Имя раздела реестра	Software\Policies\Microsoft\Windows\WindowsUpdate\AU
Имя файла ADMX	WindowsUpdate.admx

ScheduledInstallEveryWeek

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования ✅ IIoT Enterprise или IoT Enterprise LTSC	✅Windows 10, версия 1709 [10.0.16299] и более поздние

Device

```
./Device/Vendor/MSFT/Policy/Config/Update/ScheduledInstallEveryWeek
```

Позволяет ИТ-администратору планировать установку обновлений каждую неделю. Тип значения - целое число.

> ⓘ **Примечание.**
>
> Эта политика вступит в силу, только если параметр Update/AllowAutoUpdate настроен на вариант 3 или 4 для запланированной установки.

Описание свойств инфраструктуры:

Развернуть таблицу

Имя свойства	Значение свойства
Формат	`int`
Тип доступа	Добавить, удалить, получить, заменить
Значение по умолчанию	1

Допустимые значения:

Развернуть таблицу

Значение	Описание
0	Нет обновлений в расписании.
1 (по умолчанию)	Обновление планируется каждую неделю.

Сопоставление групповой политики:

Развернуть таблицу

Имя	Значение
Имя	AutoUpdateCfg
Понятное имя	Настройка автоматического обновления
Имя элемента	Каждую неделю.
Location	Конфигурация компьютера
Путь	Компоненты > Windows клиентский компонент Центра обновления Windows > управление взаимодействием с конечными пользователями
Имя раздела реестра	Software\Policies\Microsoft\Windows\WindowsUpdate\AU
Имя файла ADMX	WindowsUpdate.admx

ScheduledInstallFirstWeek

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования ✅ IIoT Enterprise или IoT Enterprise LTSC	✅Windows 10, версия 1709 [10.0.16299] и более поздние

Device
`./Device/Vendor/MSFT/Policy/Config/Update/ScheduledInstallFirstWeek`

Позволяет ИТ-администратору запланировать установку обновлений на первую неделю месяца. Тип значения - целое число.

Политики ScheduledInstall*week работают в числовых днях.

- ScheduledInstallFirstWeek: первая неделя месяца (дни 1–7).
- ScheduledInstallSecondWeek: вторая неделя месяца (дни 8–14).
- ScheduledInstallThirdWeek: третья неделя месяца (дни 15-21).
- ScheduledInstallFourthWeek: четвертая неделя месяца (дни 22-31).

Эти политики не являются эксклюзивными и могут использоваться в любой комбинации. Вместе с ScheduledInstallDay он определяет порядковый номер дня недели в месяце. Например, ScheduledInstallSecondWeek + ScheduledInstallDay = 3 — это второй вторник месяца. Если устройство недоступно в запланированное время, оно может отложить установку обновлений до следующего месяца.

> ⓘ **Примечание.**
>
> Эта политика вступит в силу, только если параметр Update/AllowAutoUpdate настроен на вариант 3 или 4 для запланированной установки.

Описание свойств инфраструктуры:

Развернуть таблицу

Имя свойства	**Значение свойства**
Формат	`int`
Тип доступа	Добавить, удалить, получить, заменить
Значение по умолчанию	0

Допустимые значения:

Развернуть таблицу

Значение	**Описание**
0 (по умолчанию)	Нет обновлений в расписании.

Значение	Описание
1	Обновление планируется каждую первую неделю месяца.

Сопоставление групповой политики:

Развернуть таблицу

Имя	Значение
Имя	AutoUpdateCfg
Понятное имя	Настройка автоматического обновления
Имя элемента	Первая неделя месяца.
Location	Конфигурация компьютера
Путь	Компоненты > Windows клиентский компонент Центра обновления Windows > управление взаимодействием с конечными пользователями
Имя раздела реестра	Software\Policies\Microsoft\Windows\WindowsUpdate\AU
Имя файла ADMX	WindowsUpdate.admx

ScheduledInstallFourthWeek

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования ✅ IIoT Enterprise или IoT Enterprise LTSC	✅Windows 10, версия 1709 [10.0.16299] и более поздние

Device

```
./Device/Vendor/MSFT/Policy/Config/Update/ScheduledInstallFourthWeek
```

Позволяет ИТ-администратору запланировать установку обновлений на четвертую неделю месяца. Тип значения - целое число.

Политики ScheduledInstall*week работают в числовых днях.

- ScheduledInstallFirstWeek: первая неделя месяца (дни 1–7).
- ScheduledInstallSecondWeek: вторая неделя месяца (дни 8–14).
- ScheduledInstallThirdWeek: третья неделя месяца (дни 15-21).
- ScheduledInstallFourthWeek: четвертая неделя месяца (дни 22-31).

Эти политики не являются эксклюзивными и могут использоваться в любой комбинации. Вместе с ScheduledInstallDay он определяет порядковый номер дня недели в месяце. Например, ScheduledInstallSecondWeek + ScheduledInstallDay = 3 — это второй вторник месяца. Если устройство недоступно в запланированное время, оно может отложить установку обновлений до следующего месяца.

> ⓘ **Примечание.**
>
> Эта политика вступит в силу, только если параметр Update/AllowAutoUpdate настроен на вариант 3 или 4 для запланированной установки.

Описание свойств инфраструктуры:

Развернуть таблицу

Имя свойства	Значение свойства
Формат	`int`
Тип доступа	Добавить, удалить, получить, заменить
Значение по умолчанию	0

Допустимые значения:

Развернуть таблицу

Значение	Описание
0 (по умолчанию)	Нет обновлений в расписании.
1	Обновление планируется каждую четвертую неделю месяца.

Сопоставление групповой политики:

Развернуть таблицу

Имя	Значение
Имя	AutoUpdateCfg
Понятное имя	Настройка автоматического обновления
Имя элемента	Четвертая неделя месяца.
Location	Конфигурация компьютера
Путь	Компоненты > Windows клиентский компонент Центра обновления Windows > управление взаимодействием с конечными пользователями
Имя раздела реестра	Software\Policies\Microsoft\Windows\WindowsUpdate\AU
Имя файла ADMX	WindowsUpdate.admx

ScheduledInstallSecondWeek

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования ✅ IIoT Enterprise или IoT Enterprise LTSC	✅Windows 10, версия 1709 [10.0.16299] и более поздние

Device

```
./Device/Vendor/MSFT/Policy/Config/Update/ScheduledInstallSecondWeek
```

Позволяет ИТ-администратору запланировать установку обновления на вторую неделю месяца. Тип значения - целое число.

Политики ScheduledInstall*week работают в числовых днях.

- ScheduledInstallFirstWeek: первая неделя месяца (дни 1–7).
- ScheduledInstallSecondWeek: вторая неделя месяца (дни 8–14).

- ScheduledInstallThirdWeek: третья неделя месяца (дни 15-21).
- ScheduledInstallFourthWeek: четвертая неделя месяца (дни 22-31).

Эти политики не являются эксклюзивными и могут использоваться в любой комбинации. Вместе с ScheduledInstallDay он определяет порядковый номер дня недели в месяце. Например, ScheduledInstallSecondWeek + ScheduledInstallDay = 3 — это второй вторник месяца. Если устройство недоступно в запланированное время, оно может отложить установку обновлений до следующего месяца.

> ⓘ **Примечание.**
>
> Эта политика вступит в силу, только если параметр Update/AllowAutoUpdate настроен на вариант 3 или 4 для запланированной установки.

Описание свойств инфраструктуры:

Развернуть таблицу

Имя свойства	Значение свойства
Формат	`int`
Тип доступа	Добавить, удалить, получить, заменить
Значение по умолчанию	0

Допустимые значения:

Развернуть таблицу

Значение	Описание
0 (по умолчанию)	Нет обновлений в расписании.
1	Обновление планируется каждую вторую неделю месяца.

Сопоставление групповой политики:

Развернуть таблицу

Имя	Значение
Имя	AutoUpdateCfg
Понятное	Настройка автоматического обновления

Имя	Значение
имя	
Имя элемента	Вторая неделя месяца.
Location	Конфигурация компьютера
Путь	Компоненты > Windows клиентский компонент Центра обновления Windows > управление взаимодействием с конечными пользователями
Имя раздела реестра	Software\Policies\Microsoft\Windows\WindowsUpdate\AU
Имя файла ADMX	WindowsUpdate.admx

ScheduledInstallThirdWeek

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования ✅ IIoT Enterprise или IoT Enterprise LTSC	✅Windows 10, версия 1709 [10.0.16299] и более поздние

Device

```
./Device/Vendor/MSFT/Policy/Config/Update/ScheduledInstallThirdWeek
```

Позволяет ИТ-администратору запланировать установку обновлений на третью неделю месяца. Тип значения - целое число.

Политики ScheduledInstall*week работают в числовых днях.

- ScheduledInstallFirstWeek: первая неделя месяца (дни 1–7).
- ScheduledInstallSecondWeek: вторая неделя месяца (дни 8–14).
- ScheduledInstallThirdWeek: третья неделя месяца (дни 15-21).
- ScheduledInstallFourthWeek: четвертая неделя месяца (дни 22-31).

Эти политики не являются эксклюзивными и могут использоваться в любой комбинации. Вместе с ScheduledInstallDay он определяет порядковый номер дня недели в месяце.

Например, ScheduledInstallSecondWeek + ScheduledInstallDay = 3 — это второй вторник месяца. Если устройство недоступно в запланированное время, оно может отложить установку обновлений до следующего месяца.

> ⓘ **Примечание.**
>
> Эта политика вступит в силу, только если параметр Update/AllowAutoUpdate настроен на вариант 3 или 4 для запланированной установки.

Описание свойств инфраструктуры:

Развернуть таблицу

Имя свойства	Значение свойства
Формат	`int`
Тип доступа	Добавить, удалить, получить, заменить
Значение по умолчанию	0

Допустимые значения:

Развернуть таблицу

Значение	Описание
0 (по умолчанию)	Нет обновлений в расписании.
1	Обновление планируется каждую третью неделю месяца.

Сопоставление групповой политики:

Развернуть таблицу

Имя	Значение
Имя	AutoUpdateCfg
Понятное имя	Настройка автоматического обновления
Имя элемента	Третья неделя месяца.
Location	Конфигурация компьютера

Имя	Значение
Путь	Компоненты > Windows клиентский компонент Центра обновления Windows > управление взаимодействием с конечными пользователями
Имя раздела реестра	Software\Policies\Microsoft\Windows\WindowsUpdate\AU
Имя файла ADMX	WindowsUpdate.admx

ScheduledInstallTime

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования ✅ IIoT Enterprise или IoT Enterprise LTSC	✅Windows 10, версия 1507 [10.0.10240] и более поздние

Device

```
./Device/Vendor/MSFT/Policy/Config/Update/ScheduledInstallTime
```

Позволяет ИТ-администратору планировать время установки обновления. Тип данных — целое число. Поддерживаемые значения: 0–23, где 0 — полночь, а 23 — 23:00. Значение по умолчанию: 3.

> ⓘ **Примечание.**
>
> - Эта политика вступит в силу, только если параметр Update/AllowAutoUpdate настроен на вариант 3 или 4 для запланированной установки.
> - Существует окно примерно в 30 минут, чтобы обеспечить более высокие показатели успешной установки.

Описание свойств инфраструктуры:

Развернуть таблицу

Имя свойства	Значение свойства
Формат	`int`
Тип доступа	Добавить, удалить, получить, заменить
Допустимые значения	Диапазон: `[0-23]`
Значение по умолчанию	3

Сопоставление групповой политики:

Развернуть таблицу

Имя	Значение
Имя	AutoUpdateCfg
Понятное имя	Настройка автоматического обновления
Имя элемента	Запланированное время установки.
Location	Конфигурация компьютера
Путь	Компоненты > Windows клиентский компонент Центра обновления Windows > управление взаимодействием с конечными пользователями
Имя раздела реестра	Software\Policies\Microsoft\Windows\WindowsUpdate\AU
Имя файла ADMX	WindowsUpdate.admx

SetDisablePauseUXAccess

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования ✅ IIoT Enterprise или IoT Enterprise LTSC	✅Windows 10, версия 1809 [10.0.17763] и более поздних версий

Device
`./Device/Vendor/MSFT/Policy/Config/Update/SetDisablePauseUXAccess`

Этот параметр позволяет удалить доступ к функции "Приостановить обновления".

После включения доступа пользователей к приостановке обновлений удаляется.

Описание свойств инфраструктуры:

Развернуть таблицу

Имя свойства	Значение свойства
Формат	`int`
Тип доступа	Добавить, удалить, получить, заменить
Значение по умолчанию	0

Допустимые значения:

Развернуть таблицу

Значение	Описание
1	Включить.
0 (по умолчанию)	Отключить.

Сопоставление групповой политики:

Развернуть таблицу

Имя	Значение
Имя	DisablePauseUXAccess
Понятное имя	Удаление доступа к функции "Приостановка обновлений"
Location	Конфигурация компьютера
Путь	Компоненты > Windows клиентский компонент Центра обновления Windows > управление взаимодействием с конечными пользователями
Имя раздела реестра	Software\Policies\Microsoft\Windows\WindowsUpdate

Имя	Значение
Имя значения реестра	SetDisablePauseUXAccess
Имя файла ADMX	WindowsUpdate.admx

SetDisableUXWUAccess

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования ✅ IIoT Enterprise или IoT Enterprise LTSC	✅Windows 10, версия 1809 [10.0.17763] и более поздних версий

Device

```
./Device/Vendor/MSFT/Policy/Config/Update/SetDisableUXWUAccess
```

Этот параметр позволяет удалить доступ к сканированию клиентский компонент Центра обновления Windows.

Если включить этот параметр для доступа пользователей к клиентский компонент Центра обновления Windows сканировать, загрузка и установка будут удалены.

Описание свойств инфраструктуры:

Развернуть таблицу

Имя свойства	Значение свойства
Формат	`int`
Тип доступа	Добавить, удалить, получить, заменить
Значение по умолчанию	0

Допустимые значения:

Развернуть таблицу

Значение	Описание
0 (по умолчанию)	Служба отключена.
1	Включено.

Сопоставление групповой политики:

Развернуть таблицу

Имя	Значение
Имя	DisableUXWUAccess
Понятное имя	Запретить доступ для использования любых средств Центра обновления Windows
Location	Конфигурация компьютера
Путь	Компоненты > Windows клиентский компонент Центра обновления Windows > управление взаимодействием с конечными пользователями
Имя раздела реестра	Software\Policies\Microsoft\Windows\WindowsUpdate
Имя значения реестра	SetDisableUXWUAccess
Имя файла ADMX	WindowsUpdate.admx

SetEDURestart

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования ✅ IIoT Enterprise или IoT Enterprise LTSC	✅Windows 10, версия 1703 [10.0.15063] и более поздние

Device

```
./Device/Vendor/MSFT/Policy/Config/Update/SetEDURestart
```

Включение этой политики для устройств EDU, которые остаются в корзинах на ночь, пропустит проверки питания, чтобы убедиться, что перезагрузка обновлений произойдет во время запланированной установки.

Включение этой политики ограничит скачивание и установку обновлений в нерабочее время. Обновления будет разрешено запускаться, даже если есть пользователь, вошедшего в систему, или устройство работает от батареи, при условии, что емкость аккумулятора превышает 70 %. Windows запланируют выход устройства из спящего режима через 1 час после времени ActiveHoursEnd со случайной задержкой в 60 минут. Устройства перезагрузятся сразу после установки обновлений. Если по-прежнему ожидаются обновления, устройство будет продолжать повторять попытку каждый час в течение 4 часов.

В отношении заряда батареи соблюдаются следующие правила:

- Более 70 % — разрешено начать работу;
- Более 40 % — разрешена перезагрузка;
- Выше 20% - разрешено продолжить работу.

Этот параметр переопределяет поведение отсрочки установки AllowAutoUpdate.

Эти параметры предназначены для образовательных устройств, которые остаются в тележках на ночь и остаются в спящем режиме. Он не предназначен для устройств 1:1.

Описание свойств инфраструктуры:

Развернуть таблицу

Имя свойства	Значение свойства
Формат	`int`
Тип доступа	Добавить, удалить, получить, заменить
Значение по умолчанию	0

Допустимые значения:

Развернуть таблицу

Значение	Описание
0 (по умолчанию)	Не настроено.
1	Сконфигурированный.

Сопоставление групповой политики:

Развернуть таблицу

Имя	Значение
Имя	SetEDURestart
Понятное имя	Обновление политики питания для перезапусков корзины
Location	Конфигурация компьютера
Путь	Компоненты > Windows клиентский компонент Центра обновления Windows > управление взаимодействием с конечными пользователями
Имя раздела реестра	Software\Policies\Microsoft\Windows\WindowsUpdate
Имя значения реестра	SetEDURestart
Имя файла ADMX	WindowsUpdate.admx

UpdateNotificationLevel

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования ✅ IIoT Enterprise или IoT Enterprise LTSC	✅Windows 10, версия 1809 [10.0.17763] и более поздних версий

Device

```
./Device/Vendor/MSFT/Policy/Config/Update/UpdateNotificationLevel
```

0 (по умолчанию) — используйте клиентский компонент Центра обновления Windows уведомления по умолчанию 1— отключить все уведомления, за исключением предупреждений о перезапуске 2 — отключить все уведомления, включая предупреждения о перезапуске.

Эта политика позволяет определить, какие клиентский компонент Центра обновления Windows уведомления видят пользователи. Эта политика не определяет, как и когда загружаются и устанавливаются обновления.

Важно, если вы решили не получать уведомления об обновлениях, а также определить другую групповую политику, чтобы устройства не получали обновления автоматически, ни вы, ни пользователи устройств не знали о критически важных обновлениях безопасности, качества или компонентов, и ваши устройства могут быть подвержены риску.

Если выбрать "Применить только в часы активности" в сочетании с вариантом 1 или 2, уведомления будут отключены только в часы активности. Вы можете задать часы активности, задав параметр "Отключить автоматический перезапуск для обновлений в активное время" или разрешить устройству устанавливать часы активности в зависимости от поведения пользователя. Чтобы обеспечить безопасность устройства, по-прежнему будет отображаться уведомление, если этот параметр выбран после достижения крайнего срока "Указать крайние сроки для автоматического обновления и перезапуска", если он настроен, независимо от времени активности.

Описание свойств инфраструктуры:

Развернуть таблицу

Имя свойства	Значение свойства
Формат	`int`
Тип доступа	Добавить, удалить, получить, заменить
Значение по умолчанию	0

Допустимые значения:

Развернуть таблицу

Значение	Описание
0 (по умолчанию)	Используйте уведомления по умолчанию клиентский компонент Центра обновления Windows.
1	Отключите все уведомления, за исключением предупреждений о перезапуске.
2	Отключите все уведомления, включая предупреждения о перезапуске.

Сопоставление групповой политики:

Развернуть таблицу

Имя	Значение
Имя	UpdateNotificationLevel
Понятное имя	Параметры отображения уведомлений об обновлении
Location	Конфигурация компьютера
Путь	Компоненты > Windows клиентский компонент Центра обновления Windows > управление взаимодействием с конечными пользователями
Имя раздела реестра	Software\Policies\Microsoft\Windows\WindowsUpdate
Имя значения реестра	SetUpdateNotificationLevel
Имя файла ADMX	WindowsUpdate.admx

Устаревшие политики

AlwaysAutoRebootAtScheduledTimeMinutes

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования ✅ IIoT Enterprise или IoT Enterprise LTSC	✅Windows 11, версия 22H2 [10.0.22621] и более поздние

Device

```
./Device/Vendor/MSFT/Policy/Config/Update/AlwaysAutoRebootAtScheduledTimeMinutes
```

- Если эта политика включена, таймер перезапуска всегда будет начинаться сразу после того, как клиентский компонент Центра обновления Windows установит важные обновления, а не уведомлять пользователей на экране входа по крайней мере за два дня.

Таймер перезапуска можно настроить для запуска с любого значения от 15 до 180 минут. По истечении таймера перезапуск будет продолжаться, даже если на компьютере есть пользователи, вошедшего в систему.

- Если вы отключите или не настроите эту политику, клиентский компонент Центра обновления Windows не изменит ее поведение перезапуска.

Если включена политика "Нет автоматического перезапуска с пользователями, вошедшего в систему для запланированных автоматических обновлений", эта политика не действует.

Описание свойств инфраструктуры:

Развернуть таблицу

Имя свойства	Значение свойства
Формат	`int`
Тип доступа	Добавить, удалить, получить, заменить
Допустимые значения	Диапазон: `[15-180]`
Значение по умолчанию	15

Сопоставление групповой политики:

Развернуть таблицу

Имя	Значение
Имя	AlwaysAutoRebootAtScheduledTime
Понятное имя	Всегда автоматически перезагружаться в запланированное время
Имя элемента	work (в минутах)
Location	Конфигурация компьютера
Путь	Компоненты > Windows клиентский компонент Центра обновления Windows > устаревшие политики
Имя раздела реестра	Software\Policies\Microsoft\Windows\WindowsUpdate\AU
Имя файла ADMX	WindowsUpdate.admx

AutoRestartDeadlinePeriodInDays

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования ✅ IIoT Enterprise или IoT Enterprise LTSC	✅Windows 10, версия 1607 [10.0.14393] и более поздние

Device

```
./Device/Vendor/MSFT/Policy/Config/Update/AutoRestartDeadlinePeriodInDays
```

Укажите крайний срок до автоматического перезапуска компьютера для применения обновлений. Крайний срок можно задать от 2 до 14 дней после даты перезапуска по умолчанию.

Перезапуск может происходить в часы активности.

Если вы отключите или не настроите эту политику, компьютер перезагрузится в соответствии с расписанием по умолчанию.

Включение любой из следующих двух политик переопределит указанную выше политику:

1. Нет автоматического перезапуска с вошедшего в систему пользователей для запланированных автоматических установок обновлений.
2. Всегда автоматически перезапускается по расписанию.

Описание свойств инфраструктуры:

Развернуть таблицу

Имя свойства	Значение свойства
Формат	`int`
Тип доступа	Добавить, удалить, получить, заменить
Допустимые значения	Диапазон: `[2-30]`
Значение по умолчанию	7

Сопоставление групповой политики:

Развернуть таблицу

Имя	Значение
Имя	AutoRestartDeadline
Понятное имя	Указание срока до автоматического перезапуска после установки обновления
Имя элемента	Обновления качества (в днях)
Location	Конфигурация компьютера
Путь	Компоненты > Windows клиентский компонент Центра обновления Windows > устаревшие политики
Имя раздела реестра	Software\Policies\Microsoft\Windows\WindowsUpdate
Имя файла ADMX	WindowsUpdate.admx

AutoRestartDeadlinePeriodInDaysForFeatureUpdates

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования ✅ IIoT Enterprise или IoT Enterprise LTSC	✅Windows 10, версия 1809 [10.0.17763] и более поздних версий

Device

```
./Device/Vendor/MSFT/Policy/Config/Update/AutoRestartDeadlinePeriodInDaysForFeatureUpdates
```

Укажите крайний срок до автоматического перезапуска компьютера для применения обновлений. Крайний срок можно задать от 2 до 14 дней после даты перезапуска по умолчанию.

Перезапуск может происходить в часы активности.

Если вы отключите или не настроите эту политику, компьютер перезагрузится в соответствии с расписанием по умолчанию.

Включение любой из следующих двух политик переопределит указанную выше политику:

1. Нет автоматического перезапуска с вошедшего в систему пользователей для запланированных автоматических установок обновлений.

2. Всегда автоматически перезапускается по расписанию.

Описание свойств инфраструктуры:

Развернуть таблицу

Имя свойства	Значение свойства
Формат	`int`
Тип доступа	Добавить, удалить, получить, заменить
Допустимые значения	Диапазон: `[2-30]`
Значение по умолчанию	7

Сопоставление групповой политики:

Развернуть таблицу

Имя	Значение
Имя	AutoRestartDeadline
Понятное имя	Указание срока до автоматического перезапуска после установки обновления
Имя элемента	Обновления функций (в днях)
Location	Конфигурация компьютера
Путь	Компоненты > Windows клиентский компонент Центра обновления Windows > устаревшие политики
Имя раздела реестра	Software\Policies\Microsoft\Windows\WindowsUpdate
Имя файла ADMX	WindowsUpdate.admx

AutoRestartNotificationSchedule

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования ✅ IIoT Enterprise или IoT Enterprise LTSC	✅Windows 10, версия 1703 [10.0.15063] и более поздние

Device

```
./Device/Vendor/MSFT/Policy/Config/Update/AutoRestartNotificationSchedule
```

Включите эту политику, чтобы указать, когда отображаются напоминания об автоматическом перезапуске.

Вы можете указать время до запланированного перезапуска, чтобы уведомить пользователя.

Если эта политика отключена или не настроена, будет использоваться период по умолчанию.

Описание свойств инфраструктуры:

Развернуть таблицу

Имя свойства	Значение свойства
Формат	`int`
Тип доступа	Добавить, удалить, получить, заменить
Значение по умолчанию	15

Допустимые значения:

Развернуть таблицу

Значение	Описание
15 (по умолчанию)	15 минут.
30	30 минут.
60	60 минут.

Значение	Описание
120	120 минут.
240	240 минут.

Сопоставление групповой политики:

Развернуть таблицу

Имя	Значение
Имя	AutoRestartNotificationConfig
Понятное имя	Настройка уведомлений напоминания об автоматическом перезапуске для обновлений
Имя элемента	Точка (мин)
Location	Конфигурация компьютера
Путь	Компоненты > Windows клиентский компонент Центра обновления Windows > устаревшие политики
Имя раздела реестра	Software\Policies\Microsoft\Windows\WindowsUpdate
Имя файла ADMX	WindowsUpdate.admx

AutoRestartRequiredNotificationDismissal

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования ✅ IIoT Enterprise или IoT Enterprise LTSC	✅Windows 10, версия 1703 [10.0.15063] и более поздние

Device

```
./Device/Vendor/MSFT/Policy/Config/Update/AutoRestartRequiredNotificationDismissal
```

Включите эту политику, чтобы указать метод, с помощью которого отклоняется требуемое уведомление об автоматическом перезапуске. Если для установки обновлений требуется перезагрузка, отображается уведомление об обязательном автоматическом перезапуске. По умолчанию уведомление автоматически отклоняется через 25 секунд.

Метод можно задать так, чтобы требовать от пользователя действия для закрытия уведомления.

Если отключить или не настроить эту политику, будет использоваться метод по умолчанию.

Описание свойств инфраструктуры:

Развернуть таблицу

Имя свойства	Значение свойства
Формат	`int`
Тип доступа	Добавить, удалить, получить, заменить
Значение по умолчанию	1

Допустимые значения:

Развернуть таблицу

Значение	Описание
1 (по умолчанию)	Автоматическое закрытие.
2	Увольнение пользователя.

Сопоставление групповой политики:

Развернуть таблицу

Имя	Значение
Имя	AutoRestartRequiredNotificationDismissal
Понятное имя	Настройка обязательного уведомления об автоматическом перезапуске для обновлений
Имя элемента	Метод.
Location	Конфигурация компьютера

Имя	Значение
Путь	Компоненты > Windows клиентский компонент Центра обновления Windows > устаревшие политики
Имя раздела реестра	Software\Policies\Microsoft\Windows\WindowsUpdate
Имя файла ADMX	WindowsUpdate.admx

DeferUpdatePeriod

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования ✅ IIoT Enterprise или IoT Enterprise LTSC	✅Windows 10, версия 1607 [10.0.14393] и более поздние

Device

```
./Device/Vendor/MSFT/Policy/Config/Update/DeferUpdatePeriod
```

> ⓘ **Примечание.**
>
> Не используйте эту политику на устройствах с Windows 10 версии 1607, вместо этого используйте новые политики, перечисленные в разделе Изменения в Windows 10 версии 1607, для управления обновлениями. Вы можете продолжать использовать DeferUpdatePeriod для устройств с Windows 10 версии 1511.

Позволяет ИТ-администраторам указывать задержки обновления на срок до четырех недель. Поддерживаемые значения: 0–4, то есть количество недель для отсрочки обновлений.

- Если включена политика **Укажите расположение службы обновлений Майкрософт в интрасети**, параметры "Отложить обновления" и "Приостановить Обновления и обновления" не будут действовать.
- Если политика **Разрешить телеметрия включена**, а для параметра Параметры задано значение 0, то параметры "Отложить обновления", "Отложить обновления" и

"Приостановить Обновления и обновления" не будут действовать.

Обновление ОС:

- Максимальная отсрочка: восемь месяцев
- Приращение отсрочки: один месяц
- Тип обновления и заметки:
  - Обновление — 3689BDC8-B205-4AF4-8D4A-A63924C5E9D5

Обновление

- Максимальная отсрочка: один месяц
- Приращение отсрочки: одна неделя
- Тип обновления и примечания. Если на компьютере включен Центр обновления Майкрософт, все Обновления Майкрософт в следующих категориях также будут соблюдать логику Отложить или приостановить:
  - Обновление для системы безопасности — 0FA1201D-4330-4FA8-8AE9-B877473B6441
  - Критическое обновление — E6CF1350-C01B-414D-A61F-263D14D133B4
  - Накопительный пакет обновления — 28BC880E-0592-4CBF-8F95-C79B17911D5F
  - Пакет обновления — 68C5B0A3-D1A6-4553-AE49-01D3A7827828
  - Инструменты — B4832BD8-E735-4761-8DAF-37F882276DAB
  - Пакет компонентов — B54E7D24-7ADD-428F-8B75-90A396FA584F
  - Обновление — CD5FFD1E-E932-4E3A-BF74-18BF0B1BBD83
  - Драйвер — EBFC1FC5-71A4-4F7B-9ACA-3B9A503104A0

Другое/не может отложить:

- Максимальная отсрочка: нет отсрочки
- Приращение отсрочки: нет отсрочки
- Тип обновления/заметки по обновлению: любая категория обновлений, не указанная выше, попадает в эту категорию. — Обновление определения — E0789628-CE08-4437-BE74-2495B842F43B

Описание свойств инфраструктуры:

Развернуть таблицу

Имя свойства	Значение свойства
Формат	`int`
Тип доступа	Добавить, удалить, получить, заменить

Имя свойства	Значение свойства
Допустимые значения	Диапазон: `[0-4]`
Значение по умолчанию	0

Сопоставление групповой политики:

Развернуть таблицу

Имя	Значение
Имя	DeferUpgrade
Путь	WindowsUpdate > AT > WindowsComponents > WindowsUpdateCat
Имя элемента	DeferUpdatePeriodId

DeferUpgradePeriod

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования ✅ IIoT Enterprise или IoT Enterprise LTSC	✅Windows 10, версия 1607 [10.0.14393] и более поздние

Device

```
./Device/Vendor/MSFT/Policy/Config/Update/DeferUpgradePeriod
```

Позволяет ИТ-администраторам указывать дополнительные задержки обновления на срок до 8 месяцев. Поддерживаемые значения: 0–8, то есть количество месяцев для отсрочки обновлений.

- Если включена политика **Укажите расположение службы обновлений Майкрософт в интрасети**, параметры Отложить обновления по, Отложить обновления по и Приостановить Обновления и Обновления не будут действовать.
- Если политика **Разрешить телеметрию** включена, а для параметра Параметры задано значение 0, то параметры Отложить обновления на, Отложить обновления по и Приостановить Обновления и Обновления не будут действовать.

> ⓘ **Примечание.**
>
> Не используйте эту политику на устройствах с Windows 10 версии 1607, вместо этого используйте новые политики, перечисленные в разделе Изменения в Windows 10 версии 1607, для управления обновлениями. Вы можете продолжать использовать DeferUpgradePeriod для устройств с Windows 10 версии 1511.

Описание свойств инфраструктуры:

Развернуть таблицу

Имя свойства	Значение свойства
Формат	`int`
Тип доступа	Добавить, удалить, получить, заменить
Допустимые значения	Диапазон: `[0-8]`
Значение по умолчанию	0

Сопоставление групповой политики:

Развернуть таблицу

Имя	Значение
Имя	DeferUpgrade
Путь	WindowsUpdate > AT > WindowsComponents > WindowsUpdateCat
Имя элемента	DeferUpgradePeriodId

DisableDualScan

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования ✅ IIoT Enterprise или IoT Enterprise LTSC	✅Windows 10, версия 1607 [10.0.14393] и более поздние

Device
`./Device/Vendor/MSFT/Policy/Config/Update/DisableDualScan`

Включите эту политику, чтобы запретить политикам отсрочки обновлений вызывать проверки клиентский компонент Центра обновления Windows.

- Если эта политика отключена или не настроена, клиент клиентский компонент Центра обновления Windows может инициировать автоматическую проверку клиентский компонент Центра обновления Windows при включении политик отсрочки обновлений.

> ⓘ **Примечание.**
>
> Эта политика применяется только в том случае, если служба обновления Майкрософт интрасети, к которому направляется компьютер, настроена для поддержки нацеливания на стороне клиента. Если политика "Указать размещение службы обновлений Майкрософт в интрасети" отключена или не настроена, эта политика не оказывает влияния.

> ⓘ **Примечание.**
>
> Дополнительные сведения о двойном сканировании см. в разделах Демистификация "Двойное сканирование" и Улучшение двойного сканирования на 1607.

Описание свойств инфраструктуры:

Развернуть таблицу

Имя свойства	Значение свойства
Формат	`int`
Тип доступа	Добавить, удалить, получить, заменить
Значение по умолчанию	0

Допустимые значения:

Развернуть таблицу

Значение	Описание
0 (по умолчанию)	Разрешить сканирование клиентский компонент Центра обновления Windows.
1	Не разрешайте политикам отсрочки обновления вызывать проверки клиентский компонент Центра обновления Windows.

Сопоставление групповой политики:

Развернуть таблицу

Имя	Значение
Имя	DisableDualScan
Понятное имя	Не разрешайте политикам отсрочки обновления вызывать проверки клиентский компонент Центра обновления Windows
Location	Конфигурация компьютера
Путь	Компоненты > Windows клиентский компонент Центра обновления Windows > устаревшие политики
Имя раздела реестра	Software\Policies\Microsoft\Windows\WindowsUpdate
Имя значения реестра	DisableDualScan
Имя файла ADMX	WindowsUpdate.admx

EngagedRestartDeadline

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования ✅ IIoT Enterprise или IoT Enterprise LTSC	✅Windows 10, версия 1703 [10.0.15063] и более поздние

Device

```
./Device/Vendor/MSFT/Policy/Config/Update/EngagedRestartDeadline
```

Включите эту политику для управления временем перед переходом с автоматических перезапусков, запланированных в нерабочее время, на Занятая перезагрузка, что требует от пользователя расписания. Период можно задать от 0 до 30 дней с момента ожидания перезапуска.

Вы можете указать количество дней, в течение которых пользователь может отложить уведомления о напоминаниях о перезапуске. Период отсрочки может быть установлен от 1 до 3 дней.

Вы можете указать крайний срок в днях перед автоматическим планированием и выполнением ожидающего перезапуска независимо от активных часов. Крайний срок может иметь значение от 2 до 30 дней с момента, когда перезапуск становится отложенным. Если этот параметр настроен, ожидающий перезапуск будет переходить от автоматического перезапуска к включенному перезапуску (ожидание пользовательского расписания) к автоматическому выполнению в течение указанного периода.

Если вы не укажете крайний срок или для него задано значение 0, компьютер не перезагрузится автоматически и потребует от пользователя запланировать его перед перезапуском.

Если вы отключите или не настроите эту политику, компьютер перезагрузится по расписанию по умолчанию.

Включение любой из следующих политик переопределит указанную выше политику:

1. Нет автоматического перезапуска для вошедшего в систему пользователей для запланированных автоматических установок обновлений
2. Всегда автоматически перезапускается по расписанию.
3. Укажите крайний срок перед автоматическим перезапуском для установки обновлений.

Описание свойств инфраструктуры:

Развернуть таблицу

Имя свойства	Значение свойства
Формат	`int`
Тип доступа	Добавить, удалить, получить, заменить

Имя свойства	Значение свойства
Допустимые значения	Диапазон: `[2-30]`
Значение по умолчанию	14

Сопоставление групповой политики:

Развернуть таблицу

Имя	Значение
Имя	EngagedRestartTransitionSchedule
Понятное имя	Указание расписания перехода с задействованным перезапуском и расписания уведомлений для обновлений
Имя элемента	Крайний срок (дни)
Location	Конфигурация компьютера
Путь	Компоненты > Windows клиентский компонент Центра обновления Windows > устаревшие политики
Имя раздела реестра	Software\Policies\Microsoft\Windows\WindowsUpdate
Имя файла ADMX	WindowsUpdate.admx

EngagedRestartDeadlineForFeatureUpdates

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования ✅ IIoT Enterprise или IoT Enterprise LTSC	✅Windows 10, версия 1809 [10.0.17763] и более поздних версий

Device

```
./Device/Vendor/MSFT/Policy/Config/Update/EngagedRestartDeadlineForFeatureUpdates
```

Включите эту политику для управления временем перед переходом с автоматических перезапусков, запланированных в нерабочее время, на Занятая перезагрузка, что требует от пользователя расписания. Период можно задать от 0 до 30 дней с момента ожидания перезапуска.

Вы можете указать количество дней, в течение которых пользователь может отложить уведомления о напоминаниях о перезапуске. Период отсрочки может быть установлен от 1 до 3 дней.

Вы можете указать крайний срок в днях перед автоматическим планированием и выполнением ожидающего перезапуска независимо от активных часов. Крайний срок может иметь значение от 2 до 30 дней с момента, когда перезапуск становится отложенным. Если этот параметр настроен, ожидающий перезапуск будет переходить от автоматического перезапуска к включенному перезапуску (ожидание пользовательского расписания) к автоматическому выполнению в течение указанного периода.

Если вы не укажете крайний срок или для него задано значение 0, компьютер не перезагрузится автоматически и потребует от пользователя запланировать его перед перезапуском.

Если вы отключите или не настроите эту политику, компьютер перезагрузится по расписанию по умолчанию.

Включение любой из следующих политик переопределит указанную выше политику:

1. Нет автоматического перезапуска для вошедшего в систему пользователей для запланированных автоматических установок обновлений
2. Всегда автоматически перезапускается по расписанию.
3. Укажите крайний срок перед автоматическим перезапуском для установки обновлений.

Описание свойств инфраструктуры:

Развернуть таблицу

Имя свойства	Значение свойства
Формат	`int`
Тип доступа	Добавить, удалить, получить, заменить
Допустимые значения	Диапазон: `[2-30]`
Значение по умолчанию	14

Сопоставление групповой политики:

Развернуть таблицу

Имя	Значение
Имя	EngagedRestartTransitionSchedule
Понятное имя	Указание расписания перехода с задействованным перезапуском и расписания уведомлений для обновлений
Имя элемента	Крайний срок (дни)
Location	Конфигурация компьютера
Путь	Компоненты > Windows клиентский компонент Центра обновления Windows > устаревшие политики
Имя раздела реестра	Software\Policies\Microsoft\Windows\WindowsUpdate
Имя файла ADMX	WindowsUpdate.admx

EngagedRestartSnoozeSchedule

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования ✅ IIoT Enterprise или IoT Enterprise LTSC	✅Windows 10, версия 1703 [10.0.15063] и более поздние

Device

```
./Device/Vendor/MSFT/Policy/Config/Update/EngagedRestartSnoozeSchedule
```

Включите эту политику для управления временем перед переходом с автоматических перезапусков, запланированных в нерабочее время, на Занятая перезагрузка, что требует от пользователя расписания. Период можно задать от 0 до 30 дней с момента ожидания перезапуска.

Вы можете указать количество дней, в течение которых пользователь может отложить уведомления о напоминаниях о перезапуске. Период отсрочки может быть установлен от 1 до 3 дней.

Вы можете указать крайний срок в днях перед автоматическим планированием и выполнением ожидающего перезапуска независимо от активных часов. Крайний срок может иметь значение от 2 до 30 дней с момента, когда перезапуск становится отложенным. Если этот параметр настроен, ожидающий перезапуск будет переходить от автоматического перезапуска к включенному перезапуску (ожидание пользовательского расписания) к автоматическому выполнению в течение указанного периода.

Если вы не укажете крайний срок или для него задано значение 0, компьютер не перезагрузится автоматически и потребует от пользователя запланировать его перед перезапуском.

Если вы отключите или не настроите эту политику, компьютер перезагрузится по расписанию по умолчанию.

Включение любой из следующих политик переопределит указанную выше политику:

1. Нет автоматического перезапуска для вошедшего в систему пользователей для запланированных автоматических установок обновлений
2. Всегда автоматически перезапускается по расписанию.
3. Укажите крайний срок перед автоматическим перезапуском для установки обновлений.

Описание свойств инфраструктуры:

Развернуть таблицу

Имя свойства	Значение свойства
Формат	`int`
Тип доступа	Добавить, удалить, получить, заменить
Допустимые значения	Диапазон: `[1-3]`
Значение по умолчанию	3

Сопоставление групповой политики:

Развернуть таблицу

Имя	Значение
Имя	EngagedRestartTransitionSchedule
Понятное имя	Указание расписания перехода с задействованным перезапуском и расписания уведомлений для обновлений
Имя элемента	Отложенный (в днях)
Location	Конфигурация компьютера
Путь	Компоненты > Windows клиентский компонент Центра обновления Windows > устаревшие политики
Имя раздела реестра	Software\Policies\Microsoft\Windows\WindowsUpdate
Имя файла ADMX	WindowsUpdate.admx

EngagedRestartSnoozeScheduleForFeatureUpdates

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования ✅ IIoT Enterprise или IoT Enterprise LTSC	✅Windows 10, версия 1809 [10.0.17763] и более поздних версий

Device

```
./Device/Vendor/MSFT/Policy/Config/Update/EngagedRestartSnoozeScheduleForFeatureUpdates
```

Включите эту политику для управления временем перед переходом с автоматических перезапусков, запланированных в нерабочее время, на Занятая перезагрузка, что требует от пользователя расписания. Период можно задать от 0 до 30 дней с момента ожидания перезапуска.

Вы можете указать количество дней, в течение которых пользователь может отложить уведомления о напоминаниях о перезапуске. Период отсрочки может быть установлен от 1 до 3 дней.

Вы можете указать крайний срок в днях перед автоматическим планированием и выполнением ожидающего перезапуска независимо от активных часов. Крайний срок может иметь значение от 2 до 30 дней с момента, когда перезапуск становится отложенным. Если этот параметр настроен, ожидающий перезапуск будет переходить от автоматического перезапуска к включенному перезапуску (ожидание пользовательского расписания) к автоматическому выполнению в течение указанного периода.

Если вы не укажете крайний срок или для него задано значение 0, компьютер не перезагрузится автоматически и потребует от пользователя запланировать его перед перезапуском.

Если вы отключите или не настроите эту политику, компьютер перезагрузится по расписанию по умолчанию.

Включение любой из следующих политик переопределит указанную выше политику:

1. Нет автоматического перезапуска для вошедшего в систему пользователей для запланированных автоматических установок обновлений
2. Всегда автоматически перезапускается по расписанию.
3. Укажите крайний срок перед автоматическим перезапуском для установки обновлений.

Описание свойств инфраструктуры:

Развернуть таблицу

Имя свойства	**Значение свойства**
Формат	`int`
Тип доступа	Добавить, удалить, получить, заменить
Допустимые значения	Диапазон: `[1-3]`
Значение по умолчанию	3

Сопоставление групповой политики:

Развернуть таблицу

Имя	**Значение**
Имя	EngagedRestartTransitionSchedule

Имя	Значение
Понятное имя	Указание расписания перехода с задействованным перезапуском и расписания уведомлений для обновлений
Имя элемента	Отложенный (в днях)
Location	Конфигурация компьютера
Путь	Компоненты > Windows клиентский компонент Центра обновления Windows > устаревшие политики
Имя раздела реестра	Software\Policies\Microsoft\Windows\WindowsUpdate
Имя файла ADMX	WindowsUpdate.admx

EngagedRestartTransitionSchedule

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования ✅ IIoT Enterprise или IoT Enterprise LTSC	✅Windows 10, версия 1703 [10.0.15063] и более поздние

Device

```
./Device/Vendor/MSFT/Policy/Config/Update/EngagedRestartTransitionSchedule
```

Включите эту политику для управления временем перед переходом с автоматических перезапусков, запланированных в нерабочее время, на Занятая перезагрузка, что требует от пользователя расписания. Период можно задать от 0 до 30 дней с момента ожидания перезапуска.

Вы можете указать количество дней, в течение которых пользователь может отложить уведомления о напоминаниях о перезапуске. Период отсрочки может быть установлен от 1 до 3 дней.

Вы можете указать крайний срок в днях перед автоматическим планированием и выполнением ожидающего перезапуска независимо от активных часов. Крайний срок

может иметь значение от 2 до 30 дней с момента, когда перезапуск становится отложенным. Если этот параметр настроен, ожидающий перезапуск будет переходить от автоматического перезапуска к включенному перезапуску (ожидание пользовательского расписания) к автоматическому выполнению в течение указанного периода.

Если вы не укажете крайний срок или для него задано значение 0, компьютер не перезагрузится автоматически и потребует от пользователя запланировать его перед перезапуском.

Если вы отключите или не настроите эту политику, компьютер перезагрузится по расписанию по умолчанию.

Включение любой из следующих политик переопределит указанную выше политику:

1. Нет автоматического перезапуска для вошедшего в систему пользователей для запланированных автоматических установок обновлений
2. Всегда автоматически перезапускается по расписанию.
3. Укажите крайний срок перед автоматическим перезапуском для установки обновлений.

Описание свойств инфраструктуры:

Развернуть таблицу

Имя свойства	**Значение свойства**
Формат	`int`
Тип доступа	Добавить, удалить, получить, заменить
Допустимые значения	Диапазон: `[0-30]`
Значение по умолчанию	7

Сопоставление групповой политики:

Развернуть таблицу

Имя	**Значение**
Имя	EngagedRestartTransitionSchedule
Понятное имя	Указание расписания перехода с задействованным перезапуском и расписания уведомлений для обновлений

Имя	Значение
Имя элемента	Переход (в днях)
Location	Конфигурация компьютера
Путь	Компоненты > Windows клиентский компонент Центра обновления Windows > устаревшие политики
Имя раздела реестра	Software\Policies\Microsoft\Windows\WindowsUpdate
Имя файла ADMX	WindowsUpdate.admx

EngagedRestartTransitionScheduleForFeatureUpdates

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования ✅ IIoT Enterprise или IoT Enterprise LTSC	✅Windows 10, версия 1809 [10.0.17763] и более поздних версий

Device

```
./Device/Vendor/MSFT/Policy/Config/Update/EngagedRestartTransitionScheduleForFeatureUpdates
```

Включите эту политику для управления временем перед переходом с автоматических перезапусков, запланированных в нерабочее время, на Занятая перезагрузка, что требует от пользователя расписания. Период можно задать от 0 до 30 дней с момента ожидания перезапуска.

Вы можете указать количество дней, в течение которых пользователь может отложить уведомления о напоминаниях о перезапуске. Период отсрочки может быть установлен от 1 до 3 дней.

Вы можете указать крайний срок в днях перед автоматическим планированием и выполнением ожидающего перезапуска независимо от активных часов. Крайний срок может иметь значение от 2 до 30 дней с момента, когда перезапуск становится отложенным. Если этот параметр настроен, ожидающий перезапуск будет переходить от

автоматического перезапуска к включенному перезапуску (ожидание пользовательского расписания) к автоматическому выполнению в течение указанного периода.

Если вы не укажете крайний срок или для него задано значение 0, компьютер не перезагрузится автоматически и потребует от пользователя запланировать его перед перезапуском.

Если вы отключите или не настроите эту политику, компьютер перезагрузится по расписанию по умолчанию.

Включение любой из следующих политик переопределит указанную выше политику:

1. Нет автоматического перезапуска для вошедшего в систему пользователей для запланированных автоматических установок обновлений
2. Всегда автоматически перезапускается по расписанию.
3. Укажите крайний срок перед автоматическим перезапуском для установки обновлений.

Описание свойств инфраструктуры:

Развернуть таблицу

Имя свойства	Значение свойства
Формат	`int`
Тип доступа	Добавить, удалить, получить, заменить
Допустимые значения	Диапазон: `[0-30]`
Значение по умолчанию	7

Сопоставление групповой политики:

Развернуть таблицу

Имя	Значение
Имя	EngagedRestartTransitionSchedule
Понятное имя	Указание расписания перехода с задействованным перезапуском и расписания уведомлений для обновлений
Имя элемента	Переход (в днях)
Location	Конфигурация компьютера

Имя	Значение
Путь	Компоненты > Windows клиентский компонент Центра обновления Windows > устаревшие политики
Имя раздела реестра	Software\Policies\Microsoft\Windows\WindowsUpdate
Имя файла ADMX	WindowsUpdate.admx

IgnoreMOAppDownloadLimit

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования ✅ IIoT Enterprise или IoT Enterprise LTSC	✅Windows 10, версия 1703 [10.0.15063] и более поздние

Device

```
./Device/Vendor/MSFT/Policy/Config/Update/IgnoreMOAppDownloadLimit
```

Указывает, следует ли игнорировать ограничение мобильного оператора (MO) на скачивание (разрешить неограниченное скачивание) по сети мобильной связи для приложений и их обновлений. Если требуются ограничения более низкого уровня (например, ограничения для мобильных устройств), эти ограничения управляются внешними политиками.

> ⚠ **Предупреждение**
>
> Настройка этой политики может привести к взиманию средств мобильными операторами (MO).

Чтобы проверить эту политику:

1. Включите политику и убедитесь, что устройство находится в сотовой сети.

2. Запустите запланированную задачу на своем устройстве, чтобы проверить наличие обновлений для приложения в фоновом режиме. Например, на устройстве выполните следующие команды в TShell:

```
TShell
exec-device schtasks.exe -arguments '/run /tn
"\Microsoft\Windows\WindowsUpdate\Automatic App Update" /I'
```

Описание свойств инфраструктуры:

Развернуть таблицу

Имя свойства	Значение свойства
Формат	`int`
Тип доступа	Добавить, удалить, получить, заменить
Значение по умолчанию	0

Допустимые значения:

Развернуть таблицу

Значение	Описание
0 (по умолчанию)	Не игнорируйте ограничение загрузки mo для приложений и их обновлений.
1	Игнорировать ограничение загрузки MO (разрешить неограниченное скачивание) для приложений и их обновлений.

IgnoreMOUpdateDownloadLimit

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования ✅ IIoT Enterprise или IoT Enterprise LTSC	✅Windows 10, версия 1703 [10.0.15063] и более поздние

Device

```
./Device/Vendor/MSFT/Policy/Config/Update/IgnoreMOUpdateDownloadLimit
```

Указывает, следует ли игнорировать ограничение мобильного оператора (MO) на скачивание (разрешить неограниченное скачивание) по сети мобильной связи для обновлений ОС. Если требуются ограничения более низкого уровня (например, ограничения для мобильных устройств), эти ограничения управляются внешними политиками.

> ⚠ **Предупреждение**
>
> Настройка этой политики может привести к взиманию средств мобильными операторами (MO).

Чтобы проверить эту политику:

1. Включите политику и убедитесь, что устройство находится в сотовой сети.
2. Запустите запланированную задачу на своем устройстве, чтобы проверить наличие обновлений для приложения в фоновом режиме. Например, на устройстве выполните следующие команды в TShell:

   TShell

   ```
   exec-device schtasks.exe -arguments '/run /tn
   "\Microsoft\Windows\WindowsUpdate\Automatic App Update" /I'
   ```

Описание свойств инфраструктуры:

Развернуть таблицу

Имя свойства	Значение свойства
Формат	`int`
Тип доступа	Добавить, удалить, получить, заменить
Значение по умолчанию	0

Допустимые значения:

Развернуть таблицу

Значение	Описание
0 (по умолчанию)	Не игнорируйте ограничение загрузки MO для обновлений ОС.
1	Игнорировать ограничение загрузки MO (разрешить неограниченное скачивание) для обновлений ОС.

PauseDeferrals

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования ✅ IIoT Enterprise или IoT Enterprise LTSC	✅Windows 10, версия 1607 [10.0.14393] и более поздние

Device

```
./Device/Vendor/MSFT/Policy/Config/Update/PauseDeferrals
```

Примечание.

Не используйте эту политику на устройствах с Windows 10 версии 1607, вместо этого используйте новые политики, перечисленные в разделе Изменения в Windows 10 версии 1607, для управления обновлениями. Можно продолжать использовать PauseDeferrals для устройств с Windows 10 версии 1511. Позволяет ИТ-администраторам приостанавливать обновления на срок до 5 недель. Приостановленные отсрочки сбрасываются через 5 недель. Если включена политика Указать размещение службы обновлений Майкрософт в интрасети, параметры Отложить изменения на срок, Отложить обновления на срок и Приостановить обновления и изменения не будут действовать. Если включена политика Разрешить телеметрию и настройке "Параметры" присвоено значение 0, параметры Отложить изменения на срок, Отложить обновления на срок и Приостановить обновления и изменения не будут действовать.

Описание свойств инфраструктуры:

Развернуть таблицу

Имя свойства	Значение свойства
Формат	`int`
Тип доступа	Добавить, удалить, получить, заменить
Значение по умолчанию	0

Допустимые значения:

Развернуть таблицу

Значение	Описание
0 (по умолчанию)	Отсрочки не приостанавливаются.
1	Отсрочки приостанавливаются.

Сопоставление групповой политики:

Развернуть таблицу

Имя	Значение
Имя	DeferUpgrade
Путь	WindowsUpdate > AT > WindowsComponents > WindowsUpdateCat
Имя элемента	PauseDeferralsId

PhoneUpdateRestrictions

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования ✅ IIoT Enterprise или IoT Enterprise LTSC	✅Windows 10, версия 1703 [10.0.15063] и более поздние

Device

```
./Device/Vendor/MSFT/Policy/Config/Update/PhoneUpdateRestrictions
```

Этот параметр политики является устаревшим. Вместо этого используйте Update/RequireUpdateApproval.

Описание свойств инфраструктуры:

Развернуть таблицу

Имя свойства	Значение свойства
Формат	`int`
Тип доступа	Добавить, удалить, получить, заменить
Допустимые значения	Диапазон: `[0-4]`
Значение по умолчанию	4

RequireDeferUpgrade

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования ✅ IIoT Enterprise или IoT Enterprise LTSC	✅Windows 10, версия 1607 [10.0.14393] и более поздние

Device

```
./Device/Vendor/MSFT/Policy/Config/Update/RequireDeferUpgrade
```

> ⓘ **Примечание.**
>
> Не используйте эту политику на устройствах с Windows 10 версии 1607, вместо этого используйте новые политики, перечисленные в разделе Изменения в Windows 10 версии 1607, для управления обновлениями. Вы можете продолжать использовать RequireDeferUpgrade для устройств с Windows 10 версии 1511. Позволяет ИТ-администратору настроить устройство для обучения Semi-Annual Channel.

Описание свойств инфраструктуры:

Развернуть таблицу

Имя свойства	Значение свойства
Формат	`int`
Тип доступа	Добавить, удалить, получить, заменить
Значение по умолчанию	0

Допустимые значения:

Развернуть таблицу

Значение	Описание
0 (по умолчанию)	Пользователь получает обновления из канала Semi-Annual (targeted).
1	Пользователь получает обновления из канала Semi-Annual.

Сопоставление групповой политики:

Развернуть таблицу

Имя	Значение
Имя	DeferUpgrade
Путь	WindowsUpdate > AT > WindowsComponents > WindowsUpdateCat
Имя элемента	DeferUpgradePeriodId

RequireUpdateApproval

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования ✅ IIoT Enterprise или IoT Enterprise LTSC	✅Windows 10, версия 1507 [10.0.10240] и более поздние

Device
`./Device/Vendor/MSFT/Policy/Config/Update/RequireUpdateApproval`

> **Примечание.**
>
> Если вы ранее использовали политику Update/PhoneUpdateRestrictions в предыдущих версиях Windows, она устарела. Используйте вместо нее эту политику. Позволяет ИТ-администратору ограничить обновления, устанавливаемые на устройстве, только теми, которые находятся в списке утверждения обновлений. Это позволяет ИТ-специалистам принять лицензионное соглашение (EULA), связанное с утвержденным обновлением от имени конечного пользователя. Соглашения EULA утверждаются после утверждения обновления.

Описание свойств инфраструктуры:

Развернуть таблицу

Имя свойства	Значение свойства
Формат	`int`
Тип доступа	Добавить, удалить, получить, заменить
Значение по умолчанию	0

Допустимые значения:

Развернуть таблицу

Значение	Описание
0 (по умолчанию)	Не настроено. Устройство устанавливает все применимые обновления.
1	Устройство устанавливает только обновления, которые применимы и находятся в списке Утвержденные Обновления. Присвойте этой политике значение 1, если ИТ-отдел хочет управлять развертыванием обновлений на устройствах, например при обязательном тестировании перед развертыванием.

ScheduleImminentRestartWarning

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования ✅ IIoT Enterprise или IoT Enterprise LTSC	✅Windows 10, версия 1703 [10.0.15063] и более поздние

Device

```
./Device/Vendor/MSFT/Policy/Config/Update/ScheduleImminentRestartWarning
```

Включите эту политику, чтобы управлять отображением уведомлений, предупреждающих пользователей о запланированном перезапуске для крайнего срока установки обновления. Пользователи не могут отложить запланированный перезапуск после достижения крайнего срока и перезапуска выполняется автоматически.

Указывает время до запланированного перезапуска для отображения напоминания о предупреждении для пользователя.

Вы можете указать время до запланированного перезапуска, чтобы уведомить пользователя о том, что автоматический перезапуск неизбежен, чтобы позволить ему сэкономить свою работу.

Если вы отключите или не настроите эту политику, будет использоваться поведение уведомлений по умолчанию.

Описание свойств инфраструктуры:

Развернуть таблицу

Имя свойства	Значение свойства
Формат	`int`
Тип доступа	Добавить, удалить, получить, заменить
Значение по умолчанию	15

Допустимые значения:

Развернуть таблицу

Значение	Описание
15 (по умолчанию)	15 минут.
30	30 минут.
60	60 минут.

Сопоставление групповой политики:

Развернуть таблицу

Имя	Значение
Имя	RestartWarnRemind
Понятное имя	Настройка расписания оповещений об автоматическом перезапуске для обновлений
Имя элемента	Предупреждение (мин.)
Location	Конфигурация компьютера
Путь	Компоненты > Windows клиентский компонент Центра обновления Windows > устаревшие политики
Имя раздела реестра	Software\Policies\Microsoft\Windows\WindowsUpdate
Имя файла ADMX	WindowsUpdate.admx

ScheduleRestartWarning

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования ✅ IIoT Enterprise или IoT Enterprise LTSC	✅Windows 10, версия 1703 [10.0.15063] и более поздние

Device

```
./Device/Vendor/MSFT/Policy/Config/Update/ScheduleRestartWarning
```

Включите эту политику, чтобы управлять отображением уведомлений, предупреждающих пользователей о запланированном перезапуске для крайнего срока установки обновления. Пользователи не могут отложить запланированный перезапуск после достижения крайнего срока и перезапуска выполняется автоматически.

Указывает время до запланированного перезапуска для отображения напоминания о предупреждении для пользователя.

Вы можете указать время до запланированного перезапуска, чтобы уведомить пользователя о том, что автоматический перезапуск неизбежен, чтобы позволить ему сэкономить свою работу.

Если вы отключите или не настроите эту политику, будет использоваться поведение уведомлений по умолчанию.

Описание свойств инфраструктуры:

Развернуть таблицу

Имя свойства	Значение свойства
Формат	`int`
Тип доступа	Добавить, удалить, получить, заменить
Значение по умолчанию	4

Допустимые значения:

Развернуть таблицу

Значение	Описание
2	2 часа.
4 (по умолчанию)	4 часа.
8	8 часов.
12	12 часов.
24	24 часа.

Сопоставление групповой политики:

Развернуть таблицу

Имя	Значение
Имя	RestartWarnRemind
Понятное имя	Настройка расписания оповещений об автоматическом перезапуске для обновлений
Имя элемента	Напоминание (часы)
Location	Конфигурация компьютера
Путь	Компоненты > Windows клиентский компонент Центра обновления Windows > устаревшие политики
Имя раздела реестра	Software\Policies\Microsoft\Windows\WindowsUpdate
Имя файла ADMX	WindowsUpdate.admx

SetAutoRestartNotificationDisable

Развернуть таблицу

Область применения	Выпуски	Применимая ОС
Устройство ✅ Пользователь ❌	✅ Pro ✅ Enterprise ✅ для образования ✅ IIoT Enterprise или IoT Enterprise LTSC	✅Windows 10, версия 1703 [10.0.15063] и более поздние

Device

```
./Device/Vendor/MSFT/Policy/Config/Update/SetAutoRestartNotificationDisable
```

Этот параметр политики позволяет контролировать, получают ли пользователи уведомления об автоматическом перезапуске для установки обновлений, включая уведомления о напоминаниях и предупреждениях.

Включите эту политику, чтобы отключить все уведомления об автоматическом перезапуске.

Если эта политика отключена или не настроена, поведение уведомлений по умолчанию будет неизменным.

Описание свойств инфраструктуры:

Развернуть таблицу

Имя свойства	Значение свойства
Формат	`int`
Тип доступа	Добавить, удалить, получить, заменить
Значение по умолчанию	0

Допустимые значения:

Развернуть таблицу

Значение	Описание
0 (по умолчанию)	Включено.
1	Служба отключена.

Сопоставление групповой политики:

Развернуть таблицу

Имя	Значение
Имя	AutoRestartNotificationDisable
Понятное имя	Отключение уведомлений об автоматическом перезапуске для установки обновлений
Location	Конфигурация компьютера
Путь	Компоненты > Windows клиентский компонент Центра обновления Windows > устаревшие политики
Имя раздела реестра	Software\Policies\Microsoft\Windows\WindowsUpdate
Имя файла ADMX	WindowsUpdate.admx

Изменения в Windows 10, версия 1607

Ниже приведены новые политики, добавленные в Windows 10 версии 1607. Используйте эти политики для устройств Windows 10 версии 1607 вместо старых политик

- ActiveHoursEnd
- ActiveHoursStart
- AllowMUUpdateService
- BranchReadinessLevel
- DeferFeatureUpdatePeriodInDays
- DeferQualityUpdatePeriodInDays
- ExcludeWUDriversInQualityUpdate
- PauseFeatureUpdates
- PauseQualityUpdates

Ниже представлен список старых политик, которые по-прежнему поддерживаются для обеспечения обратной совместимости. Эти старые политики можно использовать для устройств с Windows 10 версии 1511.

- RequireDeferUpgrade
- DeferUpgradePeriod
- DeferUpdatePeriod
- PauseDeferrals

Связанные статьи

Поставщик служб конфигурации политики

Last updated on 04.04.2025

Обновление других продуктов Майкрософт

Применяется к: ✅ Windows 11, ✅ Windows 10

Эта статья содержит список других продуктов Майкрософт, которые могут быть обновлены при использовании следующей политики:

- **Групповая политика**: Конфигурация компьютера\Административные шаблоны\Компоненты Windows\клиентский компонент Центра обновления Windows\Управление пользовательским интерфейсом\Настройка автоматического Обновления
  - `Install updates for other Microsoft products` элемент в разделе Настройка автоматического Обновления
- **MDM**: ./Device/Vendor/MSFT/Policy/Config/Update/AllowMUUpdateService

> ⓘ **Примечание.**
>
> Эта политика включает драйверы. Если необходимо исключить драйверы, используйте ExcludeWUDriversInQualityUpdate.

Список других продуктов Майкрософт

Ниже приведен список других продуктов Майкрософт, которые могут быть обновлены.

- Служба управления правами Active Directory
- AppFabric
- Агент подключенного компьютера Azure
- Синхронизация файлов Azure
- Панель Bing
- Bing IME
- BizTalk
- IME для Восточной Азии для содержимого Windows
- Exchange
- Обновление словаря IME
- Живой поиск
- MED-V
- Microsoft Advanced Threat Analytics
- Виртуализация приложений Майкрософт
- Microsoft Azure StorSimple

- Microsoft Configuration Manager
- Microsoft Dynamics CRM
- Microsoft Information Protection
- Microsoft Lync Server и Microsoft Lync
- Microsoft Monitoring Agent
- Устройство Microsoft SRS
- Microsoft StreamInsight
- Мобильные устройства и Интернет вещей
- MSRC
- .NET (также известный как .NET Core)
- Office 2016 (msi-версии Office)
- PlayReady
- Обновления аналитики безопасности для антивирусной программы Microsoft Defender и других антивредоносных программ Майкрософт
- Silverlight
- Skype для бизнеса
- SQL
- Контроллер приложений System Center
- System Center Data Protection Manager
- System Center Operations Manager
- System Center Orchestrator
- System Center Virtual Machine Manager
- Visual Studio
- Windows Admin Center
- Windows Azure Hyper-V диспетчер восстановления
- Windows Azure Pack — веб-сайты
- Windows Azure Pack
- Windows Служебная шина Azure
- Windows Embedded Developer Update
- помощник по входу в Windows Live
- Windows Small Business Server
- Zune

Last updated on 01.04.2025

Справочник по оптимизации доставки

Применяется к: ✅ Windows 11, ✅ Windows 10, ✅ Delivery Optimization

> **Ищете объекты групповая политика?** См. справочник по оптимизации доставки или основную электронную таблицу, доступную в Центре загрузки для Windows 11 или для Windows 10.

В разделе Оптимизация доставки можно задать множество параметров конфигурации, чтобы настроить процесс доставки содержимого с учетом потребностей вашей среды. В этой статье приведены общие сведения об этих конфигурациях для справки. Если вам просто нужен обзор оптимизации доставки, см. статью Что такое оптимизация доставки. Если вам нужны сведения о настройке оптимизации доставки, включая советы по лучшим параметрам в разных сценариях, см. статью Настройка оптимизации доставки для Windows.

Параметры оптимизации доставки

Вы можете использовать групповую политику или решение MDM, например Intune, для настройки оптимизации доставки.

Параметры оптимизации доставки в групповая политика находятся в разделе **Конфигурация\Политики\Административные шаблоны\Компоненты Windows\Оптимизация доставки**. В MDM те же параметры находятся в разделе **.Vendor/MSFT/Policy/Config/DeliveryOptimization/**.

Сводка параметров оптимизации доставки

Развернуть таблицу

Параметр групповой политики	Параметр MDM	Поддерживается с версии	Примечания
Режим скачивания	DODownloadMode	1511	По умолчанию настроена локальная сеть (1). Режим загрузки группы (2) в сочетании с идентификатором группы позволяет администраторам создавать пользовательские группы устройств, которые

Параметр групповой политики	Параметр MDM	Поддерживается с версии	Примечания
			совместно используют содержимое между устройствами в группе.
Идентификатор группы	DOGroupID	1511	Используется в режиме группового скачивания. Если параметр не настроен, проверка GroupIDSource. Если политики GroupID или GroupIDSource не настроены, идентификатор GroupID определяется как сайт AD (1), идентификатор домена с проверкой подлинности (2) или идентификатор клиента Microsoft Entra (5) в этом порядке.
Выберите источник идентификаторов групп.	DOGroupIDSource	1803	Если параметр не настроен, проверка идентификатор группы. Если политики GroupID или GroupIDSource не настроены, группа определяется как сайт AD (1), идентификатор домена с проверкой подлинности (2)

Параметр групповой политики	Параметр MDM	Поддерживается с версии	Примечания
			или идентификатор клиента Microsoft Entra (5) в этом порядке.
Выбор метода ограничения выбора одноранговой узла	DORestrictPeerSelectionBy	1803	Значение по умолчанию не настроено.
Минимальный объем ОЗУ (включительно), разрешенный для использования одноранговой кэширования	DOMinRAMAllowedToPeer	1703	Значение по умолчанию — 4 ГБ.
Минимальный размер диска, разрешенный для использования одноранговой кэширования	DOMinDiskSizeAllowedToPeer	1703	Значение по умолчанию — 32 ГБ.
Максимальный срок действия кэша	DOMaxCacheAge	1511	Значение по умолчанию — 259 200 секунд (три дня).
Максимальный размер кэша	DOMaxCacheSize	1511	Значение по умолчанию — 20 %.
Абсолютный максимальный размер кэша (в ГБ)	DOAbsoluteMaxCacheSize	1607	Значение по умолчанию не настроено.
Изменение диска кэша	DOModifyCacheDrive	1607	По умолчанию диск операционной системы проходит через переменную

Параметр групповой политики	Параметр MDM	Поддерживается с версии	Примечания
			среды %SYSTEMDRIVE%.
Минимальный размер файла содержимого одноранговой кэширования	DOMinFileSizeToCache	1703	Размер файла по умолчанию — 50 МБ.
Ограничение для ежемесячной отправки данных	DOMonthlyUploadDataCap	1607	Значение по умолчанию — 20 ГБ.
Минимальное качество обслуживания в фоновом режиме	DOMinBackgroundQoS	1607	Значение по умолчанию — 20 МБ/с.
Включение одноранговой кэширования при подключении устройства через VPN	DOAllowVPNPeerCaching	1709	По умолчанию запрещается пиринг при подключении к VPN.
Ключевые слова VPN	DOVpnKeywords	Windows 11 версии 22H2 с установленным обновлением за сентябрь 2023 г. или более поздней	Позволяет задать одно или несколько ключевых слов, используемых для распознавания VPN-подключений.
Запретить загрузку сервера кэша из VPN	DODisallowCacheServerDownloadsOnVPN	Windows 11 версии 22H2 с установленным обновлением за сентябрь 2023 г. или более поздней	Запретить скачивание с серверов подключенного кэша Майкрософт при подключении устройства через VPN. По умолчанию устройство может загружаться из подключенного кэша Майкрософт

Параметр групповой политики	Параметр MDM	Поддерживается с версии	Примечания
			при подключении через VPN.
Разрешить отправку, когда устройство находится в батарее при заданном уровне заряда батареи	DOMinBatteryPercentageAllowedToUpload	1709	По умолчанию пиринг не разрешен во время работы батареи.
Максимальная пропускная способность загрузки переднего плана (в процентах)	DOPercentageMaxForegroundBandwidth	1803	По умолчанию используется значение "0", которое будет динамически изменяться.
Максимальная пропускная способность фонового скачивания (в процентах)	DOPercentageMaxBackgroundBandwidth	1803	По умолчанию используется значение "0", которое будет динамически изменяться.
Максимальная пропускная способность загрузки переднего плана (в КБ/с)	DOMaxForegroundDownloadBandwidth	2004	По умолчанию используется значение "0", которое будет динамически изменяться.
Максимальная пропускная способность фонового скачивания (в КБ/с)	DOMaxBackgroundDownloadBandwidth	2004	По умолчанию используется значение "0", которое будет динамически изменяться.
Установка часов для ограничения пропускной способности загрузки переднего плана	DOSetHoursToLimitForegroundDownloadBandwidth	1803	Значение по умолчанию не настроено.
Установка часов для ограничения пропускной	DOSetHoursToLimitBackgroundDownloadBandwidth	1803	Значение по умолчанию не настроено.

Параметр групповой политики	Параметр MDM	Поддерживается с версии	Примечания
способности фонового скачивания			
Задержка загрузки переднего плана с HTTP (в секундах)	DODelayForegroundDownloadFromHttp	1803	Значение по умолчанию не настроено. Для пиринга используйте эту политику, чтобы отложить возврат к источнику HTTP. Дополнительные сведения о различных вариантах задержки.
Задержка фоновой загрузки с HTTP (в секундах)	DODelayBackgroundDownloadFromHttp	1803	Значение по умолчанию не настроено. Для пиринга используйте эту политику, чтобы отложить возврат к источнику HTTP. Дополнительные сведения о различных вариантах задержки.
Задержка загрузки резервного сервера кэша переднего плана (в секундах)	DelayCacheServerFallbackForeground	1903	Значение по умолчанию не настроено. Для содержимого подключенного кэша (Майкрософт) используйте эту политику, чтобы отложить возврат к источнику HTTP. Дополнительные сведения о различных вариантах задержки.

Параметр групповой политики	Параметр MDM	Поддерживается с версии	Примечания
Задержка резервного размещения сервера кэша фонового скачивания (в секундах)	DelayCacheServerFallbackBackground	1903	Значение по умолчанию не настроено. Для содержимого подключенного кэша (Майкрософт) используйте эту политику, чтобы отложить возврат к источнику HTTP. Дополнительные сведения о различных вариантах задержки.
Имя узла сервера кэша	DOCacheHost	1809	Значение по умолчанию не настроено.
Источник имени узла сервера кэша	DOCacheHostSource	2004	Значение по умолчанию не настроено.
Максимальная пропускная способность для скачивания	DOMaxDownloadBandwidth	1607 (не рекомендуется использовать в Windows 10 версии 2004); вместо этого используйте максимальную пропускную способность фонового скачивания (в КБ/с) или максимальную пропускную способность загрузки на переднем плане (в КБ/с)	По умолчанию используется значение "0", которое будет динамически изменяться.
Процент максимальной пропускной	DOPercentageMaxDownloadBandwidth	1607 (не рекомендуется использовать в Windows 10	По умолчанию используется значение "0", которое будет

Параметр групповой политики	Параметр MDM	Поддерживается с версии	Примечания
способности скачивания		версии 2004); вместо этого используйте максимальную пропускную способность фонового скачивания (в КБ/с) или максимальную пропускную способность загрузки на переднем плане (в КБ/с)	динамически изменяться.
Максимальная пропускная способность отправки	DOMaxUploadBandwidth	1607 (не рекомендуется в Windows 10, версия 2004)	Значение по умолчанию — "0" (неограниченно).

Дополнительные сведения о параметрах оптимизации доставки

Локально кэшированные обновления

Оптимизация доставки использует локально кэшированные обновления для доставки контактов через одноранговые узлы. Чем больше содержимого доступно в кэше, тем больше вероятность использования пиринга. В случаях, когда на устройствах достаточно локального хранилища, и вы хотите кэшировать больше содержимого. Аналогичным образом, если хранилище ограничено и вы предпочитаете кэшировать меньше, используйте следующие параметры, чтобы настроить кэш оптимизации доставки в соответствии с вашим сценарием:

- DOMaxCacheSize и DOAbsoluteMaxCacheSize управляют объемом пространства, которое может использовать кэш оптимизации доставки.
- DOMaxCacheAge управляет периодом хранения для каждого обновления в кэше.
- Системный диск является расположением по умолчанию для кэша оптимизации доставки. DOModifyCacheDrive позволяет администраторам изменять это расположение.

> ⓘ **Примечание.**

Можно настроить предпочитаемые устройства кэша. Дополнительные сведения см. в разделе DOGroupID.

Размер всех кэшированных файлов должен превышать установленное минимальное значение. Размер автоматически устанавливается облачными службами оптимизации доставки, но если локального хранилища достаточно, а сеть не перегружена, администраторы могут выбрать этот вариант для повышения производительности. Вы можете задать минимальный размер файлов для кэширования, настроив DOMinFileSizeToCache.

Влияние на сеть

Дополнительные параметры, которые определяют влияние оптимизации доставки на вашу сеть, включают следующие параметры:

- Минимальное фоновое качество обслуживания позволяет администраторам гарантировать минимальную скорость скачивания для обновлений Windows. Этот параметр изменяет объем данных, скачанных непосредственно из источников HTTP, а не из других одноранговых узлов в сети.
- Максимальная пропускная способность загрузки переднего плана указывает максимальную пропускную способность загрузки переднего плана, используемую оптимизацией доставки во всех одновременных действиях загрузки в процентах от доступной пропускной способности загрузки.
- Максимальная пропускная способность фонового скачивания указывает максимальную пропускную способность фонового скачивания, используемую оптимизацией доставки во всех одновременных действиях загрузки в процентах от доступной пропускной способности загрузки.
- Параметр "Рабочие часы" для параметра Ограничение пропускной способности фонового скачивания задает максимальную пропускную способность фонового скачивания, используемую оптимизацией доставки в рабочее время и вне рабочих часов во всех одновременных действиях загрузки в процентах от доступной пропускной способности загрузки.
- Для параметра "Рабочие часы" для параметра Ограничение пропускной способности загрузки переднего плана указывается максимальная пропускная способность загрузки переднего плана, используемая оптимизацией доставки в рабочее время и за пределами рабочих часов во всех одновременных действиях загрузки в процентах от доступной пропускной способности загрузки.
- Выбор метода для ограничения выбора одноранговых узлов ограничивает выбор одноранговых узла выбранными параметрами.
- Выбор источника идентификаторов групп ограничивает выбор одноранговых узла определенным источником.

Политики для приоритета использования одноранговых и кэш-серверных источников

Если клиент оптимизации доставки настроен для использования одноранговых узлов и подключенного кэша Майкрософт, то для достижения наилучшей возможности доставки содержимого клиент подключается как к подключенной кэшу, так и к одноранговым узлам параллельно. Если нужное содержимое не удается получить из подключенного кэша или одноранговых узлов, оптимизация доставки автоматически вернется к источнику HTTP, чтобы получить запрошенное содержимое. Существует четыре параметра, которые позволяют определить приоритет одноранговых или подключенных источников кэша, отложив немедленный возврат к источнику HTTP, что является поведением по умолчанию.

Резервные параметры задержки одноранговой связи

- Задержка загрузки переднего плана с HTTP (в секундах) позволяет отложить использование источника HTTP при загрузке на переднем (интерактивном) плане, для которой разрешено использовать P2P.
- Задержка фоновой загрузки с HTTP (в секундах) позволяет отложить использование источника HTTP в фоновой загрузке, которая может использовать P2P.

Резервные параметры задержки подключенного кэша (Майкрософт)

- Задержка загрузки резервного сервера кэша на переднем плане (в секундах) позволяет отложить использование источника HTTP при загрузке на переднем плане (интерактивном) для использования сервера кэша.
- Резервный резерв сервера кэша задержки фонового скачивания (в секундах) позволяет отложить использование источника HTTP в фоновой загрузке, которая может использовать сервер кэша.

Если настроены одноранговые и подключенные кэши, параметры задержки однорангового узла будут иметь приоритет над параметрами задержки сервера кэша. Этот параметр позволяет оптимизации доставки сначала обнаруживать одноранговые узлы, а затем распознавать резервный параметр для сервера кэша подключенного кэша.

Использование системных ресурсов

Администраторы могут дополнительно настраивать сценарии, в которых используется оптимизация доставки со следующими параметрами:

- Минимальный объем ОЗУ (включительно), разрешенный для использования одноранговое кэширования , настраивает минимальный объем ОЗУ, необходимый для включения одноранговое кэширования.
- Минимальный размер диска, разрешенный для использования одноранговое кэширования , настраивает минимальный размер диска, необходимый для включения

одноранговое кэширование.

- Включить одноранговое кэширование, когда устройство подключается через VPN позволяет клиентам, подключенным через VPN, использовать одноранговое кэширование.
- Разрешить выкладывание, когда устройство работает от аккумулятора и уровень его заряда соответствует установленному значению определяет минимальный уровень заряда аккумулятора, необходимый для выкладывания. Для отправки в режиме работы от аккумулятора необходимо включить эту политику.

Режим скачивания

Параметр MDM: **DODownloadMode**

Режим скачивания определяет, из каких источников (помимо серверов Центра обновления Windows) клиентам разрешено скачивать обновления Windows. В следующей таблице приведены доступные параметры режима скачивания и их функции. Другие технические сведения об этих политиках доступны в разделе Оптимизация доставки политики CSP.

Развернуть таблицу

Параметр режима скачивания	**Функциональные возможности при настройке**
Только HTTP (0)	Этот параметр отключает одноранговое кэширование, но по-прежнему позволяет оптимизации доставки скачивать содержимое по протоколу HTTP из исходного источника загрузки или сервера подключенного кэша Майкрософт. В этом режиме используются дополнительные метаданные, предоставляемые облачными службами оптимизации доставки, для одноранговой, надежной и эффективной загрузки.
Локальная сеть (**1 — по умолчанию**)	Это стандартный рабочий режим оптимизации доставки, обеспечивающий одноранговый обмен данными в пределах одной сети. Облачная служба оптимизации доставки находит другие клиенты, подключенные к Интернету с помощью того же общего IP-адреса, что и целевой клиент. Затем эти клиенты пытаются подключиться к другим одноранговым узлам в той же сети, используя частный IP-адрес подсети.
Группа (2)	Если задан режим группы, группа автоматически выбирается на основе сайта доменные службы Active Directory (AD DS) устройства (Windows 10, версия 1607) или домена, в который устройство проходит проверку подлинности (Windows 10, версия 1511). В групповом режиме пиринг осуществляется по внутренним подсетям между устройствами, принадлежащим к одной и той же группе, включая устройства в удаленных офисах. Параметр GroupID можно использовать для создания собственной настраиваемой группы независимо от доменов и сайтов AD DS. Начиная с Windows 10 версии 1803, параметр GroupIDSource можно использовать для динамического создания групп с помощью других методов. Режим группового скачивания рекомендуется для большинства организаций, которым требуется максимально оптимизировать использование пропускной способности с помощью оптимизации доставки.
Интернет (3)	Включение одноранговых интернет-источников для оптимизации доставки.

Параметр режима скачивания	Функциональные возможности при настройке
Простой (99)	Простой режим полностью отключает использование облачных служб оптимизации доставки (для автономных сред). Оптимизация доставки автоматически переключается в этот режим, если облачные службы оптимизации доставки недоступны, недоступны или если размер файла содержимого меньше 50 МБ по умолчанию. В этом режиме оптимизация доставки обеспечивает надежную загрузку по протоколу HTTP из исходного источника загрузки или сервера подключенного кэша Майкрософт без одноранговое кэширования.
Обход (100)	Начиная с Windows 11 этот параметр не рекомендуется использовать. Не настраивайте **режим загрузки** для параметра "100" (обход), что может привести к сбою загрузки некоторого содержимого. Если вы хотите отключить одноранговые функции, настройте DownloadMode для (0). Если устройство не имеет доступа к Интернету, настройте режим загрузки в (99). При настройке обхода (100) загрузка обходит оптимизацию доставки и использует BITS. Этот параметр не требуется настраивать, если вы используете Configuration Manager.

> ⓘ **Примечание.**
>
> При использовании Microsoft Entra клиента, сайта AD или домена AD в качестве источника идентификаторов групп не следует полагаться на связь устройств, участвующих в группе, для проверки подлинности этих устройств.

Идентификатор группы

Параметр MDM: **DOGroupID**

По умолчанию пиринговый доступ на клиентах, использующих режим групповой загрузки (вариант 2), ограничен одним доменом в Windows 10 версии 1511, а также тем же доменом и доменные службы Active Directory сайтом в Windows 10 версии 1607. С помощью параметра Идентификатор группы можно при необходимости создать пользовательскую группу, содержащую устройства, которые должны участвовать в оптимизации доставки, но не попадают в эти домены или доменные службы Active Directory границы сайта, включая устройства в другом домене. С помощью идентификатора группы можно дополнительно ограничить группу по умолчанию (например, создать подгруппу, представляющую офисное здание) или расширить группу за пределы домена, что позволит устройствам в нескольких доменах в вашей организации быть одноранговым элементом. Для этого параметра требуется указать пользовательскую группу как GUID на каждом устройстве в ее составе.

> ⓘ **Примечание.**
>
> Чтобы создать GUID с помощью Powershell, используйте [guid]::NewGuid()

Эта конфигурация необязательна и не требуется для большинства реализаций оптимизации доставки.

Выберите источник идентификаторов групп.

Параметр MDM: **DOGroupIDSource**

Начиная с Windows 10 версии 1803, настройте эту политику, чтобы ограничить выбор одноранговой узла определенным источником при использовании политики GroupID. Ниже перечислены возможные варианты.

- 0 = не задано
- 1 = сайт AD
- 2 = идентификатор безопасности домена, прошедшего проверку подлинности
- 3 = идентификатор параметра DHCP (при использовании этого параметра клиент запрашивает параметр DHCP с идентификатором 234 и использует возвращенное значение GUID в качестве идентификатора группы).
- 4 = DNS-суффикс
- 5 = Начиная с Windows 10 версии 1903 можно использовать идентификатор клиента Microsoft Entra в качестве средства определения групп. Для этого настройте для ПАРАМЕТРА DOGroupIdSource новое максимальное значение 5.

После настройки идентификатор группы будет автоматически назначен из выбранного источника. Эта политика игнорируется, если политика GroupID также настроена. По умолчанию, когда политики GroupID или GroupIDSource не настроены, заключается в определении идентификатора группы с помощью сайта AD (1), идентификатора домена с проверкой подлинности (2) или Microsoft Entra идентификатора клиента (5) в этом порядке. Если параметр GroupIDSource настроен на идентификатор параметра DHCP (3) или DNS-суффикс (4) и эти методы завершаются ошибкой, вместо этого используется поведение по умолчанию. Параметр, настроенный в этой политике, применяется только к режиму загрузки группы (2). Если группа (2) не настроена в режиме загрузки, эта политика будет игнорироваться. Если вы настроите значение, отличное от 0 до 5, политика игнорируется.

Минимальный объем ОЗУ (включительно), разрешенный для использования одноранговой кэширования

Параметр MDM: **DOMinRAMAllowedToPeer**

Этот параметр определяет минимальный размер оперативной памяти в гигабайтах, необходимый для использования одноранговой кэширования. Например, если минимальное значение равно 1 ГБ, устройствам с объемом оперативной памяти 1 ГБ и более разрешается использовать одноранговое кэширование. Рекомендуемые значения: от 1 до 4, а **значение по умолчанию — 4 ГБ**.

Минимальный размер диска, разрешенный для использования одноранговой кэширования

Параметр MDM: **DOMinDiskSizeAllowedToPeer**

Этот параметр определяет минимальный размер диска (емкость в гигабайтах), необходимый для использования одноранговой кэширования на устройстве. Рекомендуемые значения: от 64 до 256, а **значение по умолчанию — 32 ГБ**.

> ⓘ **Примечание.**
>
> Если настроена политика **Изменить диск кэша**, размер диска проверка применяется к новому рабочему каталогу, указанному в этой политике.

Максимальный срок действия кэша

Параметр MDM: **DOMaxCacheAge**

В средах, настроенных для оптимизации доставки, может потребоваться настроить срок действия кэшированных обновлений и установочных файлов приложений Windows. В таком случае этот параметр определяет в секундах максимальную длительность хранения файла в кэше службы оптимизации доставки на каждом клиентском устройстве с Windows 10. Кроме того, организации могут выбрать для этого значения значение "0", что означает "неограниченный", чтобы избежать повторной загрузки содержимого одноранговыми узлами. Если задано значение "Без ограничений", оптимизация доставки сохраняет файлы в кэше дольше и очищает кэш по мере необходимости (например, если размер кэша превысил максимально допустимое пространство). **Значение по умолчанию — 259 200 секунд (три дня).**

Максимальный размер кэша

Параметр MDM: **DOMaxCacheSize**

Этот параметр ограничивает максимальный объем пространства, доступного для кэша оптимизации доставки, в процентах от доступного места на диске (от 1 до 100). Например, если на клиентском устройстве Windows с 100 ГБ свободного места на диске настроено значение 10, то оптимизация доставки использует до 10 ГБ этого пространства. Оптимизация доставки постоянно оценивает доступное место на диске и автоматически очищает кэш, чтобы сохранить максимальный размер кэша в настроенном проценте. **Значение по умолчанию — 20 %.**.

Абсолютный максимальный размер кэша

Параметр MDM: **DOAbsoluteMaxCacheSize**

Этот параметр указывает максимальное количество гигабайт, доступных для кэша оптимизации доставки. Это отличается от параметра Max Cache Size (Максимальный размер кэша), который составляет процент доступного места на диске. Кроме того, если вы настроите эту политику, она переопределяет параметр Max Cache Size (Максимальный размер кэша). **Значение по умолчанию не настроено**.

Минимальный размер файла содержимого одноранговой кэширования

Параметр MDM: **DOMinFileSizeToCache**

Этот параметр устанавливает минимальный размер файла данных в мегабайтах, разрешенный при одноранговом кэшировании. Рекомендуемые значения : от 1 до 10 0000. **Размер файла по умолчанию составляет 50 МБ** для участия в пиринге.

Максимальная пропускная способность загрузки переднего плана

Параметр MDM: **DOPercentageMaxForegroundBandwidth**

Начиная с Windows 10 версии 1803, определяет максимальную пропускную способность загрузки переднего плана, используемую оптимизацией доставки во всех параллельных действиях загрузки в процентах от доступной пропускной способности загрузки. **Значение по умолчанию "0"** означает, что оптимизация доставки динамически настраивается для использования доступной пропускной способности для загрузки переднего плана. Однако скачивание из одноранговых узлов локальной сети не регулируется, даже если эта политика настроена.

Максимальная пропускная способность фонового скачивания

Параметр MDM: **DOPercentageMaxBackgroundBandwidth**

Начиная с Windows 10 версии 1803, определяет максимальную пропускную способность фонового скачивания, используемую оптимизацией доставки во всех одновременных действиях загрузки в процентах от доступной пропускной способности загрузки. **Значение по умолчанию "0"** означает, что оптимизация доставки динамически настраивается для использования доступной пропускной способности для фонового скачивания. Однако скачивание из одноранговых узлов локальной сети не регулируется, даже если эта политика настроена.

> ⓘ **Примечание.**

Для сред с низкой пропускной способностью рекомендуется использовать параметры скачивания с абсолютным значением DOMaxBackgroundDownloadBandwidth и DOMaxForegroundDownloadBandwidth, а не параметры на основе процента.

Настройка рабочих часов для ограничения пропускной способности загрузки переднего плана

Параметр MDM: **DOSetHoursToLimitForegroundDownloadBandwidth**

Начиная с Windows 10 версии 1803, определяет максимальную пропускную способность загрузки переднего плана, используемую оптимизацией доставки в рабочее время и в нерабочее время во всех одновременных действиях загрузки в процентах от доступной пропускной способности загрузки. Если задан параметр DOSetHoursToLimitForegroundDownloadBandwidth, он будет иметь приоритет над процентными значениями **DOPercentageMaxForegroundBandwidth** , если задано. **По умолчанию эта политика не настроена.**

Настройка рабочих часов для ограничения пропускной способности фонового скачивания

Параметр MDM: **DOSetHoursToLimitBackgroundDownloadBandwidth**

Начиная с Windows 10 версии 1803, определяет максимальную пропускную способность фонового скачивания, используемую оптимизацией доставки в рабочее и нерабочее время во всех одновременных действиях загрузки в процентах от доступной пропускной способности загрузки. Если задан параметр DOSetHoursToLimitBackgroundDownloadBandwidth, он будет иметь приоритет над процентными значениями **DOPercentageMaxBackgroundBandwidth** , если задано. **По умолчанию эта политика не настроена.**

Выбор метода ограничения выбора одноранговового узла

Параметр MDM: **DORestrictPeerSelectionBy**

Начиная с Windows 10 версии 1803, настройте эту политику для дальнейшего ограничения выбора одноранговых узлов в локальной сети режимов загрузки (1) и Группе (2). В Windows 11 был введен параметр "Обнаружение локального одноранговового узла", чтобы ограничить обнаружение одноранговых узлов локальной сетью. В настоящее время доступны следующие варианты: 0 = нет, 1 = маска подсети и 2 = локальное обнаружение одноранговового узла (DNS-SD). Выбор маски подсети (1) или обнаружения локального одноранговового узла (2) позволит избежать пиринга между подсетями.

Если настроен режим группы, оптимизация доставки подключается к локально обнаруженным одноранговым узлам, которые также входят в одну группу (имеют тот же идентификатор

группы), и предотвращает участие устройств, которые не используют один и тот же идентификатор группы.

В Windows 11 параметр обнаружения локальных одноранговых узлов (DNS-SD) можно настроить с помощью MDM или групповая политика. Однако в Windows 10 эту функцию можно включить, задав `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DeliveryOptimization\DORestrictPeerSelectionBy` значение **2**.

Поведение по умолчанию в Windows 10 и Windows 11 отличается. В Windows 10 ограничения не настроены. В Windows 11 выбор однорангового узла по умолчанию ограничен подсетью только в режиме загрузки по локальной сети (1).

Задержка загрузки переднего плана с HTTP (в секундах)

Параметр MDM: **DODelayForegroundDownloadFromHttp**

Начиная с Windows 10, версия 1803, позволяет отложить использование источника HTTP при загрузке на переднем плане (интерактивном) для использования однорангового узла. **По умолчанию эта политика не настроена.**

Задержка фоновой загрузки с HTTP (в секундах)

Параметр MDM: **DODelayBackgroundDownloadFromHttp**

Начиная с Windows 10 версии 1803, это позволяет отложить использование источника HTTP в фоновой загрузке, которая может использовать одноранговый узел. **По умолчанию эта политика не настроена.**

Задержка загрузки резервного сервера кэша переднего плана (в секундах)

Параметр MDM: **DelayCacheServerFallbackForeground**

Начиная с Windows 10 версии 1903, можно отложить откат с сервера кэша до источника HTTP для загрузки содержимого переднего плана на X секунд. Если настроена политика "Задержка загрузки на переднем плане из HTTP", она будет применяться сначала (чтобы разрешить скачивание с одноранговых узлов). **По умолчанию эта политика не настроена.**

Задержка резервного размещения сервера кэша фонового скачивания (в секундах)

Параметр MDM: **DelayCacheServerFallbackBackGround**

Начиная с Windows 10 версии 1903, настройте эту политику, чтобы отложить откат с сервера кэша до источника HTTP для загрузки фонового содержимого на X секунд. Если настроена политика "Задержка фоновой загрузки с HTTP", она будет применяться сначала (для разрешения скачивания из одноранговых узлов), а затем эта политика будет применена. **По умолчанию эта политика не настроена.**

Минимальное качество обслуживания в фоновом режиме

Параметр MDM: **DOMinBackgroundQoS**

Эта политика управляет фоновой загрузкой и измеряет пропускную способность между одноранговыми узлами. Если измеряемая скорость падает ниже заданного порогового значения, содержимое загружается как из одноранговых узлов, так и из источника HTTP. После достижения порогового значения HTTP-подключения закрываются, а скачивание продолжается только с одноранговых узлов.

Установка более низкого порогового значения упрощает выполнение ограничения, что означает, что больше содержимого будет поступать от одноранговых узлов, а HTTP-подключения не будут использоваться. **Значение по умолчанию — 20 МБ/с.**

Изменение диска кэша

Параметр MDM: **DOModifyCacheDrive**

Этот параметр позволяет изменить расположение кэша оптимизации доставки на клиентах. **По умолчанию кэш хранится на диске с операционной системой через переменную среды %SYSTEMDRIVE%.** Можно настроить значение для переменной среды (например, %SYSTEMDRIVE), буквы диска (например, D:) или пути к папке (например, D:\DOCache).

Ограничение для ежемесячной отправки данных

Параметр MDM: **DOMonthlyUploadDataCap**

Этот параметр указывает общий объем данных в гигабайтах, который клиент оптимизации доставки может отправить одноранговым клиентам через Интернет за месяц. Значение "0" означает, что может быть отправлен неограниченный объем данных. **Значение по умолчанию для этого параметра — 20 ГБ.**

Включение одноранговое кэширования при подключении устройства через VPN

Параметр MDM: **DOAllowVPNPeerCaching**

Этот параметр определяет, может ли устройство участвовать в одноранговом кэшировании, если оно подключено к VPN. **По умолчанию при обнаружении VPN-подключения пиринг не разрешен, за исключением случаев, когда выбран параметр "Локальное обнаружение" (DNS-SD).** Укажите значение true, чтобы разрешить устройству участвовать в одноранговом кэшировании при подключении к доменной сети через VPN. Устройство может скачивать или передавать на другие сетевые устройства домена либо через VPN, либо в корпоративной сети домена.

Ключевые слова VPN

Параметр MDM: **DOVpnKeywords**

Эта политика позволяет настроить одно или несколько ключевых слов, разделенных запятыми, которые используются для распознавания VPN-подключений. **По умолчанию эта политика не настроена, поэтому при обнаружении VPN устройство не будет использовать пиринг.** Оптимизация доставки автоматически обнаруживает VPN-подключение, просматривая строки "Description" и "FriendlyName" сетевого адаптера, используя список ключевое слово по умолчанию, включая "VPN", "Безопасная" и "Виртуальная частная сеть" (например, "MSFTVPN" соответствует ключевое слово VPN). По мере роста числа VPN трудно поддерживать постоянно меняющийся список имен VPN. Чтобы решить эту проблему, мы ввели этот новый параметр для добавления уникальных VPN-имен в соответствии с потребностями отдельных сред.

Запрет загрузки сервера кэша в VPN

Параметр MDM: **DODisallowCacheServerDownloadsOnVPN**

Эта политика запрещает загрузку с подключенных серверов кэша при подключении устройства через VPN. **По умолчанию устройство разрешено скачивать из подключенного кэша при подключении через VPN.** Настройте эту политику, если вы предпочитаете скачивать устройства непосредственно из Интернета при удаленном подключении (через VPN), а не извлекать из сервера Microsoft Connected Cache, развернутого в корпоративной сети.

Разрешить отправку, когда устройство находится в батарее при заданном уровне заряда батареи

Параметр MDM: **DOMinBatteryPercentageAllowedToUpload**

Этот параметр устанавливает уровни заряда аккумулятора, при которых разрешено выкладывание данных. Укажите любое значение от 1 до 100 (в процентах), чтобы разрешить устройству, работающему от аккумулятора, выкладывать данные на одноранговые устройства в локальной сети или группе. Отправка будет автоматически приостановлена, когда уровень заряда батареи падает ниже настроенного минимального уровня заряда. Рекомендуемое значение для настройки, если вы разрешаете отправку от аккумулятора, равно 40 (для 40 %).

Эта политика не влияет на скачивание, и устройство может скачивать данные с одноранговых устройств независимо от уровня заряда аккумулятора.

> ⓘ **Внимание**
>
> **По умолчанию устройства не будут загружаться от батареи**. Чтобы включить отправку от аккумулятора, необходимо включить эту политику и настроить значение батареи, при котором приостанавливается отправка.

Имя узла сервера кэша

Параметр MDM: **DOCacheHost**

Настройте эту политику, чтобы назначить один или несколько серверов подключенного кэша Майкрософт для использования оптимизацией доставки. Можно задать одно или несколько полных доменных имен или IP-адресов, разделенных запятыми, например: myhost.somerandomhost.com,myhost2.somerandomhost.com,10.10.1.7. **По умолчанию эта политика не имеет значения.** Клиент оптимизации доставки подключается к перечисленным серверам подключенного кэша Майкрософт в указанном порядке. При наличии нескольких полных доменных имен или IP-адресов резервный переход к сети CDN происходит сразу после первого сбоя при скачивании с сервера кэша, если не настроены политики DelayCacheServerFallbackBackground или DelayCacheServerFallbackForeground . Если эти политики задержки настроены, откат происходит только после заданного времени задержки, и клиент продолжает пытаться подключиться к серверам кэша в порядке циклического перебора до истечения времени задержки.

> ⓘ **Внимание**
>
> Любое значение будет означать, что политика настроена. Например, пустая строка ("") не считается пустой.

Источник имени узла сервера кэша

Параметр MDM: **DOCacheHostSource**

Эта политика позволяет указать, как клиенты могут динамически обнаруживать оптимизацию доставки на серверах сетевого кэша. Существует два варианта:

- 1 = ВАРИАНТ DHCP 235.
- 2 = параметр DHCP 235 Force.

При использовании любого из этих вариантов клиент запрашивает параметр DHCP с идентификатором 235 и использует возвращаемое значение в качестве имени узла сервера

кэша. Если политика DOCacheHost также настроена, для ее переопределения требуется параметр DHCP 235 Force (2). **По умолчанию эта политика не имеет значения.**

Настройте эту политику для назначения оптимизации доставки на серверах сетевого кэша с помощью настраиваемого параметра DHCP. Укажите настраиваемый параметр DHCP на DHCP-сервере в качестве *текстового* типа. Можно добавить одно или несколько значений в виде полных доменных имен (FQDN) или IP-адресов. Чтобы добавить несколько значений, разделите каждое полное доменное имя или IP-адрес запятыми.

> ⓘ **Примечание.**
>
> Если неправильно отформатировать идентификатор параметра DHCP, клиент вернется к значению политики имя узла сервера кэша, если это значение было настроено.
>
> Если параметр LocalPolicyMerge настроен, например часть базовых показателей безопасности, он может повлиять на DHCP-клиент и запретить получение этого параметра DHCP, особенно в сценариях Autopilot.

Максимальная пропускная способность загрузки переднего плана (в КБ/с)

Параметр MDM: **DOMaxForegroundDownloadBandwidth**

Указывает максимальную пропускную способность загрузки переднего плана в килобайтах в секунду, которую устройство может использовать во всех одновременных действиях загрузки с помощью оптимизации доставки. Если этот параметр включен, любое из ограничений пропускной способности на основе процента переднего плана — DOPercentageMaxForegroundBandwidth или DOSetHoursToLimitForegroundDownloadBandwidth — будет применяться в процентах от указанного здесь значения.

Значение по умолчанию "0" означает, что оптимизация доставки динамически настраивается, чтобы использовать доступную пропускную способность для скачивания.

Максимальная пропускная способность фонового скачивания (в КБ/с)

Параметр MDM: **DOMaxBackgroundDownloadBandwidth**

Указывает максимальную пропускную способность фонового скачивания в килобайтах в секунду, которую устройство может использовать во всех одновременных действиях загрузки с помощью оптимизации доставки. Если этот параметр включен, любой из фоновых процентных ограничений пропускной способности — DOPercentageMaxBackgroundBandwidth или DOSetHoursToLimitBackgroundDownloadBandwidth — будет применяться в процентах от указанного здесь значения.

Значение по умолчанию "0" означает, что оптимизация доставки динамически настраивается на использование доступной пропускной способности для скачивания.

Нерекомендуемые политики

Максимальная пропускная способность для скачивания

Параметр MDM: **DOMaxDownloadBandwidth**

Не рекомендуется использовать в Windows 10, версия 2004. Этот параметр указывает в килобайтах в секунду (КБ/с) максимальную пропускную способность, которая может использовать для всех одновременных скачиваний службы оптимизации доставки. **Значение по умолчанию "0"** означает, что оптимизация доставки динамически корректирует и оптимизирует максимальную используемую пропускную способность.

Процент максимальной пропускной способности скачивания

Параметр MDM: **DOPercentageMaxDownloadBandwidth**

Не рекомендуется использовать в Windows 10, версия 2004. Этот параметр указывает максимальную пропускную способность, которую оптимизация доставки может использовать для всех одновременных скачиваний, в виде процента от доступной пропускной способности скачивания. **Значение по умолчанию "0"** означает, что оптимизация доставки динамически настраивается, чтобы использовать доступную пропускную способность для скачивания.

Максимальная пропускная способность отправки

Параметр MDM: **DOMaxUploadBandwidth**

Не рекомендуется использовать в Windows 10, версия 2004. Этот параметр позволяет ограничить количество пропускной способности отправки, которые отдельные клиенты могут использовать для оптимизации доставки. Этот параметр следует использовать, если клиенты предоставляют содержимое запрашивающим его одноранговым клиентам в сети. Этот параметр настраивается в килобайтах в секунду (КБ/с). **Значение по умолчанию — "0" или "неограниченный"** , что означает, что оптимизация доставки динамически оптимизируется для минимального использования пропускной способности отправки. однако это не ограничение пропускной способности передачи с заданной скоростью.

Last updated on 30.09.2025

Как сделать функции по запросу и языковые пакеты доступными при использовании WSUS или Configuration Manager

Статья • 01.10.2024 •

Применяется к: ✅ Windows 11, ✅ Windows 10, ✅ Microsoft Configuration Manager, ✅ WSUS

В этой справочной статье описывается, как сделать функции по запросу (FoD) и языковые пакеты доступными при использовании Windows Server Update Services (WSUS) или Configuration Manager для определенных версий Windows.

Общие изменения, влияющие на функции по запросу и содержимое языкового пакета

Следующие изменения для FoD и содержимого языкового пакета повлияли на настройку политики клиента:

- Начиная с Windows 10 версии 1709, вы не можете использовать WSUS для локального размещения компонентов по запросу (FoD).
- Начиная с Windows 10 версии 1803 языковые пакеты больше не могут размещаться в WSUS.

Из-за этих изменений политика **Укажите параметры для установки дополнительных компонентов и восстановления компонентов** (ADMX_Servicing), расположенная в разделе `Computer Configuration\Administrative Templates\System`, использовалась для указания альтернативных способов получения FoD и языковых пакетов, а также содержимого для исправления повреждений. Эта политика позволяет указать одно альтернативное расположение. Важно отметить, что политика ведет себя по-разному в разных версиях ОС. Дополнительные сведения см. в разделе Сведения о конкретных версиях для функций по запросу и языковых пакетов .

Введение политики **Укажите исходную службу для определенных классов Windows Обновления** (SetPolicyDrivenUpdateSourceFor<UpdateClass>) в Windows 10 версии 2004 еще больше усложнило настройку параметров foD и содержимого языкового пакета.

Начиная с Windows 11 версии 22H2, появились обновления локальной единой платформы обновлений (UUP). FoD и языковые пакеты снова доступны в WSUS. Больше не требуется использовать политику **Укажите параметры для установки дополнительных компонентов и восстановления компонентов** для содержимого FoD и языкового пакета. Эта политика была изменена, начиная с Windows 11 версии 24H2, и следующие параметры были удалены:

- Никогда не пытайтесь скачать полезные данные из клиентский компонент Центра обновления Windows
- Скачивание содержимого восстановления и дополнительных компонентов непосредственно из клиентский компонент Центра обновления Windows вместо Windows Server Update Services (WSUS)

Сведения о конкретных версиях для функций по запросу и языковых пакетов

клиенты Windows 11, версии 22H2 и более поздних версий используют локальные обновления единой платформы обновлений (UUP) с WSUS и Microsoft Configuration Manager. Этим клиентам не нужно использовать **параметр Укажите параметры для установки дополнительных компонентов и восстановления компонентов** для FoD и языковых пакетов, так как содержимое доступно в WSUS из-за локального UUP. Политика была изменена начиная с Windows 11 версии 24H2, чтобы удалить ненужные параметры.

Для Windows 10 версии 2004–Windows 11 версии 21H2 клиенты не могут скачивать foD-файлы или языковые пакеты, если **для параметра установки дополнительных компонентов и восстановления компонентов** задано значение клиентский компонент Центра обновления Windows и **укажите исходную службу для определенных классов Windows. Обновления** (SetPolicyDrivenUpdateSourceFor<FeatureUpdates/QualityUpdates>) для обновлений компонентов или исправлений имеет значение WSUS. Если вам требуется это содержимое, можно задать параметр **Укажите параметры для дополнительной установки компонента и восстановления компонентов** клиентский компонент Центра обновления Windows, а затем:

- Измените выбор источника для обновлений компонентов и качества на клиентский компонент Центра обновления Windows
- Разрешить доступ ко всем классам обновлений из WSUS, не настроив выбор источника

> ⓘ **Примечание**

В Windows 10 версии 21H2 и более поздних учетные записи пользователей без прав администратора могут добавлять как язык интерфейса, так и соответствующие ему языковые функции.

В Windows 10 версии 1809 и более **поздних изменение параметров для установки дополнительных компонентов и восстановления компонентов** также влияет на получение языковых пакетов, однако языковые пакеты можно получить только непосредственно из клиентский компонент Центра обновления Windows (до Windows 11 версии 22H2). В настоящее время получить их из сетевой папки невозможно. Указание сетевого расположения работает для пакетов FoD или исправления повреждений в зависимости от содержимого в этом расположении.

В Windows 10 версиях 1709 и 1803 изменение **параметров для дополнительной установки компонентов и восстановления компонентов для** загрузки содержимого из клиентский компонент Центра обновления Windows позволяет получать пакеты FoD, а также включает восстановление повреждений. Указание сетевого расположения работает для любого из этих вариантов в зависимости от содержимого, найденного в этом расположении. Изменение этой политики в этих версиях ОС не влияет на способ получения языковых пакетов.

Для всех версий ОС изменение политики **Укажите параметры для установки дополнительных компонентов и восстановления компонентов** не влияет на распределение обновлений ОС. Они по-прежнему поступают из WSUS, Configuration Manager или других источников, как вы запланировали их, даже если необязательное содержимое создается из клиентский компонент Центра обновления Windows или сетевого расположения.

Сведения о других вариантах управления клиентами, включая использование групповая политика и административных шаблонов, см. в статье Управление клиентами Windows.

Дополнительные ресурсы

- Документация по WSUS
- документация по Configuration Manager

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Добавление шрифтов, отсутствующих после обновления Windows

Статья • 27.02.2025 • Применяется к: ✅ Windows 11, ✅ Windows 10

При обновлении Windows с более старых версий Windows до поддерживаемых в настоящее время версий Windows ранее доступные шрифты могут быть недоступны после обновления. Многие шрифты, которые ранее поставлялись вместе с Windows, были перемещены в дополнительные функции Windows:

- Уменьшите объем занимаемой операционной системы.
- Повышение производительности.
- Оптимизация использования дискового пространства.

В следующих экземплярах:

- Установлен новый экземпляр Windows
- Windows обновлена с более старой версии Windows

необязательные шрифты не включены по умолчанию. В результате эти шрифты отсутствуют в системе. Если документы были созданы с использованием отсутствующих шрифтов, эти документы могут отображаться по-разному в обновленной версии Windows.

Например, если установлена версия Windows на английском, французском, немецком или испанском языках, отсутствуют следующие шрифты:

- `Gautami`
- `Meiryo`
- `Narkism/Batang`
- `BatangChe`
- `Dotum`
- `DotumChe`
- `Gulim`
- `GulimChe`
- `Gungsuh`
- `GungsuhChe`

Если эти шрифты необходимы, их можно добавить в систему с помощью дополнительных функций. Удаление этих шрифтов является постоянным изменением в поведении Windows и останется таким образом в будущих выпусках.

Добавление связанных с языком функций с помощью языковых параметров

Если в системе требуются шрифты, связанные с языком, этот язык следует добавить в профиль пользователя, а затем переключиться на этот язык. Например, шрифты необходимы для:

- Просмотр веб-страниц.
- Редактирование документов.
- Используйте приложения на этом языке.

Добавить язык, а затем переключиться на него можно с помощью приложения **"Параметры** ".

Чтобы добавить шрифты, связанные с языком, а затем переключиться на этот язык, сначала откройте область **Язык & регион** в приложении **Параметры** , щелкнув следующую ссылку:

Регион & языка

или

1. Щелкните правой кнопкой мыши меню **Пуск** и выберите **Выполнить**.
2. В окне **Выполнить** рядом с **полем Открыть:**введите:

   Консоль

   ```
   ms-settings:regionlanguage
   ```

   и нажмите **кнопку ОК**.

или

1. Щелкните правой кнопкой мыши меню **Пуск** и выберите **Параметры**.
2. В левой области приложения "Параметры" выберите **Время & язык**.
3. В правой области **Время & язык** выберите **Язык & регион**.

После открытия области **Язык & времени** > **& регионе** добавьте шрифты, связанные с языком, а затем переключитесь на этот язык, выполнив следующие действия:

1. В разделе **Язык** :

a. Раскрывающееся меню рядом с **пунктом Язык интерфейса Windows** , чтобы отобразить все языки, добавленные в данный момент на устройство.

b. Если нужного языка нет в списке, добавьте шрифты для нужного языка, нажав кнопку **Добавить язык** рядом с **пунктом Предпочитаемые языки**.

c. В **открывавшемся окне Выбор языка для установки** :

   i. Найдите нужный язык, прокрутив список языков. Кроме того, найдите нужный язык в поле поиска **Введите имя языка...**

   ii. После того как нужный язык будет найден, выберите язык и нажмите кнопку **Далее** .

   iii. В окне **Установка языковых компонентов** выберите нужные параметры для языка и нажмите кнопку **Установить** .

d. Нужный язык теперь должен быть доступен в раскрывающемся меню рядом с **языком интерфейса Windows**. Раскрывающееся меню **"Язык интерфейса Windows"** и выберите нужный язык.

e. Под **языком интерфейса Windowsотображается сообщение Windows, необходимое для выхода, чтобы применить новый язык интерфейса** . Нажмите кнопку **Выйти** , чтобы завершить применение языка, включая дополнительные языковые шрифты.

> ⓘ **Важно!**
>
> клиентский компонент Центра обновления Windows используется для добавления языка, включая связанные шрифты. Устройство должно быть подключено к сети, чтобы клиентский компонент Центра обновления Windows могли скачать содержимое, которое необходимо добавить.

Добавление необязательных шрифтов вручную без изменения языковых параметров

Если шрифты, связанные с языком, необходимы, но не требуются во всей системе, этот язык следует добавить в профиль пользователя в качестве дополнительного шрифта. Добавление шрифта в качестве дополнительного шрифта не требует

переключения пользователя на этот язык. Добавить шрифт в качестве дополнительного шрифта можно с помощью приложения "**Параметры** ".

Чтобы добавить дополнительные шрифты, связанные с языком, при сохранении текущего языка:

Откройте область **Необязательные функции** в приложении "**Параметры**" , выбрав следующую ссылку:

Необязательные функции

или

1. Щелкните правой кнопкой мыши меню **Пуск** и выберите **Выполнить**.
2. В окне **Выполнить** рядом с **полем Открыть:**введите:

   ```
   Консоль
   ms-settings:optionalfeatures
   ```

   и нажмите **кнопку OK**.

или

1. Щелкните правой кнопкой мыши меню **Пуск** и выберите **Параметры**.
2. В левой области приложения "Параметры" выберите **Система**.
3. В правой области **Система** выберите **Необязательные функции**.

> ⓘ **Примечание**
>
> Шаги навигации, элементы пользовательского интерфейса и текст пользовательского интерфейса в этом разделе основаны на последней версии Windows 11 с установленным последним накопительным обновлением. Для других версий Windows 11, которые поддерживаются в настоящее время или не имеют последнего накопительного обновления, некоторые шаги навигации, элементы пользовательского интерфейса и текст пользовательского интерфейса могут отличаться. Например, область Необязательные функции может находиться в разделе **Параметры**>**приложения**.

После открытия области **Системные** > **необязательные функции** добавьте дополнительный шрифт, выполнив следующие действия:

1. Нажмите кнопку **Просмотреть компоненты** рядом с **пунктом Добавить необязательный компонент**.
2. В **открывавшемся окне Добавление дополнительного компонента** :
   a. Найдите нужный дополнительный шрифт для добавления, а затем выберите поле рядом с дополнительным шрифтом, чтобы добавить его. Можно выбрать несколько дополнительных шрифтов.
   b. После выбора всех необходимых дополнительных шрифтов нажмите кнопку **Далее** .
   c. Просмотрите выбранный список компонентов и нажмите кнопку **Добавить** , чтобы добавить выбранные компоненты.

> ⓘ **Важно!**
>
> клиентский компонент Центра обновления Windows используется для добавления дополнительных функций, включая дополнительные шрифты. Устройство должно быть подключено к сети, чтобы клиентский компонент Центра обновления Windows могли скачать содержимое, которое необходимо добавить.

Шрифты в составе необязательных компонентов шрифтов

Ниже приведен полный список семейств шрифтов в каждой из дополнительных функций. В некоторых семействах может быть несколько шрифтов с разной насыщенностью и стилем.

- Дополнительные шрифты арабской письменности: `Aldhabi, Andalus, Arabic Typesetting, Microsoft Uighur, Sakkal Majalla, Simplified Arabic, Traditional Arabic, Urdu Typesetting`
- Дополнительные шрифты для скрипта Bangla: `Shonar Bangla, Vrinda`
- Канадские аборигены syllabics Дополнительные шрифты: `Euphemia`
- Дополнительные шрифты Cherokee: `Plantagenet Cherokee`
- Дополнительные шрифты для китайского языка (упрощенное письмо): `DengXian, FangSong, KaiTi, SimHei`

- Китайский (традиционный) дополнительный шрифт: `DFKai-SB, MingLiU, MingLiU_HKSCS, PMingLiU`
- Дополнительные шрифты Devanagari: `Aparajita, Kokila, Mangal, Sanskrit Text, Utsaah`
- Этиопические дополнительные шрифты: `Nyala`
- Вспомогательные шрифты Гуджарати: `Shruti`
- Дополнительные шрифты Гурмухи: `Raavi`
- Дополнительные шрифты иврита: `Aharoni Bold, David, FrankRuehl, Gisha, Levanim MT, Miriam, Miriam Fixed, Narkism, Rod`
- Дополнительные шрифты на японском языке: `Meiryo, Meiryo UI, MS Gothic, MS PGothic, MS UI Gothic, MS Mincho, MS PMincho, Yu Mincho`
- Дополнительные шрифты каннада: `Tunga`
- Кхмерский дополнительный шрифт: `DaunPenh, Khmer UI, MoolBoran`
- Корейские дополнительные шрифты: `Batang, BatangChe, Dotum, DotumChe, Gulim, GulimChe, Gungsuh, GungsuhChe`
- Дополнительные шрифты Лаос: `DokChampa, Lao UI`
- Дополнительные шрифты Малаялама: `Karthika`
- Дополнительные шрифты Odia: `Kalinga`
- дополнительные шрифты Pan-European: `Arial Nova, Georgia Pro, Gill Sans Nova, Neue Haas Grotesk, Rockwell Nova, Verdana Pro`
- Дополнительные шрифты сингальского: `Iskoola Pota`
- Сирийские дополнительные шрифты: `Estrangelo Edessa`
- Дополнительные шрифты тамильского текста: `Latha, Vijaya`
- Дополнительные шрифты Telugu: `Gautami, Vani`
- Тайский дополнительный шрифт: `Angsana New, AngsanaUPC, Browallia New, BrowalliaUPC, Cordia New, CordiaUPC, DilleniaUPC, EucrosiaUPC, FreesiaUPC, IrisUPC, JasmineUPC, KodchiangUPC, Leelawadee, LilyUPC`

Связанное содержимое

- Скачайте список всех доступных языков FOD.
- Функции по запросу версии 2 (возможности).
- Добавление языковых пакетов в Windows.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Windows Обновления с использованием прямого и обратного дифференциалов

Статья • 19.11.2024 • Применяется к: ✅ Windows 11, ✅ Windows 10

Ежемесячные обновления качества Windows являются накопительными и содержат все ранее выпущенные исправления для обеспечения согласованности и простоты. Для платформы операционной системы, такой как Windows, которая поддерживается в течение нескольких лет, размер ежемесячных обновлений качества может быстро увеличиться, что напрямую влияет на потребление пропускной способности сети.

Сегодня эта проблема решается с помощью экспресс-загрузки, где разностные загрузки для каждого измененного файла в обновлении создаются на основе выбранных исторических редакций, а также базовой версии. В этом документе мы представляем новую методику создания компактных пакетов обновлений программного обеспечения, применимых к любой редакции базовой версии, а затем описываем, как обновления качества Windows используют этот метод.

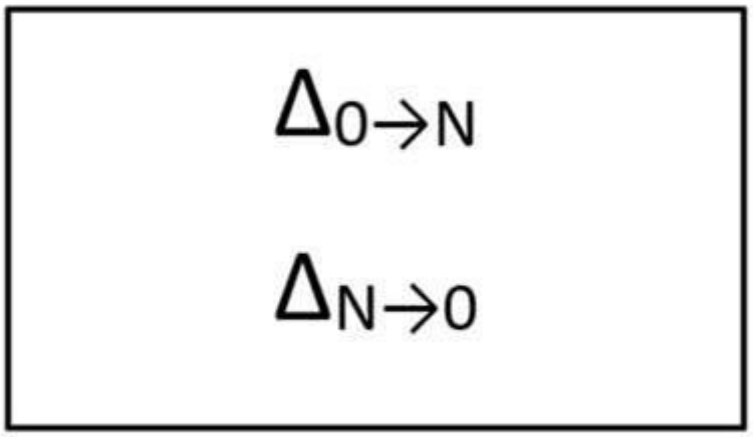
Общие условия

В этом документе применяются следующие общие термины:

- *Базовая версия*: основной выпуск программного обеспечения со значительными изменениями, например Windows 10, версия 1809 (Windows 10 сборка 17763.1).
- *Редакция*: незначительные выпуски между основными версиями, например KB4464330 (Windows 10 сборка 17763.55)
- *Файлы хранилища базовых исправлений (небазовый PSF):* файлы хранилища исправлений, содержащие полные двоичные файлы или файлы

В этом документе мы представляем новую методику, которая позволяет создавать компактные обновления программного обеспечения, оптимизированные для любой пары редакций источника и назначения. Это делается путем вычисления переадресации разностного измененного файла из базовой версии и обратного разностного файла обратно в базовую версию. Затем как прямая, так и обратная дифференциальные системы упаковываются в виде обновления и распространяются на конечные точки, на которых выполняется обновление

программного обеспечения. Содержимое пакета обновления можно обозначить следующим образом:



Конечные точки с базовой версией файла (V_0) гидратировали целевую редакцию (V_N), применяя простое преобразование:

$$V_0 + \Delta_{0\to N} = V_N$$

Конечные точки, имеющие редакцию N файла (V_N), гидратировали целевую редакцию (V_R), применяя следующий набор преобразований:

$$VN + AN{+}O = Vo$$

$$V_0 + \Delta_{0\to R} = V_R$$

Конечные точки сохраняют обратные различия для редакции программного обеспечения, в которую они включены, чтобы их можно было использовать для гидрирования и применения следующего обновления редакции.

Используя общий базовый план, этот метод создает один пакет обновления с многочисленными преимуществами:

- Компактный размер
- Применимо ко всем базовым показателям
- Простота сборки
- Эффективная установка
- Распространяемый

Исторически размеры обновлений качества Windows (Windows 10 версии 1803 и более ранних поддерживаемых версий Windows 10) были оптимизированы с помощью экспресс-скачивания. Экспресс-скачивание оптимизировано таким образом, что обновление систем Windows скачивает минимальное количество байтов. Это достигается путем создания разностных изменений для каждого обновленного файла на основе выбранных исторических базовых редакций того же файла и его базовой или RTM-версии.

Например, если ежемесячное обновление качества за октябрь обновило Notepad.exe, создаются различия для Notepad.exe изменения файлов с сентября по октябрь, с августа по октябрь, с июля по октябрь, с июня по октябрь и с первоначального выпуска функции до октября. Все эти различия хранятся в файле хранилища исправлений (PSF, также называемом файлами экспресс-загрузки) и размещаются или кэшируются на клиентский компонент Центра обновления Windows или других серверах управления обновлениями или распространения (например, Windows Server Update Services (WSUS). Microsoft Configuration Manager или сервер управления обновлениями или распространителя сторонних корпораций, поддерживающий экспресс-обновления). Устройство, применяющее экспресс-обновления, использует сетевой протокол для определения оптимальных различий, а затем загружает из конечных точек распространения обновлений только то, что необходимо.

Обратная сторона экспресс-скачивания заключается в том, что размер файлов PSF может быть большим в зависимости от количества исторических базовых показателей, по которым вычислялись разностные данные. Скачивание и кэширование больших файлов PSF на локальные или удаленные серверы распространения обновлений проблематично для большинства организаций, поэтому они не могут использовать экспресс-обновления для обновления своего парка устройств под управлением Windows. Во-вторых, из-за сложности создания разностных и размеров экспресс-файлов, которые необходимо кэшировать на серверах распространения обновлений, можно создавать файлы экспресс-скачивания только для наиболее распространенных базовых показателей, поэтому экспресс-обновления применимы только к выбранным базовым планам. Наконец, вычисление оптимальных дифференциалов является дорогостоящим с точки зрения использования системной памяти, особенно для недорогих систем, что влияет на их способность легко скачивать и применять обновление.

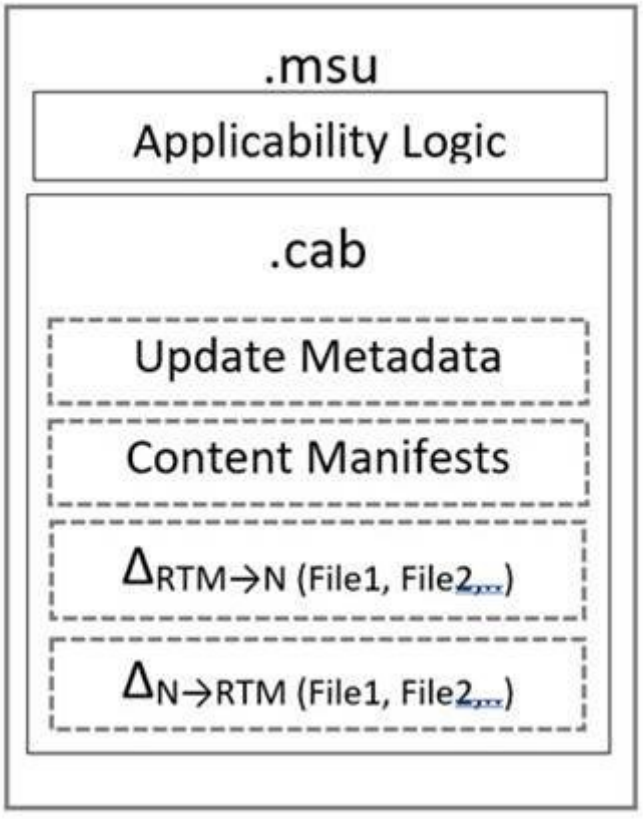
В следующих разделах описано, как обновления качества используют этот метод на основе прямого и обратного разности для новых выпусков Windows и Windows Server для решения проблем с экспресс-скачиванием.

Высокоуровневая конструкция

Обновление упаковки

Пакеты обновления качества Windows содержат переадресацию от базовых показателей RTM обновления качества (ΔRTM→N) и обратные дифференциалы обратно в RTM (ΔN→RTM) для каждого файла, который изменился с момента RTM. Используя версию RTM в качестве базового плана, мы гарантируем, что все устройства имеют одинаковые полезные данные. Метаданные пакета обновления, манифесты содержимого, а также прямой и обратный дифференциалы упаковываются в cab-файл (.cab). Этот .cab файл и логика применимости также будут упакованы в формат изолированного обновления Майкрософт (MSU).

Могут быть случаи, когда новые файлы добавляются в систему во время обслуживания. Эти файлы не будут иметь базовые показатели RTM, поэтому нельзя использовать прямую и обратную разницу. В этих сценариях для обработки обслуживания используются разностные значения NULL. Разностные значения NULL — это слегка сжатые и оптимизированные версии полных двоичных файлов. Пакеты обновления могут иметь либо прямую, либо обратную дифференциальную разницу, либо нулевая разница любого заданного двоичного файла в них. Следующее изображение символизирует содержимое установщика обновлений качества Windows:



Гидратация и установка

После того как обычные проверки применимости выполняются в пакете обновления и будут определены как применимые, инфраструктура обслуживания компонентов Windows восстанавливает все файлы во время предустановки, а затем переходит к обычной установке.

Ниже приведена последовательность действий, которые инфраструктура обслуживания компонентов выполняет в транзакции для завершения установки обновления:

- Определите все файлы, необходимые для установки обновления.
- Восстановите каждый из необходимых файлов с помощью текущей версии (V_N) файла, обратного разностного (V_N--->RTM) файла до версии RTM/base и прямого разностного (V_{RTM}--->R) от rtm/base версии до целевой версии. Кроме того, используйте разностную гидратацию NULL для гидратации сжатых файлов со значением NULL.
- Размещение гидратированных файлов (полный файл), переадресации разностных (в `f` папке) и обратных разностных (в `r` папке) или сжатых файлов null (в `n` папке) в хранилище компонентов (%windir%\WinSxS).
- Устраните все зависимости и установите компоненты.
- Очистка старого состояния (V_{N-1}); предыдущее состояние V_N сохраняется для удаления, восстановления или восстановления.

Устойчивая гидратация

Чтобы обеспечить устойчивость к повреждению хранилища компонентов или отсутствующим файлам, которые могут возникнуть из-за восприимчивости определенных типов оборудования к повреждению файловой системы, служба восстановления повреждений традиционно использовалась для автоматического восстановления хранилища компонентов (автоматическое восстановление повреждений) или по запросу (восстановление повреждения вручную) с помощью сетевого или локального источника восстановления. Эта служба будет по-прежнему предлагать возможность восстановления содержимого для восстановления и успешной установки обновления, если это необходимо.

При обнаружении повреждения во время операций обновления автоматическое восстановление повреждений начинается как обычно и использует файл хранилища базовых исправлений, опубликованный в клиентский компонент Центра обновления Windows для каждого обновления для исправления поврежденных манифестов, двоичных дифференциалов, а также гидратированных или полных файлов. Файлы безбазового хранилища исправлений содержат

обратные и обратные дифференциалы и полные файлы для каждого обновленного компонента. Целостность файлов восстановления будет проверена на хэш.

Исправление повреждения использует манифест компонента для обнаружения отсутствующих файлов и получения хэшей для обнаружения повреждений. Во время установки обновления устанавливаются новые флаги реестра для каждого разностного промежуточного размещения на компьютере. При выполнении автоматического восстановления повреждения она сканирует гидратированные файлы с помощью манифеста и разностные файлы с помощью флагов. Если не удается найти или проверить разностную разницу, она добавляется в список повреждений для исправления.

Отложенный автоматический ремонт повреждений

"Отложенное автоматическое исправление повреждения" выполняется во время операций обновления для обнаружения поврежденных двоичных файлов и разностных файлов. При применении обновления в случае сбоя восстановления любого файла автоматически запускается автоматическое исправление "отложенного" повреждения, определяет поврежденный двоичный или разностный файл, а затем добавляет его в список повреждений. Позже операция обновления продолжается насколько это возможно, так что "ленивый" автоматическое исправление повреждения может собрать как можно больше поврежденных файлов для исправления. В конце раздела восстановления обновление завершается сбоем, и начинается автоматическое исправление повреждений. Автоматическое исправление повреждений выполняется в обычном режиме и в конце своей работы добавляет список повреждений, созданный "ленивым" автоматическим исправлением повреждений, поверх нового списка для восстановления. Затем автоматическое исправление повреждений исправит файлы в списке повреждений, и установка обновления будет успешно выполнена при следующей попытке.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Настройка загрузочных образов Среды предустановки Windows

Статья • 16.08.2024 •

Применяется к: ✅ Windows 11, ✅ Windows 10, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Образы загрузки Windows PE (WinPE), входящие в состав Windows ADK, имеют минимальное количество функций и драйверов. Однако образы загрузки можно настроить, добавив драйверы, необязательные компоненты и применяя последнее накопительное обновление.

Корпорация Майкрософт рекомендует обновить загрузочные образы Windows PE с помощью последнего накопительного обновления для обеспечения максимальной безопасности и защиты. Последние накопительные обновления также могут устранять известные проблемы. Например, загрузочный образ Windows PE можно обновить с помощью последнего накопительного обновления, чтобы устранить уязвимость загрузчика BlackLotus UEFI, как описано в статье KB5025885. Управление отзывами диспетчера загрузки Windows для изменений безопасной загрузки, связанных с CVE-2023-24932 и CVE-2023-24932.

> **Совет**
>
> Образы загрузки из **ADK 10.1.26100.1 (май 2024 г.) и более поздних** версий уже содержат накопительное обновление для устранения уязвимости bootkit UEFI BlackLotus.

В этом пошаговом руководстве описано, как настроить загрузочный образ Windows PE, включая обновление с использованием последнего накопительного обновления, добавление драйверов и добавление дополнительных компонентов. Кроме того, в этом пошаговом руководстве рассматривается, как настройки образов загрузки влияют на несколько популярных продуктов, использующих загрузочные образы, таких как Microsoft Configuration Manager, Microsoft Deployment Toolkit (MDT) и Службы развертывания Windows (WDS).

Предварительные условия

- Комплект средств оценки и развертывания Windows (Windows ADK) — рекомендуется использовать последнюю версию ADK.

- Надстройка Windows PE для Windows ADK. Убедитесь, что версия Среды предустановки Windows соответствует используемой версии Windows ADK.
- Загрузочный образ Среды предустановки Windows.
- Последнее накопительное обновление, скачаемое с сайта каталога Центра обновления Майкрософт .

Действия

- Шаг 1. Скачивание и установка ADK
- Шаг 2. Скачивание накопительного обновления (CU)
- Шаг 3. Резервное копирование существующего загрузочного образа
- Шаг 4. Подключение образа загрузки к папке подключения
- Шаг 5. Добавление драйверов в образ загрузки (необязательно)
- Шаг 6. Добавление необязательных компонентов в образ загрузки
- Шаг 7. Добавление накопительного обновления (CU) в образ загрузки
- Шаг 8. Копирование загрузочных файлов из подключенного образа загрузки в путь установки ADK
- Шаг 9. Очистка компонентов
- Шаг 10. Проверка добавления всех необходимых пакетов в образ загрузки
- Шаг 11. Отключение образа загрузки и сохранение изменений
- Шаг 12. Экспорт образа загрузки для уменьшения размера
- Шаг 13. Обновление загрузочных образов в продуктах, использующих загрузочные образы (необязательно)

Шаг 1. Скачивание и установка ADK

1. Скачайте и установите **пакет средств оценки и развертывания Windows (Windows ADK)** из раздела Скачивание и установка Windows ADK.

   В этом пошаговом руководстве при установке Windows ADK необходимо установить только **средства развертывания**. Для других продуктов, таких как Microsoft Configuration Manager и Microsoft Deployment Toolkit (MDT), может потребоваться установка дополнительных компонентов, таких как **средство миграции пользовательской среды (USMT).**

   Одним из средств, установленных при установке средства **развертывания** , является командная строка **Среды средств развертывания и создания образов** . При использовании параметра **командной строки** для выполнения команд в этом пошаговом руководстве обязательно выполните команды из командной строки **среды средств развертывания и создания образов** с повышенными привилегиями. Командную строку **Среды средств**

развертывания и создания образов можно найти в меню Пуск в разделе**Среда средств развертывания и создания образовкомплектов**> Windows.

В этой статье предполагается, что Windows ADK был установлен в расположении `C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit`по умолчанию . Если Windows ADK был установлен в другом расположении, измените пути во время пошагового выполнения соответствующим образом.

2. Скачайте и установите **надстройку Windows PE для Windows ADK** из раздела Скачать и установить Windows ADK. **Надстройка Windows PE для Windows ADK** является отдельной загрузкой и установкой из **комплекта средств оценки и развертывания Windows (Windows ADK).** Убедитесь, что они по отдельности скачиваются и устанавливаются.

> ⓘ **Важно!**
>
> Настоятельно рекомендуется скачать и установить последнюю версию Windows ADK и надстройки Windows PE для Windows ADK.
>
> В некоторых случаях вместо последней версии может потребоваться использовать более старые версии надстройки Windows ADK и Windows PE. Пример
>
> - Microsoft Deployment Toolkit (MDT) не поддерживает версии Windows или Windows ADK за Windows 10. При использовании MDT рекомендуется вместо этого использовать **ADK для Windows 10 версии 2004**. Эта версия была последней версией Windows ADK, поддерживаемой MDT.
> - Последние версии **надстройки Windows PE для Windows ADK** включают только 64-разрядный загрузочный образ. Если требуется 32-разрядный загрузочный образ, рекомендуется также использовать **ADK для Windows 10 версии 2004**. Эта версия Windows ADK была последней версией, включавшей как 32-разрядные, так и 64-разрядные загрузочные образы.

Шаг 2. Скачивание накопительного обновления (CU)

1. Перейдите на сайт каталога Центра обновления Майкрософт и найдите последнее накопительное обновление. Версия windows накопительного обновления должна соответствовать версии обновляемого загрузочного образа Среды предустановки Windows.

2. При поиске на сайте каталога Центра обновления Майкрософт используйте условие `"<year>-<month> cumulative update for windows <x>"` поиска, где `year` — четырехзначный текущий год, `<month>` двухзначный текущий месяц и `<x>` версия Windows, на которой основана среда предустановки Windows. Обязательно включите кавычки (`"`). Например, чтобы найти последнее накопительное обновление для Windows 11 в августе 2023 г., снова используйте условие `"2023-08 cumulative update for Windows 11"` поиска , чтобы включить кавычки. Если накопительное обновление еще не выпущено за текущий месяц, выполните поиск по предыдущему месяцу.

   > **Совет**
   >
   > Образы загрузки в **ADK 10.1.25398.1 (сентябрь 2023 г.)** основаны на **серверной операционной системе Майкрософт версии 22H2 для 64-разрядных систем**. Обязательно обновите условие поиска соответствующим образом.

3. После обнаружения накопительного обновления скачайте соответствующую версию для версии и архитектуры Windows, которая соответствует загрузочному образу Среды предустановки Windows. Например, если версия загрузочного образа Windows PE Windows 11 64-разрядной версии 22H2, скачайте **накопительное обновление для Windows 11 версии 22H2 для 64-разрядных систем**.

4. Сохраните скачаемое накопительное обновление в известном расположении для последующего использования, например `C:\Updates`.

> **Совет**
>
> При обновлении образов загрузки с накопительным обновлением рекомендуется использовать полное накопительное обновление. Однако вместо полного накопительного обновления можно скачать и использовать накопительное обновление для SafeOS. Это приведет к уменьшению размера окончательного обновленного загрузочного образа. Если возникают проблемы с загрузочным образом, обновленным накопительным

обновлением SafeOS, используйте вместо него полное накопительное обновление.

Примечание

- При обновлении образа загрузки в ADK 10.1.25398.1 (сентябрь 2023 г.) скачайте **накопительный пакет обновления для серверной операционной системы Майкрософт версии 23H2 для 64-разрядных систем**.
- При обновлении образа загрузки в ADK для Windows 10 версии 2004 скачайте **накопительный пакет обновления для Windows 10 версии 22H2**.

Шаг 3. Резервное копирование существующего загрузочного образа

Перед изменением нужного загрузочного образа создайте резервную копию загрузочного образа, который необходимо обновить. Пример

- Для 64-разрядного загрузочного образа, включенного в **надстройку Windows PE для Windows ADK**, загрузочный образ находится по адресу `C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows Preinstallation Environment\amd64\en-us\winpe.wim`.

- Для 64-разрядного образа загрузки по умолчанию, созданного **Microsoft Configuration Manager**, загрузочный образ находится по адресу `<ConfigMgr_Install_Directory>\OSD\boot\x64\boot.wim`. Для других загрузочных образов в Configuration Manager путь к загрузочному образу отображается в поле **Путь к изображению:** на вкладке **Источник данных** в **свойствах** образа загрузки.

  Однако для **Microsoft Configuration Manager** рекомендуется вместо этого изменить `winpe.wim` загрузочный образ, включенный в **надстройку Windows PE для Windows ADK**. Дополнительные сведения см. в разделе рекомендации по Microsoft Configuration Manager.

- Для 64-разрядного образа загрузки по умолчанию, созданного **microsoft Deployment Toolkit (MDT),** загрузочный образ находится по адресу `<Deployment_Share>\Boot\LiteTouchPE_x64.wim`.

Однако для **Microsoft Deployment Toolkit (MDT)** рекомендуется вместо этого изменить `winpe.wim` загрузочный образ, включенный в **надстройку Windows PE для Windows ADK**. Дополнительные сведения см. в разделе Рекомендации по набору средств развертывания (MDT).

- Для 64-разрядных загрузочных образов в **службах развертывания Windows (WDS)** загрузочные образы находятся по адресу `<RemoteInstall>\Boot\x64\Images`.

Настройте приведенные выше пути для 32-разрядных образов загрузки (доступны только для Windows 10 ADK).

Следующая команда создает резервную копию 64-разрядного загрузочного образа, включенного в **надстройку Windows PE для Windows ADK**:

PowerShell

В командной строке **PowerShell** с повышенными привилегиями выполните следующую команду, чтобы создать резервную копию 64-разрядного образа загрузки, включенного в Windows ADK. Если образ загрузки с резервным копированием уже существует, перед перезаписью существующего загрузочного образа с резервным копированием требуется подтверждение этой команды:

PowerShell

```
Copy-Item "C:\Program Files (x86)\Windows Kits\10\Assessment and
Deployment Kit\Windows Preinstallation Environment\amd64\en-
us\winpe.wim" "C:\Program Files (x86)\Windows Kits\10\Assessment and
Deployment Kit\Windows Preinstallation Environment\amd64\en-
us\winpe.bak.wim"
```

Измените пути и имена файлов соответствующим образом, чтобы создать резервную копию других загрузочных образов.

Чтобы автоматически перезаписать существующий образ загрузки с резервной копией без подтверждения, например в скрипте, добавьте `-Force` параметр в конец командной строки.

Дополнительные сведения см. в разделе Copy-Item.

ⓘ Важно!

При использовании образа загрузки по умолчанию `winpe.wim` из **надстройки Windows PE для Windows ADK** рекомендуется всегда иметь резервную копию исходного неизмененных загрузочных образа. Это позволяет вернуться к нетронутому исходному загрузочному образу в случае возникновения проблем с любой итерацией обновленного загрузочного образа. Кроме того, при необходимости применения нового накопительного обновления к загрузочному образу рекомендуется всегда начинать заново и обновлять исходный загрузочный образ без обновлений, а не обновлять ранее обновленный загрузочный образ.

Шаг 4. Подключение образа загрузки к папке подключения

1. Создайте пустую папку для подключения образа загрузки. Например, `C:\Mount`. При использовании ранее созданной папки подключения убедитесь, что она пуста и в ней нет ранее подключенных образов.

2. Подключите загрузочный образ к папке подключения одним из следующих способов:

   PowerShell

   В командной строке **PowerShell** с повышенными привилегиями выполните следующую команду, чтобы подключить загрузочный образ к папке подключения:

   PowerShell

   ```
   Mount-WindowsImage -Path "<Mount_folder_path>" -ImagePath "
   <Boot_image_path>\<boot_image>.wim" -Index 1 -Verbose
   ```

   Пример:

   PowerShell

   ```
   Mount-WindowsImage -Path "C:\Mount" -ImagePath "C:\Program Files
   (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
   Preinstallation Environment\amd64\en-us\winpe.wim" -Index 1 -
   Verbose
   ```

   Дополнительные сведения см. в разделе Mount-WindowsImage.

Шаг 5. Добавление драйверов в образ загрузки (необязательно)

При необходимости добавьте все драйверы в загрузочный образ:

PowerShell

В командной строке **PowerShell** с повышенными привилегиями выполните одну из следующих команд, чтобы добавить драйверы в загрузочный образ:

```
PowerShell
Add-WindowsDriver -Path "<Mount_folder_path>" -Driver "
<Driver_INF_source_path>\<driver>.inf"
```

или

```
PowerShell
Add-WindowsDriver -Path "<Mount_folder_path>" -Driver "
<Drivers_source_path>" -Recurse
```

Примеры:

```
PowerShell
Add-WindowsDriver -Path "C:\Mount" -Driver "C:\Drivers\driver.inf"
```

или

```
PowerShell
Add-WindowsDriver -Path "C:\Mount" -Driver "C:\Drivers" -Recurse
```

Дополнительные сведения см. в разделе Add-WindowsDriver.

Накопительное обновление, установленное далее в этом пошаговом руководстве, не влияет на драйверы. После добавления драйвера в загрузочный образ его не нужно добавлять повторно, если к образу загрузки применяется более новое накопительное обновление.

Совет

Полный набор драйверов не требуется в загрузочных образах Windows PE. Требуется только небольшое подмножество драйверов, которые обеспечивают базовые функциональные возможности в WinPE. В большинстве случаев драйверы не нужно добавлять в загрузочный образ Windows ADK, так как в него уже встроено множество драйверов. Не добавляйте драйверы в загрузочный образ, пока не будет проверено, что они необходимы. Если требуется добавить драйверы, обычно требуются только сетевые драйверы. Иногда также может потребоваться хранилище (диск). На некоторых устройствах Surface также могут потребоваться драйверы клавиатуры и мыши.

Важно!

Для загрузочных образов Microsoft Configuration Manager и Microsoft Deployment Toolkit (MDT) не добавляйте драйверы в загрузочный образ вручную, выполнив описанные выше действия. Вместо этого добавьте драйверы в загрузочные образы с помощью Microsoft Configuration Manager или Microsoft Deployment Toolkit (MDT):

- В Configuration Manager на вкладке **Драйверы** в **свойствах** образа загрузки.
- В Microsoft Deployment Toolkit (MDT) на вкладке **Драйверы и исправления** на вкладке **Windows PE** в **свойствах** общей папки развертывания.

Это обеспечит правильное управление драйверами в загрузочном образе с помощью Configuration Manager или Microsoft Deployment Toolkit (MDT).

Шаг 6. Добавление необязательных компонентов в образ загрузки

1. Добавьте все необходимые необязательные компоненты в загрузочный образ:

PowerShell

В командной строке **PowerShell** с повышенными привилегиями выполните следующую команду, чтобы добавить необязательные компоненты в образ загрузки:

```
PowerShell

Add-WindowsPackage -PackagePath "C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows Preinstallation Environment\amd64\WinPE_OCs\<Component>.cab" -Path "<Mount_folder_path>" -Verbose
```

Пример:

```
PowerShell

Add-WindowsPackage -PackagePath "C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows Preinstallation Environment\amd64\WinPE_OCs\WinPE-Scripting.cab" -Path "C:\Mount" -Verbose
```

В этих примерах предполагается 64-разрядный загрузочный образ. Если используется другая архитектура, измените пути в командах соответствующим образом.

Дополнительные сведения см. в разделе Add-WindowsPackage.

2. После добавления дополнительного компонента в загрузочный образ обязательно добавьте компонент, зависящий от языка, для этого дополнительного компонента.

   Не все необязательные компоненты имеют компонент, зависящий от языка. Однако для дополнительных компонентов, которые имеют компонент, зависящий от языка, убедитесь, что компонент для конкретного языка установлен.

   Чтобы проверка, если дополнительный компонент имеет языковой компонент, проверка `C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows Preinstallation Environment\amd64\WinPE_OCs\<Language>\` каталог, чтобы узнать, есть ли соответствующий языковой компонент для этого необязательного компонента.

   Например, чтобы установить компонент английского языка США (en-us) для дополнительного компонента, используйте следующую командную строку:

PowerShell

В командной строке **PowerShell** с повышенными привилегиями выполните следующую команду, чтобы добавить компоненты языка для необязательных компонентов в загрузочный образ:

```
PowerShell

Add-WindowsPackage -PackagePath "C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows Preinstallation Environment\amd64\WinPE_OCs\en-us\<Component>_en-us.cab" -Path "<Mount_folder_path>" -Verbose
```

Пример:

```
PowerShell

 Add-WindowsPackage -PackagePath "C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows Preinstallation Environment\amd64\WinPE_OCs\en-us\WinPE-Scripting_en-us.cab" -Path "C:\Mount" -Verbose
```

В этих примерах предполагается 64-разрядный загрузочный образ. Если используется другая архитектура, измените пути соответствующим образом.

Дополнительные сведения см. в разделе Add-WindowsPackage.

ⓘ Важно!

При добавлении необязательных компонентов убедитесь, что проверка, если у дополнительного компонента есть необходимые условия для другого необязательного компонента. Если у дополнительного компонента есть необходимые компоненты, убедитесь, что он установлен первым. Дополнительные сведения см. в статье **Справка по дополнительным компонентам WinPE (OC): Добавление необязательных компонентов**.

ⓘ Важно!

Накопительные обновления всегда должны применяться или применяться повторно после добавления необязательных компонентов в загрузочный образ. Если после применения накопительного обновления в образ загрузки

добавляются дополнительные необязательные компоненты, то накопительное обновление необходимо применить повторно.

> ⓘ **Важно!**
>
> Для **правильной работы образов Microsoft Configuration Manager** и **Microsoft Deployment Toolkit (MDT)** требуются некоторые необязательные компоненты. Обязательно добавьте эти необходимые компоненты при использовании **Microsoft Configuration Manager** и **Microsoft Deployment Toolkit (MDT).** Дополнительные сведения см. в разделе Configuration Manager необходимых компонентов образа загрузки или необходимые компоненты образа загрузки MDT.
>
> Кроме того, при добавлении любого необязательного компонента для **образов загрузки Microsoft Configuration Manager** или **Microsoft Deployment Toolkit (MDT)** обязательно вручную добавьте необязательные компоненты, используя это пошаговое руководство, а не с помощью **Configuration Manager** или **MDT**. Дополнительные сведения и причины см. в разделе рекомендации по Microsoft Configuration Manager или Рекомендации по набору средств развертывания Майкрософт (MDT).

Популярные необязательные компоненты

В следующем списке содержатся более популярные необязательные компоненты, которые обычно добавляются в образы загрузки:

Развернуть таблицу

Функция	Имя файла	Зависимость	Описание	Требуется для ConfigMgr	Требуется mdt
Скрипты/WinPE-Scripting	`WinPE-Scripting.cab`	Отсутствует	Поддерживает выполнение сценариев, отличных от PowerShell, в WinPE	Да	Да
Network/WinPE-WDS-Tools	`WinPE-WDS-Tools.cab`	Отсутствует	Поддерживает WDS в WinPE, включая запись изображений и	Да	Нет

Функция	Имя файла	Зависимость	Описание	Требуется для ConfigMgr	Требуется mdt
			многоадресную рассылку		
Скрипты/WinPE-WMI	`WinPE-WMI.cab`	Отсутствует	Поддержка сценариев WMI и WMI в WinPE	Да	Да
Startup/WinPE-SecureStartup	`WinPE-SecureStartup.cab`	Скрипты/WinPE-WMI	Поддерживает управление BitLocker и TPM в WinPE	Да	Да
Управление файлами/WinPE-FMAPI	`WinPE-FMAPI.cab`	Отсутствует	Поддерживает доступ к API управления файлами Среды предустановки Windows	Нет	Да
Windows PowerShell/WinPE-PowerShell	`WinPE-PowerShell.cab`	Скрипты/WinPE-Scripting Скрипты/WinPE-WMI Microsoft .NET/WinPE-NetFx	Поддерживает выполнение команд и сценариев PowerShell в WinPE	Нет	Нет
Microsoft .NET/WinPE-NetFx	`WinPE-NetFx.cab`	Скрипты/WinPE-WMI	Поддержка приложений .NET в WinPE	Нет	Нет
Network/WinPE-Dot3Svc	`WinPE-Dot3Svc.cab`	Отсутствует	Поддерживает сетевой протокол 802.1X в WinPE	Нет	Нет
HTML/WinPE-HTA	`WinPE-HTA.cab`	Скрипты/WinPE-WMI	Поддержка запуска html-приложений в WinPE	Нет	Нет
Database/WinPE-MDAC	`WinPE-MDAC.cab`	Отсутствует	Поддерживает подключение к базам данных в WinPE	Нет	Нет

Полный список всех доступных необязательных компонентов WinPE, включая описания для каждого компонента, см. в статье Справка по дополнительным компонентам WinPE (OC): Дополнительные компоненты WinPE.

Шаг 7. Добавление накопительного обновления (CU) в образ загрузки

Примените накопительный пакет обновления (CU), скачанный на шаге 2. Скачивание накопительного обновления (CU) к загрузочному образу:

PowerShell

В командной строке **PowerShell** с повышенными привилегиями выполните следующую команду, чтобы добавить накопительное обновление (CU) в загрузочный образ:

PowerShell

```
Add-WindowsPackage -PackagePath "<Path_to_CU_MSU_update>\<CU>.msu" -Path
"<Mount_folder_path>" -Verbose
```

Пример:

PowerShell

```
Add-WindowsPackage -PackagePath "C:\Updates\windows11.0-kb5029263-
x64_4f5fe19bbec786f5e445d3e71bcdf234fe2cbbec.msu" -Path "C:\Mount" -
Verbose
```

Дополнительные сведения см. в разделе Add-WindowsPackage.

ⓘ Важно!

Не применяйте накопительное обновление (CU) до тех пор, пока все необходимые дополнительные компоненты не будут установлены на **шаге 6. Добавление необязательных компонентов в образ загрузки** . Ожидание установки накопительного обновления (CU) до установки всех необязательных компонентов гарантирует, что необязательные компоненты также правильно обновлены накопительным обновлением. Если в будущем в образ загрузки

потребуется добавить дополнительные необязательные компоненты, обязательно повторно примените накопительное обновление.

Обновление стека обслуживания (SSU) и 0x800f0823 ошибок

Иногда при применении накопительного обновления (CU) к загрузочному образу может возникать сообщение об ошибке `0x800f0823`:

PowerShell

```
VERBOSE: Target Image Version <WinPE version>
WARNING: Failed to add package <Cumulative_Update_Path>\
<Cumulative_Update>.msu
WARNING: Add-WindowsPackage failed. Error code = 0x800f0823
Add-WindowsPackage : An error occurred applying the Unattend.xml file
from the .msu package.
For more information, review the log file.
At line:1 char:1
+ Add-WindowsPackage -PackagePath "<Cumulative_Update_Path>\
<Cumulative_Update> ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : NotSpecified: (:) [Add-WindowsPackage],
COMException
    + FullyQualifiedErrorId :
Microsoft.Dism.Commands.AddWindowsPackageCommand
```

При проверке **DISM.log** обнаруживается следующая ошибка:

PowerShell

```
Package "Package_for_RollupFix~<Cumulative_Update>" requires Servicing
Stack v<Required_Servicing_Stack_Version> but current Servicing Stack is
v<Current_Servicing_Stack_Version>. [HRESULT = 0x800f0823 -
CBS_E_NEW_SERVICING_STACK_REQUIRED]
Failed to initialize internal package [HRESULT = 0x800f0823 -
CBS_E_NEW_SERVICING_STACK_REQUIRED]
Failed to create internal package [HRESULT = 0x800f0823 -
CBS_E_NEW_SERVICING_STACK_REQUIRED]
Failed to create windows update package [HRESULT = 0x800f0823 -
CBS_E_NEW_SERVICING_STACK_REQUIRED]
DISM Package Manager: PID=<PID> TID=<TID> Failed opening package. -
```

```
CDISMPackageManager::Internal_CreatePackageByPath(hr:0x800f0823)
DISM Package Manager: PID=<PID> TID=<TID> Failed to get the underlying
CBS package. - CDISMPackageManager::OpenPackageByPath(hr:0x800f0823)
DISM Package Manager: PID=<PID> TID=<TID> The specified package cannot
be added to this Windows Image due to a version mismatch. -
GetCbsErrorMsg
DISM Package Manager: PID=<PID> TID=<TID> Failed to open package at
location [<Temp_Path>\<Cumulative_Update>.cab]. -
CPackageManagerUnattendHandler::Internal_ProcessPackageFromSource(hr:0x8
00f0823)
DISM Package Manager: PID=<PID> TID=<TID> Failed to install package from
source [0] - trying next source location. hr = [0x800F0823] -
CPackageManagerUnattendHandler::Internal_UnattendInstallPackage
DISM Package Manager: PID=<PID> TID=<TID> Failed to Install the package
[Multiple_Packages~~~~0.0.0.0]. -
CPackageManagerUnattendHandler::Internal_UnattendInstallPackage(hr:0x800
f0823)
DISM Package Manager: PID=<PID> TID=<TID> Package failed to install
[Multiple_Packages~~~~0.0.0.0]. -
CPackageManagerUnattendHandler::Internal_UnattendProcessPackage(hr:0x800
f0823)
DISM Package Manager: PID=<PID> TID=<TID> Failed to process package at
node <package[1]>. -
CPackageManagerUnattendHandler::Apply(hr:0x800f0823)
DISM Package Manager: PID=<PID> TID=<TID> Failed to Apply the unattend.
- CDISMPackageManager::Apply(hr:0x800f0823)
DISM Unattend Manager: PID=<PID> TID=<TID> "Error applying unattend for
provider: DISM Package Manager" - CUnattendManager::Apply(hr:0x800f0823)
DISM Package Manager: PID=<PID> TID=<TID> Failed applying the unattend
file from the MSU package. -
CMsuPackage::ApplyMsuUnattend(hr:0x800f0823)
DISM Package Manager: PID=<PID> TID=<TID> Failed to apply the MSU
unattend file to the image. - CMsuPackage::Install(hr:0x800f0823)
API: PID=<PID> TID=<TID> Failed to install msu package
<Path_to_CU_MSU_update>\<MSU_Cumulative_Update>.msu -
CAddPackageCommandObject::InternalExecute(hr:0x800f0823)
API: PID=<PID> TID=<TID> InternalExecute failed -
CBaseCommandObject::Execute(hr:0x800f0823)
API: PID=<PID> TID=<TID> CAddPackageCommandObject internal execution
failed - DismAddPackageInternal(hr:0x800f0823)
```

Проблема возникает, когда обслуживаемый образ загрузки WinPE требует установки обновления стека обслуживания (SSU) перед установкой накопительного обновления (CU). Эта проблема обычно возникает при использовании более старых windows ADK и более старых версий Windows PE. Предлагаемое исправление заключается в обновлении до последней версии Windows ADK и Windows PE. Для последних версий Windows ADK и Windows PE, скорее всего, не требуется обновление стека обслуживания (SSU) перед установкой накопительного обновления (CU).

В сценариях, в которых необходимо использовать более старые версии Windows ADK и Windows PE, например при использовании Microsoft Deployment Toolkit (MDT), перед установкой накопительного обновления необходимо установить обновление стека обслуживания. Обновление стека обслуживания (SSU) содержится в накопительный пакет обновления (CU). Чтобы получить обновление стека обслуживания (SSU) для его применения, его можно извлечь из накопительного обновления (CU).

Ниже описано, как извлечь, а затем установить обновление стека обслуживания (SSU) в загрузочный образ. После установки обновления стека обслуживания (SSU) в загрузочном образе накопительный пакет обновления (CU) должен установиться в загрузочный образ без ошибок:

> ⓘ **Важно!**
>
> Эти действия необходимы только в том случае, если ошибка `0x800f0823` возникает при установке накопительного обновления (CU) в загрузочный образ. Если ошибка `0x800f0823` не произошла при установке накопительного обновления (CU) в загрузочный образ, перейдите к следующему шагу **Шаг 8. Копирование загрузочных файлов из подключенного образа загрузки в путь установки ADK**

1. Создайте папку для извлечения обновления стека обслуживания (SSU). Например, `C:\Updates\Extract`:

2. Извлеките содержимое накопительного обновления (CU) в папку, созданную на предыдущем шаге, с помощью следующей команды:

   PowerShell

   PowerShell

   ```
   Start-Process "expand.exe" -ArgumentList " -f:* `"
   <Cumulative_Update_Path>\<Cumulative_Update>.msu`" `"
   <Extract_Folder_Path>`"" -Wait -LoadUserProfile
   ```

   Пример:

   PowerShell

   ```
   Start-Process "expand.exe" -ArgumentList " -f:*
   `"C:\Updates\windows10.0-kb5028166-
   ```

```
x64_fe3aa2fef685c0e76e1f5d34d529624294273f41.msu`"
`"C:\Updates\Extract`"" -Wait -LoadUserProfile
```

Дополнительные сведения см. в разделе Запуск и развертывание.

3. Проверьте извлеченные файлы в папке extract и определите CAB-файл обновления стека обслуживания (SSU). Один из файлов должен называться `SSU-<Version>-<Arch>.cab`. Например, `SSU-19041.3205-x64.cab`. Запишите имя CAB-файла обновления стека обслуживания (SSU).

4. Используя имя CAB-файла обновления стека обслуживания (SSU), полученного на предыдущем шаге, примените CAB-файл обновления стека обслуживания (SSU) к образу загрузки с помощью следующей команды:

PowerShell

В командной строке **PowerShell** с повышенными привилегиями выполните следующую команду, чтобы добавить накопительное обновление (CU) в загрузочный образ:

PowerShell

```
Add-WindowsPackage -PackagePath "<Path_to_SSU_CAB_update>\
<SSU>.cab" -Path "<Mount_folder_path>" -Verbose
```

Пример:

PowerShell

```
Add-WindowsPackage -PackagePath "C:\Updates\Extract\SSU-19041.3205-
x64.cab" -Path "C:\Mount" -Verbose
```

Дополнительные сведения см. в разделе Add-WindowsPackage.

5. Повторите попытку применить накопительное обновление (CU) к загрузочному образу с помощью команд из шага 7. Добавление накопительного обновления (CU) в загрузочный образ.

Шаг 8. Копирование загрузочных файлов из подключенного образа загрузки в путь

установки ADK

Некоторые накопительные обновления содержат обновленные загрузочные файлы bootmgr, которые добавляются в загрузочный образ. После обновления этих загрузочных файлов bootmgr в образе загрузки рекомендуется скопировать эти обновленные загрузочные файлы bootmgr из образа загрузки обратно в Windows ADK. Копирование этих файлов гарантирует, что в Windows ADK есть обновленные загрузочные файлы начальной загрузки.

PowerShell

В командной строке **PowerShell** с повышенными привилегиями выполните следующие команды, чтобы скопировать обновленные загрузочные файлы bootmgr из подключенного образа загрузки в путь установки ADK. Эти команды также резервное копирование всех существующих загрузочных файлов начальной загрузки. Если применимо, команды должны подтвердить, чтобы перезаписать все существующие файлы:

PowerShell

```
Copy-Item "C:\Program Files (x86)\Windows Kits\10\Assessment and
Deployment Kit\Windows Preinstallation
Environment\amd64\Media\bootmgr.efi" "C:\Program Files (x86)\Windows
Kits\10\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\Media\bootmgr.bak.efi"

Copy-Item "<Mount_folder_path>\Windows\Boot\EFI\bootmgr.efi" "C:\Program
Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
Preinstallation Environment\amd64\Media\bootmgr.efi"

Copy-Item "C:\Program Files (x86)\Windows Kits\10\Assessment and
Deployment Kit\Windows Preinstallation
Environment\amd64\Media\EFI\Boot\bootx64.efi" "C:\Program Files
(x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
Preinstallation Environment\amd64\Media\EFI\Boot\bootx64.bak.efi"

Copy-Item "<Mount_folder_path>\Windows\Boot\EFI\bootmgfw.efi"
"C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment
Kit\Windows Preinstallation
Environment\amd64\Media\EFI\Boot\bootx64.efi"
```

Пример:

PowerShell

```
Copy-Item "C:\Program Files (x86)\Windows Kits\10\Assessment and
Deployment Kit\Windows Preinstallation
```

```
Environment\amd64\Media\bootmgr.efi" "C:\Program Files (x86)\Windows
Kits\10\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\Media\bootmgr.bak.efi"

Copy-Item "C:\Mount\Windows\Boot\EFI\bootmgr.efi" "C:\Program Files
(x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
Preinstallation Environment\amd64\Media\bootmgr.efi"

Copy-Item "C:\Program Files (x86)\Windows Kits\10\Assessment and
Deployment Kit\Windows Preinstallation
Environment\amd64\Media\EFI\Boot\bootx64.efi" "C:\Program Files
(x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
Preinstallation Environment\amd64\Media\EFI\Boot\bootx64.bak.efi"

Copy-Item "C:\Mount\Windows\Boot\EFI\bootmgfw.efi" "C:\Program Files
(x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
Preinstallation Environment\amd64\Media\EFI\Boot\bootx64.efi"
```

Чтобы перезаписать загрузочные файлы bootmgr и любой файл загрузки bootmgr с резервным копированием без подтверждения, например в скрипте, добавьте `-Force` параметр в конец командных строк.

Дополнительные сведения см. в разделе Copy-Item.

Этот шаг не обновляет и не изменяет загрузочный образ. Однако при создании загрузочного носителя с помощью Windows ADK он гарантирует, что последние загрузочные файлы bootmgr доступны для Windows ADK. При обновлении этих файлов в Windows ADK продукты, использующие Windows ADK для создания загрузочных носителей, например **Microsoft Deployment Toolkit (MDT),** также имеют доступ к обновленным загрузочным файлам начальной загрузки.

В частности, этот шаг необходим при устранении уязвимости bootkit UEFI в BlackLotus, как описано в статье KB5025885: Управление отзывами диспетчера загрузки Windows для изменений безопасной загрузки, связанных с CVE-2023-24932 и CVE-2023-24932.

Совет

Образы загрузки из **ADK 10.1.26100.1 (май 2024 г.) и более поздних** версий уже содержат накопительное обновление для устранения уязвимости bootkit UEFI BlackLotus.

Примечание

Microsoft Configuration Manager и **службы развертывания Windows (WDS)** автоматически извлекают файлы загрузки bootmgr из образов загрузки при обновлении загрузочных образов в этих продуктах. Они не используют загрузочные файлы bootmgr из Windows ADK.

Шаг 9. Очистка компонентов

Выполните **командыDISM.exe** , которые очищают подключенный образ загрузки и помогают уменьшить его размер:

PowerShell

В командной строке **PowerShell** с повышенными привилегиями выполните следующую команду, чтобы очистить подключенный образ загрузки и уменьшить его размер:

PowerShell

```
Start-Process "C:\Program Files (x86)\Windows Kits\10\Assessment and
Deployment Kit\Deployment Tools\amd64\DISM\dism.exe" -ArgumentList "
/Image:"<Mount_folder_path>" /Cleanup-image /StartComponentCleanup
/Resetbase /Defer" -Wait -LoadUserProfile

Start-Process "C:\Program Files (x86)\Windows Kits\10\Assessment and
Deployment Kit\Deployment Tools\amd64\DISM\dism.exe" -ArgumentList "
/Image:"<Mount_folder_path>" /Cleanup-image /StartComponentCleanup
/Resetbase" -Wait -LoadUserProfile
```

Пример:

PowerShell

```
Start-Process "C:\Program Files (x86)\Windows Kits\10\Assessment and
Deployment Kit\Deployment Tools\amd64\DISM\dism.exe" -ArgumentList "
/Image:`"C:\Mount`" /Cleanup-image /StartComponentCleanup /Resetbase
/Defer" -Wait -LoadUserProfile

Start-Process "C:\Program Files (x86)\Windows Kits\10\Assessment and
Deployment Kit\Deployment Tools\amd64\DISM\dism.exe" -ArgumentList "
/Image:"C:\Mount" /Cleanup-image /StartComponentCleanup /Resetbase" -
Wait -LoadUserProfile
```

Дополнительные сведения см. в разделах Изменение образа Windows с помощью DISM: уменьшение размера образа, пакет операционной системы

DISM (.cab или MSU) обслуживание Command-Line параметры: /Cleanup-Image и Start-Process.

Шаг 10. Проверка добавления всех необходимых пакетов в образ загрузки

После применения необязательных компонентов и накопительного обновления (CU) к загрузочному образу убедитесь, что они отображаются как установленные:

PowerShell

В командной строке **PowerShell** с повышенными привилегиями выполните следующую команду, чтобы убедиться, что все необязательные компоненты и накопительное обновление (CU) применены к загрузочному образу:

```
PowerShell
Get-WindowsPackage -Path "<Mount_folder_path>"
```

Пример:

```
PowerShell
Get-WindowsPackage -Path "C:\Mount"
```

Дополнительные сведения см. в разделе Get-WindowsPackage.

Шаг 11. Отключение образа загрузки и сохранение изменений

После применения драйверов, необязательных компонентов и накопительного обновления (CU) к загрузочному образу отключите загрузочный образ и сохраните изменения.

PowerShell

В командной строке **PowerShell** с повышенными привилегиями выполните следующую команду, чтобы отключить загрузочный образ и сохранить изменения:

PowerShell

```
Dismount-WindowsImage -Path "<Mount_folder_path>" -Save -Verbose
```

Пример:

PowerShell

```
Dismount-WindowsImage -Path "C:\Mount" -Save -Verbose
```

Дополнительные сведения см. в разделе Dismount-WindowsImage.

Шаг 12. Экспорт образа загрузки для уменьшения размера

1. После отключения и сохранения загрузочного образа его размер можно дополнительно уменьшить, экспортируя его:

   PowerShell

   В командной строке **PowerShell** с повышенными привилегиями выполните следующую команду, чтобы дополнительно уменьшить размер загрузочного образа путем его экспорта:

   PowerShell

   ```
   Export-WindowsImage -SourceImagePath "<Boot_image_path>\
   <boot_image>.wim" -SourceIndex 1 -DestinationImagePath "
   <Boot_image_path>\<boot_image>-export.wim" -CompressionType max -
   Verbose
   ```

   Пример:

   PowerShell

   ```
   Export-WindowsImage -SourceImagePath "C:\Program Files
   (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
   Preinstallation Environment\amd64\en-us\winpe.wim" -SourceIndex 1 -
   DestinationImagePath "C:\Program Files (x86)\Windows
   Kits\10\Assessment and Deployment Kit\Windows Preinstallation
   Environment\amd64\en-us\winpe-export.wim" -CompressionType max -
   Verbose
   ```

Дополнительные сведения см. в разделе Export-WindowsImage.

2. После завершения экспорта:

   a. Удалите исходный обновленный загрузочный образ:

   PowerShell

   В командной строке **PowerShell** с повышенными привилегиями выполните следующую команду, чтобы удалить исходный обновленный образ загрузки:

   ```
   PowerShell
   Remove-Item -Path "<Boot_image_path>\<boot_image>.wim" -Force
   ```

   Пример:

   ```
   PowerShell
   Remove-Item -Path "C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows Preinstallation Environment\amd64\en-us\winpe.wim" -Force
   ```

   Дополнительные сведения см. в разделе Remove-Item.

   b. Переименуйте экспортируемый загрузочный образ на имя исходного образа загрузки:

   PowerShell

   В командной строке **PowerShell** с повышенными привилегиями выполните следующую команду, чтобы переименовать экспортируемый образ загрузки именем исходного образа загрузки:

   ```
   PowerShell
   Rename-Item -Path "<Boot_image_path>\<exported_boot_image>.wim" -NewName "<original_boot_image_name>.wim"
   ```

   Пример:

   ```
   PowerShell
   ```

```
Rename-Item -Path "C:\Program Files (x86)\Windows
Kits\10\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\en-us\winpe-export.wim" -NewName "winpe.wim"
```

Дополнительные сведения см. в разделе Rename-Item.

Шаг 13. Обновление образа загрузки в продуктах, которые его используют (если применимо)

После обновления образа загрузки по умолчанию `winpe.wim` из Windows ADK в продуктах, использующих загрузочный образ, обычно необходимо выполнить дополнительные действия. Следующие ссылки содержат сведения об обновлении образа загрузки для нескольких популярных продуктов, использующих загрузочные образы:

- Microsoft Configuration Manager
- Microsoft Deployment Toolkit (MDT)
- Службы развертывания Windows
  - Исходный загрузочный образ WDS обновлен
  - Загрузочный образ WDS заменен новым обновленным загрузочным образом
  - Добавление обновленного образа загрузки в качестве нового загрузочного образа в WDS

Для любых других продуктов, использующих образы загрузки, обратитесь к документации по продукту по обновлению образа загрузки.

рекомендации по Microsoft Configuration Manager

Создание образов загрузки Microsoft Configuration Manager

Microsoft Configuration Manager создает собственные образы загрузки, принимая `winpe.wim` из Windows ADK, добавляя некоторые необязательные компоненты, необходимые для правильной работы, а затем сохраняя загрузочный образ в

`boot.wim` каталоге `<ConfigMgr_Install_Directory>\OSD\boot\<architecture>\boot.wim`. Этот `boot.wim` загрузочный образ считается первозданной достоверной копией образа загрузки Configuration Manager. Configuration Manager никогда не касается, не изменяет и не обновляет `boot.wim` загрузочный образ, за исключением некоторых конкретных сценариев. Вместо этого при внесении изменений в свойства загрузочного образа в Configuration Manager, например:

- Добавление драйверов
- Добавление необязательных компонентов
- Включение командной строки

Configuration Manager создает копию `boot.wim`, применяет изменения к копии, а затем сохраняет новый загрузочный образ как `boot.<package_id>.wim`.

Если в будущем в загрузочный образ будут внесены дополнительные изменения, Configuration Manager удаляет ранее созданный `boot.<package_id>.wim` загрузочный образ, создает новую копию `boot.wim`, применяет изменения к копии, а затем сохраняет новый загрузочный образ как `boot.<package_id>.wim`. Другими словами, `boot.wim` никогда не касается. Каждый раз, когда в загрузочный образ вносятся какие-либо изменения, новые изменения и все изменения, внесенные в прошлом, повторно применяются к новой копии `boot.wim`.

Этот процесс имеет следующие преимущества:

1. Сохраняет `boot.wim` нетронутое.

2. Убедитесь, что изменения, внесенные в образ загрузки, внесены в нетронутой неизмененную версию образа загрузки. Этот процесс помогает избежать повреждения при многократном обновлении загрузочного образа. Я также могу исправить проблемы с существующими образами загрузки.

3. Помогает управлять компонентами в образе загрузки. Процессу не нужно знать, какие компоненты может потребоваться удалить из загрузочного образа при каждом перестроении загрузочного образа. Вместо этого необходимо просто знать, какие компоненты необходимо добавить в загрузочный образ.

4. Это уменьшает размер загрузочного образа, который может возникать при многократном добавлении компонентов в образ загрузки и удалении из него.

Configuration Manager обновляет `boot.wim` загрузочный образ в двух сценариях:

1. При обновлении Configuration Manager между версиями или применении `boot.wim` исправлений для свертки (HFRU) может быть обновлено в рамках процесса обновления.

2. При выборе параметра **Перезагрузить этот загрузочный образ с текущей версией Windows PE из Windows ADK** в **мастере обновления точек распространения**.

В этих сценариях загрузочный образ обновляется с помощью `winpe.wim` загрузочного образа из Windows ADK, `boot.wim` как описано ранее в этом разделе. Этот процесс создает новую нетронутой `boot.wim` копию загрузочного образа, используя текущую версию загрузочного `winpe.wim` образа, которая является частью Windows ADK.

Какой загрузочный образ следует обновить с помощью накопительного обновления?

При добавлении накопительного обновления вручную в образ загрузки Configuration Manager рекомендуется обновить `winpe.wim` загрузочный образ из Windows ADK, а не напрямую обновлять `boot.wim` загрузочный образ, созданный Configuration Manager.

Загрузочный `winpe.wim` образ из Windows ADK должен быть обновлен, так как при `boot.wim` создании Configuration Manager обновляется, то при следующем `boot.wim` обновлении с помощью Configuration Manager обновления или **перезагрузки образа загрузки с текущей версией Windows PE из параметра Windows ADK**, а затем внесены изменения в `boot.wim`, включая примененное накопительное обновление, будет потеряно. `winpe.wim` Если образ загрузки из Windows ADK обновляется накопительным обновлением, накопительное обновление сохраняется и сохраняется, даже если Configuration Manager обновляет `boot.wim` загрузочный образ.

> ⓘ **Важно!**
>
> Никогда не обновляйте `boot.<package_id>.wim` образ загрузки вручную. Помимо проблем, возникающих при обновлении `boot.wim` образа загрузки вручную, образ `boot.<package_id>.wim` загрузки также столкнется с дополнительными проблемами, такими как:

- При любых изменениях образа загрузки (добавление драйверов, включение командной строки и т. д.) все изменения, внесенные вручную в загрузочный образ, включая накопительное обновление, будут потеряны.

- При изменении `boot.<package_id>.wim` образа загрузки вручную изменяется хэш-значение загрузочного образа. Изменение хэш-значения загрузочного образа может привести к сбою загрузки при скачивании образа загрузки из точки распространения.

Обновление `winpe.wim` из Windows ADK гарантирует, что накопительное обновление будет применяться независимо от того, какие изменения вносятся в `boot.wim` образ загрузки с помощью Configuration Manager.

Добавление необязательных компонентов вручную в Configuration Manager образы загрузки

Для Microsoft Configuration Manager загрузочных образов при применении накопительного обновления к загрузочному образу обязательно добавьте все необходимые необязательные компоненты вручную с помощью командных строк из пошагового руководства, а не через Configuration Manager. Необязательные компоненты добавляются в образы загрузки в Configuration Manager с помощью **вкладки Необязательные компоненты** в **свойствах** образа загрузки.

Необязательные компоненты необходимо добавлять в образ загрузки вручную, а не через Configuration Manager, так как:

- При применении накопительного обновления также обновляются все необязательные компоненты по мере необходимости.

- Если необязательные компоненты добавляются через Configuration Manager в загрузочный образ с накопительным обновлением, необязательные компоненты не обновляются накопительным обновлением. Добавление необязательных компонентов через Configuration Manager может привести к непредвиденному поведению и проблемам. Накопительное обновление необходимо добавить после добавления необязательных компонентов в образ загрузки, чтобы необязательные компоненты были правильно обновлены вместе с накопительным обновлением.

ⓘ Примечание

Если необязательный компонент пытается добавить с помощью **вкладки Необязательные компоненты** в **свойствах** образа загрузки в Configuration Manager но необязательный компонент уже был добавлен в загрузочный образ вручную, Configuration Manager больше не добавит этот необязательный компонент. Вместо этого Configuration Manager обнаруживает, что дополнительный компонент уже добавлен, и не будет пытаться снова добавить необязательный компонент.

необходимые компоненты образа загрузки Configuration Manager

Для правильной работы образов загрузки Microsoft Configuration Manager требуются следующие необязательные компоненты:

Развернуть таблицу

Функция	Имя файла	Зависимость	Требуется для ConfigMgr
Скрипты/WinPE-Scripting	`WinPE-Scripting.cab`	Отсутствует	Да
Скрипты/WinPE-WMI	`WinPE-WMI.cab`	Отсутствует	Да
Network/WinPE-WDS-Tools	`WinPE-WDS-Tools.cab`	Отсутствует	Да
Startup/WinPE-SecureStartup	`WinPE-SecureStartup.cab`	Скрипты/WinPE-WMI	Да

При добавлении необязательных компонентов в любой образ загрузки, используемый Configuration Manager на шаге 6. Добавление необязательных компонентов в образ загрузки, сначала добавьте в образ загрузки указанные выше обязательные компоненты в указанном выше порядке. После добавления необходимых компонентов в загрузочный образ добавьте в загрузочный образ все необходимые необязательные компоненты.

Список всех доступных необязательных компонентов WinPE, включая описания для каждого компонента, см. в статье Справочник по дополнительным компонентам WinPE(OC): Дополнительные компоненты WinPE.

Обновление образа загрузки в Configuration Manager

После обновления `winpe.wim` загрузочного образа из Windows ADK создайте новый `boot.wim` загрузочный образ для Configuration Manager, чтобы он содержал накопительное обновление. Новый `boot.wim` загрузочный образ можно создать, выполнив следующие действия.

1. Откройте консоль Microsoft Configuration Manager.
2. В консоли Microsoft Configuration Manager перейдите в раздел **Обзор библиотеки**> программного обеспечения**Загрузочные**>**образыоперационных систем**>.
3. В области **Загрузочные образы** выберите нужный загрузочный образ.
4. На панели инструментов выберите **Обновить точки распространения**.
5. Когда откроется окно **Мастера обновления точек распространения** :
   a. На странице **Общие/точки распространения обновлений с этим образом** выберите параметр **Перезагрузить этот загрузочный образ с текущей версией Windows PE из Windows ADK** , а затем нажмите кнопку **Далее >** .
   b. На странице **Сводка** нажмите кнопку **Далее >** .
   c. При сборке загрузочного образа появится страница **Ход** выполнения.
   d. После завершения сборки образа загрузки откроется**страница "Обновление точек распространения" успешно**/ завершена. Нажмите кнопку **Закрыть** .

Этот процесс обновляет загрузочный образ, используемый Configuration Manager. Он также обновляет загрузочный образ и загрузочные файлы bootmgr, используемые любыми точками распространения с поддержкой PXE.

> **ⓘ Важно!**
>
> Если в среде для точек распространения с поддержкой PXE используется несколько загрузочных образов, обязательно обновите все загрузочные образы с поддержкой PXE одинаковым накопительным обновлением. Это гарантирует, что все точки распространения с поддержкой PXE используют версию загрузочных файлов bootmgr, извлеченных из образов загрузки (если применимо).

Обновление загрузочного носителя Configuration Manager

После выполнения пошагового руководства, включая обновление образов загрузки в Configuration Manager, обновите все Configuration Manager носителя последовательности задач. Обновление любого носителя последовательности задач Configuration Manager гарантирует, что на носителе последовательности задач есть обновленный загрузочный образ. Если применимо, он также обновит загрузочные файлы bootmgr на носителе путем извлечения последних версий из загрузочного образа. Дополнительные сведения о создании Configuration Manager носителя последовательности задач см. в разделе Создание носителя последовательности задач.

Рекомендации по набору средств развертывания Майкрософт (MDT)

При добавлении накопительного обновления в загрузочный образ Microsoft Deployment Toolkit (MDT) рекомендуется обновить `winpe.wim` загрузочный образ из Windows ADK, а не напрямую обновлять `LiteTouchPE_<arch>.wim` загрузочный образ в общей папке развертывания MDT.

Загрузочный `winpe.wim` образ из Windows ADK следует обновить, так как при `LiteTouchPE_<arch>.wim` обновлении общей папки развертывания MDT при следующем обновлении изменения, внесенные `LiteTouchPE_<arch>.wim` в , включая примененное накопительное обновление, будут потеряны. `winpe.wim` Если образ загрузки из Windows ADK обновляется накопительным обновлением, накопительное обновление сохраняется и сохраняется даже при обновлении общей папки развертывания MDT.

Версии MDT и Windows ADK

Microsoft Deployment Toolkit (MDT) не поддерживает версии Windows или Windows ADK за Windows 10. При использовании MDT рекомендуется использовать ADK для Windows 10 версии 2004 вместо последней версии Windows ADK. **ADK для Windows 10 версии 2004** — последняя версия Windows ADK, поддерживаемая MDT. При обновлении образа загрузки для ADK для Windows 10 версии 2004 с накопительным обновлением используйте накопительное обновление для Windows 10 версии 22H2.

Необходимые компоненты образа загрузки MDT

Для правильной работы образов загрузки Microsoft Deployment Toolkit (MDT) требуются следующие необязательные компоненты:

Развернуть таблицу

Функция	Имя файла	Зависимость	Требуется mdt
Скрипты/WinPE-Scripting	`WinPE-Scripting.cab`	Отсутствует	Да
Скрипты/WinPE-WMI	`WinPE-WMI.cab`	Отсутствует	Да
Управление файлами/WinPE-FMAPI	`WinPE-FMAPI.cab`	Отсутствует	Да
Startup/WinPE-SecureStartup	`WinPE-SecureStartup.cab`	Скрипты/WinPE-WMI	Да
HTML/WinPE-HTA	`WinPE-HTA.cab`	Скрипты/WinPE-WMI	Да

При добавлении необязательных компонентов в любой образ загрузки, используемый MDT на шаге 6. Добавление необязательных компонентов на шаге образ загрузки , сначала добавьте указанные выше обязательные компоненты в указанном выше порядке в загрузочный образ. После добавления необходимых компонентов в загрузочный образ добавьте в загрузочный образ все необходимые необязательные компоненты.

Список всех доступных необязательных компонентов WinPE, включая описания для каждого компонента, см. в статье Справочник по дополнительным компонентам WinPE(OC): Дополнительные компоненты WinPE.

Обновление образа загрузки и загрузочного носителя в MDT

После обновления `winpe.wim` образа загрузки из Windows ADK создайте новый `LiteTouchPE_<arch>.wim` загрузочный образ для MDT, содержащий накопительное обновление, а затем создайте новый загрузочный носитель MDT. Новые образы загрузки MDT и загрузочный носитель MDT можно создать, выполнив следующие действия.

1. Убедитесь, что шаг 8. Копирование загрузочных файлов из подключенного образа загрузки в путь установки ADK завершено. MDT копирует загрузочные файлы bootmgr из пути установки Windows ADK в общую папку развертывания. После выполнения этого шага в общей папке развертывания содержатся последние загрузочные файлы bootmgr, необходимые при создании загрузочного носителя MDT.

2. Откройте консоль Microsoft Deployment Toolkit (MDT) Deployment Workbench.

3. В консоли Deployment Workbench перейдите в раздел **Deployment Workbench**>**Deployment Share**>**MDT Deployment Share**.

4. Щелкните правой кнопкой мыши **общий ресурс развертывания MDT** и выберите **Обновить общую папку развертывания**.

5. В окне **Мастер обновления общей папки развертывания** , которое отображается:

   a. На странице **Параметры** выберите параметр **Полностью повторно создать образы загрузки** , а затем нажмите кнопку **Далее >** .

   b. На странице **Сводка** нажмите кнопку **Далее >** .

   c. При сборке образа загрузки и общей папки развертывания появится страница **Ход** выполнения.

   d. После завершения сборки образа загрузки и общей папки развертывания откроется страница**Подтверждениеуспешно**/ завершенного процесса. Нажмите кнопку **Готово** .

Эти действия также обновите загрузочный носитель MDT в общей папке развертывания MDT. Выполнив описанные выше действия, используйте только что обновленные ISO-файлы в папке `<DeploymentShare>\Boot` , чтобы создать новый загрузочный носитель MDT.

Рекомендации по службам развертывания Windows (WDS)

Исходный загрузочный образ WDS обновлен

Если измененный образ загрузки WDS был исходным загрузочным образом WDS в `<RemoteInstall>` папке, то единственным дополнительным шагом является

перезапуск `Windows Deployment Services Server` службы. WDS можно перезапустить с помощью следующих командных строк:

PowerShell

В командной строке **PowerShell** с повышенными привилегиями выполните следующую команду, чтобы перезапустить `Windows Deployment Services Server` службу:

PowerShell

```
Restart-Service -Name WDSServer
```

Дополнительные сведения см. в разделе Restart-Service.

Загрузочный образ WDS заменен новым обновленным загрузочным образом

В следующем сценарии замены образа загрузки для WDS:

- Загрузочный образ, измененный в рамках этого руководства, находится за пределами `<RemoteInstall>` папки. Например, загрузочный образ, `winpe.wim` который поставляется с Windows ADK.
- Существующий загрузочный образ в WDS заменяется обновленным загрузочным образом.

Чтобы обновить загрузочный образ в WDS, выполните следующие действия.

1. Замените существующий загрузочный образ в WDS измененным загрузочным образом, используя следующие командные строки:

   PowerShell

   В PowerShell исходный загрузочный образ необходимо сначала удалить, а затем заменить новым. В командной строке **PowerShell** с повышенными привилегиями выполните следующие команды, чтобы заменить существующий загрузочный образ в WDS новым загрузочным образом:

   PowerShell

   ```
   Remove-WdsBootImage -Architecture <Architecture_x64_or_x86> -
   ImageName "<Name_Of_Existing_Boot_Image_In_WDS>"
   ```

```
Import-WdsBootImage -Path "<Path_To_Updated_Boot_Image>\
<boot_image>.wim" -NewImageName "
<Name_Of_Existing_Boot_Image_In_WDS>"
```

Пример:

PowerShell

```
Remove-WdsBootImage -Architecture x64 -ImageName "Microsoft Windows
PE (amd64)"
Import-WdsBootImage -Path "C:\Program Files (x86)\Windows
Kits\10\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\en-us\winpe.wim" -NewImageName "Microsoft Windows
PE (amd64)"
```

Дополнительные сведения см. в разделах Remove-WdsBootImage и Import-WdsBootImage.

2. После замены существующего образа загрузки в WDS перезапустите службу WDS:

PowerShell

В командной строке **PowerShell** с повышенными привилегиями выполните следующую команду, чтобы перезапустить `Windows Deployment Services Server` службу:

PowerShell

```
Restart-Service -Name WDSServer
```

Дополнительные сведения см. в разделе Restart-Service.

Добавление обновленного образа загрузки в качестве нового загрузочного образа в WDS

В следующем сценарии загрузочного образа для WDS:

- Загрузочный образ, измененный в рамках этого руководства, находится за пределами `<RemoteInstall>` папки. Например, образ загрузки, `winpe.wim` который поставляется с Windows ADK

- Обновленный загрузочный образ добавляется в качестве нового загрузочного образа в WDS

Чтобы добавить загрузочный образ в WDS, выполните следующие действия:

1. Добавьте обновленный образ загрузки в WDS с помощью следующих командных строк:

   PowerShell

   В командной строке **PowerShell** с повышенными привилегиями выполните следующие команды, чтобы добавить обновленный загрузочный образ в WDS в качестве нового загрузочного образа:

   ```
   PowerShell
   Import-WdsBootImage -Path "<Path_To_Updated_Boot_Image>\
   <boot_image>.wim" -NewImageName "<Boot_Image_Name_In_WDS>"
   ```

   Пример:

   ```
   PowerShell
   Import-WdsBootImage -Path "C:\Program Files (x86)\Windows
   Kits\10\Assessment and Deployment Kit\Windows Preinstallation
   Environment\amd64\en-us\winpe.wim" -NewImageName "Microsoft Windows
   PE (amd64) - Updated"
   ```

   Дополнительные сведения см. в разделе Import-WdsBootImage.

2. После замены существующего образа загрузки в WDS перезапустите службу WDS:

   PowerShell

   В командной строке **PowerShell** с повышенными привилегиями выполните следующую команду, чтобы перезапустить `Windows Deployment Services Server` службу:

   ```
   PowerShell
   Restart-Service -Name WDSServer
   ```

Дополнительные сведения см. в разделе Restart-Service.

Поддержка Boot.wim

Boot.wim, который является частью установочного носителя Windows, не поддерживается для развертывания Windows 11 со службами развертывания Windows (WDS). Кроме того, **boot.wim** с установочного носителя Windows 11 не поддерживается для развертывания любой версии Windows со службами развертывания Windows (WDS). Дополнительные сведения см. в разделе Поддержка boot.wim служб развертывания Windows (WDS).

Windows Server 2012 R2

Это пошаговое руководство не предназначено для использования с Windows Server 2012 R2. Действия, описанные в этой статье, могут работать с Windows Server 2012 R2 при использовании более ранних версий Windows ADK. Однако могут возникнуть проблемы совместимости с версиями Windows ADK, которые являются более новыми, чем ADK для Windows 10 версии 2004. Чтобы устранить проблемы совместимости с более новыми пакетами ADK и Windows Server 2012 R2, выполните приведенные ниже действия.

1. Обновите Windows Server 2012 R2 до более новой версии Windows Server.
2. Выполните настройку образа загрузки на компьютере под управлением версии Windows, поддерживающей более новые пакеты ADK, например Windows 10 или Windows 11, а затем перенесите измененный образ загрузки на сервер Windows Server 2012 R2.

Дополнительные сведения см. в разделе Жизненный цикл Windows Server 2012 R2.

Связанные статьи

- Создание загрузочного носителя Windows PE: обновление надстройки Windows PE для Windows ADK
- Обновление установочного носителя Windows с помощью динамического обновления: обновление WinPE
- KB5025885. Управление отзывами диспетчера загрузки Windows для изменений безопасной загрузки, связанных с CVE-2023-24932: обновление загрузочного носителя

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

MBR2GPT.EXE

Применяется к: ✅ Windows 11, ✅ Windows 10

> ⓘ **Внимание**
>
> **MBR2GPT.EXE** находится в каталоге `Windows\System32` на любом устройстве под управлением **поддерживаемой в настоящее время версии Windows**.

MBR2GPT.EXE изменяет для диска стиль раздела "Основная загрузочная запись" (MBR) на стиль раздела "Таблица разделов GPT" (GPT) без изменения или удаления данных на диске. Средство запускается из командной строки среды предустановки Windows (Windows PE), но также может быть запущено из полной операционной системы Windows с помощью `/allowFullOS` параметра .

Средство доступно в полной среде ОС и среде Windows PE.

В следующем видео содержится подробное описание и демонстрация MBR2GPT.

https://www.youtube-nocookie.com/embed/hfJep4hmg9o

MBR2GPT можно использовать для:

- Для перевода любых подключенных системных дисков из формата MBR в формат GPT. Средство не может использоваться для преобразования несистемных дисков из MBR в GPT.
- Преобразуйте диск MBR с томами, зашифрованными BitLocker, при условии, что защита приостановлена. Чтобы возобновить BitLocker после преобразования, необходимо удалить существующие предохранители, а затем повторно создать.
- Преобразуйте диск операционной системы из MBR в GPT с помощью Microsoft Configuration Manager или Microsoft Deployment Toolkit (MDT).

Автономное преобразование системных дисков с более ранними версиями Windows, такими как Windows 7, 8 или 8.1, официально не поддерживается. Для преобразования этих дисков рекомендуется обновить операционную систему до поддерживаемой в настоящее время версии Windows, а затем выполнить преобразование MBR в GPT.

> ⓘ **Внимание**
>
> После преобразования диска в формат стиля разделов GPT необходимо настроить для встроенного ПО загрузку в режиме UEFI.

Убедитесь, что устройство поддерживает UEFI, прежде чем пытаться преобразовать диск.

Предварительные требования к диску

Перед внесением изменений на диск средство MBR2GPT проверяет разметку и геометрию выбранного диска, чтобы подтвердить следующее.

- Для диска сейчас используется формат MBR
- Секции не занимают достаточно места для хранения первичных и вторичных объектов групповой политики:
  - 16 КБ + 2 сектора в передней части диска
  - 16 КБ + 1 сектор в конце диска
- В таблице разделов MBR не более трех основных секций.
- Один из разделов задан в качестве активного и является системным разделом
- Диск не имеет расширенного или логического раздела
- Хранилище данных конфигурации загрузки в системном разделе содержит стандартную запись операционной системы, указывающую на раздел операционной системы
- Идентификаторы томов можно получить для каждого тома, которому назначена буква диска.
- Все секции на диске имеют типы MBR, распознаваемые Windows, или имеют сопоставление, указанное с помощью параметра командной `/map` строки.

Если какая-либо из этих проверок завершается неудачно, преобразование не выполняется и возвращается ошибка.

Синтаксис

```
MBR2GPT /validate|convert [/disk:<diskNumber>] [/logs:<logDirectory>] [/map:<source>=<destination>] [/allowFullOS]
```

Параметры

Развернуть таблицу

Параметр	Описание
/validate	Указывает `MBR2GPT.exe` выполнять только действия по проверке диска и сообщать о том, подходит ли диск для преобразования.

Параметр	Описание
/convert	Указывает `MBR2GPT.exe` выполнить проверку диска и продолжить преобразование, если все проверочные тесты пройдены.
/disk: ***<diskNumber>***	Указывает номер диска, который нужно перевести в формат GPT. Если параметр не задан, используется системный диск. Используемый механизм совпадает с механизмом, используемым командой средства diskpart.exe **SELECT DISK SYSTEM** .
/logs: ***<logDirectory>***	Указывает каталог, в который `MBR2GPT.exe` должны записываться журналы. Если параметр не задан, используется **%windir%**. Если этот параметр задан, каталог уже должен существовать, он не создается автоматически и не перезаписывается.
/map: ***<source>*** **=** ***<destination>***	Указывает другие сопоставления типов секций между MBR и GPT. Номер раздела MBR задается в десятичной системе, не шестнадцатеричной. GUID формата GPT может содержать скобки, например: **/map:42={af9b60a0-1431-4f62-bc68-3311714a69ad}**. Если требуются несколько сопоставлений, можно задать несколько параметров /map.
/allowFullOS	По умолчанию `MBR2GPT.exe` может выполняться только из Среды предустановки Windows и запрещено работать в полной версии Windows. Данный параметр переопределяет такую блокировку и разрешает преобразование диска в полной среде Windows. **Примечание.** Так как существующий системный раздел MBR используется при выполнении полной среды Windows, его нельзя использовать повторно. В этом случае создается новый системный раздел EFI путем сжатия раздела ОС.

Примеры:

Пример проверки

В следующем примере диск 0 проходит проверку перед преобразованием. Ошибки и предупреждения регистрируются в расположении `%windir%` по умолчанию .

Командная строка Windows

```
X:\> mbr2gpt.exe /validate /disk:0
MBR2GPT: Attempting to validate disk 0
MBR2GPT: Retrieving layout of disk
MBR2GPT: Validating layout, disk sector size is: 512
MBR2GPT: Validation completed successfully
```

Пример преобразования

В приведенном ниже примере выполняется следующее:

1. При использовании DiskPart перед преобразованием отображается текущий макет раздела диска. На диске MBR (диск 0) присутствуют три секции:

    - Зарезервированная системой секция.
    - Раздел Windows.
    - Раздел восстановления.
    - Также присутствует DVD-ROM как том 0.

2. Выбран том ОС, перечислены разделы, показаны подробные сведения о разделе ОС. Тип раздела MBR — **07**, соответствует типу IFS (устанавливаемая файловая система).

3. Средство MBR2GPT используется для преобразования диска 0.

4. Средство DiskPart сообщает, что для диска 0 сейчас используется формат GPT.

5. Показана новая разметка диска — четыре раздела на диске GPT: три таких же, как и предыдущие разделы, и один новый системный раздел EFI (том 3).

6. Том ОС выбирается снова. В этом разделе отображается, что том ОС преобразуется в тип секции GPT**ebd0a0a2-b9e5-4433-87c0-68b6b72699c7** , соответствующий **типу PARTITION_BASIC_DATA_GUID** .

Как отмечалось в выходных данных средства MBR2GPT, необходимо изменить встроенное ПО компьютера, чтобы новый раздел системы EFI правильно загрузил.

▼ Развернуть, чтобы показать пример MBR2GPT

Командная строка Windows

```
X:\>DiskPart.exe

Microsoft DiskPart version 10.0.15048.0

Copyright (C) Microsoft Corporation.
On computer: MININT-K71F13N

DISKPART> list volume

  Volume ###  Ltr  Label        Fs     Type        Size     Status     Info
  ----------  ---  -----------  -----  ----------  -------  ---------  --------
  Volume 0     F   CENA_X64FRE  UDF    DVD-ROM     4027 MB  Healthy
  Volume 1     C   System Rese  NTFS   Partition    499 MB  Healthy
  Volume 2     D   Windows      NTFS   Partition     58 GB  Healthy
  Volume 3     E   Recovery     NTFS   Partition    612 MB  Healthy    Hidden

DISKPART> select volume 2
```

```
Volume 2 is the selected volume.

DISKPART> list partition

  Partition ###  Type              Size     Offset
  -------------  ----------------  -------  -------
  Partition 1    Primary            499 MB  1024 KB
* Partition 2    Primary             58 GB   500 MB
  Partition 3    Recovery           612 MB    59 GB

DISKPART> detail partition

Partition 2
Type  : 07
Hidden: No
Active: No
Offset in Bytes: 524288000

  Volume ###  Ltr  Label        Fs     Type        Size     Status     Info
  ----------  ---  -----------  -----  ----------  -------  ---------  --------
* Volume 2     D   Windows      NTFS   Partition     58 GB  Healthy

DISKPART> exit

Leaving DiskPart...

X:\>mbr2gpt /convert /disk:0

MBR2GPT will now attempt to convert disk 0.
If conversion is successful the disk can only be booted in GPT mode.
These changes cannot be undone!

MBR2GPT: Attempting to convert disk 0
MBR2GPT: Retrieving layout of disk
MBR2GPT: Validating layout, disk sector size is: 512 bytes
MBR2GPT: Trying to shrink the system partition
MBR2GPT: Trying to shrink the OS partition
MBR2GPT: Creating the EFI system partition
MBR2GPT: Installing the new boot files
MBR2GPT: Performing the layout conversion
MBR2GPT: Migrating default boot entry
MBR2GPT: Adding recovery boot entry
MBR2GPT: Fixing drive letter mapping
MBR2GPT: Conversion completed successfully
MBR2GPT: Before the new system can boot properly you need to switch the firmware to
boot to UEFI mode!

X:\>DiskPart

Microsoft DiskPart version 10.0.15048.0

Copyright (C) Microsoft Corporation.
On computer: MININT-K71F13N

DISKPART> list disk
```

```
  Disk ###  Status         Size     Free     Dyn  Gpt
  --------  -------------  -------  -------  ---  ---
  Disk 0    Online           60 GB      0 B        *

DISKPART> select disk 0

Disk 0 is now the selected disk.

DISKPART> list volume

  Volume ###  Ltr  Label        Fs     Type        Size     Status     Info
  ----------  ---  -----------  -----  ----------  -------  ---------  --------
  Volume 0     F   CENA_X64FRE  UDF    DVD-ROM     4027 MB  Healthy
  Volume 1     D   Windows      NTFS   Partition     58 GB  Healthy
  Volume 2     C   System Rese  NTFS   Partition    499 MB  Healthy    Hidden
  Volume 3                      FAT32  Partition    100 MB  Healthy    Hidden
  Volume 4     E   Recovery     NTFS   Partition    612 MB  Healthy    Hidden

DISKPART> select volume 1

Volume 1 is the selected volume.

DISKPART> list partition

  Partition ###  Type              Size     Offset
  -------------  ----------------  -------  -------
  Partition 1    Recovery           499 MB  1024 KB
* Partition 2    Primary             58 GB   500 MB
  Partition 4    System             100 MB    59 GB
  Partition 3    Recovery           612 MB    59 GB

DISKPART> detail partition

Partition 2
Type    : ebd0a0a2-b9e5-4433-87c0-68b6b72699c7
Hidden  : No
Required: No
Attrib  : 0000000000000000
Offset in Bytes: 524288000

  Volume ###  Ltr  Label        Fs     Type        Size     Status     Info
  ----------  ---  -----------  -----  ----------  -------  ---------  --------
* Volume 1     D   Windows      NTFS   Partition     58 GB  Healthy
```

Характеристики

Процесс преобразования диска

Ниже приведены основные этапы процесса преобразования MBR-GPT.

1. Выполняется проверка диска.
2. Диск повторно разделяется на разделы, чтобы создать системный раздел EFI, если он еще не существует.
3. Файлы загрузки UEFI устанавливаются в системный раздел EFI.
4. Применяются метаданные GPT и сведения о макете.
5. Хранилище данных конфигурации загрузки обновляется.
6. Восстанавливаются назначенные буквы диска.

Создание системного раздела EFI

Чтобы Windows оставалась загрузочной после преобразования, должен быть на месте системный раздел EFI. MBR2GPT создает системный раздел EFI, используя следующие правила:

1. Существующий системный раздел MBR используется повторно, если он соответствует следующим требованиям.

    - Это также не раздел ОС или Среды восстановления Windows.
    - Это не менее 100 МБ (или 260 МБ для дисков размером 4K).
    - Размер меньше или равен 1 ГБ. Этот размер является мерой безопасности, чтобы убедиться, что он не является разделом данных.
    - Преобразование не выполняется из полной ОС. В этом случае используется существующий системный раздел MBR, который не может быть переназначен.

2. Если существующий системный раздел MBR не удается использовать повторно, создается новый системный раздел EFI путем сжатия раздела ОС. Эта новая секция имеет размер 100 МБ (или 260 МБ для дисков размером с 4K секторов) и имеет формат FAT32.

Если существующий системный раздел MBR не используется повторно для системного раздела EFI, он больше не используется процессом загрузки после преобразования. Другие секции не изменяются.

> **ⓘ Внимание**
>
> Если существующий системный раздел MBR не используется повторно для системного раздела EFI, ему может быть назначена буква диска. Если эта небольшая секция не будет использоваться, ее буква диска должна быть скрыта вручную.

Сопоставление типов разделов и атрибуты раздела

Поскольку для разделов GPT используется не такой набор идентификаторов типов, как для разделов MBR, каждому разделу преобразованного диска должен быть присвоен новый идентификатор типа. Сопоставление типов разделов выполняется согласно следующим правилам.

1. Системный раздел EFI всегда имеет тип секции **PARTITION_SYSTEM_GUID** (**c12a7328-f81f-11d2-ba4b-00a0c93ec93b**).
2. Если раздел MBR имеет тип, соответствующий одной из записей, указанных в `/map` параметре, используется указанный идентификатор типа секции GPT.
3. Если раздел MBR имеет тип **0x27**, он преобразуется в раздел GPT типа **PARTITION_MSFT_RECOVERY_GUID** (**de94bba4-06d1-4d40-a16a-bfd50179d6ac**).
4. Все остальные разделы MBR, распознаваемые Windows, преобразуются в разделы GPT типа **PARTITION_BASIC_DATA_GUID** (**ebd0a0a2-b9e5-4433-87c0-68b6b72699c7**).

Помимо применения правильных типов, для разделов типа PARTITION_MSFT_RECOVERY_GUID также используется указанный далее набор атрибутов GPT.

- **GPT_ATTRIBUTE_PLATFORM_REQUIRED** (**0x0000000000000001**)
- **GPT_BASIC_DATA_ATTRIBUTE_NO_DRIVE_LETTER** (**0x8000000000000000**)

Дополнительные сведения о типах разделов см. в следующих статьях.

- Типы разделов GPT
- Типы разделов MBR

Сохранение присвоенных букв диска

Средство преобразования пытается переназначить все сведения о назначении букв диска, содержащиеся в реестре, которые соответствуют томам преобразованного диска. Если не удается восстановить назначение буквы диска, в консоли и в журнале отображается ошибка, что позволяет выполнить правильное назначение буквы диска вручную.

> ⓘ **Внимание**
>
> Этот код выполняется после преобразования макета, поэтому на данном этапе операцию невозможно отменить.

Средство преобразования получает сведения об уникальном идентификаторе тома до и после преобразования разметки, упорядочивая эту информацию в таблице подстановки.

Затем он выполняет итерацию по всем записям в **HKLM\SYSTEM\MountedDevices** и для каждой записи выполняет следующие действия:

1. Проверяет, соответствует ли уникальный идентификатор любому из уникальных идентификаторов для любого тома, который является частью преобразованного диска.
2. Если да, то задайте новый уникальный идентификатор, полученный после преобразования разметки.
3. Если новый уникальный идентификатор не удается задать, а имя значения начинается с **\DosDevices**, выведите предупреждение консоли и журнала о необходимости вмешательства вручную при правильном восстановлении назначения буквы диска.

Поиск и устранение неисправностей

Средство отображает сведения о состоянии в выходных данных. Если обнаружены ошибки, то сведения о проверке и преобразовании отсутствуют. Например, если одна или несколько секций не преобразуются должным образом, эта информация отображается, а преобразование не выполняется. Дополнительные сведения о выявленных ошибках см. в связанных файлах журнала.

Журналы

Средство MBR2GPT создает четыре файла журнала:

- diagerr.xml
- diagwrn.xml
- setupact.log
- setuperr.log

Эти файлы содержат ошибки и предупреждения, возникающие во время проверки и преобразования диска. Сведения в этих файлах могут быть полезны для диагностики проблем с помощью данного средства. Файлы `setupact.log` и `setuperr.log` содержат наиболее подробные сведения о макетах дисков, процессах и других сведениях, относящихся к проверке и преобразованию диска.

> ⓘ **Примечание.**
>
> Файлы *setupact.log*отличаются от файлов программы установки Windows, которые находятся в каталоге `%Windir%\Panther` .

Расположение по умолчанию для всех таких файлов журнала в среде Windows PE — **%windir%**.

Интерактивная справка

Чтобы просмотреть список параметров, доступных при использовании средства, введите следующую команду в командной строке с повышенными привилегиями:

Командная строка Windows

```
mbr2gpt.exe /?
```

Отображается следующий текст.

Командная строка Windows

```
C:\> mbr2gpt.exe /?

Converts a disk from MBR to GPT partitioning without modifying or deleting data on
the disk.

MBR2GPT.exe /validate|convert [/disk:<diskNumber>] [/logs:<logDirectory>] [/map:
<source>=<destination>] [/allowFullOS]

Where:

 /validate
         - Validates that the selected disk can be converted
           without performing the actual conversion.

 /convert
         - Validates that the selected disk can be converted
           and performs the actual conversion.

 /disk:<diskNumber>
         - Specifies the disk number of the disk to be processed.
           If not specified, the system disk is processed.

 /logs:<logDirectory>
         - Specifies the directory for logging. By default logs
           are created in the %windir% directory.

 /map:<source>=<destination>
         - Specifies the GPT partition type to be used for a
           given MBR partition type not recognized by Windows.
           Multiple /map switches are allowed.

 /allowFullOS
         - Allows the tool to be used from the full Windows
```

```
        environment. By default, this tool can only be used
        from the Windows Preinstallation Environment.
```

Коды возврата

Для MBR2GPT используются коды возврата, указанные ниже.

Развернуть таблицу

Код возврата	Описание
0	Преобразование успешно завершено.
1	Преобразование отменено пользователем.
2	Сбой преобразования из-за внутренней ошибки.
3	Сбой преобразования из-за ошибки инициализации.
4	Сбой преобразования из-за недопустимых параметров командной строки.
5	Сбой преобразования из-за ошибки чтения геометрии и разметки выбранного диска.
6	Преобразование не выполнено, так как один или несколько томов на диске зашифрованы.
7	Сбой преобразования, так как геометрия и макет выбранного диска не соответствуют требованиям.
8	Сбой преобразования из-за ошибки при создании системного раздела EFI.
9	Сбой преобразования из-за ошибки при установке файлов загрузки.
10	Сбой преобразования из-за ошибки при применении разметки GPT.
100	Преобразование в макет GPT выполнено, но некоторые записи данных конфигурации загрузки восстановить не удалось.

Определение типа раздела

Тип секции можно определить одним из трех способов:

- Использование Windows PowerShell
- Использование средства управления дисками
- Использование средства DiskPart

Windows PowerShell

В Windows PowerShell командной строке можно ввести следующую команду, чтобы отобразить номер диска и тип секции:

PowerShell

```
Get-Disk | ft -Auto
```

Пример выходных данных:

PowerShell

```
PS C:\> Get-Disk | ft -Auto

Number Friendly Name      Serial Number        HealthStatus OperationalStatus Total
Size Partition Style
------ -------------      -------------        ------------ ----------------- ------
---- ---------------
0      MTFDDAK256MAM-1K1  13050928F47C         Healthy      Online
238.47 GB MBR
1      ST1000DM003-1ER162 Z4Y3GD8F             Healthy      Online
931.51 GB GPT
```

Средство управления дисками

Тип секции диска можно просмотреть с помощью средства управления дисками:

1. Щелкните правой кнопкой мыши меню "Пуск" и выберите **Пункт Управление дисками**. Кроме того, щелкните правой кнопкой мыши меню "Пуск" и выберите **команду Выполнить**. В появившемся диалоговом окне **Выполнить** введите `diskmgmt.msc` и нажмите кнопку **ОК**.

2. В появившемся окне **Управление дисками** :

   a. В нижней области выберите интересующий номер диска.

   b. Выберите меню **Действие**, а затем выберите **Свойства всех задач**>. Кроме того, щелкните правой кнопкой мыши интересующий номер диска и выберите **Пункт Свойства**.

   c. В диалоговом окне **Свойства** диска выберите вкладку **Тома** .

   d. На вкладке **Тома** рядом с полем **Стиль секции** отображается тип секции.

Средство DiskPart

Тип секции можно определить с помощью средства DiskPart. Средство DiskPart полезно в сценариях, когда средство управления дисками и PowerShell недоступны, например в WinPE. PowerShell недоступен в WinPE, если дополнительный компонент PowerShell не загружен. Чтобы использовать средство DiskPart для определения типа секции, выполните следующие действия:

1. Откройте командную строку с повышенными привилегиями.
2. В открывающейся командной строке с повышенными привилегиями введите следующую команду:

   Командная строка Windows

   ```
   DiskPart.exe
   ```

3. В окнах командной строки отображается запрос **DISKPART>** . В командной строке **DISKPART>** введите следующую команду:

   Командная строка Windows

   ```
   list disk
   ```

4. Тип секции отображается в столбце **Gpt** . Если раздел имеет значение GPT, в столбце отображается звездочка (*). Если раздел имеет значение MBR, столбец будет пустым.

Ниже показан пример выходных данных средства DiskPart с типом секции для двух дисков:

Командная строка Windows

```
X:\>DiskPart.exe

Microsoft DiskPart version 10.0.15048.0

Copyright (C) Microsoft Corporation.
On computer: MININT-K71F13N

DISKPART> list disk

  Disk ###  Status         Size     Free     Dyn  Gpt
  --------  -------------  -------  -------  ---  ---
  Disk 0    Online          238 GB      0 B
  Disk 1    Online          931 GB      0 B        *
```

В этом примере для диска "Disk 0" использован стиль раздела MBR, а для диска "Disk 1" — GPT.

Last updated on 07.05.2025

Настройка PXE-сервера для загрузки Windows PE

Статья • 18.03.2023

Относится к:

- Windows 10

В этом пошаговом руководстве описано, как настроить PXE-сервер для загрузки Windows PE при запуске клиентского компьютера по сети. С помощью средств Windows PE и файла образа Windows 10 можно установить Windows 10 по сети.

Необходимые условия

- Компьютер развертывания. Компьютер с пакетом средств оценки и развертывания Windows (Windows ADK) и надстройкой Windows PE с установленным ADK.
- DHCP-сервер: DHCP-сервер или прокси-сервер DHCP, настроенный для отправки ответов на запросы PXE-клиентов.
- PXE-сервер: сервер под управлением службы TFTP, на котором могут размещаться файлы загрузки Windows PE для скачивания клиентом.
- Файловый сервер: сервер с общей сетевой папкой.

Все четыре перечисленных выше роли могут размещаться на одном компьютере, также можно выделить отдельный компьютер для каждой роли.

Шаг 1: скопируйте исходные файлы Windows PE

1. На компьютере развертывания выберите **Пуск** и введите **deployment**.

2. Щелкните правой кнопкой мыши элемент **Среда средств развертывания и работы с образами** и выберите команду **Запуск от имени администратора**. Будет запущен ярлык среды средств развертывания и создания образов, который открывает окно командной строки и автоматически задает переменные среды таким образом, чтобы они указывали на все необходимые средства.

3. Чтобы скопировать базовые файлы Windows PE в новую папку, выполните следующую команду. Сценарий требует два аргумента: архитектуру

оборудования и целевое расположение. Значение **<архитектуры>** может быть **x86**, **amd64** или **arm**, а **<назначение>** может соответствовать пути к локальному каталогу. Если каталог еще не существует, он будет создан.

Командная строка Windows

```
copype.cmd <architecture> <destination>
```

Например, следующая команда копирует файлы архитектуры **amd64** в каталог **C:\winpe_amd64**:

Командная строка Windows

```
copype.cmd amd64 C:\winpe_amd64
```

Сценарий создает структуру каталогов назначения и копирует все необходимые файлы для этой архитектуры. В предыдущем примере создаются следующие каталоги:

Командная строка Windows

```
C:\winpe_amd64
C:\winpe_amd64\fwfiles
C:\winpe_amd64\media
C:\winpe_amd64\mount
```

4. Подключите базовый образ Windows PE (winpe.wim) в каталог \mount с помощью средства DISM. При подключении файла образа его содержимое распаковывается в папку, что позволяет вносить изменения напрямую или с помощью таких программ, как DISM. См. приведенный ниже пример.

Командная строка Windows

```
dism.exe /mount-image /imagefile:c:\winpe_amd64\media\sources\boot.wim
/index:1 /mountdir:C:\winpe_amd64\mount
```

Убедитесь, что отображается сообщение **Операция успешно завершена** .

> **Примечание**
>
> Чтобы просмотреть подключенные в данный момент образы, введите `dism.exe /get-MountedWiminfo`.

5. Выполните сопоставление общего сетевого ресурса корневому каталогу TFTP на сервере PXE/TFTP и создайте папку \Boot. Обратитесь к документации сервера TFTP, чтобы определить корневой каталог сервера TFTP, а затем включите общий доступ к этой папке и убедитесь, что она доступна в сети. В следующем примере PXE-сервер имеет имя PXE-1, а корневой каталог TFTP используется по сетевому пути **\\PXE-1\TFTPRoot**:

   Командная строка Windows

   ```
   net.exe use y: \\PXE-1\TFTPRoot
   y:
   md Boot
   ```

6. Скопируйте файлы загрузки PXE из подключенного каталога в папку \boot. Пример.

   Командная строка Windows

   ```
   copy c:\winpe_amd64\mount\windows\boot\pxe\*.* y:\Boot
   ```

7. Скопируйте файл boot.sdi на сервер PXE/TFTP.

   Командная строка Windows

   ```
   copy C:\winpe_amd64\media\boot\boot.sdi y:\Boot
   ```

8. Скопируйте загрузочный образ Windows PE (boot.wim) в папку \boot.

   Командная строка Windows

   ```
   copy C:\winpe_amd64\media\sources\boot.wim y:\Boot
   ```

9. (Необязательно) Копирование шрифтов TrueType в папку \boot

   Командная строка Windows

   ```
   copy C:\winpe_amd64\media\Boot\Fonts y:\Boot\Fonts
   ```

Шаг 2: настройка параметров загрузки и копирование файла BCD

1. Создайте хранилище BCD с помощью bcdedit.exe:

Командная строка Windows

```
bcdedit.exe /createstore c:\BCD
```

2. Настройте параметры RAMDISK:

Командная строка Windows

```
bcdedit.exe /store c:\BCD /create {ramdiskoptions} /d "Ramdisk options"
bcdedit.exe /store c:\BCD /set {ramdiskoptions} ramdisksdidevice boot
bcdedit.exe /store c:\BCD /set {ramdiskoptions} ramdisksdipath
\Boot\boot.sdi
bcdedit.exe /store c:\BCD /create /d "winpe boot image" /application
osloader
```

Последняя команда возвращает идентификатор GUID, например:

Консоль

```
The entry {a4f89c62-2142-11e6-80b6-00155da04110} was successfully
created.
```

Скопируйте этот идентификатор GUID для использования в следующих командах. В каждой приведенной команде замените "GUID1" своим идентификатором GUID.

3. Создайте новую загрузочную запись приложения для образа Windows PE:

Командная строка Windows

```
bcdedit.exe /store c:\BCD /set {GUID1} device ramdisk=
[boot]\Boot\boot.wim,{ramdiskoptions}
bcdedit.exe /store c:\BCD /set {GUID1} path
\windows\system32\winload.exe
bcdedit.exe /store c:\BCD /set {GUID1} osdevice ramdisk=
[boot]\Boot\boot.wim,{ramdiskoptions}
bcdedit.exe /store c:\BCD /set {GUID1} systemroot \windows
bcdedit.exe /store c:\BCD /set {GUID1} detecthal Yes
bcdedit.exe /store c:\BCD /set {GUID1} winpe Yes
```

4. Настройте параметры BOOTMGR (не забудьте заменить GUID1 в третьей команде своим идентификатором GUID):

Командная строка Windows

```
bcdedit.exe /store c:\BCD /create {bootmgr} /d "boot manager"
bcdedit.exe /store c:\BCD /set {bootmgr} timeout 30
```

```
bcdedit.exe /store c:\BCD -displayorder {GUID1} -addlast
```

5. Скопируйте файл BCD на свой TFTP-сервер:

Командная строка Windows

```
copy c:\BCD \\PXE-1\TFTPRoot\Boot\BCD
```

Теперь ваш сервер PXE/TFTP настроен. Параметры BCD, настроенные с помощью команды bcdedit.exe /store <BCD location> /enum all. См. следующий пример. Примечание. Ваш идентификатор GUID будет отличаться от приведенного ниже.

Командная строка Windows

```
C:\>bcdedit.exe /store C:\BCD /enum all
Windows Boot Manager
--------------------
identifier              {bootmgr}
description             boot manager
displayorder            {a4f89c62-2142-11e6-80b6-00155da04110}
timeout                 30

Windows Boot Loader
-------------------
identifier              {a4f89c62-2142-11e6-80b6-00155da04110}
device                  ramdisk=[boot]\Boot\boot.wim,{ramdiskoptions}
description             winpe boot image
osdevice                ramdisk=[boot]\Boot\boot.wim,{ramdiskoptions}
systemroot              \Windows
detecthal               Yes
winpe                   Yes

Setup Ramdisk Options
---------------------
identifier              {ramdiskoptions}
description             ramdisk options
ramdisksdidevice        boot
ramdisksdipath          \Boot\boot.sdi
```

Совет

Если вы запускаете процесс загрузки PXE, но получаете сообщение об ошибке **Данные конфигурации загрузки для компьютера отсутствуют или содержат ошибку**, убедитесь, что `\boot` каталог установлен в правильном корневом каталоге сервера TFTP. В используемом здесь примере имя этого каталога — TFTPRoot, но сервер TFTP может быть другим.

Сводка по процессу загрузки PXE

В следующем процессе приводится сводка загрузки PXE-клиента.

> ⓘ **Примечание**
>
> Ниже предполагается, что клиент и PXE-сервер находятся в одной сети, подсети или виртуальной локальной сети или что PXE-запросы были соответствующим образом перенаправлены с клиента на PXE-сервер с помощью вспомогательных IP-адресов, настроенных в маршрутизаторе или коммутаторе. Дополнительные сведения о вспомогательных ip-адресах см. в разделе **Настройка маршрутизатора для перенаправления широковещательных передач**.

1. Клиент связывается с PXE-сервером. Если клиент находится в другой сети, подсети или vlan в качестве PXE-сервера, клиент направляется на PXE-сервер с помощью вспомогательных IP-адресов.

2. PXE-сервер отправляет клиенту параметры DHCP 060 (идентификатор клиента **PXEClient**), 066 (имя узла загрузочного сервера) и 067 (имя загрузочного файла).

3. Клиент скачивает `boot\PXEboot.n12` с сервера TFTP на основе параметра DHCP 067 имя загрузочного файла, полученное от PXE-сервера.

4. `PXEboot.n12` немедленно начинает загрузку сети.

5. Клиент скачивает `boot\bootmgr.exe` и `boot\BCD` файл с сервера TFTP.

   > ⓘ **Примечание**
   >
   > Хранилище BCD должно находиться в каталоге `\boot` на сервере TFTP и иметь имя BCD.

6. `Bootmgr.exe` считывает записи операционной системы BCD и загрузки, а также образ Среды предустановки `boot\boot.sdi` Windows (`boot\boot.wim`). Необязательные файлы, которые также можно скачать, включают шрифты TrueType (`boot\Fonts\wgl4_boot.ttf`) и файл состояния гибернации (`\hiberfil.sys`), если эти файлы присутствуют.

7. `Bootmgr.exe` запускает Windows PE путем вызова `winload.exe` в образе Windows PE.

8. Среда предустановки Windows загружается, открывается командная строка и `wpeinit.exe` выполняется для инициализации Среды предустановки Windows.

9. Клиент Среды предустановки Windows предоставляет доступ к таким средствам, как `imagex.exe`, `diskpart.exe` и `bcdboot.exe` с помощью командной строки Windows PE. С помощью этих средств вместе с файлом образа Windows 10 конечный компьютер можно правильно отформатировать для загрузки полной Windows 10 операционной системы.

Связанные статьи

Краткие руководства по Windows PE

Поддержка boot.wim служб развертывания Windows (WDS)

Статья • 20.07.2024 •

Применяется к: ✅ Windows 11, ✅ Windows 10, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Функциональность развертывания операционной системы служб развертывания Windows (WDS) частично устарела. Начиная с Windows 11 рабочие процессы, использующие **boot.wim** с установочного носителя или при запуске программы установки Windows в режиме WDS, больше не поддерживаются.

При загрузке PXE с сервера WDS, который использует файл **boot.wim** с установочного носителя в качестве образа загрузки, программа установки Windows автоматически запускается в режиме WDS. Этот рабочий процесс устарел для образов загрузки Windows 11 и более поздних версий. Отображается следующее сообщение о прекращении поддержки:

> Программа установки Windows
>
> Клиентские функции служб развертывания Windows частично устарели. Дополнительные сведения о том, что не рекомендуется использовать и что по-прежнему поддерживается, см. на странице https://aka.ms/WDSSupport .

Затронутые сценарии развертывания

В следующей таблице приведены сведения о поддержке конкретных сценариев развертывания. Boot.wim — это файл, `boot.wim` полученный из исходных файлов Windows для каждой указанной версии Windows.

Развернуть таблицу

Развертываемая версия Windows	Boot.wim из Windows 10	Boot.wim из Windows Server 2016	Boot.wim из Windows Server 2019	Boot.wim из Windows Server 2022	Boot.wim из Windows 11
Windows 11	Не поддерживается, заблокировано.	Не поддерживается, заблокировано.	Не поддерживается, заблокировано.	Не поддерживается, заблокировано.	Не поддерживается, заблокировано.
Windows 10	Поддерживается при использовании образа загрузки соответствующей или более новой версии.	Поддерживается с использованием загрузочного образа из поддерживаемой в настоящее время версии Windows 10.	Поддерживается с использованием загрузочного образа из поддерживаемой в настоящее время версии Windows 10.	Не поддерживается.	Не поддерживается.
Windows Server 2025	Не поддерживается.	Не поддерживается.	Не поддерживается.	Не поддерживается.	Не поддерживается.
Windows Server 2022	Не рекомендуется, с предупреждающим сообщением.	Не рекомендуется, с предупреждающим сообщением.	Не рекомендуется, с предупреждающим сообщением.	Не рекомендуется, с предупреждающим сообщением.	Не поддерживается.

Развертываемая версия Windows	Boot.wim из Windows 10	Boot.wim из Windows Server 2016	Boot.wim из Windows Server 2019	Boot.wim из Windows Server 2022	Boot.wim из Windows 11
Windows Server 2019	Поддерживается с использованием загрузочного образа из поддерживаемой в настоящее время версии Windows 10.	Поддерживается.	Поддерживается.	Не поддерживается.	Не поддерживается.
Windows Server 2016	Поддерживается с использованием загрузочного образа из поддерживаемой в настоящее время версии Windows 10.	Поддерживается.	Не поддерживается.	Не поддерживается.	Не поддерживается.

> ⓘ **Примечание**
>
> При попытке использовать **boot.wim** в WDS под управлением Windows Server 2025 может отобразиться следующее сообщение об ошибке:
>
> `A media driver your computer needs is missing. This could be a DVD, USB or Hard disk driver. If you have a CD, DVD, or USB flash drive with the driver on it, please insert it now.`
>
> Ожидается сообщение об ошибке, так как использование **boot.wim** в WDS под управлением Windows Server 2025 не поддерживается.

Причина изменения

Альтернативы WDS, такие как Microsoft Configuration Manager, обеспечивают более удобный, гибкий и функциональный интерфейс для развертывания образов Windows.

Не влияет

Это изменение не влияет на загрузку PXE WDS. WDS по-прежнему можно использовать для загрузочных устройств PXE с пользовательскими образами загрузки, но **boot.wim** нельзя использовать в качестве образа загрузки и запустить программу установки Windows в режиме WDS.

Программа установки Windows по-прежнему может выполняться из общей сетевой папки. Это изменение не изменяет рабочие процессы, использующие настраиваемый boot.wim, например Microsoft Deployment Toolkit (MDT) или Microsoft Configuration Manager.

Сводка

- Рабочие процессы Windows 11, использующие **boot.wim** с установочного носителя, блокируются. Комплексное развертывание Windows 11 с использованием только WDS невозможно.

- Это изменение не влияет на Windows 10, Windows Server 2019 и предыдущие версии операционной системы.
- Рабочие процессы Windows Server 2022, использующие **boot.wim** с установочного носителя, отображают уведомление о неблокировочном прекращении поддержки. Уведомление может быть отклонено, и в настоящее время рабочий процесс не заблокирован.
- Рабочие процессы Windows Server после Windows Server 2022, использующие **boot.wim** с установочного носителя, заблокированы.

Если WDS используется с **boot.wim** с установочного носителя для комплексного развертывания операционной системы, а версия ОС не поддерживается, не рекомендуется или блокируется, корпорация Майкрософт рекомендует использовать средства развертывания, такие как Microsoft Configuration Manager, или решение сторонних поставщиков, использующее пользовательский образ boot.wim.

Связанное содержимое

- Функции удалены или больше не разрабатываются начиная с Windows Server 2022.
- Настройка загрузочных образов с помощью Configuration Manager.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Windows ADK для сценариев Windows для ИТ-специалистов

Статья • 27.02.2025 • Применяется к: ✅ Windows 11, ✅ Windows 10

Пакет средств оценки и развертывания Windows (Windows ADK) содержит средства, которые ИТ-специалисты могут использовать для развертывания Windows. Обзор новых возможностей в последней версии Windows ADK см. в статье Новые возможности средств ADK. Справочные материалы по ADK см. в разделе Производство компьютеров.

Создание образа Windows с помощью средств командной строки

DISM используется для подключения и обслуживания образов Windows.

Ниже приведены некоторые действия, которые можно выполнить с помощью DISM:

- Подключение образа в автономном режиме.
- Добавление и удаление пакетов драйверов в автономный образ Windows.
- Включение или отключение компонентов Windows с помощью DISM.
- Добавление или удаление пакетов в автономном режиме с помощью DISM.
- Добавление языков в образы Windows.
- Предварительная установка приложений с помощью DISM.
- Измените образ Windows на более высокий выпуск с помощью DISM.

Sysprep подготавливает установку Windows к созданию образов и позволяет записывать настраиваемую установку Windows.

Ниже приведены некоторые действия, которые можно выполнить с помощью Sysprep:

- Обобщение установки Windows.
- Настройте профиль пользователя по умолчанию с помощью CopyProfile.
- Используйте файлы ответов.

Windows PE (WinPE) — это небольшая операционная система, используемая для загрузки компьютера без операционной системы. Windows PE можно загрузить для установки новой операционной системы, восстановления данных или восстановления существующей операционной системы.

Образ WinPE можно создать с помощью статьи Создание загрузочного носителя Windows PE. Типы загрузочных носителей:

- Создайте загрузочный USB-накопитель Windows PE.
- Создайте winPE ISO, DVD-диск или компакт-диск.
- Создайте VHD среды предустановки Windows для использования с Hyper-V.

Среда восстановления Windows (Windows RE) — среда восстановления, которая может исправить распространенные проблемы в работе операционной системы.

Ниже приведены некоторые действия, которые можно выполнить с помощью Windows RE.

- Настройка Windows RE.
- Сброс нажатия кнопки.

Диспетчер системных образов Windows (WSIM) помогает создавать файлы ответов, которые изменяют параметры Windows и выполняют скрипты во время установки Windows.

Ниже приведены некоторые действия, которые можно выполнить с помощью WSIM.

- Создайте или откройте файл ответов.
- Добавьте путь к драйверу устройства в файл ответов.
- Добавьте пакет в файл ответов.
- Добавьте пользовательскую команду в файл ответов.

Список параметров, которые можно изменить, см. в справочнике по автоматической установке Windows.

Создание пакета подготовки с помощью Windows ICD

Designer образов и конфигурации Windows (ICD) упрощает настройку и подготовку образа Windows для настольных компьютеров (домашняя, pro, корпоративная и для образовательных учреждений) или образа Windows IoT Core (IoT Core). Создание, применение и экспорт пакетов подготовки с помощью Windows ICD рассматривается в статье Создание пакета подготовки.

Средства развертывания Windows для ИТ-специалистов

В Windows ADK также есть несколько средств, относящихся к ИТ-специалистам:

- Технический справочник по средство управления активацией корпоративных лицензий (VAMT)
- Технический справочник по средству миграции пользовательской среды (USMT)

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Общие сведения о средстве миграции пользовательской среды (USMT)

Применяется к: ✅ Windows 11, ✅ Windows 10

Средство миграции пользовательской среды (USMT) можно использовать для оптимизации и упрощения миграции пользовательской среды во время крупных развертываний операционных систем Windows. USMT записывает учетные записи пользователей, файлы пользователей, параметры операционной системы и параметры приложений, а затем переносит их в новую установку Windows. USMT можно использовать как для замены компьютера, так и для миграции обновления компьютера. Дополнительные сведения см. в разделе Общие сценарии миграции.

USMT позволяет выполнять следующие действия:

- Настройте миграцию в соответствии с бизнес-потребностями организации, используя файлы правила миграции (.xml), чтобы точно контролировать, какие файлы и параметры переносятся и как они переносятся. Дополнительные сведения об изменении этих файлов см. в справочнике по XML-файлам USMT.

- Настройте миграцию в автоматизированный процесс развертывания с помощью средств **ScanState** и **LoadState** , которые управляют сбором и восстановлением пользовательских файлов и параметров. Дополнительные сведения см. в разделе Синтаксис командной строки средства миграции пользовательской среды (USMT).

- Выполнение автономной миграции. Миграцию можно выполнить в автономном режиме с помощью команды **ScanState** в среде предустановки Windows (WinPE) или миграцию можно выполнить из предыдущих установок Windows, содержащихся в каталогах **Windows.old** . Дополнительные сведения о типах миграции см . в разделах Выбор типа хранилища миграции и Справочник по автономной миграции.

Преимущества

USMT предоставляет следующие преимущества компаниям, которые развертывают операционные системы Windows:

- Безопасно переносит учетные записи пользователей, параметры операционной системы и приложений.
- Снижает затраты на развертывание Windows за счет сохранения состояния пользователя.
- Сокращает время простоя конечных пользователей, необходимое для настройки рабочих столов и поиска отсутствующих файлов.

- Сокращает количество обращений в службу поддержки.
- Сокращает время, необходимое пользователю для ознакомления с новой операционной системой.
- Повышает удовлетворенность сотрудников процессом миграции.

Ограничения

USMT предназначен для администраторов, выполняющих крупномасштабные автоматизированные развертывания. Если переносятся пользовательские состояния только нескольких компьютеров, можно использовать PCmover Express . PCmover не является бесплатной служебной программой. PCmover Express — это средство, созданное партнером Корпорации Майкрософт Laplink.

В некоторых сценариях использование USMT не рекомендуется. К этим сценариям относятся:

- Миграции, требующие взаимодействия с конечным пользователем.
- Миграции, требующие настройки на основе каждого компьютера.

Скачивание и установка USMT

USMT входит в комплект средств оценки и развертывания Windows (Windows ADK), его можно скачать по следующей ссылке:

Скачивание и установка Windows ADK

После загрузки установщика Windows ADK запустите установщик, а затем на странице **Выберите компоненты, которые требуется установить**, убедитесь, что выбран **параметр Средство миграции пользовательской среды (USMT).**

Связанные статьи

- Технический справочник по средству миграции пользовательской среды (USMT).

Last updated on 28.03.2025

Начало работы со средством миграции пользовательской среды (USMT)

Применяется к: ✅ Windows 11, ✅ Windows 10

В этой статье описывается общий процесс переноса файлов и параметров.

Шаг 1. Скачивание и установка USMT

USMT входит в комплект средств оценки и развертывания Windows (Windows ADK), его можно скачать по следующей ссылке:

Скачивание и установка Windows ADK

После загрузки установщика Windows ADK запустите установщик, а затем на странице **Выберите компоненты, которые требуется установить**, убедитесь, что выбран **параметр Средство миграции пользовательской среды (USMT).**

Шаг 2. Планирование миграции

1. Планирование миграции. В зависимости от того, обновляется ли сценарий миграции или заменяет компьютеры, можно выбрать миграцию по сети или автономную миграцию. Для автономной миграции можно использовать среду предварительной установки Windows (WinPE) или файлы в каталоге **Windows.old** . Дополнительные сведения см. в разделе Общие сценарии миграции.

2. Определите, что следует перенести. Данные для переноса включают сведения о пользователе, параметры приложений, параметры операционной системы, файлы, папки и разделы реестра.

3. Определение места хранения данных. В зависимости от размера хранилища миграции данные могут храниться в одном из следующих расположений:

   - Отдалённо.
   - Локально в хранилище миграции с жесткой компоновкой или на локальном внешнем запоминающем устройстве.
   - Непосредственно на конечном компьютере.

   Дополнительные сведения см. в разделе Выбор типа хранилища миграции.

4. Используйте параметр командной `/GenMigXML` строки, чтобы определить, какие файлы включены в миграцию, и определить, необходимы ли какие-либо изменения.

Дополнительные сведения см. в разделе Синтаксис ScanState.

5. При необходимости измените `Migration.xml` копии файлов и и `MigDocs.xml` создайте пользовательские **файлы.xml** . Чтобы изменить поведение миграции, например перенос папки **"Документы"** , а не папку **"Музыка"** , можно создать пользовательский **файл.xml** или изменить правила в существующих **файлах.xml** миграции. Средство поиска документов или `MigXmlHelper.GenerateDocPatterns` вспомогатель можно использовать для автоматического поиска документов пользователей на компьютере без создания обширной пользовательской **миграции.xml** файлов.

   > ⓘ **Внимание**
   >
   > Корпорация Майкрософт рекомендует всегда создавать копии **файлов.xml** , включенных в средство миграции пользовательской среды (USMT), а затем изменять копии. Никогда не изменяйте исходные **файлы.xml** .

   Файл `MigXML.xsd` можно использовать для записи и проверки **файлов.xml** . Дополнительные сведения об изменении этих файлов см. в справочнике по XML-файлам USMT.

6. Создайте файлConfig.xml , чтобы исключить какие-либо компоненты из миграции. Чтобы создать этот файл, выполните `ScanState.exe` команду со следующими параметрами:

   - /genconfig.
   - /i — в качестве аргументов указываются **.xml** файлы, используемые с `ScanState.exe`.

   Например, следующая команда создает `Config.xml` файл с помощью `MigDocs.xml` файлов и `MigApp.xml` :

   Командная строка Windows

   ```
   ScanState.exe /genconfig:Config.xml /i:MigDocs.xml /i:MigApp.xml /v:13
   /l:ScanState.log
   ```

7. Откройте объект , `Config.xml` созданный на предыдущем шаге. Проверьте состояние миграции каждого из компонентов, перечисленных в `Config.xml` файле. При необходимости измените `Config.xml` файл и укажите `migrate=no` для всех компонентов, которые не нужно переносить.

Шаг 3. Сбор файлов и параметров с исходного компьютера

1. Создайте резервную копию исходного компьютера.

2. Закройте все приложения. Если некоторые приложения выполняются при выполнении `ScanState.exe` команды, USMT может не переносить все указанные данные. Например, если Microsoft Office Outlook открыт, USMT может не переносить PST-файлы.

   > ⓘ **Примечание.**
   >
   > UsMT завершается ошибкой, если не удается перенести файл или параметр, если `/c` не указан параметр. При указании `/c` параметра USMT игнорирует ошибки и регистрирует ошибку при каждом обнаружении файла, который используется для миграции USMT. Раздел `<ErrorControl>` в `Config.xml` файле можно использовать, чтобы указать, какие ошибки следует игнорировать, а какие должны привести к сбою миграции.

3. Чтобы собрать файлы и параметры, выполните `ScanState.exe` команду на исходном компьютере. Необходимо указать все **.xml** файлы, которые `ScanState.exe` необходимо использовать команде. Например:

   Командная строка Windows

   ```
   ScanState.exe \\server\migration\mystore /config:Config.xml /i:MigDocs.xml
   /i:MigApp.xml /v:13 /l:ScanState.log
   ```

   > ⓘ **Примечание.**
   >
   > Команда `ScanState.exe` должна выполняться в режиме **администратора** на исходном компьютере. Чтобы запустить в режиме **администратора** , щелкните правой кнопкой мыши **командную строку** и выберите **запуск от имени администратора**. Дополнительные сведения о том, как `ScanState.exe` команда обрабатывает и сохраняет данные, см. в разделе Как работает USMT.

4. Чтобы убедиться, что созданное хранилище не повреждено, выполните `UsmtUtils.exe` команду с параметром `/Verify` .

Шаг 4. Подготовка целевого компьютера и восстановление файлов и параметров

1. Установите операционную систему на целевом компьютере.

2. Установите все приложения, которые находились на исходном компьютере. Хотя это не всегда обязательно, корпорация Майкрософт рекомендует установить все приложения на целевом компьютере перед восстановлением пользовательского состояния. Установка всех приложений перед восстановлением пользовательского состояния гарантирует сохранение перенесенных параметров.

   > ⓘ **Примечание.**
   >
   > Версия приложения, установленная на конечном компьютере, должна совпадать с версией на исходном компьютере. USMT не поддерживает перенос параметров для более старой версии приложения на более новую версию. Исключением для этого правила является Microsoft Office. USMT может перейти с более старой версии Microsoft Office на более новую версию Microsoft Office.

3. Закройте все приложения. Если некоторые приложения выполняются при выполнении `LoadState.exe` команды, USMT может переносить не все указанные данные. Например, если Microsoft Office Outlook открыт, USMT может не переносить PST-файлы.

   > ⓘ **Примечание.**
   >
   > Используйте `/c` для продолжения миграции при обнаружении ошибок. `<ErrorControl>` Используйте раздел в файле, `Config.xml` чтобы указать, какие ошибки следует игнорировать, а какие ошибки должны привести к сбою миграции.

4. `LoadState.exe` Выполните команду на конечном компьютере. Укажите тот же набор **.xml** файлов, которые были указаны при `ScanState.exe` использовании команды. Однако `Config.xml` не всегда требуется указывать файл. Этот `Config.xml` файл необходимо указать только для исключения некоторых файлов и параметров, перенесенных в хранилище. Например, папка **Documents** была перенесена в хранилище, но ее не нужно переносить на конечный компьютер. Например, измените `Config.xml` файл и укажите обновленный файл с помощью `LoadState.exe` команды . `LoadState.exe` Затем команда переносит только файлы и параметры,

которые необходимо перенести. Дополнительные сведения о том, как `LoadState.exe` команда обрабатывает и переносит данные, см. в разделе Как работает USMT.

Например, следующая команда переносит файлы и параметры:

Командная строка Windows

```
LoadState.exe  \\server\migration\mystore /config:Config.xml /i:MigDocs.xml
/i:MigApp.xml /v:13 /l:LoadState.log
```

> ⓘ **Примечание.**
>
> `LoadState.exe` Выполните команду в режиме администратора. Для этого щелкните правой кнопкой мыши **командную строку** и выберите **запуск от имени администратора**.

5. Выйдите из нее `LoadState.exe` после выполнения команды. Некоторые параметры, такие как шрифты, обои и параметры заставки, не вступают в силу до следующего входа пользователя.

Last updated on 27.03.2025

Исключение файлов и параметров

Статья • 29.01.2025 • Применяется к: ✅ Windows 11, ✅ Windows 10

При **указании.xml** файлов `MigApp.xml` миграции , `MigDocs.xml` и `MigUser.xml` средство миграции пользовательской среды (USMT) переносит перечисленные параметры и компоненты, как описано в разделе Что такое миграция USMT? Можно создать пользовательский **файл.xml** , чтобы указать, что следует включить или исключить при миграции. Кроме того, можно создать файл, `Config.xml` чтобы исключить весь компонент из миграции. Тем не менее, пользователи не могут быть исключены с помощью **.xml** файлов миграции `Config.xml` или файла. Единственный способ указать, какие пользователи следует включать и исключать, — использовать параметры пользователя в командной **строке средства ScanState** . Дополнительные сведения см. в разделе Параметры пользователя статьи о синтаксисе ScanState .

Методы настройки миграции, включения и исключения файлов и параметров:

- Создайте пользовательский файл .xml. Чтобы указать, что следует исключить, можно использовать следующие элементы:
  - Включить и исключить. Элементы **<include>** и **<exclude>** можно использовать для исключения объектов с условиями. Например, можно перенести все файлы, расположенные на `C:\` диске, кроме любых `.mp3` файлов. Важно помнить, что к этим элементам применяются конфликты и приоритет .
  - unconditionalExclude: **<элемент unconditionalExclude>** можно использовать для глобального исключения данных. Этот элемент имеет приоритет над всеми остальными правилами включения и исключения в **файлах.xml** . Таким образом, этот элемент исключает объекты независимо от других **<правил включения>** , которые находятся в **файлах.xml** . Например, все **.mp3** файлы можно исключить на компьютере или исключить все файлы из C:\UserData.
- Создание файла Config.xml. Файл `Config.xml` можно создать и изменить, чтобы исключить весь компонент из миграции. Например, этот файл можно использовать для исключения параметров для одного из приложений по умолчанию. Кроме того, создание и изменение `Config.xml` файла — единственный способ исключить параметры операционной системы, перенесенные на компьютеры под управлением Windows. Исключить

компоненты, использующие этот файл, проще, чем изменять файлы **миграции.xml** , так как знание правил и синтаксиса миграции не требуется.

Создание пользовательского файла .xml

Корпорация Майкрософт рекомендует создавать пользовательский **файл.xml** вместо изменения **.xmlфайлов** миграции по умолчанию. При использовании пользовательского **файла.xml** изменения можно хранить отдельно от **файла.xml** по умолчанию, что упрощает отслеживание изменений.

<включение> и <исключение>

Файлы **.xml** миграции , `MigApp.xml` `MigDocs.xml` и `MigUser.xml` содержат **<элемент компонента>**, который обычно представляет автономный компонент или приложение, например Microsoft Office Outlook и Word. Чтобы исключить файлы и параметры реестра, связанные с этими компонентами, используйте **<элементы include>** и **<exclude>** . Например, эти элементы можно использовать для переноса всех файлов и параметров с шаблоном X, за исключением файлов и параметров с шаблоном Y, где Y является более конкретным, чем X. Синтаксис этих элементов см. в справочнике по XML USMT.

> ⓘ **Примечание**
>
> Если указано правило **исключения>, всегда указывайте соответствующее правило включения.<<>** В противном случае, если **<правило включения>** не указано, конкретные файлы или параметры не включаются. Они уже исключены из миграции. Таким образом, несопровождаемое **<правило исключения>** не требуется.

- Пример 1. Перенос всех файлов из C:\ за исключением .mp3 файлов
- Пример 2. Перенос всех файлов, расположенных в C:\Data, кроме файлов в C:\Data\tmp
- Пример 3. Как исключить файлы из папки, но включить все вложенные папки
- Пример 4. Исключение файла из определенной папки
- Пример 5. Как исключить файл из любого расположения

Пример 1. Перенос всех файлов, `C:\` кроме `.mp3` файлов

Следующий **.xml** файл переносит все файлы, расположенные на диске C:, за исключением **файлов.mp3** .

XML

```
<migration
urlid="http://www.microsoft.com/migration/1.0/migxmlext/mp3files">
    <!-- This component migrates all files except those with .mp3 extension-
->
    <component type="Documents" context="UserAndSystem">
        <displayName _locID="miguser.sharedvideo">MP3 Files</displayName>
        <role role="Data">
            <rules>
                <include filter='MigXmlHelper.IgnoreIrrelevantLinks()'>
                    <objectSet>
                        <pattern type="File">C:\* [*]</pattern>
                    </objectSet>
                </include>
                <exclude>
                    <objectSet>
                        <pattern type="File">C:\* [*.mp3]</pattern>
                    </objectSet>
                </exclude>
            </rules>
        </role>
    </component>
</migration>
```

Пример 2. Перенос всех файлов, расположенных в `C:\Data` , кроме файлов в `C:\Data\tmp`

Следующий **.xml** файл переносит все файлы и вложенные папки в `C:\Data`, за исключением файлов и вложенных папок в `C:\Data\tmp`.

XML

```
<migration urlid="http://www.microsoft.com/migration/1.0/migxmlext/test">
    <component type="Documents" context="System">
        <displayName _locID="miguser.sharedvideo">Test
component</displayName>
        <role role="Data">
            <rules>
                <include>
                    <objectSet>
                        <pattern type="File">C:\Data\* [*]</pattern>
```

```
                    </objectSet>
                </include>
                <exclude>
                    <objectSet>
                        <pattern type="File"> C:\Data\temp\* [*]</pattern>
                    </objectSet>
                </exclude>
            </rules>
        </role>
    </component>
</migration>
```

Пример 3. Как исключить файлы из папки, но включить все вложенные папки

Следующий **.xml** файл переносит все вложенные папки в `C:\EngineeringDrafts`, но исключает все файлы, которые находятся в `C:\EngineeringDrafts`.

XML

```
<migration urlid="http://www.microsoft.com/migration/1.0/migxmlext/test">
    <component type="Documents" context="System">
        <displayName>Component to migrate all Engineering Drafts Documents
without subfolders</displayName>
        <role role="Data">
            <rules>
                <include>
                    <objectSet>
                        <pattern type="File"> C:\EngineeringDrafts\* [*]
</pattern>
                    </objectSet>
                </include>
                <exclude>
                    <objectSet>
                        <pattern type="File"> C:\EngineeringDrafts\ [*]
</pattern>
                    </objectSet>
                </exclude>
            </rules>
        </role>
    </component>
</migration>
```

Пример 4. Исключение файла из определенной папки

Следующий **.xml** файл переносит все файлы и вложенные папки в `C:\EngineeringDrafts`, за исключением `Sample.doc` файла в `C:\EngineeringDrafts`.

XML

```
<migration urlid="http://www.microsoft.com/migration/1.0/migxmlext/test">
    <component type="Documents" context="System">
        <displayName>Component to migrate all Engineering Drafts Documents
except Sample.doc</displayName>
        <role role="Data">
            <rules>
                <include>
                    <objectSet>
                        <pattern type="File"> C:\EngineeringDrafts\* [*]
</pattern>
                    </objectSet>
                </include>
                <exclude>
                    <objectSet>
                        <pattern type="File"> C:\EngineeringDrafts\
[Sample.doc]</pattern>
                    </objectSet>
                </exclude>
            </rules>
        </role>
    </component>
</migration>
```

Пример 5. Как исключить файл из любого расположения

Чтобы исключить файл Sample.doc из любого расположения на диске C:, используйте **<элемент pattern>** . Если на диске C: существует несколько файлов с одинаковыми именами, все эти файлы будут исключены.

XML

```
<pattern type="File"> C:\* [Sample.doc] </pattern>
```

Чтобы исключить файл Sample.doc с любого диска на компьютере, используйте **<элемент script>** . Если существует несколько файлов с одинаковыми именами, все эти файлы исключаются.

XML

```
<script>MigXmlHelper.GenerateDrivePatterns("* [sample.doc]", "Fixed")
</script>
```

Примеры использования XML для исключения файлов, папок и разделов реестра

Ниже приведены некоторые примеры использования XML для исключения файлов, папок и разделов реестра. Дополнительные сведения см. в справочнике по XML USMT.

Пример 1. Исключение всех `.mp3` файлов

Следующий **файл.xml** исключает все `.mp3` файлы из миграции:

XML

```
<migration
urlid="http://www.microsoft.com/migration/1.0/migxmlext/excludefiles">
    <component context="System" type="Documents">
        <displayName>Test</displayName>
        <role role="Data">
            <rules>
                <unconditionalExclude>
                    <objectSet>
                        <script>MigXmlHelper.GenerateDrivePatterns ("*
[*.mp3]", "Fixed")</script>
                    </objectSet>
                </unconditionalExclude>
            </rules>
        </role>
    </component>
</migration>
```

Пример 2. Исключение всех файлов на определенном диске

Следующий **файл.xml** исключает только файлы, расположенные на диске C: .

XML

```
<migration
urlid="http://www.microsoft.com/migration/1.0/migxmlext/allfiles">
    <component type="Documents" context="System">
        <displayName>Test</displayName>
        <role role="Data">
            <rules>
                <unconditionalExclude>
                    <objectSet>
                        <pattern type="File">c:\*[*]</pattern>
                    </objectSet>
                </unconditionalExclude>
            </rules>
```

```
        </role>
    </component>
</migration>
```

Пример 3. Исключение разделов реестра

Следующий **.xml** файл безоговорочно исключает `HKEY_CURRENT_USER` раздел реестра и все его подразделы.

XML

```
<?xml version="1.0" encoding="UTF-8"?>
<migration urlid="http://www.microsoft.com/migration/1.0/migxmlext/miguser">
    <component type="Documents" context="User">
        <displayName>Test</displayName>
        <role role="Data">
            <rules>
                <include>
                    <objectSet>
                        <pattern type="Registry">HKCU\testReg[*]</pattern>
                    </objectSet>
                </include>
                <unconditionalExclude>
                    <objectSet>
                        <pattern type="Registry">HKCU\*[*]</pattern>
                    </objectSet>
                </unconditionalExclude>
            </rules>
        </role>
    </component>
</migration>
```

Пример 4. Как исключить `C:\Windows` и `C:\Program Files`

В следующем **.xml** файле безоговорочно исключаются системные папки `C:\Windows` и `C:\Program Files`. Все `*.docx` файлы и `*.ppt` `*.xls` не переносятся, так как **<элемент unconditionalExclude>** имеет приоритет над элементом **<include>**.

XML

```
<?xml version="1.0" encoding="UTF-8"?>
<migration urlid="http://www.microsoft.com/migration/1.0/migxmlext/miguser">
    <component type="Documents" context="System">
        <displayName>Test</displayName>
        <role role="Data">
            <rules>
                <include>
                    <objectSet>
```

```
                        <script>MigXmlHelper.GenerateDrivePatterns ("*
[*.doc]", "Fixed")</script>
                        <script>MigXmlHelper.GenerateDrivePatterns ("*
[*.xls]", "Fixed")</script>
                        <script>MigXmlHelper.GenerateDrivePatterns ("*
[*.ppt]", "Fixed")</script>
                    </objectSet>
                </include>
                <unconditionalExclude>
                    <objectSet>
                        <pattern type="File">C:\Program Files\* [*]
</pattern>
                        <pattern type="File">C:\Windows\* [*]</pattern>
                    </objectSet>
                </unconditionalExclude>
            </rules>
        </role>
    </component>
</migration>
```

Создание XML-файла конфигурации

Файл `Config.xml` можно создать и изменить, чтобы исключить компоненты из миграции. Исключить компоненты, использующие этот файл, проще, чем изменять файлы **миграции.xml** , так как знание правил и синтаксиса миграции не требуется. `Config.xml` — это необязательный файл, который можно создать с помощью `/genconfig` параметра командной строки с помощью средства **ScanState** . Например, файл `Config.xml` можно использовать для исключения параметров для одного из приложений по умолчанию. Кроме того, создание и изменение этого файла — единственный способ исключить параметры операционной системы, перенесенные на компьютеры под управлением Windows.

- **Чтобы исключить параметры для приложения по умолчанию, выполните следующие действия.** Укажите `migrate="no"` для приложения в **<разделе Приложения> файла**.`Config.xml`

- **Чтобы исключить параметр операционной системы, выполните следующие действия:** Укажите `migrate="no"` параметр **<в разделе WindowsComponents>** .

- **Чтобы исключить папку Documents, выполните следующие действия:** Укажите `migrate="no"` папку **Документы** в **<разделе Документы>** . Все **<правила включения>** в **файлах.xml** по-прежнему применяются. Например, если существует правило, включающее все **.docx** файлы в папке **Документы** , **.docx** файлы по-прежнему переносятся. Однако все дополнительные файлы, которые не **.docx** , не переносятся.

Дополнительные сведения см. в разделе файлConfig.xml.

> **Примечание**
>
> Чтобы исключить компонент из `Config.xml` файла, задайте для **параметра миграции** значение **"нет".** Удаление XML-тега компонента из `Config.xml` файла не исключает компонент из миграции.

Связанные статьи

- Настройка XML-файлов USMT.
- Справочник по XML-файлу USMT.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Извлечение файлов из сжатого хранилища миграции USMT

Статья • 29.01.2025 • Применяется к: ✅ Windows 11, ✅ Windows 10

При переносе файлов и параметров во время обычной миграции с обновлением компьютера в промежуточном хранилище обычно создается сжатый файл хранилища миграции. Это хранилище миграции представляет собой один файл образа, содержащий все переносимые файлы, а также файл каталога. Чтобы защитить сжатый файл, его можно зашифровать с помощью различных алгоритмов шифрования. При переносе файла обратно на исходный компьютер после установки операционной системы можно выполнить команду **UsmtUtils** с параметром `/extract` для восстановления файлов из сжатого хранилища миграции. Команду **UsmtUtils** с параметром `/extract` также можно использовать в любой момент, когда данные необходимо восстановить из хранилища миграции.

Параметры, используемые с параметром , `/extract` могут указывать:

- Алгоритм шифрования, который использовался для создания хранилища миграции.
- Ключ шифрования или текстовый файл, содержащий ключ шифрования.
- Включение и исключение шаблонов для выборочного извлечения данных.

Кроме того, шаблоны файлов, которые необходимо извлечь, можно указать с помощью `/i` параметра для включения шаблонов файлов или `/e` параметра исключения шаблонов файлов. `/i` Если и параметр, и `/e` параметр используются в одной команде, шаблоны включения имеют приоритет над шаблонами исключения. Параметры `/i` и `/e` отличаются от правил включения и исключения, используемых в средствах **ScanState** и **LoadState** .

Запуск средства UsmtUtils с параметром /extract

Чтобы извлечь файлы из сжатого хранилища миграции на целевой компьютер, используйте следующий синтаксис UsmtUtils:

Командная строка Windows

```
UsmtUtils.exe /extract <filePath> <destinationPath> [/i:<includePattern>]
[/e:<excludePattern>] [/l:<logfile>] [/decrypt[:<AlgID>] {/key:<keystring> |
/keyfile:<filename>}] [/o]
```

Где заполнители имеют следующие значения:

- **<USMTpath>** — это расположение, в котором сохраняются файлы и средства USMT.
- **<FilePath>** — это расположение хранилища миграции.
- **<Путь назначения>** — это расположение файла, в котором параметр **/extract** должен помещать содержимое извлеченного хранилища миграции.
- **<includePattern>** задает шаблон для файлов, которые будут включены в извлечение.
- **<excludePattern>** задает шаблон для файлов, которые следует исключить из извлечения.
- **<AlgID>** — это алгоритм шифрования, который использовался для создания хранилища миграции в командной строке `ScanState.exe` .
- **<logfile>** — это расположение и имя файла журнала.
- **<keystring>** — это ключ шифрования, который использовался для шифрования хранилища миграции.
- **<filename>** — это расположение и имя текстового файла, содержащего ключ шифрования.

Извлечение всех файлов из сжатого хранилища миграции

Чтобы извлечь все данные из сжатого хранилища миграции в файл на `C:\` диске, введите:

Командная строка Windows

```
UsmtUtils.exe /extract D:\MyMigrationStore\USMT\store.mig C:\ExtractedStore
```

Извлечение файлов определенных типов из зашифрованного сжатого хранилища миграции

Чтобы извлечь определенные файлы, такие как `.txt` и `.pdf` файлы, из зашифрованного сжатого хранилища миграции, введите:

Командная строка Windows

```
UsmtUtils.exe /extract D:\MyMigrationStore\USMT\store.mig /i:"*.txt,*.pdf"
C:\ExtractedStore /decrypt /keyfile:D:\encryptionKey.txt
```

В этом примере файл зашифрован, а ключ шифрования находится в текстовом файле encryptionKey.

Извлечение всех типов файлов, кроме одного или нескольких типов из зашифрованного сжатого хранилища миграции

Чтобы извлечь все файлы, кроме одного типа, например `.exe` файлов, из зашифрованного сжатого хранилища миграции, введите:

Командная строка Windows

```
UsmtUtils.exe /extract D:\MyMigrationStore\USMT\store.mig /e:*.exe
C:\ExtractedStore /decrypt:AES_128 /key:password /l:C:\usmtutilslog.txt
```

Извлечение типов файлов с помощью шаблона включения и шаблона исключения

При извлечении файлов из сжатого хранилища миграции можно одновременно использовать шаблоны включения и исключения. Файлы одного типа можно исключить, а файлы другого типа можно включить. Пример:

Командная строка Windows

```
UsmtUtils.exe /extract D:\MyMigrationStore\USMT\store.mig /i:myProject.*
/e:*.exe C:\ExtractedStore /o
```

В этом примере, если файл **myProject.exe** , он также извлекается, так как параметр включить шаблон имеет приоритет над параметром шаблона исключения.

Связанные статьи

- Синтаксис UsmtUtils.

- Коды возврата.
- Проверьте состояние сжатого хранилища миграции.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Включение файлов и параметров

Статья • 29.01.2025 • Применяется к: ✅ Windows 11, ✅ Windows 10

При указании файлов **.xml** миграции средство миграции пользовательской среды (USMT) переносит параметры и компоненты, указанные в разделе Что такое миграция USMT?. Чтобы включить дополнительные файлы и параметры, корпорация Майкрософт рекомендует создать пользовательский **файл.xml** , а затем включить этот файл при использовании `ScanState.exe` команд и `LoadState.exe` .

Создание пользовательского **файла.xml** позволяет хранить изменения отдельно от **файлов.xml** по умолчанию. Создание пользовательского **файла.xml** упрощает отслеживание изменений.

Перенос одного раздела реестра

Следующий **файл.xml** переносит один раздел реестра.

XML

```
<migration urlid="http://www.microsoft.com/migration/1.0/migxmlext/test">
     <component type="Application" context="System">
          <displayName>Component to migrate only registry value
string</displayName>
          <role role="Settings">
          <rules>
               <include>
                    <objectSet>
                         <pattern
type="Registry">HKLM\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\Cache [Persistent]</pattern>
                    </objectSet>
               </include>
          </rules>
          </role>
     </component>
</migration>
```

Перенос определенной папки

В следующих примерах показано, как перенести папку с определенного диска и из любого расположения на компьютере.

Перенос папки с определенного диска

- **Включая вложенные папки.** Следующий **.xml** файл переносит все файлы и вложенные папки из `C:\EngineeringDrafts` на конечный компьютер.

```
XML

<migration
urlid="http://www.microsoft.com/migration/1.0/migxmlext/test">
<component type="Documents" context="System">
  <displayName>Component to migrate all Engineering Drafts Documents
including subfolders</displayName>
  <role role="Data">
    <rules>
      <include>
        <objectSet>
          <pattern type="File">C:\EngineeringDrafts\* [*]</pattern>
        </objectSet>
      </include>
    </rules>
  </role>
</component>
</migration>
```

- **Исключение вложенных папок.** Следующий **.xml** файл переносит все файлы из `C:\EngineeringDrafts`, но не переносит вложенные папки в .`C:\EngineeringDrafts`

```
XML

<migration
urlid="http://www.microsoft.com/migration/1.0/migxmlext/test">
<component type="Documents" context="System">
  <displayName>Component to migrate all Engineering Drafts Documents
without subfolders</displayName>
  <role role="Data">
    <rules>
      <include>
        <objectSet>
          <pattern type="File"> C:\EngineeringDrafts\ [*]</pattern>
        </objectSet>
      </include>
    </rules>
  </role>
</component>
</migration>
```

Перенос папки из любого расположения

Следующий **.xml** файл переносит все файлы и вложенные `EngineeringDrafts` папки папки с любого диска на компьютере. Если существует несколько папок с одинаковым именем, переносятся все файлы с этим именем.

XML

```
<migration urlid="http://www.microsoft.com/migration/1.0/migxmlext/test">
<component type="Documents" context="System">
  <displayName>Component to migrate all Engineering Drafts Documents folder
on any drive on the computer </displayName>
  <role role="Data">
    <rules>
         <include>
            <objectSet>
         <script>MigXmlHelper.GenerateDrivePatterns ("\EngineeringDrafts\*
[*] ", "Fixed")</script>
         <script>MigXmlHelper.GenerateDrivePatterns ("*\EngineeringDrafts\*
[*] ", "Fixed")</script>
       </objectSet>
          </include>
    </rules>
  </role>
</component>
</migration>
```

Следующий **.xml** файл переносит все файлы и вложенные `EngineeringDrafts` папки папки из любого расположения на `C:\` диске. Если существует несколько папок с одинаковыми именами, все они переносятся.

XML

```
<migration urlid="http://www.microsoft.com/migration/1.0/migxmlext/test">
<component type="Documents" context="System">
  <displayName>Component to migrate all Engineering Drafts Documents
EngineeringDrafts folder from where ever it exists on the C: drive
</displayName>
  <role role="Data">
    <rules>
         <include>
            <objectSet>
<pattern type="File"> C:\*\EngineeringDrafts\* [*]</pattern>
<pattern type="File"> C:\EngineeringDrafts\* [*]</pattern>
       </objectSet>
          </include>
    </rules>
  </role>
</component>
</migration>
```

Перенос типа файла в определенную папку

Следующий **файл.xml** переносит файлы, расположенные на указанных `.mp3` дисках исходного компьютера, в папку `C:\Music` на конечном компьютере.

XML

```
<migration urlid="http://www.microsoft.com/migration/1.0/migxmlext/test">
<component type="Documents" context="System">
  <displayName>All .mp3 files to the Documents folder</displayName>
  <role role="Data">
    <rules>
      <include>
        <objectSet>
          <script>MigXmlHelper.GenerateDrivePatterns ("* [*.mp3]", "Fixed")
</script>
        </objectSet>
      </include>
      <!-- Migrates all the .mp3 files in the store to the C:\Music folder
during LoadState -->
      <locationModify script="MigXmlHelper.Move('C:\Music')">
        <objectSet>
          <script>MigXmlHelper.GenerateDrivePatterns ("* [*.mp3]", "Fixed")
</script>
        </objectSet>
      </locationModify>
    </rules>
  </role>
</component>
</migration>
```

Перенос определенного файла

В следующих примерах показано, как перенести файл из определенной папки и как перенести файл из любого расположения.

- **Перенос файла из папки.** Следующий **файл.xml** переносит только `Sample.doc` файл с `C:\EngineeringDrafts` исходного компьютера на конечный компьютер.

  XML

  ```
  <migration
  urlid="http://www.microsoft.com/migration/1.0/migxmlext/test">
  <component type="Documents" context="System">
    <displayName>Component to migrate all Engineering Drafts
  Documents</displayName>
    <role role="Data">
      <rules>
  ```

```
      <include>
        <objectSet>
          <pattern type="File"> C:\EngineeringDrafts\ [Sample.doc]
</pattern>
        </objectSet>
      </include>
    </rules>
  </role>
</component>
</migration>
```

- **Перенос файла из любого расположения.** Чтобы перенести `Sample.doc` файл из любого расположения на `C:\` диске, используйте **<элемент pattern>** , как показано в следующем примере. Если на `C:\` диске существует несколько файлов с одинаковыми именами, переносятся все файлы с этим именем.

  XML

  ```
  <pattern type="File"> C:\* [Sample.doc] </pattern>
  ```

  Чтобы перенести файл Sample.doc с любого диска на компьютере, используйте <скрипт> , как показано в следующем примере. Если существует несколько файлов с одинаковыми именами, все файлы с этим именем переносятся.

  XML

  ```
  <script>MigXmlHelper.GenerateDrivePatterns("* [sample.doc]", "Fixed")
  </script>
  ```

Связанные статьи

- Настройка XML-файлов USMT.
- Пользовательские примеры XML.
- Конфликты и приоритет.
- Справочник по XML-файлу USMT.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Перенос параметров приложений

Статья • 29.01.2025 • Применяется к: ✅ Windows 11, ✅ Windows 10

Можно создать пользовательский **файл.xml** для переноса определенных параметров бизнес-приложения или для изменения поведения миграции по умолчанию средства миграции пользовательской среды (USMT). Чтобы использовать этот файл **в ScanState** и **LoadState** , в обеих командных строках должен быть указан пользовательский **файл.xml** .

В этой статье описывается, как создать пользовательский **файл.xml** миграции, который переносит параметры приложения, которое не переносится по умолчанию с помощью `MigApp.xml`. Параметры следует перенести после установки приложения, но до того, как пользователь запустит приложение в первый раз.

В этой статье не содержатся сведения о переносе приложений, которые хранят параметры в хранилище, относящееся к конкретному приложению, а только приложения, которые хранят сведения в файлах или в реестре. Он также не содержит сведений о переносе данных, создаваемых пользователями с помощью приложения. Например, если приложение создает **.doc** файлы с помощью определенного шаблона, в этой статье не рассматривается перенос **самих файлов и** шаблонов.doc.

Перед началом

Должен быть определен тестовый компьютер, содержащий операционную систему исходных компьютеров. На тестовом компьютере также должны быть приложения, параметры которых необходимо перенести. Например, при миграции с Windows 10 на Windows 11 установите Windows 10 на тестовом компьютере, а затем установите приложения.

Шаг 1. Убедитесь в том, что приложение установлено на исходном компьютере и что оно совпадает с версией, установленной на конечном компьютере.

Перед переносом параметров USMT проверка, установлено ли приложение на исходном компьютере и что это правильная версия. Если приложение не установлено на исходном компьютере, USMT по-прежнему тратит время на поиск

параметров приложения. Что еще более важно, если USMT собирает параметры для приложения, которое не установлено, оно может перенести параметры, которые приводят к неправильной работы конечного компьютера. Также определите, существует ли несколько версий приложения, так как новая версия может хранить параметры в другом расположении. Несоответствие версий приложений может привести к непредвиденным результатам на конечном компьютере.

Существует множество способов определить, установлено ли приложение. Рекомендуется проверка для раздела удаления приложения в реестре. Затем на компьютере можно найти исполняемый файл, в котором установлено приложение. Важно проверка для обоих этих элементов, так как иногда разные версии одного приложения используют один и тот же ключ удаления. Даже если ключ есть, он может соответствовать другой версии приложения, которая требуется.

Проверка раздела удаления приложения в реестре

При установке большого числа приложений, особенно приложений, установленных с помощью технологии Установщика Microsoft Windows, ключ удаления приложения создается в следующих разделах:

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall`

Например, при установке Adobe Acrobat Reader 7 создается ключ с именем:

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall \{AC76BA86-7AD7-1033-7B44-A70000000000}`

Таким образом, если компьютер содержит этот ключ, на компьютере устанавливается Adobe Acrobat Reader 7. Существование раздела реестра можно проверить с помощью вспомогательной `DoesObjectExist` функции.

Раздел "**Удаление** реестра" для определенного приложения можно найти в следующем разделе реестра:

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall`

Чтобы найти раздел **Uninstall** для определенного приложения, найдите один из следующих элементов в разделе **Реестра удаления** :

- Имя приложения.
- Имя исполняемого файла приложения.
- Название компании, которая создает приложение.

Для поиска в реестре используйте реестр Редактор `Regedit.exe`. `Regedit.exe` находится в пути, хранящемся в `%SystemRoot%`, как правило `C:\Windows`, .

Проверка файловой системы на наличие исполняемого файла приложения

Следует также проверить двоичные файлы приложения для исполняемого файла, в котором установлено приложение. Чтобы проверка двоичных файлов приложения, определите, где установлено приложение и как называется исполняемый файл. Большинство приложений хранят расположение установки двоичных файлов приложения в реестре. В реестре следует выполнять поиск по одному из следующих элементов, пока не будет найдено значение реестра, содержащее путь установки:

- Имя приложения.
- Имя исполняемого файла приложения.
- Название компании, которая создает приложение.

После определения пути к исполняемому файлу приложения вспомогательную `DoesFileVersionMatch` функцию можно использовать для проверка для правильной версии исполняемого файла приложения. Пример использования вспомогательной `DoesFileVersionMatch` функции см. в разделе Windows Live™ Messenger файла `MigApp.xml` .

Шаг 2. Определение параметров для сбора и определение места хранения каждого параметра на компьютере

Затем просмотрите пользовательский интерфейс и составьте список всех доступных параметров. Список можно уменьшить, если есть параметры, которые не требуется переносить. Чтобы определить, где хранится каждый параметр, измените его. При изменении параметра отслеживайте действия в реестре и файловой системе с помощью такого средства, как монитор процессов. Двоичные файлы и параметры реестра, создаваемые при установке приложения, переносить не требуется. Когда приложение переустановлено на целевом компьютере, оно повторно создает эти параметры. Необходимо перенести только настроенные параметры.

Как определить, где хранится каждый параметр

1. Скачайте средство мониторинга файлов и реестра, например Монитор процессов (Procmon), с веб-сайта Sysinternals.

2. Завершите работу как можно больше приложений, чтобы ограничить работу реестра и файловой системы на компьютере.

3. Отфильтруйте выходные данные инструментов, чтобы отображались только изменения, внесенные приложением.

   > ⓘ **Примечание**
   >
   > Большинство приложений хранят свои параметры в профиле пользователя. То есть параметры, хранящиеся в файловой системе, находятся в каталоге `%UserProfile%` , а параметры, хранящиеся в реестре, находятся в кусте `HKEY_CURRENT_USER` . Для этих приложений выходные данные средств мониторинга файлов и реестра можно отфильтровать для отображения действий только в этих расположениях. Такая фильтрация значительно сокращает объем выходных данных, которые необходимо проверить.

4. Запустите средства мониторинга, измените параметр и найдите записи реестра и файловой системы, которые произошли при изменении параметра. Убедитесь, что внесенные изменения вступили в силу. Например, при изменении параметра в Microsoft Word путем выбора проверка в диалоговом окне **Параметры** изменение обычно не вступают в силу, пока диалоговое окно не будет закрыто, нажав кнопку **ОК**.

5. При изменении параметра обратите внимание на изменения файловой системы и реестра. Для каждого параметра может быть несколько файлов или значений реестра. Необходимо определить минимальный набор изменений файлов и реестра, необходимых для изменения этого параметра. Этот набор файлов и разделов реестра необходимо перенести для переноса параметра.

   > ⓘ **Примечание**
   >
   > Изменение параметра приложения неизбежно приводит к записи в разделы реестра. По возможности отфильтруйте выходные данные средства мониторинга файлов и реестра, чтобы отображались только записи в файлы и разделы и значения реестра.

Шаг 3. Определение способа применения собранных параметров

Если версия приложения на исходном компьютере совпадает с версией на конечном компьютере, то собранные файлы и разделы реестра изменять не нужно. По умолчанию USMT переносит файлы и разделы реестра из исходного расположения в соответствующее расположение на конечном компьютере. Например, если файл был собран из `C:\Users\User1\Documents` папки, а каталог профилей на конечном компьютере находится по адресу `D:\Users\User1`, то USMT автоматически переносит файл в `D:\Users\User1\Documents`. Однако расположение некоторых параметров может потребоваться изменить в следующих трех случаях:

Случай 1. Версия приложения на конечном компьютере новее, чем на исходном компьютере

В этом случае более новая версия приложения может считывать параметры с исходного компьютера без изменений. То есть данные, собранные из более старой версии приложения, иногда совместимы с более новой версией приложения. Однако расположение параметров может потребоваться изменить, если выполняется одно из следующих условий:

- **Более новая версия приложения имеет возможность импортировать параметры из более старой версии.** Обычно это сопоставление происходит при первом запуске пользователем новой версии после переноса параметров. Некоторые приложения импортируют параметры автоматически после переноса параметров. Однако другие приложения импортируют параметры только в том случае, если приложение было обновлено с более старой версии. При обновлении приложения устанавливается набор файлов и (или) разделов реестра, указывающий на то, что более старая версия приложения была установлена ранее. Если выполняется чистая установка более новой версии, компьютер не содержит эти файлы и разделы реестра. Если файлы и разделы реестра отсутствуют, сопоставление не выполняется. Чтобы заставить новую версию приложения инициировать этот процесс импорта, скрипту миграции может потребоваться создать эти файлы и (или) разделы реестра на конечном компьютере.

  Чтобы определить, какие файлы и (или) разделы и значения реестра необходимо создать, чтобы обеспечить работу импорта, выполните следующие действия:

  1. Обновите старую версию приложения до более новой.

2. Отслеживайте изменения, внесенные в файловую систему и реестр, с помощью процесса, описанного в разделе Определение места хранения каждого параметра.

После того как набор файлов, необходимых компьютеру, станет известен, **<элемент addObjects>** можно использовать для их добавления на целевой компьютер.

- **Более новая версия приложения не может считывать параметры с исходного компьютера, а также не может импортировать параметры в новый формат.** В этом случае создайте сопоставление для каждого параметра из старых расположений в новые. Чтобы создать сопоставление, определите, где в новой версии хранится каждый параметр, используя процесс, описанный в разделе Определение места хранения каждого параметра. После создания сопоставления примените параметры к новому расположению на конечном компьютере с помощью **<элемента locationModify>** и `RelativeMove` вспомогательных функций и `ExactMove` .

Случай 2. Конечный компьютер уже содержит параметры для приложения

Корпорация Майкрософт рекомендует перенести параметры после установки приложения, но до того, как пользователь запустит приложение в первый раз. Корпорация Майкрософт рекомендует этот процесс, так как этот процесс гарантирует отсутствие параметров на конечном компьютере при переносе параметров. Если приложение необходимо установить перед миграцией, все существующие параметры должны быть удалены с помощью **<элемента destinationCleanup>** . Если по какой-либо причине необходимо сохранить параметры, которые находятся на конечном компьютере, **<можно использовать элемент merge>** и `DestinationPriority` вспомогающую функцию.

Вариант 3. Приложение перезаписывает параметры при установке

Корпорация Майкрософт рекомендует перенести параметры после установки приложения, но до того, как пользователь запустит приложение в первый раз. Корпорация Майкрософт рекомендует этот процесс, так как этот процесс гарантирует отсутствие параметров на конечном компьютере при переносе параметров. Кроме того, при установке некоторых приложений они перезаписывают все существующие на компьютере параметры. В этом сценарии,

если данные были перенесены до установки приложения, настраиваемые параметры будут перезаписаны. Этот сценарий распространен для приложений, в которых параметры хранятся в расположениях за пределами профиля пользователя (как правило, эти параметры применяются ко всем пользователям). Эти универсальные параметры иногда перезаписываются при установке приложения и заменяются значениями по умолчанию. Чтобы избежать этой проблемы, эти приложения необходимо установить перед переносом файлов и параметров на конечный компьютер. По умолчанию с помощью USMT данные с исходного компьютера перезаписывают данные, которые уже существуют в том же расположении на конечном компьютере.

Шаг 4. Создание XML-компонента миграции для приложения

После выполнения шагов 1–3 создайте пользовательский **файл.xml** миграции, который переносит приложение на основе обновленных сведений. Файл `MigApp.xml` можно использовать в качестве модели, так как он содержит примеры многих концепций, рассмотренных в этой статье. Также см . раздел Пользовательские xml-примеры для другого примера **.xml** файла.

> ⓘ **Примечание**
>
> Корпорация Майкрософт рекомендует создавать отдельный **файл.xml** вместо добавления в него скрипта `MigApp.xml` . Рекомендуется использовать отдельный **файл.xml** , так как `MigApp.xml` файл является большим и его трудно читать и редактировать. Кроме того, при переустановке `MigApp.xml` USMT файл перезаписывается версией файла по умолчанию, а настроенная версия теряется.

> ⓘ **Важно!**
>
> Некоторые приложения хранят информацию в профиле пользователя, например пути установки приложения, имя компьютера и т. д. Сведения о приложении, хранящиеся в профиле пользователя, не должны переноситься и должны быть исключены из миграции.

Скрипт должен выполнить следующие действия:

1. Проверьте, установлена ли правильная версия приложения:

- Выполните поиск ключа удаления установки в разделе `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall` с помощью вспомогательной `DoesObjectExist` функции.
- Проверьте правильную версию исполняемого файла приложения с помощью вспомогательной `DoesFileVersionMatch` функции.

2. Если установлена правильная версия приложения, убедитесь, что каждый параметр перенесен в соответствующее расположение на конечном компьютере.
    - Если версии приложений одинаковы как на исходном, так и на целевом компьютерах, перенесите каждый параметр с помощью **<элементов include>** и **<exclude>** .
    - Если версия приложения на конечном компьютере является более новой, чем версия на исходном компьютере, и приложение не может импортировать параметры, сценарий должен:
        a. Добавьте набор файлов, запускающих импорт, с помощью **<элемента addObjects>** .
        b. Создайте сопоставление, которое применяет старые параметры к правильному расположению на конечном компьютере с помощью **<элемента locationModify>** и `RelativeMove` вспомогательных функций и `ExactMove` .
    - Если приложение необходимо установить перед переносом параметров, удалите все параметры, которые уже есть на конечном компьютере, с помощью **<элемента destinationCleanup>** .

Сведения об **.xml** элементах и вспомогательных функциях см. в разделе Библиотека XML-элементов.

Шаг 5. Тестирование миграции параметров приложения

На тестовом компьютере установите операционную систему, которая будет установлена на конечных компьютерах. Например, если планируется переход с Windows 10 на Windows 11, установите Windows 11, а затем установите приложение в Windows 11. Затем запустите **LoadState** на тестовом компьютере и убедитесь, что все параметры перенесены. При необходимости внесите исправления и повторите процесс, пока все необходимые параметры не будут перенесены правильно.

Чтобы ускорить сбор и перенос данных, одновременно можно перенести только одного пользователя. Все остальные компоненты можно исключить из миграции, за исключением тестируемого приложения. Чтобы указать только **User1** в миграции, введите:

Командная строка Windows

```
/ue:*\* /ui:user1
```

Дополнительные сведения см. в статье Об исключении файлов и параметров и разделе Параметры пользователя в статье Синтаксис ScanState . Чтобы устранить проблему, проверка журнал хода выполнения, журнал **ScanState** и журнал **LoadState**. Журналы содержат предупреждения и ошибки, которые могут указывать на проблемы с миграцией.

Связанные статьи

- Справочник по XML-файлу USMT.
- Конфликты и приоритет.
- Библиотека XML-элементов.
- Файлы журнала.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Перенос файлов и сертификатов EFS

Статья • 29.01.2025 • Применяется к: ✅ Windows 11, ✅ Windows 10

В этой статье описывается перенос сертификатов шифрованной файловой системы (EFS). Дополнительные сведения о параметре см. в `/efs` разделе Параметры зашифрованных файлов в синтаксисе ScanState.

Перенос файлов и сертификатов EFS

Сертификаты шифруемой файловой системы (EFS) переносятся автоматически. Однако по умолчанию средство миграции пользовательской среды (USMT) завершается сбоем, если найден зашифрованный файл, если `/efs` не указан параметр . Поэтому, если на устройстве есть зашифрованные файлы EFS, `/efs` параметр должен быть указан с любым из следующих параметров:

- `abort`
- `skip`
- `decryptcopy`
- `copyraw`
- `hardlink`

при выполнении `ScanState.exe` команды для переноса зашифрованных файлов. Затем при выполнении `LoadState.exe` команды на конечном компьютере зашифрованный файл и сертификат EFS переносятся автоматически.

> ⓘ **Примечание**
>
> Параметры `/efs` не используются с командой `LoadState.exe` .

Перед использованием средства **ScanState** для миграции, которая включает зашифрованные файлы и сертификаты EFS, все файлы в зашифрованной папке также должны быть зашифрованы. В противном случае удалите атрибут шифрования из папок, содержащих незашифрованные файлы. Если атрибут шифрования удален из файла, но не из родительской папки, файл шифруется во время миграции с помощью учетных данных учетной записи, используемой для запуска средства **LoadState** .

Средство Cipher.exe можно запустить в командной строке Windows для просмотра и изменения параметров шифрования файлов и папок. Например, чтобы удалить

шифрование из папки, в командной строке введите:

Командная строка Windows

```
cipher.exe /D /S:<PATH>
```

где <*Путь*> — это полный путь к верхнему родительскому каталогу, в котором задан атрибут шифрования.

Связанные статьи

- Что переносит USMT?.
- Определение типов файлов, файлов и папок.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Миграция учетных записей пользователей

Статья • 29.01.2025 • Применяется к: ✅ Windows 11, ✅ Windows 10

По умолчанию переносятся все пользователи. Единственный способ указать, какие пользователи следует включать и исключать, — это в командной строке с помощью параметров ScanState User и LoadState User. Пользователи не могут быть указаны в XML-файлах миграции или с помощью `Config.xml` файла.

Перенос всех учетных записей пользователей и параметров пользователей

Ссылки на подробные объяснения команд доступны в разделе Связанные статьи .

1. Войдите на исходный компьютер с правами администратора.
2. Введите следующую `ScanState.exe` командную строку в окне командной строки:

   Командная строка Windows

   ```
   ScanState.exe \\server\share\migration\mystore /i:MigDocs.xml
   /i:MigApp.xml /o
   ```

3. Войдите на целевой компьютер с правами администратора.
4. Введите одну из следующих `LoadState.exe` командных строк в окне командной строки:

   - При переносе учетных записей домена введите:

     Командная строка Windows

     ```
     LoadState.exe  \\server\share\migration\mystore /i:MigDocs.xml
     /i:MigApp.xml
     ```

   - При переносе локальных учетных записей вместе с учетными записями домена введите:

     Командная строка Windows

```
LoadState.exe  \\server\share\migration\mystore /i:MigDocs.xml
/i:MigApp.xml /lac /lae
```

> **Примечание**
>
> Параметр `/lae` не требуется указывать, что позволяет использовать учетную запись, созданную с параметром `/lac` . Вместо этого создайте отключенную локальную учетную запись, указав только `/lac` параметр , а затем локальный администратор должен включить учетную запись на конечном компьютере.

Перенос двух учетных записей домена (User1 и User2)

Ссылки на подробные объяснения команд доступны в разделе Связанные статьи .

1. Войдите на исходный компьютер с правами администратора.
2. Введите следующую `ScanState.exe` командную строку в окне командной строки:

   Командная строка Windows

   ```
   ScanState.exe \\server\share\migration\mystore /ue:*\*
   /ui:contoso\user1 /ui:fabrikam\user2 /i:MigDocs.xml /i:MigApp.xml /o
   ```

3. Войдите на целевой компьютер с правами администратора.
4. Введите следующую `LoadState.exe` командную строку в окне командной строки:

   Командная строка Windows

   ```
   LoadState.exe  \\server\share\migration\mystore /i:MigDocs.xml
   /i:MigApp.xml
   ```

Перенос двух учетных записей домена (User1 и User2) и перемещение обеих учетных

записей из домена Contoso в домен Fabrikam

Ссылки на подробные объяснения команд доступны в разделе Связанные статьи .

1. Войдите на исходный компьютер с правами администратора.
2. Введите следующую `ScanState.exe` командную строку в окне командной строки:

   Командная строка Windows

   ```
   ScanState.exe \\server\share\migration\mystore /ue:*\*
   /ui:contoso\user1 /ui:contoso\user2 /i:MigDocs.xml /i:MigApp.xml /o
   ```

3. Войдите на целевой компьютер с правами администратора.
4. Введите следующую `LoadState.exe` командную строку в окне командной строки:

   Командная строка Windows

   ```
   LoadState.exe  \\server\share\migration\mystore
   /mu:contoso\user1:fabrikam\user1 /mu:contoso\user2:fabrikam\user2
   /i:MigDocs.xml /i:MigApp.xml
   ```

Связанные статьи

- Определение пользователей.
- Синтаксис ScanState.
- Синтаксис LoadState.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Перенаправление файлов и параметров

Статья • 29.01.2025 • Применяется к: ✅ Windows 11, ✅ Windows 10

Чтобы перенаправить файлы и параметры, создайте пользовательский **файл.xml** и укажите имя `ScanState.exe` **файла.xml** в командной строках и `LoadState.exe` . Пользовательский **файл.xml** позволяет хранить изменения отдельно от файлов **.xml** по умолчанию, чтобы было проще отслеживать изменения.

Перенаправка папки

Следующий пользовательский **файл.xml** переносит каталоги и файлы из `C:\EngineeringDrafts` в папку **Документы** каждого пользователя. **%CSIDL_PERSONAL%** — это виртуальная папка, представляющая **<элемент рабочего стола Пользователя>** , что эквивалентно **CSIDL_MYDOCUMENTS**.

XML

```
<migration urlid="http://www.microsoft.com/migration/1.0/migxmlext/test">
<component type="Documents" context="User">
  <displayName>Engineering Drafts Documents to Personal Folder</displayName>
  <role role="Data">
    <rules>
      <!-- Migrate all directories and files present in c:\EngineeringDrafts
folder -->
      <include>
        <objectSet>
          <pattern type="File">C:\EngineeringDrafts\* [*]</pattern>
        </objectSet>
      </include>
      <!-- This migrates all files and directories from C:\EngineeringDrafts
to every user's personal folder.-->
      <locationModify
script="MigXmlHelper.RelativeMove('C:\EngineeringDrafts','%CSIDL_PERSONAL%')
">
        <objectSet>
          <pattern type="File">C:\EngineeringDrafts\* [*]</pattern>
        </objectSet>
      </locationModify>
    </rules>
  </role>
</component>
</migration>
```

Перенаправка определенного типа файла

Следующий пользовательский **файл.xml** перенаправляет **.mp3** файлы, расположенные на фиксированных дисках исходного компьютера, в папку `C:\Music` на конечном компьютере.

XML

```
<migration urlid="http://www.microsoft.com/migration/1.0/migxmlext/test">
<component type="Documents" context="System">
  <displayName>All .mp3 files to the Documents folder</displayName>
  <role role="Data">
    <rules>
      <include>
        <objectSet>
          <script>MigXmlHelper.GenerateDrivePatterns ("* [*.mp3]", "Fixed")
</script>
        </objectSet>
      </include>
      <!-- Migrates all the .mp3 files in the store to the C:\Music folder
during LoadState -->
      <locationModify script="MigXmlHelper.Move('C:\Music')">
        <objectSet>
          <script>MigXmlHelper.GenerateDrivePatterns ("* [*.mp3]", "Fixed")
</script>
        </objectSet>
      </locationModify>
    </rules>
  </role>
</component>
</migration>
```

Перенаправка определенного файла

Следующий пользовательский **файл.xml** переносит `Sample.doc` файл из `C:\EngineeringDrafts` в папку **Документы** каждого пользователя.

%CSIDL_PERSONAL% — это виртуальная папка, представляющая **<элемент рабочего стола Пользователя>** , что эквивалентно **CSIDL_MYDOCUMENTS**.

XML

```
<migration urlid="http://www.microsoft.com/migration/1.0/migxmlext/test">
<component type="Documents" context="User">
<displayName>Sample.doc into the Documents folder</displayName>
    <role role="Data">
      <rules>
        <include>
          <objectSet>
```

```
                <pattern type="File"> C:\EngineeringDrafts\ [Sample.doc]
</pattern>
          </objectSet>
        </include>
       <locationModify
script="MigXmlHelper.RelativeMove('C:\EngineeringDrafts','%CSIDL_PERSONAL%')
">
        <objectSet>
                <pattern type="File"> C:\EngineeringDrafts\ [Sample.doc]
</pattern>
        </objectSet>
       </locationModify>
      </rules>
    </role>
</component>
</migration>
```

Связанные статьи

- Настройка XML-файлов USMT.
- Конфликты и приоритет.
- Справочник по XML-файлу USMT.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Проверка состояния сжатого хранилища миграции

Статья • 29.01.2025 • Применяется к: ✅ Windows 11, ✅ Windows 10

Когда файлы и параметры переносятся во время обычной миграции с обновлением компьютера, состояние пользователя обычно сохраняется в сжатой папке промежуточного хранилища. Эта сжатая папка, также называемая сжатым хранилищем миграции, представляет собой один файл образа, содержащий:

- Все переносимые файлы.
- Параметры пользователя.
- Файл каталога, содержащий метаданные для всех файлов в хранилище миграции.

При выполнении `LoadState.exe` команды для загрузки данных из этих файлов на конечный компьютер **LoadState** требуется допустимый файл каталога, чтобы открыть хранилище миграции. Команду `UsmtUtils.exe` можно выполнить с параметром `/verify` , чтобы определить, является ли сжатое хранилище миграции нетронутым, содержит ли оно поврежденные файлы или поврежденный каталог. Параметр `/verify` следует запустить в хранилище миграции перед перезаписью исходных файлов и параметров пользовательского состояния.

`/verify` При использовании параметра можно указать тип сведений, которые следует сообщить в файле журнала **UsmtUtils**. Ниже перечислены типы отчетов.

- **Каталог**: отображает состояние только файла каталога.
- **Все**: отображает состояние всех файлов, включая файл каталога.
- **Только сбой**. Отображает только поврежденные файлы.

В следующих разделах показано, как выполнить `UsmtUtils.exe` команду с параметром `/verify` и указать сведения для отображения в файле журнала **UsmtUtils** .

Синтаксис UsmtUtils для параметра /verify

Чтобы проверить состояние сжатого хранилища миграции, используйте следующий синтаксис UsmtUtils:

> UsmtUtils.exe /verify[:<*reportType*>] <*filePath*> [/l:<*logfile*>] [/decrypt [:<*AlgID*>] {/key:<*keystring*> | /keyfile:<*filename*>}]

Где заполнители имеют следующие значения:

- <*USMTpath*> — это расположение, в котором сохраняются файлы и средства USMT.
- <*reportType*> указывает, следует ли сообщать обо всех файлах, только поврежденных файлах или о состоянии каталога.
- <*filePath*> — это расположение сжатого хранилища миграции.
- <*logfile*> — это расположение и имя файла журнала.
- <*AlgID*> — это алгоритм шифрования, который использовался для создания хранилища миграции в командной строке `ScanState.exe` .
- <*keystring*> — это ключ шифрования, который использовался для шифрования хранилища миграции.
- <*filename*> — это расположение и имя текстового файла, содержащего ключ шифрования.

Проверка сохранения хранилища миграции

Чтобы проверить, является ли хранилище миграции нетронутым или содержит поврежденные файлы или поврежденный каталог, введите:

Командная строка Windows

```
UsmtUtils.exe /verify D:\MyMigrationStore\store.mig
```

Так как тип отчета не указан, **UsmtUtils** отображает сводный отчет по умолчанию.

Проверка состояния только файла каталога

Чтобы проверить, поврежден или не поврежден файл каталога, введите:

Командная строка Windows

```
UsmtUtils.exe /verify:catalog D:\MyMigrationStore\store.mig
```

Проверка состояния всех файлов

Чтобы проверить наличие поврежденных файлов в сжатом хранилище миграции, а также указать имя и расположение файла журнала, введите:

Командная строка Windows

```
UsmtUtils.exe /verify:all D:\MyMigrationStore\store.mig /decrypt
/l:D:\UsmtUtilsLog.txt`
```

Помимо проверки состояния всех файлов, в этом примере файлы расшифровываются. Так как алгоритм шифрования не указан, **UsmtUtils** использует алгоритм шифрования 3DES по умолчанию.

Проверка состояния файлов и возврат только поврежденных файлов

В этом примере в файле журнала перечислены только файлы, которые были повреждены во время процесса **ScanState** . Этот список содержит файл каталога, если файл каталога также поврежден.

Командная строка Windows

```
UsmtUtils.exe /verify:failureonly D:\MyMigrationStore\USMT\store.mig
/decrypt:AES_192 /keyfile:D:\encryptionKey.txt
```

В этом примере файлы также расшифровываются путем указания алгоритма шифрования и расположения файла, содержащего ключ шифрования.

Дальнейшие действия

Если параметр `/verify` указывает на наличие поврежденных файлов в хранилище миграции, `/extract` параметр в средстве **UsmtUtils** можно использовать для восстановления данных из некоторых поврежденных хранилищ. Дополнительные сведения см. в разделе Извлечение файлов из сжатого хранилища миграции USMT.

Связанные статьи

- Синтаксис UsmtUtils.
- Коды возврата.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Требования USMT

Статья • 29.01.2025 • Применяется к: ✅ Windows 11, ✅ Windows 10

Поддерживаемые операционные системы

Средство миграции пользовательской среды (USMT) не имеет явных требований к ОЗУ или скорости ЦП для исходного или конечного компьютеров. Если компьютер соответствует системным требованиям операционной системы, он также соответствует требованиям к USMT. Требуется промежуточное хранилище, достаточно большое для хранения всех перенесенных данных и параметров. Для перенесенных файлов и параметров на конечном компьютере также требуется тот же объем места на жестком диске.

В следующей таблице перечислены операционные системы, поддерживаемые в USMT.

Развернуть таблицу

Операционный Системы	**ScanState (Источник Устройство)**	**LoadState (Назначение Устройство)**
Windows 7	✅	❌
Windows 8	✅	❌
Windows 10	✅	✅
Windows 11	✅	✅

Примечание

- 32-разрядную операционную систему можно перенести в 64-разрядную операционную систему. Однако 64-разрядную операционную систему нельзя перенести в 32-разрядную операционную систему.
- Поддерживается сбор данных с исходного устройства с помощью **ScanState** для версии Windows, которая не поддерживается. Однако восстановление данных на целевом устройстве с помощью **LoadState** в версии Windows, которая не поддерживается, не поддерживается.

Неподдерживаемые сценарии

- USMT не поддерживает ни одну из операционных систем Windows Server.
- USMT не поддерживает Microsoft Entra присоединенные устройства в качестве исходного или целевого устройства.
- USMT может работать с Microsoft Entra устройствами с гибридным присоединением, но это не проверенный сценарий, поэтому не поддерживается.
- USMT не поддерживает перенос параметров для приложений Microsoft Store.
- USMT не следует использовать для миграции между предыдущими версиями Windows. USMT предназначен только для:
  - Миграция на поддерживаемую в настоящее время версию Windows
  - Миграция между поддерживаемыми в настоящее время версиями Windows при условии, что версия Windows, в которой выполняется миграция, является более новой или той же, что и предыдущая версия Windows, из которой выполняется миграция.

Дополнительные сведения о предыдущих выпусках средств USMT см. в статье Общие сведения о средстве миграции пользовательской среды (USMT).

Windows PE

- **Необходимо использовать последнюю версию Среды предустановки Windows.** Дополнительные сведения см. в статье Новые возможности Windows PE.

Учетные данные

- **Запуск от имени администратора.**

  При запуске средств **ScanState** и **LoadState** они должны выполняться из командной строки с повышенными привилегиями, чтобы обеспечить миграцию всех указанных пользователей. Если USMT не запускается из запроса с повышенными привилегиями, в миграцию включается только профиль пользователя, вошедший в систему.

Чтобы открыть командную строку с повышенными привилегиями, выполните следующие действия:

1. Нажмите кнопку **Пуск**.
2. Введите `cmd` в функции поиска.

3. **Отображается cmd** или **командная строка** .
4. Щелкните правой кнопкой мыши **cmd** или **Командная строка**, а затем выберите **Запуск от имени администратора**.
5. Если текущий пользователь еще не является администратором, он предлагает ввести учетные данные администратора.

> ⓘ **Важно!**
>
> USMT должен работать с учетной записью с полными административными разрешениями, включая следующие привилегии:
>
> - SeBackupPrivilege (резервное копирование файлов и каталогов)
> - SeDebugPrivilege (программы отладки)
> - SeRestorePrivilege (восстановление файлов и каталогов)
> - SeSecurityPrivilege (управление аудитом и журналом безопасности)
> - Привилегия SeTakeOwnership (владение файлами или другими объектами)

Config.xml

`/c` Укажите параметр и <параметры ErrorControl> в `Config.xml` файле

UsMT завершается ошибкой, если не удается перенести файл или параметр, если `/c` не указан параметр. `/c` Если указан параметр, USMT регистрирует ошибку при каждом обнаружении используемого файла, который не был перенесен, но миграция не прерывается. В USMT в файле можно указать, какие типы ошибок должны позволить продолжить миграцию, а какие должны привести к сбою миграции `Config.xml` . Дополнительные сведения об отчетах об ошибках и **<элементе ErrorControl>** см. в разделе файлConfig.xml, файлы журнала и библиотека XML-элементов.

LoadState

Установка приложений перед выполнением команды LoadState

Установите все приложения на целевом компьютере перед восстановлением пользовательского состояния. Установка приложений перед выполнением

`LoadState.exe` команды гарантирует сохранение перенесенных параметров.

Требования к жесткому диску

Убедитесь, что в хранилище миграции, а также на исходном и целевом компьютерах достаточно свободного места. Дополнительные сведения см. в статье Оценка размера хранилища миграции.

Предварительные требования для пользователей

В этой документации предполагается, что ИТ-специалисты, использующие USMT, понимают средства командной строки. В документации также предполагается, что ИТ-специалисты, использующие USMT для разработки правил MigXML, понимают следующие понятия:

- Навигация и иерархия реестра Windows.
- Файлы и типы файлов, используемые приложениями.
- Методы извлечения приложений и сведений о настройке вручную из приложений, созданных внутренними группами разработки программного обеспечения и издателями программного обеспечения сторонних разработчиков.
- Основы разработки XML.

Связанные статьи

- Планирование миграции.
- Оценка размера хранилища миграции.
- Обзор средства миграции пользовательской среды (USMT).

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Рекомендации по USMT

Статья • 29.01.2025 • Применяется к: ✅ Windows 11, ✅ Windows 10

В этой статье рассматриваются общие рекомендации и рекомендации по обеспечению безопасности при использовании средства миграции пользовательской среды (USMT).

Общие рекомендации

- **Установите приложения перед запуском средства LoadState.**

  Хотя это не всегда важно, рекомендуется установить все приложения на конечном компьютере перед восстановлением пользовательского состояния. Установка приложений перед восстановлением состояния пользователя помогает обеспечить сохранение перенесенных параметров.

- **Не используйте MigUser.xml и MigDocs.xml вместе.**

  Если и , `MigUser.xml` и `MigDocs.xml` используются вместе, некоторые перенесенные файлы могут дублироваться, если предоставляются конфликтующие инструкции о целевых расположениях. Параметр `/genmigxml` командной строки можно использовать, чтобы определить, какие файлы включены в миграцию, и определить, необходимы ли какие-либо изменения. Дополнительные сведения см. в статье Определение типов файлов, файлов и папок.

- **Используйте MigDocs.xml для более эффективной миграции.**

  Если набор данных неизвестен или много файлов хранится вне стандартных папок профиля пользователя, `MigDocs.xml` этот файл лучше, чем `MigUser.xml` файл, так как `MigDocs.xml` он собирает более широкий область данных. Файл `MigDocs.xml` переносит папки данных на основе расположения и зарегистрированного типа файла, запрашивая в реестре зарегистрированные расширения приложений. Файл `MigUser.xml` переносит только файлы с указанными расширениями.

- **Закройте все приложения перед запуском средств ScanState или LoadState.**

  Несмотря на `/vsc` то, что с помощью этого параметра можно перенести многие файлы, открытые с помощью другого приложения, рекомендуется закрыть все приложения, чтобы обеспечить перенос всех файлов и

параметров. `/vsc` Без параметра или `/c` средство USMT завершается ошибкой, если не удается перенести файл или параметр. `/c` При использовании параметра USMT игнорирует все файлы или параметры, которые нельзя перенести, и каждый раз регистрирует ошибку.

- **Выйдите из системы после запуска LoadState.**

  Некоторые параметры, такие как шрифты, обои и параметры скринсейвера, не вступают в силу до следующего входа пользователя. По этой причине выйдите из службы после запуска средства **LoadState** .

- **Управляемая среда.**

  Чтобы создать управляемую среду, все документы пользователя можно переместить в папку **Документы** (%CSIDL_PERSONAL%). Корпорация Майкрософт рекомендует переносить файлы в минимально возможное количество папок на конечном компьютере. Минимизация папок помогает очистить файлы на конечном компьютере в случае `LoadState.exe` сбоя команды перед завершением.

- **Chkdsk.exe.**

  Корпорация Майкрософт рекомендует запустить **Chkdsk.exe** перед запуском средств **ScanState** и **LoadState** . **Chkdsk.exe** создает отчет о состоянии жесткого диска, а также перечисляет и исправляет распространенные ошибки. Дополнительные сведения о **средствеChkdsk.exe** см. в разделе Chkdsk.

- **Миграция в группах.**

  Если миграция выполняется, когда пользователи используют сеть, лучше перенести учетные записи пользователей в группах. Чтобы свести к минимуму влияние на производительность сети, определите размер групп на основе размера каждой учетной записи пользователя. Миграция поэтапно также позволяет убедиться, что каждый этап успешно выполняется перед началом следующего этапа. Если используется этот метод, в план между группами можно внести любые необходимые изменения.

Рекомендации по безопасности

Полномочный администратор несет ответственность за защиту конфиденциальности пользователей и обеспечение безопасности во время и после миграции. В частности, необходимо рассмотреть следующие вопросы:

- **Файловая система шифрования (EFS).**

  Соблюдайте особую осторожность при переносе зашифрованных файлов, так как для отслеживания состояния пользователя не требуется вход в систему. По умолчанию USMT завершается ошибкой при обнаружении зашифрованного файла. Конкретные инструкции по рекомендациям ПО EFS см. в разделе Перенос файлов и сертификатов EFS.

  > ⓘ **Примечание**
  >
  > Если зашифрованный файл переносится без переноса сертификата, конечные пользователи не смогут получить доступ к файлу после миграции.

- **Зашифруйте хранилище.**

  Рассмотрите `/encrypt` возможность использования параметра с командой `ScanState.exe` и `/decrypt` параметра с командой `LoadState.exe` . Однако будьте осторожны с этим набором параметров, так как любой пользователь, имеющий доступ к скрипту `ScanState.exe` командной строки, также имеет доступ к ключу шифрования.

- **Проверка на вирусы.**

  Корпорация Майкрософт рекомендует проверять исходный и конечный компьютеры на наличие вирусов перед запуском USMT. Кроме того, необходимо проверить целевой образ компьютера. Чтобы защитить данные от вирусов, корпорация Майкрософт настоятельно рекомендует запустить антивирусную программу перед миграцией.

- **Обеспечение безопасности файлового сервера и сервера развертывания.**

  Корпорация Майкрософт рекомендует управлять безопасностью файловых серверов и серверов развертывания. Важно убедиться, что файловый сервер, на котором хранится хранилище, защищен. Сервер развертывания также должен быть защищен, чтобы данные пользователей, которые есть в файлах журнала, не были предоставлены. Корпорация Майкрософт также рекомендует передавать данные только через безопасное сетевое подключение, например виртуальную частную сеть. Дополнительные сведения о безопасности сети см. в разделе Microsoft Security Compliance Manager.

- **Миграция паролей.**

Чтобы обеспечить конфиденциальность конечных пользователей, USMT не переносит пароли, включая пароли для приложений или сопоставленных сетевых дисков. Важно убедиться, что конечные пользователи знают свои пароли.

- **Создание локальной учетной записи.**

  Перед переносом локальных учетных записей см. раздел Миграция локальных учетных записей статьи Идентификация пользователей .

Рекомендации по XML-файлам

- **Укажите один и тот же набор MIG*.xml файлов в средствах ScanState и LoadState.**

  Если с помощью средства **ScanState** используется определенный набор файлов mig*.xml, вызываемых с помощью `/auto` параметра или по `/i` отдельности, то этот же параметр следует использовать для вызова тех же файлов mig*.xml в **средстве LoadState** .

- **Значение <CustomFileName> в URL-адресе миграции должно соответствовать имени файла.**

  Хотя это не является обязательным требованием, рекомендуется <, **чтобы CustomFileName**> соответствовало имени файла. Например, следующий пример из `MigApp.xml` файла:

  ```
  XML
  ```

  ```xml
  <?xml version="1.0" encoding="UTF-8"?>
  <migration
  urlid="http://www.microsoft.com/migration/1.0/migxmlext/migapp">
  ```

- **Используйте схему XML (MigXML.xsd) при создании .xml файлов для проверки синтаксиса.**

  Файл `MigXML.xsd` схемы не должен быть включен в командную строку или в любой из **.xml** файлов.

- **Используйте XML-файлы миграции по умолчанию в качестве моделей.**

  Чтобы создать пользовательский **файл.xml** , файлы миграции **.xml** можно использовать в качестве моделей для создания настраиваемых версий. Если файлы данных пользователя необходимо перенести, смоделировать

пользовательский **файл.xml** в `MigUser.xml`. Чтобы перенести параметры приложения, моделировайте пользовательский **.xml** файл в `MigApp.xml` файле.

- **Учитывайте влияние на производительность при использовании параметра контекста<>.**

  Производительность миграции может быть затронута, **<если элемент контекста>** используется вместе с элементом **<компонента>** . Например, при инкапсуляции логических единиц файлов **<или путей включают>** и **<исключают>** правила.

  В контексте **пользователя** правило обрабатывается один раз для каждого пользователя в системе.

  В контексте **системы** правило обрабатывается один раз для системы.

  В контексте **UserAndSystem** правило обрабатывается один раз для каждого пользователя в системе и один раз для системы.

  > ⓘ **Примечание**
  >
  > Количество обработки правила не влияет на количество переносов файла. Подсистема миграции USMT гарантирует, что каждый файл переносится только один раз.

- **Корпорация Майкрософт рекомендует создать отдельный файл .xml вместо добавления .xml кода в один из существующих файлов .xml миграции.**

  Например, для кода, который переносит параметры приложения, код не должен быть просто добавлен в `MigApp.xml` файл.

- **Пользовательские .xml файлы не должны создаваться для изменения перенесенных параметров операционной системы.**

  Файлы манифеста определяют, какие параметры переносятся. Файлы манифеста нельзя изменить. Так как файлы манифеста нельзя изменить, чтобы исключить некоторые параметры операционной системы из миграции, создайте и измените `Config.xml` файл.

- **Подстановочный знак звездочки (*) можно использовать в любом созданном XML-файле миграции.**

  > ⓘ **Примечание**

Вопросительный знак недопустим в качестве подстановочного знака в файлах **.xml** USMT.

Связанные статьи

- Шифрование хранилища миграции.
- Планирование миграции.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Принцип работы USMT

Статья • 29.01.2025 • Применяется к: ✅ Windows 11, ✅ Windows 10

USMT включает два средства для переноса параметров и данных: **ScanState** и **LoadState**. **ScanState** собирает сведения с исходного компьютера, и **LoadState** применяет эти сведения к конечному компьютеру.

> ⓘ **Примечание**
>
> Дополнительные сведения о том, как USMT обрабатывает правила и XML-файлы, см. в разделе **Конфликты и приоритет**.

Процесс ScanState

При запуске средства **ScanState** на исходном компьютере выполняется следующий процесс:

1. Он анализирует и проверяет параметры командной строки, создает `ScanState.log` файл, а затем начинает ведение журнала.

2. Он собирает сведения обо всех компонентах миграции, которые необходимо перенести. *Компонент миграции* — это логическая группа файлов, разделов реестра и значений. Например, набор файлов, разделов реестра и значений, в которые хранятся параметры Adobe Acrobat, сгруппирован в один компонент миграции.

   Существует три типа компонентов:

   - Компоненты, переносимые параметры операционной системы.
   - Компоненты, переносимые параметры приложения.
   - Компоненты, которые переносит файлы пользователей.

   Средство **ScanState** собирает сведения о параметрах приложения и компонентах пользовательских данных из **.xml** файлов, указанных в командной строке.

   В поддерживаемых в настоящее время версиях Windows файлы манифеста управляют переносом параметров операционной системы. Эти файлы нельзя

изменить. Чтобы исключить некоторые параметры операционной `Config.xml` системы, необходимо создать и изменить файл.

3. **ScanState** определяет, какие профили пользователей следует перенести. По умолчанию переносятся все профили пользователей на исходном компьютере. Однако пользователи могут быть включены и исключены с помощью параметров Пользователя. Профиль системы и общедоступный профиль на исходном компьютере под управлением поддерживаемых в настоящее время версий Windows всегда переносятся, и эти профили нельзя исключить из миграции.

4. На этапе **сканированияScanState** выполняет следующие действия для каждого профиля пользователя, выбранного для миграции:

   a. Для каждого компонента **ScanState** проверяет тип компонента. Если текущий профиль пользователя является системным профилем, а тип компонента — **System** или **UserAndSystem**, компонент выбирается для этого пользователя. В противном случае компонент игнорируется. Кроме того, если текущий профиль пользователя не является системным профилем, а тип компонента — **User** или **UserAndSystem**, компонент выбирается для этого пользователя. В противном случае этот компонент игнорируется.

   > ⓘ **Примечание**
   >
   > С этого момента **ScanState** не проводит различий между компонентами, которые переносят параметры операционной системы, компонентами, которые переносят параметры приложений, и компонентами, которые переносят файлы пользователей. **ScanState** обрабатывает все компоненты одинаково.

   b. Каждый компонент, выбранный на предыдущем шаге, обрабатывается далее. Все переменные, зависящие от профиля (например **, CSIDL_PERSONAL**) оцениваются в контексте текущего профиля. Например, если обрабатываемый профиль принадлежит **пользователю User1**, **то CSIDL_PERSONAL** будет расширяться до `C:\Users\User1\Documents`, при условии, что профили пользователей хранятся в каталоге `C:\Users` .

   c. Для каждого выбранного компонента **ScanState** оценивает **<раздел обнаружения>** . Если условие в **<разделе обнаружения>** принимает значение false, компонент больше не обрабатывается. В противном случае обработка этого компонента продолжается.

d. Для каждого выбранного компонента **ScanState** оценивает **<разделы правил>** . Для каждого **<раздела правил>** , если текущий профиль пользователя является системным профилем, а контекст **<раздела правил>** — **System** или **UserAndSystem**, правило обрабатывается далее. В противном случае это правило игнорируется. Кроме того, если текущий профиль пользователя не является системным профилем и контекстом **<раздела правил>** является **User** или **UserAndSystem**, правило обрабатывается далее. В противном случае это правило игнорируется.

e. **ScanState** создает список единиц миграции, которые необходимо перенести, обработать различные подразделы в этом **<разделе правил>** . Каждая единица собирается, если единица упоминается в **<подразделе include>**, если в подразделе **exclude> в том же разделе правил нет более конкретного правила**<.>< Дополнительные сведения о приоритете в **файлах.xml** см. в разделе Конфликты и приоритет.

Кроме того, любая единица миграции (например, файл, раздел реестра или набор значений реестра), которая находится в <разделе UnconditionalExclude> , не переносится.

> ⓘ **Примечание**
>
> **ScanState** игнорирует некоторые подразделы, такие как <destinationCleanup> и <locationModify>. Эти разделы оцениваются только на конечном компьютере.

5. На этапе **сбораScanState** создает центральный список единиц миграции, объединяя списки, созданные для каждого выбранного профиля пользователя.

6. На этапе **сохраненияScanState** записывает собранные единицы миграции в расположение хранилища.

> ⓘ **Примечание**
>
> **ScanState** не изменяет исходный компьютер каким-либо образом.

Процесс LoadState

Процесс **LoadState** аналогичен процессу **ScanState** . Средство **ScanState** собирает единицы миграции, такие как файл, раздел реестра или значения реестра, с

исходного компьютера и сохраняет их в хранилище. Аналогичным образом средство **LoadState** собирает единицы миграции из хранилища и применяет их к конечному компьютеру.

1. **ScanState** анализирует и проверяет параметры командной строки, создает `ScanState.log` файл, а затем начинает ведение журнала.

2. **LoadState** собирает сведения о компонентах миграции, которые необходимо перенести.

   LoadState получает сведения о компонентах параметров приложения и пользовательских данных из **файлов миграции.xml** , указанных командой `LoadState.exe` .

   В поддерживаемых в настоящее время версиях Windows файлы манифеста управляют переносом параметров операционной системы. Эти файлы нельзя изменить. Чтобы исключить некоторые параметры операционной `Config.xml` системы, необходимо создать и изменить файл.

3. **LoadState** определяет, какие профили пользователей следует перенести. По умолчанию переносятся все профили пользователей, присутствующие на исходном компьютере. Однако пользователи могут быть включены и исключены с помощью параметров Пользователя. Профиль системы и общедоступный профиль на исходном компьютере под управлением поддерживаемых в настоящее время версий Windows всегда переносятся, и эти профили нельзя исключить из миграции.

   - Если выполняется миграция учетных записей локальных пользователей и учетные записи еще не существуют на конечном компьютере, `/lac` необходимо использовать параметр командной строки. `/lac` Если параметр не указан, все локальные учетные записи пользователей, которые еще не присутствуют на конечном компьютере, не переносятся.

   - При указании `LoadState.exe` с помощью команды `/md` параметры и `/mu` обрабатываются для переименования профиля пользователя на конечном компьютере.

   - Для каждого профиля пользователя, выбранного из хранилища, **LoadState** создает соответствующий профиль пользователя на конечном компьютере. Для создания профилей пользователей домена целевой компьютер не требуется подключать к домену. Если USMT не может определить домен, он пытается применить параметры к локальной

учетной записи. Дополнительные сведения см. в разделе Определение пользователей.

4. На этапе **сканированияLoadState** выполняет следующие действия для каждого профиля пользователя:

   a. Для каждого компонента **LoadState** проверяет тип компонента. Если текущий профиль пользователя является системным профилем, а тип компонента — **System** или **UserAndSystem**, компонент выбирается для этого пользователя. В противном случае компонент игнорируется. Кроме того, если текущий профиль пользователя не является системным профилем, а тип компонента — **User** или **UserAndSystem**, компонент выбирается для этого пользователя. В противном случае этот компонент игнорируется.

   > ⓘ **Примечание**
   >
   > С этого момента **LoadState** не различает компоненты, которые переносят параметры операционной системы, компоненты, которые переносят параметры приложения, и компоненты, которые переносят файлы пользователей. **LoadState** оценивает все компоненты одинаково.

   b. Каждый выбранный компонент обрабатывается далее. Все переменные, зависящие от профиля (например **, CSIDL_PERSONAL**) оцениваются в контексте текущего профиля. Например, если обрабатываемый профиль принадлежит **пользователю User1**, **то CSIDL_PERSONAL** будет расширяться до `C:\Users\User1\Documents` (при условии, что профили пользователей хранятся в каталоге `C:\Users`).

   > ⓘ **Примечание**
   >
   > **LoadState** игнорирует **<раздел обнаружения,>** указанный в компоненте. На этом этапе все указанные компоненты считаются обнаруженными и выбираются для миграции.

   c. Для каждого выбранного компонента **LoadState** оценивает **<разделы правил>** . Для каждого **<раздела правил>** , если текущий профиль пользователя является системным профилем, а контекст **<раздела правил>** — **System** или **UserAndSystem**, правило обрабатывается далее. В противном случае это правило игнорируется. Кроме того, если текущий профиль

пользователя не является системным профилем и контекстом **<раздела правил>** является **User** или **UserAndSystem**, правило обрабатывается далее. В противном случае это правило игнорируется.

d. **LoadState** создает центральный список единиц миграции путем обработки различных подразделов в **<разделе правил>** . Каждая единица миграции, которая находится в **<подразделе включения>** , переносится до тех пор, пока нет более конкретного правила для нее в подразделе **<exclude>** в том же **<разделе правил>** . Дополнительные сведения о приоритете см. в разделе Конфликты и приоритет.

e. **LoadState** вычисляет подразделы целевого компьютера, например **<destinationCleanup>** и **<locationModify>** .

f. Если конечный компьютер работает под управлением поддерживаемой в настоящее время версии Windows, то migunits, собранные **ScanState** с помощью файлов манифеста нижнего уровня, обрабатываются **LoadState** с помощью соответствующего манифеста компонента из нижней версии Windows. Файлы манифеста нижнего уровня не используются во время **LoadState**.

> ⓘ **Важно!**
>
> Чтобы **LoadState** использовал **файлы.xml** , важно указать их с `LoadState.exe` помощью команды . В противном случае все правила назначения, например **<locationModify>**, в этих **.xml** файлах игнорируются, даже если при `ScanState.exe` выполнении команды были предоставлены те же **.xml** файлы.

5. На этапе **ПримененияLoadState** записывает собранные единицы миграции в различные расположения на конечном компьютере. Если существуют конфликты и для объекта не **<существует правила слияния>** , по умолчанию для реестра источник перезаписывает назначение. Поведение по умолчанию для файлов — постепенное переименование источника, например OriginalFileName(1). OriginalExtension. Некоторые параметры, такие как шрифты, обои и параметры заставки экрана, не вступают в силу до следующего входа пользователя. По этой причине выйдите из системы после `LoadState.exe` завершения действий команды.

Связанные статьи

- Синтаксис командной строки средства миграции пользовательской среды (USMT).

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Планирование миграции

Статья • 29.01.2025 • Применяется к: ✅ Windows 11, ✅ Windows 10

Перед использованием средства миграции пользовательской среды (USMT) корпорация Майкрософт рекомендует тщательно спланировать миграцию. Планирование может помочь миграции провести гладко и снизить риск сбоя миграции.

При планировании миграции организации и отдельные пользователи должны сначала определить, что следует перенести, включая параметры пользователей, приложения и параметры приложений, а также файлы и папки с личными данными. Определение приложений для миграции особенно важно, чтобы избежать сбора данных о приложениях, которые могут быть прекращены.

Одним из наиболее важных требований для переноса параметров и данных является восстановление только сведений, необходимых конечному компьютеру. Хотя данные, которые записываются на исходном компьютере, могут быть более полными, чем данные восстановления для резервного копирования, восстановление данных или параметров для приложений, которые не установлены в целевой системе, является избыточным. Восстановление данных или параметров для приложений, которые не установлены, также может привести к нестабильности на только что развернутом компьютере.

В этом разделе

Развернуть таблицу

Ссылка	Описание
Распространенные сценарии миграции	Определите, следует ли выполнить миграцию обновления или заменить миграцию.
Что переносит USMT?	Узнайте, какие приложения, пользовательские данные и компоненты операционной системы переносит USMT.
Выбор типа хранилища миграции	Выберите несжатое, сжатое или жесткое хранилище миграции.
Определение того, что следует перенести	Определите учетные записи пользователей, параметры приложений, параметры операционной системы и файлы, которые необходимо перенести внутри организации.
Тестирование миграции	Протестируйте миграцию перед развертыванием Windows для

Ссылка	Описание
	всех пользователей.

Связанные статьи

- Справочник по XML-файлу USMT.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Общие сценарии переноса

Статья • 29.01.2025 • Применяется к: ✅ Windows 11, ✅ Windows 10

Средство миграции пользовательской среды (USMT) можно использовать, когда планируется обновление оборудования и (или) операционной системы для большого количества компьютеров. USMT управляет миграцией цифрового удостоверения конечного пользователя, записывая с исходного компьютера следующие элементы пользователя:

- Параметры операционной системы.
- Параметры приложения.
- Личные файлы.

После записи этих элементов они переустановляются на конечном компьютере после завершения обновления.

Одним из распространенных сценариев является обновление операционной системы на существующем оборудовании без замены оборудования. Этот сценарий называется **обновлением компьютера**. Второй распространенный сценарий называется **заменой пк**, когда один элемент оборудования заменяется, как правило, новым оборудованием и более новой операционной системой.

Обновление компьютера

На следующей схеме показана миграция с обновлением компьютера, также известная как миграция обновления компьютера. Сначала администратор переносит состояние пользователя с исходного компьютера в промежуточное хранилище. После установки операционной системы администратор переносит состояние пользователя обратно на исходный компьютер.

1. Состояние scan собирает состояние пользователя и сохраняет данные в Хранилище переноса
2. Установлена новая операционная система
3. Состояние загрузки восстанавливает состояние пользователя

Первый сценарий. Обновление компьютера в автономном режиме с помощью Среды предустановки Windows и хранилища миграции с жесткой компоновкой

Организация получает средства на обновление операционной системы на всех компьютерах в бухгалтерии до последней поддерживаемой версии Windows. Каждый сотрудник хранит один и тот же компьютер, но операционная система на каждом компьютере будет обновлена. В этом сценарии обновление обрабатывается в автономном режиме без сетевого подключения. Администратор использует среду предварительной установки Windows (WinPE) и хранилище миграции с жесткой привязкой для сохранения каждого пользовательского состояния на соответствующем компьютере.

1. На каждом компьютере администратор загружает компьютер в WinPE и запускает программу командной строки **ScanState** , указывая параметры командной `/hardlink /nocompress` строки. **ScanState** сохраняет состояние пользователя в хранилище миграции с жесткой связью на каждом компьютере, повышая производительность за счет минимизации сетевого трафика и минимизации сбоев миграции на компьютерах с ограниченным пространством на жестком диске.

2. На каждом компьютере администратор устанавливает стандартную операционную среду (SOE) организации, которая включает в себя последнюю поддерживаемую версию Windows и других приложений организации.

3. Администратор запускает программу командной строки **LoadState** на каждом компьютере. **LoadState** восстанавливает состояние каждого пользователя на каждом компьютере.

Сценарий 2. Обновление компьютера с помощью сжатого хранилища миграции

Организация получает средства на обновление операционной системы на всех компьютерах до последней поддерживаемой версии Windows. Каждый сотрудник хранит один и тот же компьютер, но операционная система на каждом компьютере будет обновлена. В этом сценарии администратор использует сжатое хранилище миграции для сохранения пользовательских состояний на сервере.

1. Администратор запускает программу командной строки **ScanState** на каждом компьютере. **ScanState** сохраняет каждое пользовательское состояние на сервере.

2. На каждом компьютере администратор устанавливает стандартную soE организации, которая включает последнюю поддерживаемую версию Windows и других приложений организации.

3. Администратор запускает программу командной строки **LoadState** на каждом исходном компьютере, и **LoadState** восстанавливает состояние каждого пользователя обратно на компьютер.

Сценарий третий. Обновление компьютера с помощью хранилища миграции с жесткой компоновкой

Организация получает средства на обновление операционной системы на всех компьютерах до последней поддерживаемой версии Windows. Каждый сотрудник хранит один и тот же компьютер, но операционная система на каждом компьютере будет обновлена. В этом сценарии администратор использует хранилище миграции с жесткой связью, чтобы сохранить каждое пользовательское состояние на соответствующем компьютере.

1. Администратор запускает программу командной строки **ScanState** на каждом компьютере, указывая параметры командной `/hardlink /nocompress` строки. **ScanState** сохраняет состояние пользователя в хранилище миграции с жесткой связью на каждом компьютере, повышая производительность за счет

минимизации сетевого трафика и минимизации сбоев миграции на компьютерах с ограниченным пространством на жестком диске.

2. На каждом компьютере администратор устанавливает soE организации, включающую последнюю поддерживаемую версию Windows и других приложений организации.

3. Администратор запускает программу командной строки **LoadState** на каждом компьютере. **LoadState** восстанавливает состояние каждого пользователя на каждом компьютере.

Сценарий четвертый: обновление компьютера с помощью папки Windows.old и хранилища миграции с жесткой компоновкой

Организация решает обновить операционную систему на всех своих компьютерах до последней поддерживаемой версии Windows. Каждый сотрудник хранит один и тот же компьютер, но операционная система на каждом компьютере будет обновлена. В этом сценарии администратор использует **Windows.old** и хранилище миграции с жесткой ссылкой для сохранения каждого пользовательского состояния на соответствующем компьютере.

1. Администратор устанавливает последнюю поддерживаемую версию Windows на каждом компьютере. Во время установки они должны убедиться, что каталог **Windows.old** создан, выполнив следующие действия:

    - Выполнение установки без форматирования или повторного разделения диска.
    - Выбор раздела, содержащего предыдущую версию Windows.

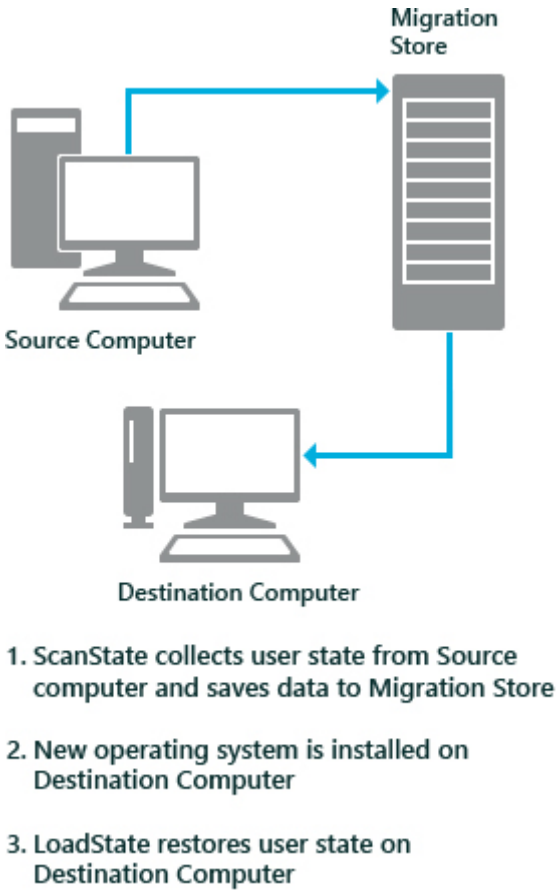
2. На каждом компьютере администратор устанавливает soE организации, включающую приложения организации.

3. Администратор последовательно запускает программы **командной строки ScanState** и **LoadState** на каждом компьютере, указывая параметры командной `/hardlink /nocompress` строки.

Замена ПК

На следующей схеме показана миграция с заменой компьютера. Сначала администратор переносит состояние пользователя с исходного компьютера в промежуточное хранилище. После установки операционной системы на целевом

компьютере администратор переносит состояние пользователя из хранилища на конечный компьютер.



Первый сценарий. Автономная миграция с помощью Среды предустановки Windows и внешнего хранилища миграции

Организация выделяет 20 новых компьютеров пользователям в бухгалтерии. Каждый из пользователей имеет исходный компьютер со своими файлами и параметрами. В этом сценарии миграция выполняется в автономном режиме без сетевого подключения.

1. На каждом исходном компьютере администратор загружает компьютер в WinPE и запускает **ScanState** для сбора пользовательского состояния на сервере или на внешнем жестком диске.

2. На каждом новом компьютере администратор устанавливает soE организации, включающую последнюю поддерживаемую версию Windows и других приложений организации.

3. На каждом из новых компьютеров администратор запускает средство **LoadState** , восстанавливая каждое пользовательское состояние из хранилища миграции на один из новых компьютеров.

Сценарий второй: миграция сети вручную

Организация получает 50 новых ноутбуков для своих руководителей и должна перераспределить 50 старых ноутбуков для новых сотрудников. В этом сценарии администратор запускает средство **ScanState** из командной строки на каждом компьютере, чтобы собрать состояния пользователей и сохранить их на сервере в сжатом хранилище миграции.

1. Администратор запускает средство **ScanState** на каждом из старых ноутбуков руководителя и сохраняет каждое пользовательское состояние на сервере.

2. На новых ноутбуках администратор устанавливает soE организации, которая включает в себя последнюю поддерживаемую версию Windows и других приложений организации.

3. Администратор запускает средство **LoadState** на новых ноутбуках, чтобы перенести пользовательские состояния менеджеров на соответствующий компьютер. Теперь новые ноутбуки готовы для использования руководителями.

4. На старых компьютерах администратор устанавливает soE организации, в том числе последнюю поддерживаемую версию Windows, Microsoft Office и других приложений организации. Старые компьютеры теперь готовы для использования новыми сотрудниками.

Третий сценарий: управляемая сетевая миграция

Организация выделяет 20 новых компьютеров пользователям в бухгалтерии. Каждый из пользователей имеет исходный компьютер с файлами и параметрами. Администратор использует технологию управления, например сценарий входа или пакетный файл, чтобы запустить **ScanState** на каждом исходном компьютере, чтобы собрать состояния пользователей и сохранить их на сервере в сжатом хранилище миграции.

1. На каждом исходном компьютере администратор запускает средство **ScanState** с помощью Microsoft Configuration Manager, Microsoft Deployment Toolkit (MDT), скрипта входа, пакетного файла или технологии управления сторонних корпораций. **ScanState** собирает пользовательское состояние с каждого исходного компьютера, а затем сохраняет его на сервере.

2. На каждом новом компьютере администратор устанавливает soE организации, в том числе последнюю поддерживаемую версию Windows и других приложений организации.

3. На каждом из новых компьютеров администратор запускает средство **LoadState** с помощью Microsoft Configuration Manager, скрипта входа, пакетного файла или технологии управления сторонних корпораций. **LoadState** переносит каждое пользовательское состояние из хранилища миграции на один из новых компьютеров.

Связанные статьи

- Планирование миграции.
- Выберите тип хранилища миграции.
- Справочник по автономной миграции.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Что переносит USMT?

Статья • 29.01.2025 • Применяется к: ✅ Windows 11, ✅ Windows 10

Скрипты миграции по умолчанию

Средство миграции пользовательской среды (USMT) разработано таким образом, что ИТ-инженер может точно определить миграции с помощью языка сценариев **.xml** USMT. USMT предоставляет следующие примеры скриптов:

- **MigApp.XML** — правила для переноса параметров приложения.
- **MigDocs.XML** — правила, использующие вспомогающую функцию **MigXmlHelper.GenerateDocPatterns** , которая может использоваться для автоматического поиска документов пользователей на компьютере без необходимости создавать обширные пользовательские **миграции.xml** файлов.
- **MigUser.XML** — правила для переноса профилей пользователей и данных пользователей.

  `MigUser.xml` собирает все данные в профиле пользователя, а затем выполняет поиск других данных пользователя на основе расширения файла в большей части системы. Если данные не соответствуют ни один из этих критериев, данные не переносятся. Как правило, в этом файле описывается миграция ядра.

  Следующие данные не переносятся с `MigUser.xml` помощью :
  - Файлы за пределами профиля пользователя, которые не соответствуют одному из расширений файлов в `MigUser.xml`.
  - Списки управления доступом (ACL) для папок за пределами профиля пользователя.

Пользовательские данные

В этом разделе описываются пользовательские данные, которые USMT переносит по умолчанию с помощью `MigUser.xml` файла. Он также определяет, как переносить списки управления доступом (ACL).

- **Папки из каждого профиля пользователя.** При указании `MigUser.xml` файла USMT переносит все данные в профилях пользователя, включая следующие элементы папок:

- Документы.
- Видео.
- Музыка.
- Живопись.
- Файлы рабочего стола.
- Меню "Пуск".
- Параметры быстрого запуска.
- Избранное.

> **ⓘ Важно!**
>
> USMT не переносит макет меню "Пуск". Чтобы перенести меню "Пуск" пользователя, необходимо экспортировать и импортировать параметры с помощью командлетов `Export-StartLayout` Windows PowerShell и **Import-StartLayout**. Дополнительные сведения см. в статье Распространенные проблемы с USMT.

- **Папки из всех пользователей и общедоступных профилей.** `MigUser.xml` Если указан файл, USMT также переносит следующие данные из **общедоступного** профиля в Windows:
  - Общие документы
  - Общее видео
  - Общая музыка
  - Общие файлы рабочего стола
  - Общие изображения
  - Общее меню "Пуск"
  - Общее избранное
- **Типы файлов.** `MigUser.xml` Если файл указан, средство **ScanState** выполняет поиск на фиксированных дисках, собирает и переносит файлы с любым из следующих расширений:

`.accdb`, `.ch3`, `.csv`, `.dif`, `.doc*`, `.dot*`, `.dqy`, `.iqy`, `.mcw`, `.mdb*`, `.mpp`, `.one*`, `.oqy`, `.or6`, `.pot*`, `.ppa`, `.pps*`, `.ppt*`, `.pre`, `.pst`, `.pub`, `.qdf`, `.qel`, `.qph`, `.qsd`, `.rqy`, `.rtf`, `.scd`, `.sh3`, `.slk`, `.txt`, `.vl*`, `.vsd`, `.wk*`, `.wpd`, `.wps`, `.wq1`, `.wri`, `.xl*`, `.xla`, `.xlb`, `.xls*`

> ⓘ **Примечание**
>
> Звездочка (`*`) означает ноль или больше символов.

> ⓘ **Примечание**
>
> Расширения OpenDocument (`*.odt`, `*.odp`, `*.ods`), которые могут использовать приложения Microsoft Office, по умолчанию не переносятся.

- **Списки управления доступом.** USMT переносит списки управления доступом (ACL) для указанных файлов и папок с компьютеров под управлением Windows. Например, если файл с именем `File1.txt` , который доступен только для чтения для **User1** и для **чтения и записи** для **User2**, будет перенесен, эти параметры **по-прежнему** будут применяться на конечном компьютере после миграции.

  > ⓘ **Важно!**
  >
  > Чтобы перенести списки управления доступом, каталог для миграции должен быть указан в `MigUser.xml` файле. Использование шаблонов файлов, таких как *.doc, не приведет к переносу каталога. Исходные сведения ACL переносятся только при явном указании каталога. Например, `<pattern type="File">c:\test docs</pattern>`.

Компоненты операционной системы

USMT переносит компоненты операционной системы на конечный компьютер. Следующие компоненты переносятся по умолчанию с помощью файлов манифеста:

- Параметры специальных возможностей.
- "Адресная книга".

- Параметры командной строки.
- Обои для рабочего стола. [1]
- ФАЙЛЫ EFS.
- Избранное.
- Параметры папки.
- Шрифты.
- Членство в группах. USMT переносит параметры группы пользователей. Чтобы просмотреть группы, к которой принадлежит пользователь, выполните следующие действия.

  1. Щелкните правой кнопкой мыши меню Пуск и выберите **Пункт Управление компьютером**.
  2. В консоли "**Управление компьютером**" разверните узел **Системные инструменты**>**Локальные пользователи и Группы**>**Группы**.
  3. Проверьте отдельные группы в области результатов, чтобы узнать, какие пользователи относятся к каким группам.

  При выполнении автономной миграции необходимо использовать раздел **ProfileControl> в файле.<** `Config.xml`
- Параметры подключения к базе данных (ODBC) (Майкрософт).
- Параметры мыши и клавиатуры.
- Сопоставление сетевого диска.
- Сопоставление сетевых принтеров. [1]
- Автономные файлы. [1]
- Параметры телефона и модема. [1]
- Файлы подключения RAS и телефонной книги (PBK).
- Региональные параметры. [1]
- Удаленный доступ.
- Параметры панели задач. [1]
- Личные сертификаты пользователя (все).

- Почта Windows.
- Медиаплеер Windows. [1]
- Управление правами Windows.

[1] Эти параметры недоступны для автономной миграции. Дополнительные сведения см. в справочнике по автономной миграции.

> ⓘ **Важно!**
>
> Этот список может быть неполным. Могут быть перенесены дополнительные компоненты.

> ⓘ **Примечание**
>
> Некоторые параметры, такие как шрифты, не применяются средством **LoadState** до тех пор, пока не будет перезапущен конечный компьютер. По этой причине перезагрузите целевой компьютер после запуска средства **LoadState** .

Поддерживаемые приложения

Несмотря на то, что она не требуется для всех приложений, рекомендуется установить все приложения на целевом компьютере перед восстановлением пользовательского состояния. Установка приложений перед переносом параметров помогает убедиться, что установщики приложений не перезаписывают перенесенные параметры.

> ⓘ **Примечание**
>
> Версии установленных приложений должны совпадать на исходном и целевом компьютерах. USMT не поддерживает перенос параметров более ранней версии приложения на более позднюю версию, за исключением Microsoft Office.

> ⓘ **Примечание**
>
> USMT переносит только параметры, которые были изменены на исходном компьютере. Если параметр приложения не изменяется по умолчанию на

исходном компьютере, параметр может не переноситься.

При указании `MigApp.xml` файла USMT переносит параметры для определенных приложений, определенных `MigApp.xml` в файле. Обратитесь к файлу `MigApp.xml` для поддерживаемых приложений.

Что USMT не переносится

Ниже перечислены параметры, которые USMT не переносит. Если возникла проблема, которая не указана здесь, см. раздел Распространенные проблемы.

Параметры приложений

USMT не переносит следующие параметры приложения:

- Параметры для приложений Microsoft Store.
- Параметры из более ранних версий приложения. Версии каждого приложения должны совпадать на исходном и целевом компьютерах. USMT не поддерживает перенос параметров более ранней версии приложения на более позднюю версию, за исключением Microsoft Office. USMT может перейти с более ранней версии Microsoft Office на более позднюю версию.
- Параметры приложения и некоторые параметры операционной системы при создании локальной учетной записи. Например, если `/lac` указано для создания локальной учетной записи на конечном компьютере, USMT переносит данные пользователя, но не выполняет миграцию:
  - Некоторые параметры операционной системы. Переносятся только некоторые параметры операционной системы, такие как обои и параметры заставки.
  - Параметры приложения.

параметры Operating-System

USMT не переносит следующие параметры операционной системы.

- Локальные принтеры, связанные с оборудованием параметры, драйверы, пароли, двоичные файлы приложений, файлы синхронизации, DLL-файлы или другие исполняемые файлы.

- Разрешения для общих папок. После миграции все папки, к которым был предоставлен общий доступ на исходном компьютере, должны быть повторно переданы вручную.
- Перенос файлов и параметров между операционными системами с разными языками. Операционная система исходного компьютера должна соответствовать языку операционной системы на конечном компьютере.
- Настраиваемые значки для ярлыков могут не переноситься.

Кроме того, обратите внимание на следующие элементы:

- Запустите USMT из учетной записи с учетными данными администратора. В противном случае некоторые данные не переносятся. При запуске средств **ScanState** и **LoadState** они должны выполняться в режиме администратора из учетной записи с учетными данными администратора. Если USMT не выполняется в режиме администратора, в миграцию включается только профиль пользователя, вошедший в систему.
- Используйте параметр , `/localonly` чтобы исключить данные со съемных дисков и сетевых дисков, сопоставленных на исходном компьютере. Дополнительные сведения о том, что исключается при `/localonly` указании, см. в разделе Синтаксис ScanState.

Макет меню "Пуск"

USMT не переносит макет меню "Пуск". Чтобы перенести меню "Пуск" пользователя, необходимо экспортировать и импортировать параметры с помощью командлетов `Export-StartLayout` Windows PowerShell и **Import-StartLayout**. Дополнительные сведения см. в статье Распространенные проблемы с USMT.

Профили пользователей из Active Directory в Microsoft Entra ID

- USMT не поддерживает перенос профилей пользователей с устройств, присоединенных к домену Active Directory, на устройства, присоединенные к Microsoft Entra.
- USMT не поддерживает перенос профилей пользователей с устройств, присоединенных к Microsoft Entra, на устройства, присоединенные к домену Active Directory.

- USMT не поддерживает перенос профилей пользователей между Microsoft Entra присоединенными устройствами.
- USMT может работать при переносе профилей пользователей между Microsoft Entra устройствами с гибридным присоединением или между устройствами, присоединенными к домену Active Directory, и Microsoft Entra устройствами с гибридным присоединением, но это не тестируемый сценарий, поэтому не поддерживается.

Связанные статьи

- Планирование миграции.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Выбор типа хранилища миграции

Статья • 29.01.2025 • Применяется к: ✅ Windows 11, ✅ Windows 10

Одним из main рекомендаций по планированию миграции является определение типа хранилища миграции, который лучше всего соответствует потребностям организации. В рамках этих рекомендаций определите следующие элементы:

- Сколько места требуется для запуска компонентов средства миграции пользовательской среды (USMT) на исходном и целевом компьютерах.
- Сколько места требуется для создания и размещения хранилища миграции.
- Следует ли использовать локальную общую папку, сетевую папку или запоминающее устройство.
- Убедитесь, что целостность даты пользователя поддерживается путем шифрования хранилища миграции.

В этом разделе

Развернуть таблицу

Ссылка	Описание
Общие сведения о типах хранилищ миграции	Выберите тип хранилища миграции, который лучше всего подходит для потребностей организации и сценария миграции.
Оценка размера хранилища миграции	Оцените объем дискового пространства, необходимого для компьютеров в организации, на основе сведений об инфраструктуре организации.
Хранилище миграции с жесткой компоновкой	Узнайте о хранилищах миграции с жесткой привязкой и сценариях, в которых они используются.
Шифрование хранилища миграции	Сведения об использовании шифрования хранилища миграции для защиты целостности данных пользователей во время миграции.

Связанные статьи

- Планирование миграции
- Инструкции по средству миграции пользовательской среды (USMT)

Обратная связь

-

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Обзор типов хранилищ переноса

Статья • 29.01.2025 • Применяется к: ✅ Windows 11, ✅ Windows 10

При планировании миграции следует определить, какой тип хранилища миграции лучше всего соответствует потребностям организации. В рамках этих рекомендаций определите, сколько места требуется для запуска компонентов средства миграции пользовательской среды (USMT) на исходном и целевом компьютерах. Также необходимо определить пространство, необходимое для создания и размещения хранилища миграции, будь то локальный общий ресурс, сетевой ресурс или запоминающее устройство.

Типы хранилищ миграции

В этом разделе описываются три типа хранилища миграции, доступные в USMT.

Несжатый (UNC)

Несжатое хранилище миграции (UNC) — это несжатый каталог с зеркало изображением иерархии папок, которые переносятся. Каждый каталог и файл сохраняет те же разрешения на доступ, что и в локальной файловой системе. Windows Обозреватель можно использовать для просмотра этого типа хранилища миграции. Параметры хранятся в файле каталога, в котором также описывается восстановление файлов на конечном компьютере.

Сжатый

Сжатое хранилище миграции — это один файл образа, содержащий все переносимые файлы и файл каталога. Этот файл образа часто шифруется и защищен паролем, и его нельзя перемещать с помощью windows Обозреватель.

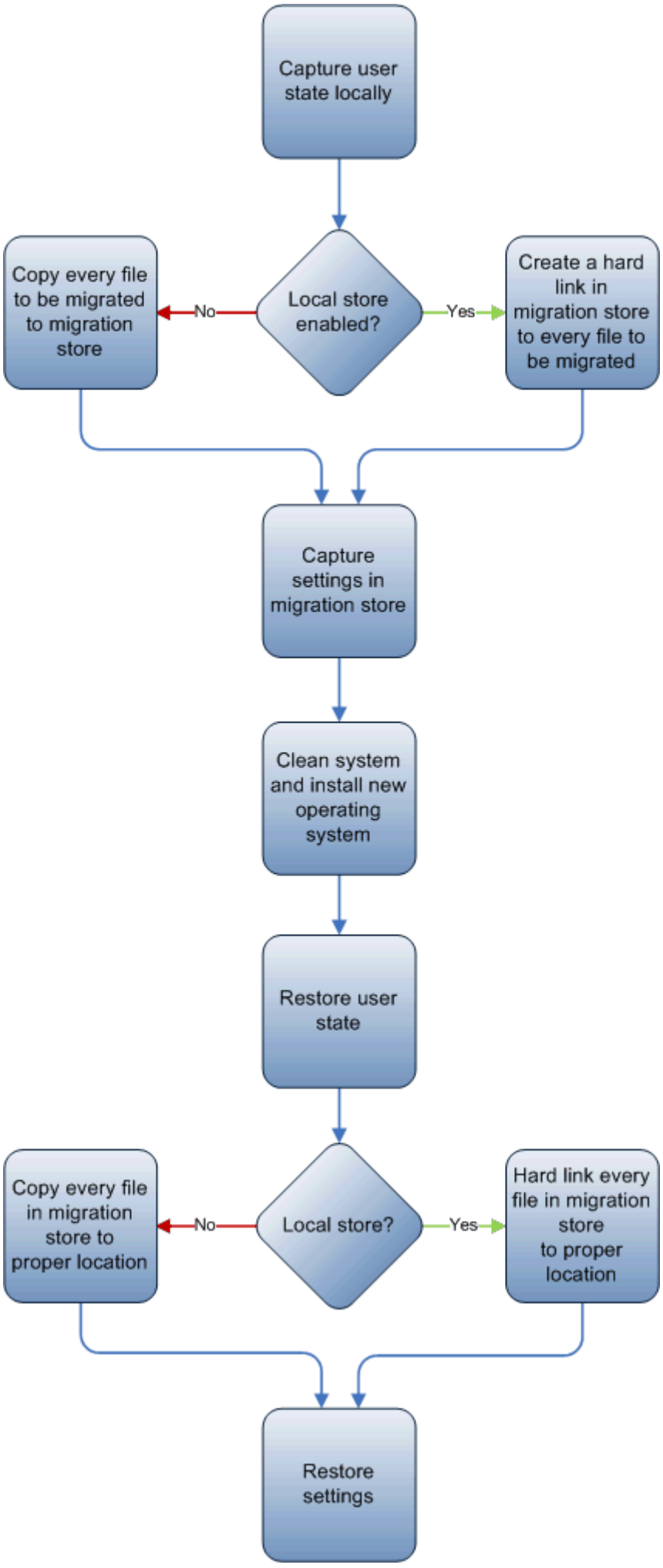
Hard-Link

Хранилище миграции с жесткой связью функционирует как карта, которая определяет, как коллекция битов на жестком диске "подключается" к файловой системе. Хранилище миграции с жесткой компоновкой USMT используется только в сценарии обновления компьютера. Хранилища миграции с жесткой компоновкой используются только в сценариях обновления, так как хранилище миграции с жесткой компоновкой поддерживается на локальном компьютере. Хранилище жесткой связи сохраняется на компьютере, пока старая операционная

система удаляется и устанавливается новая операционная система. Использование хранилища миграции с жесткой связью экономит пропускную способность сети и сводит к минимуму использование сервера, необходимого для выполнения миграции.

Параметр `/hardlink` командной строки используется для создания хранилища миграции с жесткой компоновкой, которое работает так же, как несжатое хранилище миграции. Файлы не дублируются на локальном компьютере при записи состояния пользователя. Они также не дублируются при восстановлении состояния пользователя. Дополнительные сведения см. в разделе Хранилище миграции с жесткой компоновкой.

На следующей блок-схеме показаны процедурные различия между локальным хранилищем миграции и удаленным хранилищем миграции. В этом примере для локального хранилища используется хранилище миграции с жесткой компоновкой.


Capture user state locally
Local store enabled?
No
Yes
Copy every file to be migrated to migration store
Create a hard link in migration store to every file to be migrated
Capture settings in migration store
Clean system and install new operating system
Restore user state
Local store?
No
Yes
Copy every file in migration store to proper location
Hard link every file in migration store to proper location
Restore settings

Локальное и удаленное хранилище

Если места достаточно и состояние пользователя переносится обратно на тот же компьютер, хранение данных на локальном устройстве обычно является лучшим вариантом для снижения затрат на хранилище сервера и проблем с производительностью сети. Данные также могут храниться локально либо в другой секции, либо на съемных устройствах, таких как USB-устройство флэш-памяти (UFD). Кроме того, данные могут храниться в секции, в которой выполняется повторное изображение, если данные можно защитить от удаления в процессе создания образа. Одним из примеров технологии создания образов, которая может хранить данные в переосмысленном разделе, является Microsoft Configuration Manager. Чтобы повысить производительность, храните данные на высокоскоростных дисках, использующих высокоскоростное сетевое подключение. Также рекомендуется убедиться, что миграция является единственной задачей, выполняемой сервером.

Если места на локальном диске недостаточно или при перемещении пользовательского состояния на другой компьютер, данные должны храниться удаленно, например в одном из следующих назначений:

- Общая папка.
- Съемный носитель.
- Непосредственно на конечном компьютере.

Пример:

1. Создание и совместное использование `C:\store` на конечном компьютере.
2. `ScanState.exe` Выполните команду на исходном компьютере и сохраните файлы и параметры в `\\<DestinationComputerName>\store`.
3. `LoadState.exe` Выполните команду на конечном компьютере и укажите `C:\Store` в качестве расположения хранилища.

При выполнении этого процесса файлы не нужно хранить на сервере.

> **ⓘ Важно!**
>
> По возможности пользователи должны хранить свои данные в папках `%UserProfile%\Documents` и `%UserProfile%\Application Data` . Если пользователи хранят свои данные в этих расположениях, снижается вероятность отсутствия

критически важных пользовательских данных, которые находятся в каталоге, для проверка который usMT не настроен.

Параметр командной строки /localonly

Этот параметр следует использовать для исключения данных со съемных и сетевых дисков, сопоставленных на исходном компьютере. Дополнительные сведения о том, что исключается при `/LocalOnly` указании, см. в разделе Синтаксис ScanState.

Связанные статьи

- Планирование миграции.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Оценка размера хранилища миграции

Статья • 29.01.2025 • Применяется к: ✅ Windows 11, ✅ Windows 10

Требования к дисковом пространству для миграции зависят от размера хранилища миграции и типа миграции. Объем дискового пространства, необходимого для компьютеров в организации, можно оценить на основе информации об инфраструктуре организации. Требования к дисковом пространству также можно вычислить с помощью средства **ScanState** .

Требования к месту на жестком диске

- **Хранилище**. Для миграций без жесткой компоновки убедитесь, что в расположении, где сохраняется хранилище, достаточно свободного места на диске. Хранилище содержит переносимые данные. Хранилище можно сохранить в другой секции, на внешнем запоминающее устройство, например НА USB-устройстве флэш-памяти или на сервере. Дополнительные сведения см. в разделе Выбор типа хранилища миграции.

- **Исходный компьютер**. Исходному компьютеру требуется достаточно свободного места для следующих элементов:

  - **Минимум места на жестком диске E250 мегабайт (МБ):** место требуется для поддержки операций средства миграции пользовательской среды (USMT), например для увеличения размера файла страницы. Если каждый том, участвующий в миграции, имеет формат NTFS, 250 МБ должно быть достаточно места, чтобы обеспечить успешное выполнение почти каждой миграции с жесткой компоновкой независимо от размера миграции. Средство USMT, которое собирает данные (ScanState), не создает хранилище миграции, если не доступно 250 МБ дискового пространства.

  - **Временное пространство для выполнения USMT**. Для работы средств USMT требуется дополнительное дисковое пространство. Это требование не включает минимальные 250 МБ, необходимые для создания хранилища миграции. Требуемый объем временного пространства можно вычислить с помощью средства **ScanState** .

  - **Хранилище миграции с жесткой компоновкой**. Не нужно оценивать размер хранилища миграции с жесткой компоновкой. Единственный случай, когда хранилище жесткой связи может быть большим, — это когда в системе существуют тома файлов, отличные от NTFS, и эти тома содержат переносимые данные.

- **Конечный компьютер**. Целевому компьютеру требуется достаточно свободного места для следующих компонентов:
  - **Операционная система**.
  - **Приложения**.
  - **Переносимые данные**. Переносимые данные включают файлы и сведения о реестре.
  - **Временное пространство для выполнения USMT**. Для работы средств USMT требуется дополнительное дисковое пространство. Требуемый объем временного пространства можно вычислить с помощью средства **ScanState** .

Вычисление требований к дисковом пространству с помощью средства ScanState

Средство **ScanState** можно использовать для вычисления требований к дисковом пространству для конкретной сжатой или несжатой миграции. Не нужно оценивать размер хранилища миграции для миграции с жесткой компоновкой, так как этот метод не создает отдельное хранилище миграции. Средство **ScanState** предоставляет требования к месту на диске для состояния компьютера на момент запуска средства. Состояние компьютера может меняться во время повседневного использования. По этой причине при планировании миграции используйте вычисления в качестве оценки.

Чтобы запустить средство **ScanState на исходном** компьютере с установленным USMT, выполните следующие действия:

1. Откройте командную строку с правами администратора.
2. Перейдите к средствам USMT. Например, введите:

   Командная строка Windows

   ```
   cd /d "C:\Program Files (x86)\Windows Kits\10.0\Assessment and Deployment Kit\User State Migration Tool\<architecture>"
   ```

   где< архитектура> — x86 или amd64.

3. Запустите средство **ScanState** , чтобы создать XML-отчет о требованиях к пространству. В командной строке введите:

Командная строка Windows

```
ScanState.exe <StorePath> /p:<path to a file>
```

Где:

- <*StorePath*> — это путь к каталогу, в котором сохраняется хранилище миграции.
- <*путь к файлу*> — это путь и имя файла, в которых сохраняется XML-отчет о требованиях к пространству.

Пример

Командная строка Windows

```
ScanState.exe c:\store /p:c:\spaceRequirements.xml
```

Хотя хранилище миграции не создается с помощью этой команды, *StorePath*> *по-прежнему*< является обязательным параметром.

Средство **ScanState** также позволяет оценить требования к дисковом пространству на основе настраиваемой миграции. Например, папку **Документы** может потребоваться перенести на конечный компьютер. Это условие можно указать в файле конфигурации при запуске средства **ScanState** . Дополнительные сведения см. в разделе Настройка XML-файлов USMT.

> ⓘ **Примечание**
>
> Чтобы сохранить функциональные возможности существующих приложений или скриптов, для которых требуется предыдущее поведение USMT, параметр по-прежнему `/p` доступен в USMT без указания пути к файлу. Дополнительные сведения см. в разделе **Параметры мониторинга**.

Отчет о требованиях к пространству содержит два элемента: <**storeSize**> и <**temporarySpace**>. Значение <**temporarySpace**> показывает дисковое пространство (в байтах), которое USMT использует для работы во время миграции, но не включает минимальные 250 МБ, необходимые для поддержки USMT. Значение <**storeSize**> показывает место на диске (в байтах), необходимое для размещения содержимого хранилища миграции на исходном и целевом компьютерах. В следующем примере показан отчет, созданный по `/p:`<*пути к файлу*>.

XML

```xml
<?xml version="1.0" encoding="UTF-8"?>
<PreMigration>
  <storeSize>
    <size clusterSize="4096">11010592768</size>
  </storeSize>
  <temporarySpace>
    <size>58189144</size>
  </temporarySpace>
</PreMigration>
```

Кроме того, USMT выполняет проверка соответствия требованиям для требуемого не менее 250 МБ доступного места на диске и не создает хранилище в случае сбоя проверка соответствия.

Оценка размера хранилища миграции

Определите, сколько места требуется для хранения перенесенных данных. Вычисления должны основываться на объеме электронной почты, личных документов и параметров системы для каждого пользователя. Лучший способ оценить требуемое пространство — обследовать несколько компьютеров, чтобы получить среднее значение для необходимого хранилища.

Объем необходимого места в хранилище зависит от локальных стратегий хранения, которые использует организация. Например, одним из ключевых элементов, определяющих размер наборов данных миграции, является хранилище электронной почты. Если электронная почта хранится централизованно, наборы данных меньше. Если электронная почта хранится локально, например файлы автономного хранения, наборы данных больше. Мобильные пользователи обычно имеют большие наборы данных, чем пользователи рабочей станции. Необходимо выполнить тесты и провести инвентаризацию сети, чтобы определить средний размер набора данных в организации.

> ⓘ **Примечание**
>
> Файл оценки пространства (`Usmtsize.txt`) можно создать для оценки размера хранилища с помощью устаревшего параметра командной `/p` строки.

При попытке определить, сколько дискового пространства требуется, учитывайте следующие проблемы:

- **Электронная почта**. Если пользователи имеют дело с большим объемом электронной почты или хранят почту на локальных компьютерах, а не на почтовом сервере, электронная почта может занимать столько же места на диске, сколько и все остальные файлы пользователей вместе взятые. Перед переносом пользовательских данных убедитесь, что пользователи, хранящие электронную почту, синхронизируют свои папки "Входящие" с почтовым сервером.

- **Пользовательские документы**. Часто все документы пользователя занимают менее 50 МБ места в зависимости от типа используемых файлов. Эта оценка предполагает типичную офисную работу, например текстовые документы и электронные таблицы. Эта оценка может существенно отличаться в зависимости от типов документов, которые использует организация. Например, архитектурная фирма, которая преимущественно использует файлы автоматизированного проектирования (CAD), требует больше места, чем юридическая фирма, которая в основном использует текстовые документы. Документы, которые пользователи хранят на файловых серверах с помощью таких механизмов, как перенаправление папок, не нужно переносить, если после миграции у пользователей будет доступ к этим расположениям.

- **Параметры пользовательской системы**: пяти мегабайтам достаточно места для сохранения параметров реестра. Однако это требование может меняться в зависимости от количества установленных приложений. Однако редко размер пользовательской части реестра превышает 5 МБ.

Связанные статьи

- Распространенные сценарии миграции.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Хранилище переноса с жесткой связью

Статья • 29.01.2025 • Применяется к: ✅ Windows 11, ✅ Windows 10

Хранилище миграции с жесткой связью позволяет выполнять миграцию на месте, когда на компьютере сохраняется все пользовательское состояние, а старая операционная система удаляется и устанавливается новая операционная система. Эта функция делает **хранилище миграции с жесткой компоновкой** наиболее подходящим для сценария обновления компьютера. Использование хранилища миграции с жесткой связью для сценария обновления компьютера значительно повышает производительность миграции и значительно сокращает использование жесткого диска, сокращает затраты на развертывание и обеспечивает совершенно новые сценарии миграции.

Когда следует использовать миграцию с жесткой компоновкой

Хранилище миграции с жесткой связью можно использовать, если запланированная миграция соответствует обоим из следующих критериев:

- Операционная система обновляется на существующем оборудовании вместо миграции на новые компьютеры.
- Операционная система обновляется на том же томе компьютера.

Хранилище миграции с жесткой связью нельзя использовать, если запланированная миграция включает в себя одну из следующих задач:

- Данные переносятся с одного компьютера на другой.
- Данные переносятся с одного тома на компьютере на другой том на том же компьютере, например с `C:` `D:` на .
- Диск, содержащий хранилище миграции, отформатируется или повторно секционируется за пределами программы установки Windows или во время установки Windows.

Основные сведения о миграции с жесткой связью

Хранилище миграции с жесткой компоновкой создается с помощью параметра `/hardlink` командной строки , и эквивалентно другим типам хранилищ миграции. Однако он отличается тем, что жесткие ссылки используются для хранения файлов, хранящихся на исходном компьютере во время миграции. Сохранение файлов на исходном компьютере устраняет избыточное дублирование файлов. Это также обеспечивает преимущества производительности и сокращение использования дисков, которые определяют этот сценарий.

При создании жесткой ссылки существующий файл получает еще один путь. Например, можно создать жесткую ссылку на `c:\file1.txt` . `c:\hard link\myFile.txt` Эти два пути относятся к одному и тому же файлу. Если `c:\file1.txt` объект открыт, то изменения, внесенные в файл, за которым следует сохраненный файл. Эти изменения отображаются при `c:\hard link\myFile.txt` открытии. Если `c:\file1.txt` файл удален, файл по-прежнему существует на компьютере как `c:\hardlink\myFile.txt`. Чтобы удалить файл, необходимо удалить обе ссылки на файл.

> ⓘ **Примечание**
>
> Жесткую ссылку можно создать только для файла на том же томе. Если хранилище миграции с жесткой компоновкой копируется на другой диск или внешнее устройство, файлы, а не ссылки, копируются, как в сценарии не сжатого хранилища миграции.

Дополнительные сведения о жестких ссылках см. в разделе Жесткие ссылки и соединения.

В большинстве аспектов хранилище миграции с жесткой компоновкой идентично несжатым хранилищам миграции. Хранилище миграции с жесткой компоновкой расположено в соответствии cScanState.exe **средства командной** строки. Содержимое хранилища можно просмотреть с помощью Windows Обозреватель. После создания его можно удалить или скопировать в другое расположение без изменения состояния пользователя. Восстановление хранилища миграции с жесткой привязкой аналогично восстановлению любого другого хранилища миграции. Однако, как и при создании хранилища, для хранения файлов на месте используется та же функциональность жесткой компоновки.

Рекомендуется удалить хранилище миграции с жесткой компоновкой после подтверждения успешной миграции файлов с помощью средства **LoadState** . Так как **LoadState** создает новые пути к файлам в новой установке операционной системы Windows, при удалении жестких ссылок в хранилище миграции удаляется

только один путь к файлам. Фактические файлы или пути к ним не удаляются из новой операционной системы.

> ⓘ **Важно!**
>
> `/c` При использовании параметра средство **LoadState** продолжает применять файлы при возникновении неустранимых ошибок. `/c` Если параметр используется, убедитесь, что в журналах не отображаются ошибки, прежде чем удалять хранилище миграции с жесткой связью, чтобы избежать потери данных.

Сохранение хранилища миграции с жесткой связью может привести к дополнительному потреблению дискового пространства или проблемам с некоторыми приложениями по следующим причинам:

- Приложения, предоставляющие статистику файловой системы, например используемое пространство и свободное место, могут неправильно сообщать эти статистические данные при наличии хранилища миграции с жесткой компоновкой. Файл может быть сообщен дважды из-за двух путей, ссылающихся на этот файл.
- Жесткая ссылка может потерять подключение к исходному файлу. Некоторые приложения сохраняют изменения в файле путем создания временного файла, а затем переименования исходного файла в имя файла резервной копии. Путь, который не использовался для открытия файла в этом приложении, продолжает ссылаться на неизмененные файлы. Неизмененные файлы, которые не используются, занимают больше места на диске. Хранилище миграции с жесткой связью должно быть создано непосредственно перед выполнением миграции. После создания хранилища приложения не следует использовать, чтобы убедиться, что переносятся последние версии всех файлов.
- Одновременное изменение файла с использованием разных путей может привести к повреждению данных.

> ⓘ **Важно!**
>
> Атрибут файла только для чтения для перенесенных файлов теряется при удалении хранилища миграции с жесткой компоновкой. Это связано с ограничением жестких ссылок файловой системы NTFS.

Сценарий миграции с жесткой связью

Например, организация решает развернуть последнюю поддерживаемую версию Windows на всех своих компьютерах. Каждый сотрудник хранит один и тот же компьютер, но операционная система на каждом компьютере будет обновлена.

1. Администратор запускает программу командной строки **ScanState** на каждом компьютере, указывая параметр командной `/hardlink` строки. Средство **ScanState** сохраняет пользовательское состояние в хранилище миграции с жесткой связью на каждом компьютере, повышая производительность за счет уменьшения дублирования файлов, за исключением определенных конкретных экземпляров.

   > ⓘ **Примечание**
   >
   > Корпорация Майкрософт рекомендует не создавать хранилище миграции с жесткой компоновкой, пока не будет выполнена миграция, чтобы перенести последние версии файлов. Программные приложения не следует использовать на компьютере после создания хранилища миграции до завершения миграции файлов с помощью **LoadState**.

2. На каждом компьютере администратор устанавливает стандартную операционную среду (SOE) организации, которая включает в себя последнюю поддерживаемую версию Windows и другие приложения, которые в настоящее время используются организацией.

3. Администратор запускает программу командной строки **LoadState** на каждом компьютере. Средство **LoadState** восстанавливает состояние пользователя на каждом компьютере.

> ⓘ **Примечание**
>
> Во время обновления присоединенного к домену компьютера профили пользователей, идентификатор безопасности которых не может быть разрешен, не будут перенесены. При использовании хранилища миграции с жесткой компоновкой это может привести к потере данных.

Сведения о хранилище миграции с жесткой компоновкой

В этом разделе содержатся сведения о хранилищах миграции с жесткой компоновкой.

Место на жестком диске

Параметр `/hardlink` командной строки продолжает создавать хранилище миграции, только если на жестком диске имеется 250 МБ свободного места. Если каждый том, участвующий в миграции, имеет формат NTFS, 250 МБ должно быть достаточно места, чтобы обеспечить успешное выполнение почти каждой жесткой миграции независимо от размера миграции.

Оценка размера хранилища с жесткой привязкой

Не нужно оценивать размер хранилища миграции с жесткой компоновкой, так как хранилище миграции с жесткой компоновкой на томе NTFS относительно невелико и требует гораздо меньше добавочного пространства, чем другие параметры хранилища. Оценка размера хранилища миграции полезна только в тех случаях, когда хранилище миграции велико. Единственный случай, когда локальное хранилище может быть большим при миграции с жесткой компоновкой:

- В системе существует файловая система, не относясь к NTFS.
- Файловая система, не относящаяся к NTFS, содержит данные, которые необходимо перенести.

Так как NTFS является форматом файловой системы по умолчанию для всех поддерживаемых в настоящее время версий Windows, такая ситуация является необычной.

Путь к хранилищу миграции на нескольких томах

На каждом томе NTFS создаются отдельные хранилища жесткой компоновки миграции, содержащие переносимые данные. В этом сценарии основное расположение хранилища миграции указывается в командной строке и должно быть томом операционной системы. Хранилища миграции с идентичными именами и именами каталогов создаются для каждого тома, содержащего переносимые данные. Пример

Командная строка Windows

```
ScanState.exe /hardlink c:\USMTMIG […]
```

При выполнении этой команды в системе, содержащей операционную систему на диске C: и данные пользователя на диске D: создаются хранилища миграции в следующих расположениях, при условии, что оба диска являются NTFS:

`C:\USMTMIG\`

`D:\USMTMIG\`

Диск, указанный в командной строке для хранилища миграции с жесткой компоновкой, имеет важное значение, так как он определяет место размещения **хранилища миграции master**. Хранилище **миграции master** — это место, где хранятся данные, переносимые с томов, отличных от NTFS. Этот том должен иметь достаточно места для хранения всех данных, поступающих из томов, отличных от NTFS. Как и в других сценариях, если хранилище миграции уже существует по указанному `/o` пути, необходимо использовать параметр для перезаписи существующих данных в хранилище.

Изменения расположения

Изменения расположения, которые перенаправляют перенесенное содержимое из одного тома в другой, негативно влияют на производительность миграции с жесткой компоновкой. Производительность зависит от того, что переносимые данные, которые должны находиться между системными томами, не могут оставаться в хранилище миграции с жесткой связью. Они должны быть скопированы по системным томам.

Перенос сертификатов и файлов шифруемой файловой системы (EFS)

Чтобы перенести файлы шифрованной файловой системы (EFS) в новую установку операционной системы на том же томе компьютера, укажите `/efs:hardlink` параметр в синтаксисе командной `ScanState.exe` строки.

Если файлы EFS восстанавливаются в `/efs:hardlink` другую секцию `/efs:copyraw`, вместо параметра следует использовать параметр . Жесткие ссылки можно создать только для файлов на том же томе. Для перемещения файлов в другую секцию во время миграции требуется создать копию файлов в новой секции. Параметр `/efs:copyraw` копирует файлы в новую секцию в зашифрованном формате.

Дополнительные сведения см. в разделах Перенос файлов и сертификатов EFS и Параметры зашифрованных файлов.

Перенос заблокированных файлов с помощью хранилища миграции с жесткой компоновкой

Если в приложении или операционной системе есть блокировка файла, файл обрабатывается по-разному при использовании хранилища миграции с жесткой компоновкой.

Файлы, заблокированные операционной системой, не могут оставаться на месте и должны быть скопированы в хранилище миграции с жесткой компоновкой. В результате выбор большого количества файлов операционной системы для миграции значительно снижает производительность при миграции с жесткой привязкой. Корпорация Майкрософт рекомендует не переносить файлы из `\Windows` каталога, что сводит к минимуму проблемы, связанные с производительностью.

Файлы, заблокированные приложением, обрабатываются так же при миграции с жесткой компоновкой, что и в других сценариях, когда служба теневого копирования томов не используется. Службу теневого копирования томов нельзя использовать при миграциях с жесткой компоновкой. Однако, изменив новый **<раздел HardLinkStoreControl>** в `Config.xml` файле, можно включить миграцию файлов, заблокированных приложением.

> **ⓘ Важно!**
>
> Существует несколько сценариев, в которых изменение **<раздела HardLinkStoreControl>** в `Config.xml` файле усложняет удаление хранилища миграции с жесткой компоновкой. В этих сценариях `UsmtUtils.exe` необходимо использовать для планирования удаления хранилища миграции при следующей перезагрузке.

XML-элементы в файле Config.xml

В новом разделе файла `Config.xml` можно настроить необязательную настройку некоторых действий миграции с жесткой компоновкой, представленных с параметром `/HardLink` .

⛶ Развернуть таблицу

Элемент	Описание
<Политики>	Этот элемент содержит элементы, описывающие политики, которым следует USMT при создании хранилища миграции.
<HardLinkStoreControl>	Этот элемент содержит элементы, описывающие обработку файлов во время создания хранилища миграции с жесткой компоновкой.
<fileLocked>	Этот элемент содержит элементы, описывающие обработку файлов, заблокированных для редактирования.
<createHardLink>	Этот элемент определяет стандартный шаблон MigXML, описывающий пути к файлам, в которых должны создаваться жесткие ссылки, даже если файл заблокирован для редактирования другим приложением. Синтаксис: `<createHardLink>` [шаблон] `</createHardLink>`
<errorHardLink>	Этот элемент определяет стандартный шаблон MigXML, описывающий пути к файлам, в которых не следует создавать жесткие ссылки, если файл заблокирован для редактирования другим приложением. `<errorHardLink>` [шаблон] `</errorHardLink>`

> **ⓘ Важно!**
>
> Параметр `/nocompress` должен использоваться с параметром `/HardLink` .

Следующий пример XML указывает, что файлы, заблокированные приложением в каталоге `\Users` , могут оставаться на месте во время миграции. Он также указывает, что заблокированные файлы, которые не находятся в каталоге `\Users` , должны привести к ошибке **Файл в использовании** . Важно соблюдать осторожность при указании путей с помощью **`<createhardlink>`** тега, чтобы свести к минимуму сценарии, которые затрудняют удаление хранилища миграции с жесткой связью.

XML

```
<Policies>
    <HardLinkStoreControl>
          <fileLocked>
            <createHardLink>c:\Users\* [*]</createHardLink>
            <errorHardLink>C:\* [*]</errorHardLink>
          </fileLocked>
```

```
    </HardLinkStoreControl>
</Policies>
```

Связанные статьи

- Планирование миграции.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Шифрование хранилища миграции

Статья • 29.01.2025 • Применяется к: ✅ Windows 11, ✅ Windows 10

В этой статье рассматриваются параметры средства миграции пользовательской среды (USMT) для шифрования хранилища миграции для защиты целостности пользовательских данных во время миграции.

Параметры шифрования USMT

USMT обеспечивает поддержку более надежных алгоритмов шифрования, называемых расширенной Standard шифрования (AES), в нескольких вариантах битового уровня. AES — это спецификация Национального института стандартов и технологий (NIST) для шифрования электронных данных.

Выбранный алгоритм шифрования должен быть указан как для команд, так `ScanState.exe` и `LoadState.exe` для команд, чтобы эти команды могли создавать или считывать хранилище во время шифрования и расшифровки. Новые алгоритмы шифрования можно указать в командной строке `ScanState.exe` и `LoadState.exe` с помощью `/encrypt` параметров командной строки :*encryption_strength* и `/decrypt`:*encryption_strength* . Все программные интерфейсы шифрования приложений (API), используемые USMT, доступны в поддерживаемых в настоящее время версиях Windows. Однако ограничения на экспорт могут ограничить набор алгоритмов, доступных для компьютеров в определенных языковых стандартах. Файл `UsmtUtils.exe` можно использовать, чтобы определить, какие алгоритмы шифрования доступны для языковых стандартов компьютеров до начала миграции.

В следующей таблице описаны параметры шифрования командной строки в USMT.

Развернуть таблицу

Компонент	Параметр	Описание
ScanState	**/шифровать**<*AES, AES_128, AES_192, AES_256, 3DES, 3DES_112*>	Этот параметр и аргумент указывают, что хранилище миграции зашифровано и какой алгоритм следует использовать. Если аргумент алгоритма не указан, средство **ScanState** использует алгоритм **3DES** .
LoadState	**/расшифровать**<*AES, AES_128, AES_192, AES_256, 3DES, 3DES_112*>	Этот параметр и аргумент указывают, что хранилище должно быть расшифровывается и какой алгоритм следует использовать. Если

Компонент	Параметр	Описание
		аргумент алгоритма не указан, средство **LoadState** использует алгоритм **3DES** .

> **ⓘ Важно!**
>
> Некоторые алгоритмы шифрования могут быть недоступны в некоторых системах. Доступные алгоритмы можно проверить, выполнив `UsmtUtils.exe` команду с параметром `/ec` . Дополнительные сведения см. в разделе Синтаксис UsmtUtils.

Связанные статьи

- Планирование миграции.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Определение того, что следует перенести

Статья • 29.01.2025 • Применяется к: ✅ Windows 11, ✅ Windows 10

По умолчанию средство миграции пользовательской среды (USMT) переносит элементы, перечисленные в разделе Что выполняет миграция USMT?, в зависимости от **.xml** указанных файлов миграции. Эти параметры по умолчанию часто достаточно для базовой миграции.

Однако при рассмотрении того, какие параметры следует перенести, также учитывайте:

- Какие параметры может настроить пользователь, если они есть.
- Какие параметры должны быть стандартизированы.

Многие организации используют миграцию как возможность создать и начать применять более управляемую среду. Некоторые параметры, которые пользователи могут настроить на неуправляемых компьютерах до миграции, можно заблокировать на новых управляемых компьютерах. Например, стандартные обои и конфигурация рабочего стола — это некоторые элементы, которые можно стандартизировать.

Чтобы снизить сложность и повысить стандартизацию, организация должна рассмотреть возможность создания *стандартной операционной среды (SOE)*. SOE — это сочетание оборудования и программного обеспечения, которое распространяется среди всех пользователей. Создание SOE означает выбор:

- Базовые показатели для всех компьютеров, включая стандартные драйверы оборудования.
- Основные функции операционной системы.
- Основные приложения для повышения производительности, особенно если они находятся под корпоративным лицензированием.
- Основные служебные программы.
- Стандартный набор функций безопасности, как описано в корпоративной политике организации.

Использование SOE может значительно упростить миграцию и снизить общие проблемы с развертыванием.

В этом разделе

Развернуть таблицу

Ссылка	Описание
Идентификация пользователей	Используйте параметры командной строки, чтобы указать, какие пользователи следует перенести и как они должны быть перенесены.
Определение параметров приложений	Определите, какие приложения необходимо перенести, и подготовьте список параметров приложений для переноса.
Определение параметров операционной системы	Используйте миграцию, чтобы создать новую стандартную среду на каждом из конечных компьютеров.
Определение типов файлов, файлов и папок	Для следующих элементов, которые необходимо перенести: • Типы файлов. • файлы. • Папки. • "Параметры". определите, где могут находиться эти элементы. Пример • Standard расположения ОС по умолчанию. • Расположения, указанные организацией. • Нестандартные расположения.

Связанные статьи

- Что переносит USMT?.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Идентификация пользователей

Статья • 29.01.2025 • Применяется к: ✅ Windows 11, ✅ Windows 10

Важно тщательно продумать и спланировать перенос пользователей. По умолчанию средство миграции пользовательской среды (USMT) переносит всех пользователей. Какие пользователи следует включить, необходимо указать с помощью командной строки. Пользователи не могут быть указаны в **файлах.xml** . Инструкции по переносу пользователей см. в разделе Перенос учетных записей пользователей.

Перенос локальных учетных записей

Перед переносом локальных учетных записей следует учитывать следующие элементы:

- **Локальные учетные записи, которые не на конечном компьютере, должны быть явно указаны, если они должны быть перенесены.** Если миграция локальных учетных записей и локальной учетной записи не существует на конечном компьютере, `/lac` при использовании `LoadState.exe` команды необходимо указать параметр . `/lac` Если параметр не указан, локальные учетные записи пользователей не переносятся.
- **Определите, следует ли включать учетные записи пользователей, новые для конечного компьютера.** Параметр `/lae` включает учетную запись, созданную с параметром `/lac` . Однако если отключенная локальная учетная запись создается только `/lac` с помощью параметра , локальный администратор должен включить учетную запись на конечном компьютере.
- **Будьте внимательны при указании пароля для локальных учетных записей.** Если локальная учетная запись создана с пустым паролем, любой пользователь может войти в нее на конечном компьютере. Если локальная учетная запись создана с паролем, пароль будет доступен всем пользователям, имеющим доступ к средствам командной строки USMT.

> ⓘ **Примечание**
>
> Если на компьютере есть несколько пользователей и с параметром указан `/lac` пароль, все перенесенные пользователи имеют один и тот же пароль.

Перенос учетных записей домена

Исходный и конечный компьютеры не должны быть подключены к домену для переноса профилей пользователей домена.

Параметры командной строки

USMT предоставляет несколько вариантов переноса нескольких пользователей на один компьютер. Следующие параметры командной строки определяют пользователей для миграции.

- **Указание пользователей.** Какие пользователи следует перенести, можно указать с помощью `/all` параметров , `/ui`, `/uel` и `/ue` с помощью средств командной строки **ScanState** и **LoadState** .

  > ⓘ **Важно!**
  >
  > Параметр `/uel` исключает пользователей на основе даты `Ntuser.dat` **последнего обновления** файла. Параметр `/uel` недопустим при автономной миграции.

- **Перемещение пользователей в другой домен.** Учетные записи пользователей можно переместить в другой домен с помощью `/md` параметра с помощью средства командной строки **LoadState** .

- **Создание локальных учетных записей.** Локальные учетные записи можно создать и включить с помощью `/lac` параметров и `/lae` с помощью средства командной строки **LoadState** .

- **Переименование учетных записей пользователей.** Учетные записи пользователей можно переименовать с помощью `/mu` параметра .

  > ⓘ **Примечание**
  >
  > По умолчанию, если имя пользователя не указано ни в одном из параметров командной строки, пользователь переносится.

Связанные статьи

- Определите, что следует перенести.

- Синтаксис ScanState.
- Синтаксис LoadState.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Определение параметров приложений

Статья • 29.01.2025 • Применяется к: ✅ Windows 11, ✅ Windows 10

Какие приложения и параметры необходимо перенести, следует определить при планировании миграции. Дополнительные сведения о создании пользовательского **файла.xml** для переноса параметров другого приложения см. в разделе Настройка XML-файлов USMT.

Приложения

Во-первых, создайте список приложений, которые необходимо перенести, и определите приоритеты. Может быть полезно просмотреть списки приложений и решить, какие приложения необходимо повторно развернуть, а какие из них следует прекратить. Часто то, как используется приложение и насколько сложно приложение, определяет приоритет перенесенных приложений.

Затем определите владельца приложения, который будет отвечать за каждое приложение. Определение владельца приложения необходимо, так как разработчики не являются экспертами по всем приложениям в организации. Владелец приложения должен иметь наибольший опыт работы с приложением. Владелец приложения предоставляет сведения о том, как организация устанавливает, настраивает и использует приложение.

Параметры приложений

Затем определите и найдите параметры приложения для миграции. Большая часть информации, необходимой для этого шага, можно получить при тестировании новых приложений на совместимость с новой операционной системой.

После завершения списка приложений для миграции просмотрите список и обратитесь к каждому владельцу приложения в списке параметров для переноса. Для каждого параметра определите, требуется ли переносить его или параметры по умолчанию являются достаточными. Затем определите, где находится параметр, например в реестре или в **файле.ini** . Затем рассмотрите следующие вопросы, чтобы определить, что необходимо сделать для успешной миграции параметра:

- Является ли целевая версия приложения более новой, чем исходная версия?
- Работают ли эти параметры с новой версией?

- Нужно ли перемещать или изменять параметры?
- Может ли процесс первого запуска заставить приложение отображаться так, как если бы оно уже выполнялось? Если это так, правильно ли это работает или нарушает работу приложения?

Ответив на эти вопросы, создайте пользовательский **файл.xml** для переноса параметров. Обратитесь к владельцу приложения для разработки тестовых случаев и определения типов файлов, которые необходимо перенести для приложения.

Поиск места хранения параметров

См . раздел Перенос параметров приложения и следуйте указаниям.

Связанные статьи

- Определите, что следует перенести.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Определение параметров операционной системы

Статья • 29.01.2025 • Применяется к: ✅ Windows 11, ✅ Windows 10

При планировании миграции необходимо определить параметры операционной системы, которые необходимо перенести. Кроме того, следует определить, в какой степени на каждом из компьютеров должна быть создана новая стандартная среда. Средство миграции пользовательской среды (USMT) включает перенос выбранных параметров и сохраняет значения по умолчанию для всех остальных. Параметры операционной системы включают следующие параметры:

- **Внешность**

  Фактор внешнего вида включает в себя такие элементы, как обои, цвета, звуки и расположение панели задач.

- **Действие**

  Фактор действия включает в себя такие элементы, как:
  - Частота повторения ключа.
  - При двойном щелчке папки она открывается в новом окне или в том же окне.
  - Независимо от того, открывается ли элемент при однократном или двойном щелчке.

- **Интернет**

  Интернет-фактор включает параметры, необходимые для подключения к Интернету, и управляет тем, как работает браузер. Параметры включают такие элементы, как URL-адрес домашней страницы, избранное, закладки, файлы cookie, параметры безопасности и параметры прокси-сервера. Эти параметры могут поддерживаться не во всех браузерах.

- **Mail**

  Коэффициент почты включает сведения, необходимые для подключения почтового сервера, файла подписи, представлений, правил почты, локальной почты и контактов. Эти параметры могут поддерживаться не во всех приложениях электронной почты.

Чтобы определить параметры для миграции, рассмотрите все предыдущие возможности миграции и результаты проведенных опросов и тестов. Также

рассмотрите количество обращений в службу поддержки, связанных с параметрами операционной системы из прошлого, и сможете обрабатывать их в будущем. Также определите, сколько новых функциональных возможностей операционной системы необходимо использовать.

Ниже указаны параметры, которые необходимо перенести:

- Параметры, позволяющие пользователям выполнять свою работу.
- Параметры, которые делают рабочую среду комфортной.
- Параметры, которые позволят сократить количество обращений в службу поддержки после миграции.

Несмотря на то, что перенос пользовательских настроек легко закрыть, следует учитывать фактор, который пользователи тратят время на восстановление таких элементов, как:

- Обои.
- Заставки.
- Другие настраиваемые функции пользовательского интерфейса.

Большинство пользователей не помнят, как применялись эти параметры. Хотя эти элементы не имеют решающего значения для успешной миграции, перенос этих элементов повышает производительность пользователей и повышает общую удовлетворенность процесса миграции.

> ⓘ **Примечание**
>
> Дополнительные сведения об изменении перенесенных параметров операционной системы см. в **статьях с инструкциями по средству миграции пользовательской среды (USMT)**.

Сведения о параметрах операционной системы, которые переносит USMT, см. в статье Что такое миграция USMT?

Связанные статьи

- Определите, что следует перенести.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Определение типов файлов, файлов и папок

Статья • 29.01.2025 • Применяется к: ✅ Windows 11, ✅ Windows 10

Если миграция планируется и `MigDocs.xml` не используется, необходимо определить типы файлов, файлы, папки и параметры, которые необходимо перенести. Во-первых, необходимо определить стандартные расположения файлов на каждом компьютере, например папку **"Документы"** `C:\Data` и расположения, указанные организацией, такие как `\\EngineeringDrafts`. Затем необходимо определить и найти нестандартные расположения. Для нестандартных расположений рассмотрите следующие элементы:

- **Типы файлов**. Определите, какие типы файлов необходимо включить и исключить из миграции. Этот список можно создать на основе распространенных приложений, используемых в организации. Приложения обычно используют определенные расширения имен файлов. Например, Microsoft Office Word в основном использует `.doc` расширение и `.docx` `.dotx` имя файла. Однако он также использует другие типы файлов, такие как шаблоны (`.dot` файлы), на менее частой основе.

- **Исключенные расположения**. Рассмотрите расположения на компьютере, которые должны быть исключены из миграции (например, `%WINDIR%` и **Program Files**).

- **Новые расположения**. Определите, куда следует перенести файлы на конечном компьютере, например папку **Документы** , назначенную папку или папку, соответствующую имени файлов и расположению на исходном компьютере. Например, общие данные могут существовать на исходном компьютере или документы за пределами профилей пользователей в исходной системе, возможно, потребуется очистить. Определите все данные, которые необходимо перенаправить в новое расположение на этапе применения. Перенаправление можно выполнить с помощью правил изменения расположения.

После проверки файлов и типов файлов, с которыми пользователи регулярно работают, найдите файлы и типы файлов. Файлы могут сохраняться в одной папке или разбросаны по диску. Хорошей отправной точкой для поиска типов файлов для включения является просмотр зарегистрированных типов файлов на компьютере.

Чтобы найти зарегистрированные типы файлов на компьютере с поддерживаемой версией Windows, выполните следующие действия:

1. Щелкните правой кнопкой мыши **меню "Пуск"** и выберите **Параметры**.
2. Когда откроется окно **Параметры** , выберите **Приложения**.
3. Выберите **Приложения по умолчанию**.
4. Прокрутите вниз и выберите **Выбрать значения по умолчанию по типу файлов** или **Выберите приложения по умолчанию по типу файлов**.
5. В открывавшемся окне отображаются зарегистрированные типы файлов.

Дополнительные сведения об изменении типов файлов, файлов и папок, которые переносятся при `MigUser.xml` указании файла, см. в статьях с инструкциями по средству миграции пользовательской среды (USMT).

Связанные статьи

- Определите, что следует перенести.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Тестирование миграции

Статья • 29.01.2025 • Применяется к: ✅ Windows 11, ✅ Windows 10

Всегда тестируйте план миграции в управляемой лабораторной среде перед его развертыванием во всей организации. В тестовой среде для каждого типа операционной системы, из которой переносятся данные, требуется по крайней мере один компьютер.

После тестирования всего процесса миграции на одном компьютере под управлением каждой из исходных операционных систем организации выполните пилотную миграцию с небольшой группой пользователей. После переноса нескольких типичных пользовательских состояний в промежуточное хранилище обратите внимание на требуемое пространство и соответствующим образом настройте начальные вычисления. Дополнительные сведения об оценке пространства, необходимого для миграции, см. в разделе Оценка размера хранилища миграции. Сведения о параметрах реестра и расположении файлов может потребоваться изменить в файлах правил миграции. Если изменения внесены, протестируйте миграцию еще раз и убедитесь, что все данные и параметры перенесены должным образом. Пилотная миграция также дает возможность протестировать оценки пространства для промежуточного хранилища.

Если при тестовой миграции возникают какие-либо ошибки, **просмотрите журналы ScanState** и **LoadState** , чтобы получить точный код возврата средства миграции пользовательской среды (USMT) и связанные с ними сообщения об ошибках или сообщение об ошибке интерфейса прикладного программирования (API) Windows. Дополнительные сведения о кодах возврата USMT и сообщениях об ошибках см. в разделе Коды возврата. Дополнительные сведения о любых перечисленных кодах системных ошибок **Windows** можно получить, введя в окне командной строки следующую команду:

Командная строка Windows

```
net.exe helpmsg <error_number>
```

где *<error_number>* — номер кода ошибки, сформированный сообщением об ошибке. Дополнительные сведения о системных кодах ошибок см. в разделе Коды системных ошибок (0–499).

В большинстве случаев журналы **ScanState** и **LoadState** указывают, почему миграция USMT завершается сбоем. Корпорация Майкрософт рекомендует

использовать параметр `/v:5` при тестировании миграции. Этот уровень детализации можно изменить в рабочей миграции. Снижение уровня детализации может затруднить диагностику сбоев, возникающих во время миграции рабочей среды. Более высокий уровень детализации можно использовать, если файлы журнала должны выводить данные для перехода в отладчик.

> ⓘ **Примечание**
>
> При запуске средств **ScanState** и **LoadState** с параметром `/v:5` создается подробный файл журнала. Хотя этот параметр делает файл журнала большим, он полезен при определении места возникновения ошибок миграции.

После проверки пилотной миграции, успешной миграции указанных файлов и параметров, USMT готов к использованию в среде для переноса данных. Например, использование USMT с Microsoft Configuration Manager. Дополнительные сведения см. в разделе [Управление состоянием пользователя в Configuration Manager]/(mem/configmgr/osd/get-started/manage-user-state).

> ⓘ **Примечание**
>
> В целях тестирования можно создать несжатое хранилище с помощью `/hardlink /nocompress` параметра . Если сжатие отключено, средство **ScanState** сохраняет файлы и параметры в скрытой папке **с именем File** по адресу `<StorePath>\USMT`. Несжатое хранилище можно использовать для просмотра хранимых USMT или устранения проблемы. Для файлов также можно запустить антивирусную программу. Кроме того, для устранения проблем с миграцией можно использовать следующие элементы:
>
> - Параметр `/listfiles` командной строки.
> - Журнал диагностики, в который перечислены собранные файлы.

Связанные статьи

- Планирование миграции.
- Файлы журнала.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Синтаксис командной строки средства миграции пользовательской среды (USMT)

Статья • 29.01.2025 • Применяется к: ✅ Windows 11, ✅ Windows 10

Средство миграции пользовательской среды (USMT) переносит пользовательские файлы и параметры во время крупных развертываний Windows. Чтобы улучшить и упростить процесс миграции, USMT записывает параметры рабочего стола, сети и приложения в дополнение к файлам пользователя. Затем USMT переносит эти элементы в новую установку Windows.

В этом разделе

Развернуть таблицу

Ссылка	Описание
Синтаксис **ScanState**	Списки параметры командной строки для использования средства **ScanState**.
Синтаксис LoadState	Списки параметры командной строки для использования средства **LoadState**.
Синтаксис UsmtUtils	Списки параметры командной строки для использования средства UsmtUtils.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Синтаксис ScanState

Статья • 29.01.2025 • Применяется к: ✅ Windows 11, ✅ Windows 10

Команда `ScanState.exe` используется в средстве миграции пользовательской среды (USMT) для сканирования исходного компьютера, сбора файлов и параметров и создания хранилища. В этой статье рассматривается `ScanState.exe` синтаксис команды и доступные с ним параметры.

Перед началом

Перед выполнением `ScanState.exe` команды обратите внимание на элементы:

- Чтобы обеспечить миграцию всех параметров операционной системы, выполните `ScanState.exe` команды в режиме администратора из учетной записи с учетными данными администратора.
- Если хранилище миграции зашифровано, требуется ключ шифрования или путь к файлу с ключом шифрования. Обязательно запишите ключ или расположение файла ключа, так как эти сведения не хранятся в хранилище миграции. Эти сведения необходимы при выполнении `LoadState.exe` команды для расшифровки хранилища миграции или при необходимости использования служебной программы восстановления. Неправильный или отсутствующий ключ или файл ключа приводит к сообщению об ошибке.
- Сведения о требованиях к программному обеспечению для выполнения команды см. в `ScanState.exe` разделе Требования USMT.
- Если не указано иное, используйте каждый параметр только один раз при запуске средства в командной строке.
- Учетные записи домена можно собирать без доступа к контроллеру домена на исходном компьютере. Эта функция доступна без дополнительной настройки.
- В таблице Несовместимые параметры командной строки перечислены параметры, которые можно использовать вместе, а какие параметры командной строки несовместимы.
- Расположение каталога, в котором сохраняется хранилище миграции, исключается из сканирования. Например, если хранилище миграции

сохраняется в корне диска D, диск D и все его подкаталоги исключаются из сканирования.

Синтаксис

В этом разделе объясняется синтаксис и использование параметров командной строки, доступных при использовании `ScanState.exe` команды . Параметры можно указать в любом порядке. Если параметр содержит параметр, можно использовать двоеточие или разделитель пробела.

Синтаксис `ScanState.exe` команды:

> ScanState.exe [*StorePath*] [/apps] [/ppkg:*FileName*] [/i:[*Path*\]*FileName*] [/o] [/v:*VerbosityLevel*] [/nocompress] [/localonly] [/encrypt /key:*KeyString*|/keyfile: [Path\]*Имя_файла*] [/l:[*Path*\]*Имя_файла*] [/progress:[*Path*\]*Имя_файла*] [/r:*TimesToRetry*] [/w:*SecondsBeforeRetry*] [/c] [/p] [/all] [/ui:[*Имя_доменаИмя_*| компьютера\]*Имя_пользователя*] [/ue:[*имя_домена Имя_*| *компьютера*\]*Имя_пользователя*] [/uel:*NumberOfDays*|*YYYY/MM/DD*|0] [/efs:abort|skip|decryptcopy|copyraw] [/genconfig:[*Path*\]*FileName*[/config: [*Path*\]*FileName*] [/?|справка]

Например, чтобы создать `Config.xml` файл в текущем каталоге, используйте:

Командная строка Windows

```
ScanState.exe /i:MigApp.xml /i:MigDocs.xml /genconfig:Config.xml /v:13
```

Чтобы создать зашифрованное хранилище с помощью `Config.xml` файла и миграции по умолчанию **.xml** файлов, используйте следующую команду:

`ScanState.exe \\server\share\migration\mystore /i:MigApp.xml /i:MigDocs.xml /o /config:Config.xml /v:13 /encrypt /key:"mykey"`

Варианты хранения

Развернуть таблицу

Параметр Command-Line	Описание
StorePath	Указывает папку, в которой сохраняются файлы и параметры. *StorePath* не может быть `C:\`. Параметр *StorePath* должен быть указан в команде `ScanState.exe` , за исключением случаев, когда используется `/genconfig` параметр . Невозможно указать несколько расположений *StorePath* .
/Приложения	Проверяет образ на наличие приложений и включает их и связанные с ними параметры реестра.
/ppkg [<*Имя_*>*файла*]	Экспортирует в определенное расположение файла.
/o	Требуется для перезаписи всех существующих данных в хранилище или `Config.xml` файле миграции. Если этот параметр не указан, команда завершается ошибкой `ScanState.exe` , если хранилище миграции уже содержит данные. Этот параметр нельзя использовать более одного раза в командной строке.
/vsc	Этот параметр позволяет службе теневого копирования томов переносить файлы, которые заблокированы или используются. Этот параметр командной строки устраняет большинство ошибок блокировки файлов, которые обычно возникают в **<разделе ErrorControl>** . Этот параметр используется только с исполняемым файлом **ScanState** и не может сочетаться с параметром `/hardlink` .
/hardlink	Позволяет создать хранилище миграции с жесткой компоновкой в указанном расположении. Параметр `/nocompress` должен быть указан с параметром `/hardlink` .
/encrypt [{**/key:** <*KeyString*> | **/keyfile**: <*file*>]}	Шифрует хранилище указанным ключом. Шифрование отключено по умолчанию. При использовании этого параметра ключ шифрования необходимо указать одним из следующих способов: • `/key`: *KeyString* указывает ключ шифрования. Если в *KeyString* есть пробел, *KeyString* должен быть заключен в кавычки (`"`). • `/keyfile`: *FilePathAndName* указывает текстовый файл (`.txt`), содержащий ключ шифрования. *KeyString* рекомендуется содержать не менее восьми символов, но не может превышать 256 символов. Параметры `/key` и `/keyfile` нельзя использовать в одной командной строке. Параметры `/encrypt` и `/nocompress` нельзя использовать в одной командной строке.

Параметр Command-Line	Описание
	Важно! Будьте внимательны при использовании `/key` параметров или `keyfile` . Например, любой пользователь, имеющий доступ к сценариям, выполняющим `ScanState.exe` команду с этими параметрами, также имеет доступ к ключу шифрования. В следующем примере показана `ScanState.exe` команда и `/key` параметр: `ScanState.exe /i:MigDocs.xml /i:MigApp.xml \server\share\migration\mystore /encrypt /key:mykey`
/encrypt: *<EncryptionStrength>*	Параметр `/encrypt` принимает параметр командной строки для определения надежности шифрования, используемой для шифрования хранилища миграции. Дополнительные сведения о поддерживаемых алгоритмах шифрования см. в разделе Шифрование хранилища миграции.
/nocompress	Отключает сжатие данных и сохраняет файлы в скрытой папке с именем "Файл" в *StorePath*\USMT. Сжатие включено по умолчанию. Объединение `/nocompress` параметра с параметром `/hardlink` создает хранилище миграции с жесткой компоновкой. Несжатое хранилище можно использовать для просмотра хранимых USMT, устранения неполадок или запуска антивирусной программы для файлов. Этот параметр следует использовать только в средах тестирования. Корпорация Майкрософт рекомендует использовать сжатое хранилище во время миграции рабочей среды, если только параметр не объединяется `/nocompress` с параметром `/hardlink` . Параметры `/nocompress` и `/encrypt` не могут использоваться вместе в одной инструкции в командной строке. Однако при переносе `LoadState.exe` несжатого хранилища команда переносит каждый файл непосредственно из хранилища в правильное расположение на конечном компьютере без временного расположения. Пример: `ScanState.exe /i:MigDocs.xml /i:MigApp.xml \server\share\migration\mystore /nocompress`

Выполнение команды ScanState в автономной системе Windows

Команду `ScanState.exe` можно выполнить в среде предустановки Windows (WinPE). Кроме того, USMT поддерживает миграцию из предыдущих установок Windows, содержащихся в каталогах **Windows.old** . Автономный каталог может быть каталогом Windows при выполнении `ScanState.exe` команды в WinPE или каталогом **Windows.old** при выполнении `ScanState.exe` команды в Windows.

Выполнение команды в автономном `ScanState.exe` образе Windows имеет несколько преимуществ, в том числе:

- **Улучшенная производительность.**

  Так как WinPE — это тонкая операционная система, количество работающих служб меньше. В этой среде `ScanState.exe` команда имеет больше доступа к локальным аппаратным ресурсам, что позволяет **ScanState** выполнять операции миграции быстрее.

- **Упрощенный процесс комплексного развертывания.**

  Перенос данных из **Windows.old** упрощает комплексный процесс развертывания, позволяя выполнять процесс миграции после установки новой операционной системы.

- **Улучшено успешное выполнение миграции.**

  Коэффициент успешного выполнения миграции увеличивается из-за следующих способов:
  - Файлы не блокируются для редактирования в автономном режиме.
  - WinPE предоставляет администратору доступ к файлам в автономной файловой системе Windows, устраняя необходимость в доступе уровня администратора к сетевой системе.

- **Возможность восстановления с компьютера, который не загружается.**

  Возможно, можно восстановить и перенести данные с компьютера, который не загружается.

Варианты автономной миграции

Развернуть таблицу

Параметр Command-Line	Определение
/offline:"*путь к файлу Offline.xml*"	Этот параметр используется для определения пути к автономному **.xml** файлу, который может указывать другие параметры автономной миграции. Например, при миграции требуется автономный каталог Windows или любой домен или перенаправление папок.
/offlinewindir:"*путь к каталогу Windows*"	Этот параметр указывает автономный каталог Windows, из который `ScanState.exe` команда собирает состояние пользователя. Автономный каталог может быть **Windows.old** при выполнении `ScanState.exe` команды в Windows или каталогОм Windows при выполнении `ScanState.exe` команды в WinPE.
/offlinewinold:"*Каталог Windows.old*"	Этот параметр командной строки включает режим автономной миграции и запускает миграцию из указанного расположения. Этот параметр предназначен только для использования в сценариях миграции **Windows.old** , когда миграция выполняется из каталога **Windows.old** .

Параметры правил миграции

USMT предоставляет следующие параметры, чтобы указать, какие файлы следует перенести.

Развернуть таблицу

Параметр Command-Line	Описание
/i: [*путь*]*Имя_файла*	**(включая)** Указывает **файл.xml** , содержащий правила, определяющие, какое состояние пользователя, приложения или системы требуется перенести. Этот параметр можно указать несколько раз, чтобы включить все **файлы.xml** (`MigApp.xml`, и `MigDocs.xml` все созданные пользовательские **.xml** файлы). *Путь* может быть относительным или полным. Если переменная *Path* не указана, *имя_файла* должно находиться в текущем каталоге. Дополнительные сведения о том, какие файлы следует указать, см. в разделе "XML-файлы" статьи Часто задаваемые вопросы .
/genconfig: [*путь*]*Имя_файла*	(Создание **Config.xml**) Создает необязательный `Config.xml` файл, но не создает хранилище миграции. Чтобы убедиться, что этот файл содержит все, что

Параметр Command-Line	Описание
	необходимо перенести, создайте этот файл на исходном компьютере, который содержит все: • Компоненты • Приложения • settings • присутствует на конечных компьютерах. Кроме того, при указании этого параметра следует указать другие **.xml** файлов миграции с помощью параметра **/i** . После создания этого файла его можно использовать с командой `ScanState.exe` с помощью параметра **/config** . Единственными параметрами, которые можно указать с помощью этого параметра, являются `/i` параметры , `/v` и `/l` . Невозможно указать *StorePath*, так как `/genconfig` параметр не создает хранилище. *Путь* может быть относительным или полным. Если переменная *Path* не указана, *fileName* создается в текущем каталоге. Примеры: • В следующем примере создается `Config.xml` файл в текущем каталоге: `ScanState.exe /i:MigApp.xml /i:MigDocs.xml /genconfig:Config.xml /v:13`

/config: [*путь*]*Имя_файла*	Указывает `Config.xml` файл, который `ScanState.exe` команда должна использовать для создания хранилища. Этот параметр нельзя использовать более одного раза в командной строке. *Путь* может быть относительным или полным. Если переменная *Path* не указана, *имя_файла* должно находиться в текущем каталоге.
	
	В следующем примере создается хранилище с помощью `Config.xml` файлов , `MigDocs.xml` и `MigApp.xml` :
	`ScanState.exe \server\share\migration\mystore /config:Config.xml /i:MigDocs.xml /i:MigApp.xml /v:13 /l:ScanState.log`
	
	В следующем примере файлы и параметры переносятся на конечный компьютер с помощью `Config.xml` файлов , `MigDocs.xml` и `MigApp.xml` :
	`LoadState.exe \server\share\migration\mystore /config:Config.xml /i:MigDocs.xml /i:MigApp.xml /v:13 /l:LoadState.log`

/auto:*путь к файлам скриптов*	Этот параметр позволяет указать расположение файлов по умолчанию **.xml** . Если путь не указан, USMT ссылается на каталог, в котором

Параметр Command-Line	Описание
	находятся двоичные файлы USMT. Этот `/auto` параметр имеет тот же эффект, что и при использовании следующих параметров: `/i:MigDocs.xml /i:MigApp.xml /v:5`.
/genmigxml:*путь к файлу*	Этот параметр указывает, что `ScanState.exe` команда должна использовать средство поиска документов для создания и экспорта **файла.xml** , определяющего способ переноса всех файлов на компьютере, на котором `ScanState.exe` выполняется команда.
/localonly	Переносит только файлы, хранящиеся на локальном компьютере, независимо от правил в **.xml** файлов, указанных в командной строке. Этот параметр следует использовать для исключения данных со съемных дисков на исходном компьютере и при наличии сетевых дисков, сопоставленных на исходном компьютере. Примерами съемных дисков являются USB-устройства флэш-памяти (UFD) и некоторые внешние жесткие диски. `/localonly` Если параметр не указан, команда `ScanState.exe` копирует файлы с этих съемных или сетевых дисков в хранилище. `/localonly` исключает все, что не считается фиксированным диском в ОС. В некоторых случаях большие внешние жесткие диски считаются фиксированными. Эти диски можно явно исключить из миграции с помощью пользовательского **файла.xml** . Дополнительные сведения об исключении всех файлов на определенном диске см. в разделе Исключение файлов и параметров. Параметр `/localonly` командной строки включает или исключает данные при миграции, указанные в следующих местах хранения: • **Съемные диски, такие как USB-устройство флэш-памяти** — исключены • **Сетевые диски** — исключены • **Фиксированные диски** — включено

Параметры мониторинга

USMT предоставляет несколько вариантов, которые можно использовать для анализа проблем, возникающих во время миграции.

> ⓘ **Примечание**

Журнал **ScanState** создается по умолчанию, но имя и расположение журнала можно указать с помощью параметра **/l** .

Развернуть таблицу

Параметр Command-Line	**Описание**
/listfiles:<FileName>	Параметр `/listfiles` командной строки можно использовать вместе с командой `ScanState.exe` для создания текстового файла со списком всех файлов, включенных в миграцию.
/l:[*путь*]*Имя_файла*	Указывает расположение и имя журнала **ScanState** . Файлы журнала не могут храниться в *StorePath*. *Путь* может быть относительным или полным. Если переменная *Path* не указана, журнал создается в текущем каталоге. Параметр `/v` можно использовать для настройки объема выходных данных. `ScanState.exe` Если команда выполняется из ресурса общей сети, `/l` необходимо указать параметр, иначе usmt завершается ошибкой со следующей ошибкой: ***USMT не удалось создать файлы журналов*** Чтобы устранить эту проблему, обязательно укажите `/l` параметр при запуске `ScanState.exe` из общего сетевого ресурса.
/v:<*VerbosityLevel*>	**(Детализация)** Включает подробные выходные данные в файле журнала **ScanState** . Значение по умолчанию — 0. Для *verbosityLevel* можно задать один из следующих уровней: • **0** — включены только ошибки и предупреждения по умолчанию. • **1** — включает подробные выходные данные. • **4** . Включает вывод ошибок и состояния. • **5** . Включает подробные выходные данные и выходные данные состояния. • **8** . Включает вывод ошибок в отладчик. • **9** . Включает подробные выходные данные в отладчик. • **12** . Включает вывод ошибок и состояния в отладчик. • **13** . Включает подробные, состояние и выходные данные отладчика. Пример

Параметр Command-Line	Описание
	`ScanState.exe \server\share\migration\mystore /v:13 /i:MigDocs.xml /i:MigApp.xml`
/progress: [*Path*]*Имя_файла*	Создает необязательный журнал выполнения. Файлы журнала не могут храниться в *StorePath*. *Путь* может быть относительным или полным. Если переменная *Path* не указана, *fileName* создается в текущем каталоге. Пример: `ScanState.exe /i:MigApp.xml /i:MigDocs.xml \server\share\migration\mystore /progress:Progress.log /l:scanlog.log`
/c	Если указан этот параметр, `ScanState.exe` команда продолжает выполняться, даже если возникают неустранимые ошибки. Все файлы или параметры, вызывающие ошибку, регистрируются в журнале выполнения. Например, если есть большой файл, который не помещается в хранилище, `ScanState.exe` команда регистрирует ошибку и продолжает миграцию. Кроме того, если файл открыт или используется приложением, USMT не сможет перенести файл и регистрирует ошибку. Без параметра `/c` `ScanState.exe` команда завершает работу при первой ошибке. Раздел <**ErrorControl**> в `Config.xml` файле можно использовать, чтобы указать, какие ошибки чтения и записи файла или реестра можно безопасно игнорировать и которые могут привести к сбою миграции. Это преимущество в `Config.xml` файле позволяет параметру командной `/c` строки безопасно пропускать все ошибки ввода-вывода в среде. Кроме того, параметр `/genconfig` теперь создает пример < раздела **ErrorControl**>, который включается путем указания сообщений об ошибках и требуемого `Config.xml` поведения в файле.
/r:<*TimesToRetry*>	**(Повторите попытку)** Указывает количество повторных попыток при возникновении ошибки при сохранении пользовательского состояния на сервере. Значение по умолчанию — три раза. Этот параметр полезен в средах, где сетевое подключение не является надежным. При хранении пользовательского состояния параметр не может восстановить данные, `/r` потерянные из-за сбоя оборудования сети, например неисправного или отключенного сетевого кабеля, или при сбое подключения к виртуальной частной сети (VPN). Вариант повтора предназначен для больших, загруженных сетей, где

Параметр Command-Line	Описание
	подключение является удовлетворительным, но задержка связи является проблемой.
/w: *<SecondsBeforeRetry>*	**(Подождите)** Указывает время ожидания (в секундах) перед повтором операции с сетевым файлом. Значение по умолчанию — 1 секунда.
/p:*<pathToFile>*	При выполнении `ScanState.exe` команды создается **файл.xml** по указанному пути. Этот **файл.xml** содержит улучшенные оценки пространства для хранилища миграции. В следующем примере показано, как создать этот **файл.xml** : `ScanState.exe C:\MigrationLocation [additional parameters] /p:"C:\MigrationStoreSize.xml"` Дополнительные сведения см. в статье Оценка размера хранилища миграции. Чтобы сохранить функциональные возможности существующих приложений или скриптов, для которых требуется предыдущее поведение USMT, `/p` можно использовать параметр без указания *pathtoafile* в USMT. Если указан только `/p` параметр, оценки дискового пространства создаются так же, как и в выпусках USMT 3.x.
/? или **/help**	Отображает справку в командной строке.

Параметры пользователя

По умолчанию переносятся все пользователи. Единственный способ указать, какие пользователи следует включать и исключать, — использовать следующие параметры. Пользователи не могут быть исключены из **миграции.xml** файлов или с помощью `Config.xml` файла. Дополнительные сведения см. в разделах Определение пользователей и Перенос учетных записей пользователей.

Развернуть таблицу

Параметр Command-Line	Описание
/все	Переносит всех пользователей на компьютере. USMT переносит все учетные записи пользователей на компьютере, если только учетная запись специально не исключена с параметрами

Параметр Command-Line	Описание
	`/ue` или `/uel` . По этой причине этот параметр не требуется указывать в командной строке. Однако если `/all` параметр указан, `/ui` параметры , `/ue` или `/uel` также нельзя указать.

/ui:<*Имя_домена Имя_*>\<*пользователя*> или **/ui**:<*ComputerName*>\<*LocalUserName*>	**(Включение пользователя)**
	
	Переносит указанных пользователей. По умолчанию все пользователи включаются в миграцию. Поэтому этот параметр полезен только при использовании с параметрами `/ue` или `/uel` . Можно указать несколько `/ui` параметров, но `/ui` параметр нельзя использовать с параметром `/all` . *DomainName* и *UserName* могут содержать подстановочные знаки звездочки (`*`). Если указано имя пользователя, содержащее пробелы, оно должно быть заключено в кавычки (`"`).
	
	Примечание
	Если пользователь указан для включения с параметром `/ui` и также указан для исключения с помощью `/ue` параметров или `/uel` , он включается в миграцию.
	
	Пример
	
	• Чтобы включить только **User2** из домена Fabrikam, введите:
	
	`/ue:*\* /ui:fabrikam\user2`
	
	• Чтобы перенести всех пользователей из домена Fabrikam и только учетные записи пользователей из других доменов, которые были активны или иным образом изменены за последние 30 дней, введите:
	
	`/uel:30 /ui:fabrikam\*`
	
	В этом примере учетная запись пользователя из домена Contoso, которая была изменена два месяца назад, не переносится.
	
	Дополнительные примеры см. в описании `/ue` параметров и `/ui` в этой таблице.

/uel:<*NumberOfDays*> или **/uel**:<*ГГГГ/ММ/ДД*>	**(Пользователь исключается на основе последнего входа)** Переносит пользователей, вошедшего в систему, на исходный компьютер в течение указанного периода времени на основе даты

Параметр Command-Line	Описание
или **/uel:0**	**последнего изменения** файла Ntuser.dat на исходном компьютере. Параметр `/uel` выступает в качестве правила включения. Например, параметр `/uel:30` переносит пользователей, выполнивших вход или учетную запись которых была изменена, в течение последних 30 дней с даты `ScanState.exe` выполнения команды. Можно указать количество дней или дату. Этот параметр нельзя использовать с параметром `/all` . USMT извлекает сведения о последнем входе с локального компьютера, поэтому при запуске этого параметра компьютер не нужно подключать к сети. Кроме того, если пользователь домена входит на другой компьютер, USMT не учитывает этот экземпляр входа. **Примечание** Параметр `/uel` недопустим при автономной миграции. • `/uel:0` переносит всех пользователей, вошедших в систему. • `/uel:90` переносит пользователей, которые вошли в систему или чьи учетные записи были изменены иным образом в течение последних 90 дней. • `/uel:1` переносит пользователей, учетная запись которых была изменена в течение последних 24 часов. • `/uel:2020/2/15` переносит пользователей, которые вошли в систему или были изменены 15 февраля 2020 г. или позже. Пример: `ScanState.exe /i:MigApp.xml /i:MigDocs.xml \\server\share\migration\mystore /uel:0`
/ue:<*Имя_домена Имя_*>\<*пользователя*> -или- **/ue**:<*ComputerName*>\<*LocalUserName*>	**(Исключение пользователя)** Исключает указанных пользователей из миграции. Можно указать несколько `/ue` параметров. Этот параметр нельзя использовать с параметром `/all` . <*DomainName*> и <*UserName*> могут содержать подстановочные знаки звездочки (`*`). Если указано имя пользователя, содержащее пробелы, оно должно быть заключено в кавычки (`"`). Пример: `ScanState.exe /i:MigDocs.xml /i:MigApp.xml \\server\share\migration\mystore /ue:contoso\user1`

Использование /ui и /ue

Следующие примеры применимы к параметрам `/ui` и `/ue` . Параметр `/ue` можно заменить параметром `/ui` для включения, а не исключения указанных пользователей.

Развернуть таблицу

Поведение	Команда
Исключите пользователя с именем User One в домене Fabrikam.	`/ue:"fabrikam\user one"`
Исключите пользователя с именем User1 в домене Fabrikam.	`/ue:fabrikam\user1`
Исключите локального пользователя с именем User1.	`/ue:%computername%\user1`
Исключите всех пользователей домена.	`/ue:Domain\*`
Исключите всех локальных пользователей.	`/ue:%computername%\*`
Исключите пользователей во всех доменах с именами User1, User2 и т. д.	`/ue:*\user*`

Совместное использование параметров

Параметры `/uel` и `/ue` `/ui` можно использовать вместе для миграции только пользователей, которые необходимо перенести.

Параметр `/ui` имеет приоритет над параметрами `/ue` и `/uel` . Если пользователь указан для включения с параметром `/ui` и также указан для исключения с помощью `/ue` параметров или `/uel` , он включается в миграцию. Например, если `/ui:contoso\* /ue:contoso\user1` задано значение , пользователь **User1** переносится, так как `/ui` параметр имеет приоритет над параметром `/ue` .

Параметр `/uel` имеет приоритет над параметром `/ue` . Если пользователь вошел в систему в течение указанного периода времени, заданного `/uel` параметром , профиль этого пользователя переносится, даже если он исключен с помощью `/ue` параметра . Например, если `/ue:fixed\user1 /uel:14` задан параметр , пользователь User1 переносится, если пользователь выполнил вход на компьютер в течение последних 14 дней.

Развернуть таблицу

Поведение	Команда
Включите только User2 из домена Fabrikam и исключите всех остальных пользователей.	`/ue:*\* /ui:fabrikam\user2`
Включите только локального пользователя с именем User1 и исключите всех остальных пользователей.	`/ue:*\* /ui:user1`
Включите только пользователей домена из Contoso, за исключением Contoso\User1.	Это поведение не может быть выполнено с помощью одной команды. Вместо этого, чтобы перенести этот набор пользователей, укажите следующие команды: • В командной строке введите `ScanState.exe` : `/ue:*\* /ui:contoso\*` • В командной строке введите `LoadState.exe` : `/ue:contoso\user1`
Включать только локальных (не доменных) пользователей.	`/ue:*\* /ui:%computername%\*`

Параметры зашифрованного файла

Для переноса зашифрованных файлов можно использовать следующие параметры. Во всех случаях по умолчанию USMT завершается ошибкой, если найден зашифрованный файл, если `/efs` не указан параметр . Чтобы перенести зашифрованные файлы, необходимо изменить поведение по умолчанию.

Дополнительные сведения см. в разделе Перенос файлов и сертификатов EFS.

> ⓘ **Примечание**
>
> Сертификаты EFS переносятся автоматически во время миграции. `/efs:copyraw` Поэтому для переноса зашифрованных файлов необходимо указать параметр с `ScanState.exe` помощью команды .

> ⊗ **Внимание!**
>
> Будьте осторожны при переносе зашифрованных файлов. Если зашифрованный файл переносится без переноса сертификата, конечные пользователи не смогут получить доступ к файлу после миграции.

Развернуть таблицу

Параметр Command-Line	Объяснение
/efs:hardlink	Создает жесткую ссылку на файл EFS, а не копирует его. Используйте только с параметрами `/hardlink` `/nocompress` и .
/efs:abort	Вызывает сбой `ScanState.exe` команды с кодом ошибки, если на исходном компьютере обнаружен файл шифрованной файловой системы (EFS). Включено по умолчанию.
/efs:skip	Заставляет `ScanState.exe` команду игнорировать файлы EFS.
/efs:decryptcopy	Приводит к тому, что команда расшифровывает `ScanState.exe` файл, если это возможно, перед сохранением его в хранилище миграции и завершается сбоем, если не удается расшифровать файл. Если команда выполнена `ScanState.exe` успешно, файл незашифровывается в хранилище миграции, а после `LoadState.exe` выполнения команды файл копируется на целевой компьютер.
/efs:copyraw	Заставляет `ScanState.exe` команду копировать файлы в зашифрованном формате. Файлы недоступны на конечном компьютере до тех пор, пока не будут перенесены сертификаты EFS. Сертификаты EFS переносятся автоматически; однако по умолчанию USMT завершается ошибкой, если найден зашифрованный файл, если `/efs` не указан параметр . `/efs:copyraw` Поэтому для переноса зашифрованного файла необходимо указать параметр с `ScanState.exe` помощью команды . При выполнении `LoadState.exe` команды зашифрованный файл и сертификат EFS переносятся автоматически. Пример: `ScanState.exe /i:MigDocs.xml /i:MigApp.xml \server\share\migration\mystore /efs:copyraw` **Важно!** Все файлы должны быть зашифрованы, если родительская папка зашифрована. Если атрибут шифрования в файле в зашифрованной папке удален, файл шифруется во время миграции с использованием учетных данных учетной записи, используемой для запуска средства **LoadState** . Дополнительные сведения см. в разделе **Перенос файлов и сертификатов EFS**.

Несовместимые параметры командной строки

В следующей таблице показано, какие параметры командной строки несовместимы с командой `ScanState.exe` . Если запись таблицы для определенной комбинации имеет ✅значение , параметры совместимы, и их можно использовать вместе. Символ ❌ означает, что параметры несовместимы. Например, параметр `/nocompress` нельзя использовать с параметром `/encrypt` .

Развернуть таблицу

Параметр Command-Line	/keyfile	/nocompress	/genconfig	/все
/я	✅	✅	✅	✅
/o	✅	✅	✅	✅
/v	✅	✅	✅	✅
/nocompress	✅	✅	✅	Н/Д
/localonly	✅	✅	❌	✅
/ключ	❌	✅	❌	✅
/шифровать	Обязательно*	❌	❌	✅
/keyfile	Н/Д	✅	❌	✅
/l	✅	✅	✅	✅
/listfiles	✅	✅	❌	✅
/прогресс	✅	✅	❌	✅
/r	✅	✅	❌	✅
/w	✅	✅	❌	✅
/c	✅	✅	❌	✅
/p	✅	✅	❌	Н/Д
/все	✅	✅	❌	✅
/Пользовательского интерфейса	✅	✅	❌	❌
/ue	✅	✅	❌	❌
/uel	✅	✅	❌	❌

Параметр Command-Line	/keyfile	/nocompress	/genconfig	/все
/efs:*<option>*	✅	✅	❌	✅
/genconfig	✅	✅	Н/Д	✅
/config	✅	✅	❌	✅
<StorePath>	✅	✅	❌	✅

> ⓘ **Примечание**
>
> `/key` Параметр или `/keyfile` должен быть указан с параметром `/encrypt` .

Связанные статьи

- Библиотека XML-элементов.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Синтаксис LoadState

Статья • 29.01.2025 • Применяется к: ✅ Windows 11, ✅ Windows 10

Команда `LoadState.exe` используется со средством миграции пользовательской среды (USMT) для восстановления хранилища, ранее записанного командой, `ScanState.exe` на целевой компьютер. В этой статье рассматривается `LoadState.exe` синтаксис команды и доступные с ним параметры.

Перед началом

Перед выполнением `LoadState.exe` команды обратите внимание на следующие элементы:

- Чтобы обеспечить перенос всех параметров операционной системы, корпорация Майкрософт рекомендует выполнять `LoadState.exe` команды в режиме администратора из учетной записи с учетными данными администратора.
- Сведения о требованиях к программному обеспечению для выполнения команды см. в `LoadState.exe` разделе Требования USMT.
- Выйдите из нее `LoadState.exe` после выполнения команды. Некоторые параметры, например шрифты, обои и параметры скринсейвера, не вступают в силу до следующего входа пользователя.
- Если не указано иное, каждый параметр можно использовать только один раз при запуске средства из командной строки.
- **LoadState** не требует доступа контроллера домена для применения профилей домена. Эта функция доступна без дополнительной настройки. Для исходного компьютера не требуется доступ к контроллеру домена, когда профиль пользователя был собран с помощью **ScanState**. Однако профили домена недоступны, пока конечный компьютер не будет присоединен к домену.
- В таблице Несовместимые параметры командной строки перечислены параметры, которые можно использовать вместе, а какие параметры командной строки несовместимы.

Синтаксис

В этом разделе объясняется синтаксис и использование параметров командной строки, доступных при использовании `LoadState.exe` команды . Параметры можно указать в любом порядке. Если параметр содержит параметр, можно указать двоеточие или разделитель пробела.

Синтаксис `LoadState.exe` команды:

> LoadState.exe *StorePath* [/i:[*Path*\]*FileName*] [/v:*VerbosityLevel*] [/nocompress] [/decrypt /key:*KeyString*|/keyfile:[Path\]*FileName*] [/l:[*Path*\]*FileName*] [/progress:[*Path*\]*FileName*] [/r:*TimesToRetry*] [/w:*SecondsToWait*] [/c] [/all] [/ui:[*Имя_*|домена_*имя_компьютера*\]*Имя_пользователя*] [/ue:[*Имя_домена Имя_*|компьютера].\]*Имя_пользователя*] [/uel:*NumberOfDays*|*YYYY/MM/DD*|0] [/md:*OldDomain*:*NewDomain*] [/mu:*OldDomain**OldUserName*:[*NewDomain*\]*NewUserName*] [/lac:[*Password*]] [/lae] [/config:[*Path*\]*FileName*] [/?|справка]

Например, чтобы расшифровать хранилище и перенести файлы и параметры на компьютер, введите следующую команду:

```
LoadState.exe \\server\share\migration\mystore /i:MigApp.xml /i:MigDocs.xml /v:13 /decrypt /key:"mykey"
```

Варианты хранения

USMT предоставляет следующие параметры, с помощью которых можно указать, как и где хранятся перенесенные данные.

Развернуть таблицу

Параметр Command-Line	Описание
StorePath	Указывает папку, в которой хранятся файлы и данные параметров. При использовании `LoadState.exe` команды Необходимо указать *StorePath*. Невозможно указать несколько *StorePath* .

Параметр Command-Line	Описание
/decrypt /key:*KeyString* или **/decrypt /key**:"*Key String*" или **/decrypt /keyfile**: [*путь*]*Имя_файла*	Расшифровывает хранилище с указанным ключом. При использовании этого параметра ключ шифрования необходимо указать одним из следующих способов: • `/key`:*KeyString* указывает ключ шифрования. Если в *KeyString* есть пробел, аргумент должен быть заключен в кавычки (`"`). • `/keyfile`:*FilePathAndName* указывает текстовый файл (`.txt`), содержащий ключ шифрования. *Значение KeyString* не может превышать 256 символов. Параметры `/key` и `/keyfile` нельзя использовать в одной командной строке. Параметры `/decrypt` и `/nocompress` нельзя использовать в одной командной строке. **Важно!** Будьте внимательны при использовании `/key` параметров или `keyfile` . Например, любой пользователь, имеющий доступ к сценариям, выполняющим `LoadState.exe` команду с этими параметрами, также имеет доступ к ключу шифрования. Пример `LoadState.exe /i:MigApp.xml /i:MigDocs.xml \server\share\migration\mystore /decrypt /key:mykey`
/decrypt:"*сила шифрования*"	Параметр `/decrypt` принимает параметр командной строки для определения надежности шифрования, указанной для шифрования хранилища миграции. Дополнительные сведения о поддерживаемых алгоритмах шифрования см. в разделе Шифрование хранилища миграции.
/hardlink	Позволяет восстанавливать данные пользовательского состояния из хранилища миграции с жесткой компоновкой. Параметр `/nocompress` должен быть указан с параметром `/hardlink` .
/nocompress	Указывает, что хранилище не сжимается. Этот параметр следует использовать только в средах тестирования. Корпорация Майкрософт рекомендует использовать сжатое хранилище во время фактической миграции. Этот параметр нельзя использовать с параметром `/decrypt` . Пример: `LoadState.exe /i:MigApp.xml /i:MigDocs.xml \server\share\migration\mystore /nocompress`

Параметры правил миграции

USMT предоставляет следующие параметры, чтобы указать, какие файлы следует перенести.

Развернуть таблицу

Параметр Command-Line	Описание
/i: [*путь*]*Имя_файла*	**(включая)** Указывает **файл.xml** , содержащий правила, определяющие, какие данные следует перенести. Этот параметр можно указать несколько раз, чтобы включить все **файлы.xml** (`MigApp.xml`, , `MigSys.xml` `MigDocs.xml` и все созданные пользовательские **.xml** файлы). *Путь* может быть относительным или полным. Если переменная *Path* не указана, *имя_файла* должно находиться в текущем каталоге. Дополнительные сведения о том, какие файлы следует указать, см. в разделе "XML-файлы" статьи Часто задаваемые вопросы .
/config: [*путь*]*Имя_файла*	Указывает `Config.xml` файл, который `LoadState.exe` должна использовать команда. Этот параметр нельзя указать более одного раза в командной строке. *Путь* может быть относительным или полным. Если переменная *Path* не указана, имя *_файла* должно находиться в текущем каталоге. В этом примере переносятся файлы и параметры на основе правил в файлах `Config.xml`, `MigDocs.xml` и `MigApp.xml` : `LoadState.exe \server\share\migration\mystore /config:Config.xml /i:MigDocs.xml /i:MigApp.xml /v:5 /l:LoadState.log`
/auto:"*путь к файлам скриптов*"	Этот параметр позволяет указать расположение файлов по умолчанию **.xml** . Если путь не указан, USMT использует каталог, в котором находятся двоичные файлы USMT. Этот `/auto` параметр имеет тот же эффект, что и при использовании следующих параметров: `/i:MigDocs.xml` `/i:MigApp.xml /v:5`.

Параметры мониторинга

USMT предоставляет несколько параметров командной строки, которые можно использовать для анализа проблем, возникающих во время миграции.

Развернуть таблицу

Параметр Command-Line	**Описание**
/l:[*путь*]*Имя_файла*	Указывает расположение и имя журнала **LoadState** . Файлы журнала не могут храниться в *StorePath*. *Путь* может быть относительным или полным. Если переменная *Path* не указана, журнал создается в текущем каталоге. Параметр `/v` можно указать для настройки детализации журнала. При выполнении `LoadState.exe` команды из общего сетевого ресурса `l` необходимо указать параметр, иначе USMT завершается ошибкой: ***USMT не удалось создать файлы журналов*** Чтобы устранить эту проблему, обязательно укажите `/l` параметр при запуске `LoadState.exe` из общего сетевого ресурса.
/v:`<VerbosityLevel>`	**(Детализация)** Включает подробные выходные данные в файле журнала **LoadState** . Значение по умолчанию — 0. Для *verbosityLevel* можно задать один из следующих уровней: • **0** — включены только ошибки и предупреждения по умолчанию. • **1** — включает подробные выходные данные. • **4** . Включает вывод ошибок и состояния. • **5** . Включает подробные выходные данные и выходные данные состояния. • **8** . Включает вывод ошибок в отладчик. • **9** . Включает подробные выходные данные в отладчик. • **12** . Включает вывод ошибок и состояния в отладчик. • **13** . Включает подробные, состояние и выходные данные отладчика. Пример `LoadState.exe \server\share\migration\mystore /v:5 /i:MigDocs.xml /i:MigApp.xml`
/progress: [*Path*]*Имя_файла*	Создает необязательный журнал выполнения. Файлы журнала не могут храниться в *StorePath*. *Путь* может быть относительным или полным. Если переменная *Path* не указана, *fileName* создается в текущем каталоге. Пример: `LoadState.exe /i:MigApp.xml /i:MigDocs.xml \server\share\migration\mystore /progress:Progress.log /l:loadlog.log`

Параметр Command-Line	Описание
/c	Если указан этот параметр, `LoadState.exe` команда продолжает выполняться, даже если возникают неустранимые ошибки. Все файлы или параметры, вызывающие ошибку, регистрируются в журнале выполнения. Например, если на компьютере есть большой файл, который не помещается, `LoadState.exe` команда регистрирует ошибку и продолжает миграцию. Без параметра `/c` `LoadState.exe` команда завершает работу при первой ошибке. Раздел <**ErrorControl**> можно использовать в `Config.xml` файле, чтобы указать, какие ошибки чтения и записи файла или реестра можно безопасно игнорировать, а какие могут привести к сбою миграции. Это управление ошибками позволяет параметру командной `/c` строки безопасно пропускать все ошибки ввода-вывода в среде. Кроме того, `/genconfig` теперь параметр создает пример < раздела **ErrorControl**>, который включается путем указания сообщений об ошибках и требуемого `Config.xml` поведения в файле.
/r:*`<TimesToRetry>`*	**(Повторите попытку)** Указывает количество повторных попыток при возникновении ошибки при переносе пользовательского состояния с сервера. Значение по умолчанию — три раза. Этот параметр полезен в средах, где сетевое подключение не является надежным. При восстановлении пользовательского состояния параметр не восстанавливает данные, `/r` которые были потеряны из-за сбоя оборудования сети, например неисправного или отключенного сетевого кабеля, или при сбое подключения к виртуальной частной сети (VPN). Вариант повтора предназначен для больших, загруженных сетей, где подключение является удовлетворительным, но задержка связи является проблемой.
/w: *`<SecondsBeforeRetry>`*	**(Подождите)** Указывает время ожидания (в секундах) перед повтором операции с сетевым файлом. Значение по умолчанию — 1 секунда.
/? или **/help**	Отображает справку в командной строке.

Параметры пользователя

По умолчанию переносятся все пользователи. Единственный способ указать, какие пользователи следует включать и исключать, — использовать следующие параметры. Пользователи не могут быть исключены из **.xml** файлов миграции или с

помощью `Config.xml` файла. Дополнительные сведения см. в разделе Определение пользователей.

Развернуть таблицу

Параметр Command-Line	Описание
/все	Переносит всех пользователей на компьютере. USMT переносит все учетные записи пользователей на компьютере, если только учетная запись специально не исключена с параметрами `/ue` или `/uel` . По этой причине этот параметр не требуется указывать в командной строке. Однако при использовании `/all` параметра `/ui`также нельзя использовать параметры , `/ue` или `/uel` .
/ui:*Имя_домена Имя_пользователя* или **/ui**:"*DomainName User Name*" или **/ui**:*ComputerName LocalUserName*	**(Включение пользователя)** Переносит указанного пользователя. По умолчанию все пользователи включаются в миграцию. Поэтому этот параметр полезен только при использовании с параметром `/ue` . Можно указать несколько `/ui` параметров, но `/ui` параметр нельзя использовать с параметром `/all` . *DomainName* и *UserName* могут содержать подстановочные знаки звездочки (`*`). Если указано имя пользователя, содержащее пробелы, оно должно быть заключено в кавычки (`"`). Например, чтобы включить только **User2** из корпоративного домена, введите: `/ue:* /ui:corporate\user2` **Примечание** Если пользователь указан для включения с параметром `/ui` и также указан для исключения с помощью `/ue` параметров или `/uel` , он включается в миграцию. Дополнительные примеры см. в описании `/uel`параметров , `/ue`и `/ui` в этой таблице.
/uel:`<NumberOfDays>` или	**(Пользователь исключается на основе последнего входа)**

Параметр Command-Line	Описание
/uel:`<YYYY/MM/DD>` или **/uel**:0	Переносит только пользователей, которые вошли на исходный компьютер в течение указанного периода времени на основе даты **последнего измененияфайла Ntuser.dat** на исходном компьютере. Параметр `/uel` выступает в качестве правила включения. Например, параметр `/uel:30` переносит пользователей, выполнивших вход или измененную учетную запись пользователя, в течение последних 30 дней с даты `ScanState.exe` выполнения команды. Можно указать количество дней или дату. Этот параметр нельзя использовать с параметром `/all` . USMT извлекает сведения о последнем входе с локального компьютера, поэтому при запуске этого параметра компьютер не нужно подключать к сети. Кроме того, если пользователь домена входит на другой компьютер, USMT не учитывает этот экземпляр входа. **Примечание** Параметр `/uel` недопустим при автономной миграции. Примеры: • `/uel:0` переносит учетные записи, которые были вошли в систему, на исходный компьютер при выполнении `ScanState.exe` команды. • `/uel:90` переносит пользователей, которые вошли в систему или чьи учетные записи были изменены иным образом в течение последних 90 дней. • `/uel:1` переносит пользователей, учетные записи которых были изменены за последние 24 часа. • `/uel:2020/2/15` переносит пользователей, которые вошли в систему или чьи учетные записи были изменены с 15 февраля 2020 г. Пример: `LoadState.exe /i:MigApp.xml /i:MigDocs.xml \server\share\migration\mystore /uel:0`
/ue:*DomainName\UserName* или **/ue**"*Имя_домена\Имя пользователя*"	**(Исключение пользователя)** Исключает указанных пользователей из миграции.

Параметр Command-Line	Описание
или **/ue**:*ComputerName**LocalUserName*	Можно использовать несколько `/ue` параметров, `/ue` но параметр нельзя использовать с параметром `/all` . *DomainName* и *UserName* могут содержать подстановочные знаки звездочки (`*`). Если указано имя пользователя, содержащее пробелы, оно должно быть заключено в кавычки (`"`). Пример `LoadState.exe /i:MigApp.xml /i:MigDocs.xml \server\share\migration\mystore /ue:contoso\user1` Дополнительные примеры см. в описании `/uel` параметров , `/ue` и `/ui` в этой таблице.
/md:*OldDomain*:*NewDomain* или **/md**:*LocalComputerName:NewDomain*	**(Перемещение домена)** Указывает новый домен для пользователя. Используйте этот параметр, чтобы изменить домен для пользователей на компьютере или перенести локального пользователя в учетную запись домена. *OldDomain* может содержать подстановочный знак звездочки (). Этот параметр можно указать несколько раз. При консолидации пользователей в нескольких доменах в одном домене может потребоваться указать несколько `/md` параметров. Например, чтобы объединить пользователей из доменов Corporate и FarNorth в домен Fabrikam, укажите следующие параметры: `/md:corporate:fabrikam` и `/md:farnorth:fabrikam`. При наличии конфликтов между двумя `/md` командами применяется первое указанное правило. Например, если `/md:corporate:fabrikam` указаны команды и `/md:corporate:farnorth` , корпоративные пользователи будут сопоставлены с доменом Fabrikam. **Примечание** Если указан домен, который не существовал на исходном компьютере, команда будет выполнена `LoadState.exe` успешно, без ошибок или предупреждений. Однако в этом случае пользователи не перемещаются в *NewDomain* , а остаются в исходном

Параметр Command-Line	Описание
	домене. Например, если **contoso** написана с ошибкой и вместо этого указан **параметр /md:contso:fabrikam** , пользователи остаются в **contoso** на конечном компьютере. Пример `LoadState.exe /i:MigApp.xml /i:MigDocs.xml \server\share\migration\mystore /progress:Progress.log /l:LoadState.log /md:contoso:fabrikam`
/mu:*OldDomain OldUserName*:[*NewDomain*]*NewUserName* или **/mu**:*OldLocalUserName*:*NewDomain NewUserName*	**(Перемещение пользователя)** Указывает новое имя пользователя для указанного пользователя. Если хранилище содержит несколько пользователей, можно указать несколько `/mu` параметров. С этим параметром нельзя использовать подстановочные знаки. Пример: `LoadState.exe /i:MigApp.xml /i:MigDocs.xml \server\share\migration\mystore /progress:Progress.log /l:LoadState.log /mu:contoso\user1:fabrikam\user1`
/lac:[*пароль*]	**(Создание локальной учетной записи)** Если учетная запись пользователя: • Локальная (внедоменная) учетная запись • Учетная запись, которая не существует на конечном компьютере этот параметр указывает на создание учетной записи на конечном компьютере. Однако учетная запись отключена. Чтобы включить учетную запись, `/lae` также необходимо использовать параметр . `/lac` Если параметр не указан, все локальные учетные записи пользователей, которые еще не существуют на конечном компьютере, не переносятся. *Пароль* — это пароль для созданной учетной записи. По умолчанию используется пустой пароль.

Параметр Command-Line	Описание
	Предостережение Используйте переменную *Password* с осторожностью. Переменная *Password* предоставляется в виде обычного текста, и любой пользователь с доступом к компьютеру `LoadState.exe` , на котором выполняется команда, может получить пароль. Кроме того, если на компьютере несколько пользователей, все перенесенные пользователи имеют один и тот же пароль. Пример: `LoadState.exe /i:MigApp.xml /i:MigDocs.xml \server\share\migration\mystore` Инструкции см. в разделе Миграция учетных записей пользователей.
`/lae`	**(Включение локальной учетной записи)** Включает учетную запись, созданную с параметром `/lac` . Параметр `/lac` должен быть указан с помощью этого параметра. Пример: `LoadState.exe /i:MigApp.xml /i:MigDocs.xml \server\share\migration\mystore /progress:Progress.log /l:LoadState.log /lac:password /lae` Инструкции см. в разделе Миграция учетных записей пользователей.

Примеры параметров /ui и /ue

Следующие примеры применяются к параметрам **/ui** и **/ue** . Параметр **/ue** можно заменить параметром **/ui** , чтобы включить, а не исключить указанных пользователей.

Развернуть таблицу

Поведение	Команда
Исключите пользователя с именем User One в корпоративном домене.	`/ue:"corporate\user one"`
Исключите пользователя с именем User1 в корпоративном домене.	`/ue:corporate\user1`
Исключите локального пользователя с именем User1.	`/ue:%computername%\user1`
Исключите всех пользователей домена.	`/ue:Domain`
Исключите всех локальных пользователей.	`/ue:%computername%`
Исключите пользователей во всех доменах с именами User1, User2 и т. д.	`/ue:\user`

Совместное использование параметров

Параметры `/uel` и `/ue` `/ui` можно использовать вместе для миграции только пользователей, которые необходимо перенести.

Параметр /ui имеет приоритет над параметрами /ue и /uel. Если пользователь включается с помощью `/ui` параметра и также исключается с помощью `/ue` параметров или `/uel` , он включается в миграцию. Например, если `/ui:contoso\*` `/ue:contoso\user1` задано значение , пользователь User1 переносится, так как `/ui` параметр имеет приоритет над параметром `/ue` .

Параметр /uel имеет приоритет над параметром /ue. Если пользователь вошел в систему в течение указанного периода времени, заданного `/uel` параметром , профиль этого пользователя переносится, даже если он исключен с помощью `/ue` параметра . Например, если `/ue:contoso\user1 /uel:14` задан параметр , пользователь User1 переносится, если пользователь выполнил вход на компьютер в течение последних 14 дней.

Развернуть таблицу

Поведение	Команда
Включите только User2 из домена Fabrikam и исключите всех остальных пользователей.	`/ue:* /ui:fabrikam\user2`

Поведение	Команда
Включите только локального пользователя с именем User1 и исключите всех остальных пользователей.	`/ue:* /ui:user1`
Включите только пользователей домена из Contoso, за исключением Contoso\User1.	Это поведение не может быть выполнено с помощью одной команды. Вместо этого, чтобы перенести этот набор пользователей, укажите следующие параметры: • С помощью средства командной строки **ScanState** введите: `/ue:* /ui:contoso` • С помощью программы командной строки **LoadState** введите: `/ue:contoso\user1`
Включать только локальных (не доменных) пользователей.	`/ue: /ui:%computername%*`

Несовместимые параметры командной строки

В следующей таблице показано, какие параметры командной строки несовместимы с командой `LoadState.exe` . Если запись таблицы для определенной комбинации имеет ✅значение , параметры совместимы, и их можно использовать вместе. Символ ❌ означает, что параметры несовместимы. Например, параметр `/nocompress` нельзя использовать с параметром `/encrypt` .

Развернуть таблицу

Параметр Command-Line	/keyfile	/nocompress	/genconfig	/все
/я	✅	✅	✅	✅
/v	✅	✅	✅	✅
/nocompress	✅	Н/Д	❌	✅
/ключ	❌	✅	❌	✅
/расшифровать	Обязательно*	❌	❌	✅
/keyfile	Н/Д	✅	❌	✅
/l	✅	✅	✅	✅

Параметр Command-Line	/keyfile	/nocompress	/genconfig	/все
/прогресс	✅	✅	❌	✅
/r	✅	✅	❌	✅
/w	✅	✅	❌	✅
/c	✅	✅	❌	✅
/p	✅	✅	❌	Н/Д
/все	✅	✅	❌	✅
/Пользовательского интерфейса	✅	✅	❌	❌
/ue	✅	✅	❌	❌
/uel	✅	✅	❌	❌
/genconfig	✅	✅	Н/Д	✅
/config	✅	✅	❌	✅
StorePath	✅	✅	✅	✅
/md	✅	✅	✅	✅
/мю	✅	✅	✅	✅
/Лаэ	✅	✅	✅	✅
/природный лак	✅	✅	✅	✅

> ⓘ **Примечание**
>
> `/key` Параметр или `/keyfile` должен быть указан с параметром `/decrypt` .

Связанные статьи

- Библиотека XML-элементов.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Синтаксис UsmtUtils

Статья • 29.01.2025 • Применяется к: ✅ Windows 11, ✅ Windows 10

В этой статье описывается синтаксис служебных программ, доступных в средстве миграции пользовательской среды (USMT) через интерфейс командной строки. Эти служебные программы:

- Улучшение возможности определения параметров шифрования для миграции.
- Помощь в удалении хранилищ с жесткой связью, которые в противном случае не могут быть удалены из-за блокировки общего доступа.
- Проверьте, поврежден ли файл каталога или любой другой файл в сжатом хранилище миграции.
- Извлеките файлы из сжатого хранилища миграции, созданного при переносе файлов и параметров на конечный компьютер.

UsmtUtils.exe

В следующей таблице перечислены параметры командной строки для `UsmtUtils.exe`. В следующих разделах содержатся дополнительные параметры командной `/verify` строки для параметров и `/extract` .

Синтаксис для `UsmtUtils.exe` :

> UsmtUtils.exe [/ec | /rd <*storeDir*> | /verify <*filepath*> [options] | /extract <*filepath*> <*destinationPath*> [параметры]]

Развернуть таблицу

Параметр командной строки	Описание
/Европейское сообщество	Возвращает список поддерживаемых алгоритмов шифрования (AlgID) в текущей системе. Этот параметр можно использовать на конечном компьютере, чтобы определить, какой алгоритм следует использовать с командой `/encrypt` перед запуском средства **ScanState** на исходном компьютере.

Параметр командной строки	Описание
/rd<*storeDir*>	Удаляет путь к каталогу, указанный аргументом <*storeDir*> на компьютере. Эту команду можно использовать для удаления хранилищ миграции с жесткой компоновкой, которые не могут быть удалены в командной строке из-за блокировки общего доступа. Если хранилище миграции охватывает несколько томов на заданном диске, хранилище миграции удаляется из всех этих томов. Пример `UsmtUtils.exe /rd D:\MyHardLinkStore`
/y	Переопределяет запрос на принятие удалений при использовании с параметром `/rd` . `/y` Если параметр используется вместе с параметром `/rd`, не отображается запрос на принятие удалений, прежде чем USMT удалит каталоги.
/проверять	Возвращает сведения о том, является ли сжатое хранилище миграции нетронутым или содержит поврежденные файлы или поврежденный каталог. См . раздел Проверка параметров синтаксиса и параметров для использования с `/verify`.
/экстракт	Восстанавливает файлы из сжатого хранилища миграции USMT. См . раздел Извлечение параметров для синтаксиса и параметров для использования с `/extract`.

Параметры проверки

Используйте параметр , `/verify` чтобы определить, является ли сжатое хранилище миграции нетронутым или содержит ли оно поврежденные файлы или поврежденный каталог. Дополнительные сведения об использовании параметра см. в `/verify` разделе Проверка состояния сжатого хранилища миграции.

Синтаксис для `/verify` :

> UsmtUtils.exe /verify[:<*reportType*>] <*filePath*> [/l:<*logfile*>] [/v:*VerbosityLevel*] [/decrypt [:<*AlgID*>] {/key:<*keystring*> | /keyfile:<*filename*>}]

Развернуть таблицу

Параметр командной строки	Описание
<reportType>	Указывает, следует ли сообщать обо всех файлах, только поврежденных файлах или о состоянии каталога. • **Сводка**. Возвращает как количество нетронутых файлов, так и количество поврежденных файлов в хранилище миграции. Если алгоритм не указан, сводный отчет отображается по умолчанию. • **все**. Возвращает список всех файлов в сжатом хранилище миграции с разделителями табуляции и состояние каждого файла. Каждая строка содержит имя файла, за которым следует интервал между вкладками, и в зависимости от состояния файла либо **ПОВРЕЖДЕНо** , либо **ОК** . Последняя запись сообщает о состоянии повреждения **КАТАЛОГА** хранилища. Файл каталога содержит метаданные для всех файлов в хранилище миграции. Чтобы открыть хранилище миграции, **инструменту LoadState** требуется допустимый файл каталога. Возвращает значение "ОК", если файл каталога нетронут и **LoadState** может открыть хранилище миграции и "ПОВРЕЖДЕНо", если хранилище миграции повреждено. • **только сбой**. Возвращает список только файлов, поврежденных в сжатом хранилище миграции с разделителями табуляции. • **Каталог**. Возвращает только состояние файла каталога.
/l: *<logfilePath>*	Указывает расположение и имя файла журнала.
/v:*<VerbosityLevel>*	**(Детализация)** Включает подробные выходные данные в файле журнала **UsmtUtils** . Значение по умолчанию — 0. Для *verbosityLevel* можно задать один из следующих уровней: • **0** — включены только ошибки и предупреждения по умолчанию. • **1** — включает подробные выходные данные. • **4** . Включает вывод ошибок и состояния. • **5** . Включает подробные выходные данные и выходные данные состояния. • **8** . Включает вывод ошибок в отладчик. • **9** . Включает подробные выходные данные в отладчик. • **12** . Включает вывод ошибок и состояния в отладчик. • **13** . Включает подробные, состояние и выходные данные отладчика.
/decrypt*<AlgID>***/:** *<KeyString>* или	Указывает, что `/encrypt` параметр использовался для создания хранилища миграции с помощью средства **ScanState** . Чтобы

Параметр командной строки	Описание
/decrypt<*AlgID*>**/**:<"*Key String*"> или **/decrypt:**<*AlgID*>**/keyfile**:<*FileName*>	расшифровать хранилище миграции, укажите `/key` параметр или `/keyfile` следующим образом: • <*AlgID*> указывает криптографический алгоритм, который использовался для создания хранилища миграции в командной строке `ScanState.exe` . Если алгоритм не указан, **ScanState** и **UsmtUtils** используют алгоритм 3DES по умолчанию. <*Допустимые значения AlgID*> : `AES_128`, `AES_192`, `AES_256`, `3DES` или `3DES_112`. • `/key:` <*KeyString*> указывает ключ шифрования. Если в <*KeyString*> есть пробел, аргумент должен быть заключен в кавычки. • `/keyfile`: <*FileName*> указывает расположение и имя текстового (.txt) файла, содержащего ключ шифрования. Дополнительные сведения о поддерживаемых алгоритмах шифрования см. в разделе Шифрование хранилища миграции.

Примеры `/verify` команд:

- `UsmtUtils.exe /verify D:\MyMigrationStore\store.mig`
- `UsmtUtils.exe /verify:catalog D:\MyMigrationStore\store.mig`
- `UsmtUtils.exe /verify:all D:\MyMigrationStore\store.mig /decrypt /l:D:\UsmtUtilsLog.txt`
- `UsmtUtils.exe /verify:failureonly D:\MyMigrationStore\store.mig /decrypt:AES_192 /keyfile:D:\encryptionKey.txt`

Параметры извлечения

`/extract` Используйте параметр для восстановления файлов из сжатого хранилища миграции USMT, если оно не восстанавливается нормально с **помощью LoadState**. Дополнительные сведения об использовании параметра см. в `/extract` разделе Извлечение файлов из сжатого хранилища миграции USMT.

Синтаксис для `/extract` :

> /extract <*filePath*><*destinationPath*> [/i:<*includePattern*>] [/e: <*excludePattern*>] [/l: <*logfile*>] [/v: *VerbosityLevel*>] [/decrypt[:<*AlgID*>] {key: <*keystring*> | /keyfile:

> *<filename>*}] [/o]

Развернуть таблицу

Параметр командной строки	Описание
<filePath>	Путь к хранилищу миграции USMT. Пример: `D:\MyMigrationStore\USMT\store.mig`
<destinationPath>	Путь к папке, в которой средство помещает отдельные файлы.
/i:*<includePattern>*	Задает шаблон для файлов, которые будут включены в извлечение. Можно указать несколько шаблонов. Разделяйте узоры запятой или точкой с запятой. Параметры `/i`: *<includePattern>* и `/e`: *<excludePattern>* можно использовать в одной команде. Если в командной строке используются шаблоны включения и исключения, шаблоны включения имеют приоритет над шаблонами исключения.
/e:*<excludePattern>*	Указывает шаблон для файлов, которые следует исключить из извлечения. Можно указать несколько шаблонов. Разделяйте узоры запятой или точкой с запятой. Параметры `/i`: *<includePattern>* и `/e`: *<excludePattern>* можно использовать в одной команде. Если в командной строке используются шаблоны включения и исключения, шаблоны включения имеют приоритет над шаблонами исключения.
/l:*<logfilePath>*	Указывает расположение и имя файла журнала.

Параметр командной строки	Описание
/v:<*VerbosityLevel*>	**(Детализация)** Включает подробные выходные данные в файле журнала **UsmtUtils** . Значение по умолчанию — 0. Для *verbosityLevel* можно задать один из следующих уровней: • **0** — включены только ошибки и предупреждения по умолчанию. • **1** — включает подробные выходные данные. • **4** . Включает вывод ошибок и состояния. • **5** . Включает подробные выходные данные и выходные данные состояния. • **8** . Включает вывод ошибок в отладчик. • **9** . Включает подробные выходные данные в отладчик. • **12** . Включает вывод ошибок и состояния в отладчик. • **13** . Включает подробные, состояние и выходные данные отладчика.
/decrypt*<AlgID>***/key***: <KeyString> *или* ***/расшифровать***<AlgID>***/***: <"Key String"> *или* ***/расшифровать:*** <AlgID>***/keyfile***: <FileName>*	Указывает, что `/encrypt` параметр использовался для создания хранилища миграции с помощью средства **ScanState** . Чтобы расшифровать хранилище миграции `/key` , также необходимо указать параметр или `/keyfile` следующим образом: • <*AlgID*> указывает криптографический алгоритм, который использовался для создания хранилища миграции в командной строке `ScanState.exe` . Если алгоритм не указан, **ScanState** и **UsmtUtils** используют алгоритм 3DES по умолчанию. <*Допустимые значения AlgID*> : `AES_128`, `AES_192`, `AES_256`, `3DES` или `3DES_112`. • `/key`: <*KeyString*> указывает ключ шифрования. Если в <*KeyString*> есть пробел, аргумент должен быть заключен в кавычки. • `/keyfile`:<*FileName*> указывает текстовый (.txt) файл, содержащий ключ шифрования. Дополнительные сведения о поддерживаемых алгоритмах шифрования см. в разделе Шифрование хранилища миграции.
/o	Перезаписывает существующие выходные файлы.

Примеры `/extract` команд:

- `UsmtUtils.exe /extract D:\MyMigrationStore\USMT\store.mig C:\ExtractedStore`

- `UsmtUtils.exe /extract D:\MyMigrationStore\USMT\store.mig /i:"*.txt, *.pdf" C:\ExtractedStore /decrypt /keyfile:D:\encryptionKey.txt`
- `UsmtUtils.exe /extract D:\MyMigrationStore\USMT\store.mig /e:*.exe C:\ExtractedStore /decrypt:AES_128 /key:password /l:C:\usmtlog.txt`
- `UsmtUtils.exe /extract D:\MyMigrationStore\USMT\store.mig /i:myProject.* /e:*.exe C:\ExtractedStore /o`

Связанные статьи

- Синтаксис командной строки средства миграции пользовательской среды (USMT).
- Коды возврата.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Справочник по XML-файлу USMT

Статья • 29.01.2025 • Применяется к: ✅ Windows 11, ✅ Windows 10

В этом разделе содержатся статьи, которые можно использовать для работы и настройки XML-файлов миграции.

В этом разделе

Развернуть таблицу

Ссылка	Описание
Общие сведения о XML-файлах миграции	Содержит общие сведения о XML-файлах по умолчанию и пользовательских файлах миграции, а также содержит рекомендации по созданию и редактированию `MigDocs.xml` настраиваемой версии файла.
файлConfig.xml	Описывает `Config.xml` файл и политики, касающиеся его конфигурации.
Настройка XML-файлов USMT	Описывает настройку XML-файлов USMT.
Пользовательские примеры XML	Содержит примеры XML-файлов для различных сценариев миграции.
Конфликты и приоритет	Описывает приоритет правил миграции и способы обработки конфликтов.
Общие соглашения	Описывает вспомогательные функции XML.
Требования к XML-файлам	Описывает требования к пользовательским XML-файлам.
Распознанные переменные среды	Описывает переменные среды, распознаваемые USMT.
Библиотека XML-элементов	Описывает XML-элементы и вспомогательные функции для создания XML-файлов миграции для использования с USMT.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Общие сведения о XML-файлах миграции

Статья • 29.01.2025 • Применяется к: ✅ Windows 11, ✅ Windows 10

Поведение базовой миграции средства миграции пользовательской среды (USMT) можно изменить с помощью XML-файлов. Эти файлы содержат инструкции о том, где и как средства USMT должны собирать и применять файлы и параметры. USMT включает три XML-файла, которые можно использовать для настройки базовой миграции: `MigDocs.xml` файлы и `MigUser.xml` , которые изменяют способ обнаружения файлов на исходном компьютере, и файл MigApps.xml, необходимый для переноса поддерживаемых параметров приложения. Пользовательские XML-файлы и `Config.xml` файл можно создать и изменить для дальнейшей настройки миграции.

В этой статье представлен обзор XML-файлов по умолчанию и пользовательских файлов миграции, а также рекомендации по созданию и редактированию настраиваемой `MigDocs.xml` версии файла. Файл `MigDocs.xml` использует новую `GenerateDocPatterns` функцию, доступную в USMT, для автоматического поиска документов пользователей на исходном компьютере.

Обзор файла Config.xml

Файл `Config.xml` — это файл конфигурации, созданный параметром `/genconfig` средства **ScanState** . Его можно использовать для изменения компонентов операционной системы, переносимых USMT. Файл `Config.xml` можно использовать с другими XML-файлами, например в следующем примере:

```
ScanState.exe /i:migapps.xml /i:MigDocs.xml /genconfig:c:\myFolder\Config.xml
```

При использовании таким образом `Config.xml` файл строго контролирует аспекты миграции, включая профили пользователей, данные и параметры, без изменения или создания других XML-файлов. Дополнительные сведения о файле см. в `Config.xml` разделе Настройка XML-файлов USMT и файлаConfig.xml.

> **Примечание**
>
> При изменении XML-элементов в `Config.xml` файле присвойте свойству **migrate** для элемента **значение Нет** , а не удалите элемент из файла. Если

элемент удаляется вместо задания свойства, правила в других XML-файлах по-прежнему могут переносить компонент.

Обзор файла MigApp.xml

Файл, установленный `MigApp.xml` с USMT, содержит инструкции по переносу параметров для приложений, перечисленных в разделе Что такое миграция USMT?. Чтобы перенести параметры приложения, `MigApp.xml` файл должен быть включен при использовании средств **ScanState** и **LoadState** с помощью `/i` параметра . Файлы `MigDocs.xml` и `MigUser.xml` не переносятся параметры приложения. Можно создать пользовательский XML-файл для включения дополнительных приложений. Дополнительные сведения см. в разделе Настройка XML-файлов USMT.

> ⓘ **Важно!**
>
> Файл `MigApps.xml` обнаруживает и переносит только **PST-файлы** , связанные с Microsoft Office Outlook. Дополнительные сведения о переносе **PST-файлов** , которые не связаны с Outlook, см **. в разделе Примеры правил миграции для настраиваемых версий XML-файлов**.

Обзор файла MigDocs.xml

В `MigDocs.xml` файле используется новая `GenerateDocPatterns` вспомогащая функция для создания инструкций для USMT по переносу файлов с исходного компьютера на основе расположения файлов. Файл `MigDocs.xml` можно использовать со средствами **ScanState** и **LoadState** для выполнения более целевой миграции, чем с помощью USMT без инструкций XML.

Файл по умолчанию `MigDocs.xml` переносит следующие данные:

- Все файлы в корневой части диска, кроме `%WINDIR%`, `%PROGRAMFILES%`, `%PROGRAMDATA%` или `%USERS%`.
- Все папки в корневом каталоге всех фиксированных дисков. Например: `c:\data_mail\*[*]`.
- Все файлы из корневой папки Profiles, за исключением файлов в системном профиле. Например: `c:\users\name[mail.pst]`.

- Все папки из корневого каталога папки Profiles, за исключением папок системного профиля. Например: `c:\users\name\new folder\*[*]`.
- Standard общих папок:
  - CSIDL_COMMON_DESKTOPDIRECTORY
  - CSIDL_COMMON_FAVORITES
  - CSIDL_COMMON_DOCUMENTS
  - CSIDL_COMMON_MUSIC
  - CSIDL_COMMON_PICTURES
  - CSIDL_COMMON_VIDEO
  - FOLDERID_PublicDownloads
- Standard для каждого пользователя:
  - CSIDL_MYDOCUMENTS
  - CSIDL_MYPICTURES
  - FOLDERID_OriginalImages
  - CSIDL_MYMUSIC
  - CSIDL_MYVIDEO
  - CSIDL_FAVORITES
  - CSIDL_DESKTOP
  - CSIDL_QUICKLAUNCH
  - FOLDERID_Contacts
  - FOLDERID_Libraries
  - FOLDERID_Downloads
  - FOLDERID_SavedGames
  - FOLDERID_RecordedTV

Файл по умолчанию `MigDocs.xml` не переносит следующие данные:

- Файлы, помеченные **как скрытыми** , так и **системными** атрибутами.
- Файлы и папки на съемных дисках.
- Данные из папок %WINDIR%, %PROGRAMDATA% и %PROGRAMFILES%.
- Папки, содержащие установленные приложения.

Параметр `/genmigxml` можно использовать вместе со средством **ScanState** для просмотра и изменения перенесенных файлов.

Обзор файла MigUser.xml

Файл `MigUser.xml` содержит инструкции для USMT по переносу пользовательских файлов на основе расширений имен файлов. Файл `MigUser.xml` можно использовать со средствами **ScanState** и **LoadState** для выполнения более целевой миграции, чем с помощью USMT без инструкций XML. Файл `MigUser.xml` собирает все файлы из стандартных папок профиля пользователя и все файлы на компьютере с указанными расширениями имен файлов.

Файл по умолчанию `MigUser.xml` переносит следующие данные:

- Все файлы из стандартных папок профиля пользователя, которые описаны следующим образом:
  - CSIDL_MYVIDEO
  - CSIDL_MYMUSIC
  - CSIDL_DESKTOP
  - CSIDL_STARTMENU
  - CSIDL_PERSONAL
  - CSIDL_MYPICTURES
  - CSIDL_FAVORITES
  - CSIDL_QUICK LAUNCH
- Файлы со следующими расширениями:

  `.accdb`, `.ch3`, `.csv`, `.dif`, `.doc*`, `.dot*`, `.dqy`, `.iqy`, `.mcw`, `.mdb*`, `.mpp`, `.one*`, `.oqy`, `.or6`, `.pot*`, `.ppa`, `.pps*`, `.ppt*`, `.pre`, `.pst`, `.pub`, `.qdf`, `.qel`, `.qph`, `.qsd`,

`.rqy`, `.rtf`, `.scd`, `.sh3`, `.slk`, `.txt`, `.vl*`, `.vsd`, `.wk*`, `.wpd`, `.wps`, `.wq1`, `.wri`, `.xl*`, `.xla`, `.xlb`, `.xls*`

> ⓘ **Примечание**
>
> Звездочка (`*`) означает ноль или больше символов.

> ⓘ **Примечание**
>
> Расширения OpenDocument (`*.odt`, `*.odp`, `*.ods`), которые могут использовать приложения Microsoft Office, по умолчанию не переносятся.

Файл по умолчанию `MigUser.xml` не переносит следующие данные:

- Файлы, помеченные как **скрытыми** , так и **системными** атрибутами.
- Файлы и папки на съемных дисках.
- Данные из `%WINDIR%` папок , `%PROGRAMFILES%`, `%PROGRAMDATA%` .
- ACLS для файлов в папках вне профиля пользователя.

Файл `MigUser.xml` можно скопировать, а затем изменить копию, чтобы включить или исключить стандартные папки профиля пользователя и расширения имен файлов. Если известны все расширения для файлов, которые необходимо перенести с исходного компьютера, используйте `MigUser.xml` файл для перемещения всех соответствующих данных независимо от расположения файлов. Однако добавление всех расширений файлов, которые необходимо перенести в файл, может привести к `MigUser.xml` миграции, содержащей больше файлов, чем предполагалось. Например, если переносятся все **файлы.jpg** , он также может переносить файлы изображений, такие как эскизы и логотипы, из устаревших приложений, установленных на исходном компьютере.

> ⓘ **Примечание**
>
> Каждое расширение имени файла, включенное в правила в `MigUser.xml` файле, увеличивает время, необходимое средству **ScanState** для сбора файлов для миграции. Если переносится более 300 типов файлов, процесс миграции может быть медленным. Дополнительные сведения о других способах

организации переноса данных см. в разделе Использование нескольких XML-файлов этой статьи.

Использование нескольких XML-файлов

С инструментами **ScanState** и **LoadState можно использовать несколько XML-файлов** . Каждый из XML-файлов по умолчанию, включенных или создаваемых USMT, настраивается для определенного компонента миграции. Пользовательские XML-файлы также можно использовать для дополнения этих файлов по умолчанию дополнительными правилами миграции.

Развернуть таблицу

Файл миграции XML	Изменяет следующие компоненты:
файлConfig.xml	Компоненты операционной системы, такие как обои для рабочего стола и фоновая тема. Можно `Config.xml` также расширить, чтобы включить некоторые параметры приложения и документа, создав `Config.xml` файл с другими XML-файлами по умолчанию. Дополнительные сведения см. в разделе Настройка XML-файлов USMT и файлаConfig.xml.
файлMigApps.xml	Параметры приложений.
файлыMigUser.xml или **MigDocs.xml**	Пользовательские файлы и параметры профиля.
Пользовательские XML-файлы	Параметры приложения, параметры профиля пользователя или файлы пользователей, помимо правил, содержащихся в других XML-файлах.

Например, все типы файлов миграции XML можно использовать для одной миграции, как показано в следующем примере:

Командная строка Windows

```
ScanState.exe <store> /config:c:\myFolder\Config.xml /i:migapps.xml
/i:MigDocs.xml /i:CustomRules.xml
```

Правила XML для переноса пользовательских файлов

Важно!

Файлы `MigUser.xml` и `MigDocs.xml` не должны использоваться вместе в одной команде. Использование обоих XML-файлов может привести к дублированию некоторых перенесенных файлов. Дублирование некоторых перенесенных файлов может произойти, если в каждом XML-файле предоставляются конфликтующие инструкции по расположению целевого объекта. Целевой файл сохраняется один раз во время миграции, но каждый XML-файл применяет его к другому расположению на конечном компьютере.

Если набор данных неизвестен или много файлов хранится за пределами стандартных папок профиля пользователя, `MigDocs.xml` лучше выбрать, чем `MigUser.xml` файл, так как `MigDocs.xml` файл собирает более широкий область данных. Файл `MigDocs.xml` переносит папки данных в зависимости от расположения. Файл `MigUser.xml` переносит только файлы с указанными расширениями имен файлов.

Чтобы получить дополнительный контроль над миграцией, создайте пользовательские XML-файлы. Дополнительные сведения о создании пользовательских XML-файлов см. в статье Создание и редактирование настраиваемого XML-файла.

Создание и редактирование пользовательского XML-файла

Параметр `/genmigxml` командной строки можно использовать для определения файлов, включенных в миграцию. Параметр `/genmigxml` создает файл в указанном расположении. Затем можно просмотреть XML-правила в файле и при необходимости внести изменения.

ⓘ Примечание

Если USMT переустановлен, XML-файлы миграции по умолчанию перезаписываются, а все настройки, внесенные в эти файлы, теряются. Рассмотрите возможность создания отдельных XML-файлов для пользовательских правил миграции и их сохранения в безопасном расположении.

Чтобы создать файл правил миграции XML для исходного компьютера, выполните следующие действия:

1. Выберите **Запустить**>**все программы**>**Аксессуары**
2. Щелкните правой кнопкой мыши **командную строку** и выберите **Пункт Запустить от имени**.
3. Выберите учетную запись с правами администратора, введите пароль и нажмите **кнопку ОК**.
4. В командной строке введите:

   Командная строка Windows

   ```
   cd /d <USMTpath>
   ScanState.exe /genmigxml: <filepath.xml>
   ```

   где:

   - **<USMTpath>** — расположение на исходном компьютере сохраненных файлов и средств USMT.
   - **< >filepath.xml** — полный путь к файлу, в котором можно сохранить отчет.

   Например, введите:

   Командная строка Windows

   ```
   cd /d c:\USMT
   ScanState.exe /genmigxml:"C:\Users\USMT Tester\Desktop\genMig.xml"
   ```

Функция GenerateDocPatterns

Файл `MigDocs.xml` вызывает функцию `GenerateDocPatterns` , которая принимает три логических значения. Параметры можно изменить, чтобы изменить способ создания xml-правил для миграции в `MigDocs.xml` файле.

- `ScanProgramFiles`: этот аргумент действителен, только если `GenerateDocPatterns` функция вызывается в системном контексте. Этот аргумент определяет, следует ли сканировать каталог Program Files для сбора зарегистрированных расширений имен файлов для известных приложений.

  Значение по умолчанию: False

  Например, если задано значение **TRUE**, функция обнаруживает и переносит **файлы.doc** в каталог Microsoft Office, так как **.doc** — это расширение имени

файла, зарегистрированное в приложении Microsoft Office. Функция `GenerateDocPatterns` создает этот шаблон включения для `.doc` файлов:

```
<pattern type="File">C:\Program Files\Microsoft Office[.doc]</pattern>
```

Если дочерняя папка включенной папки содержит установленное приложение, `ScanProgramFiles` также создает правило исключения для дочерней папки. Все папки в папке приложения проверяются рекурсивно на наличие зарегистрированных расширений имен файлов.

- `IncludePatterns`: этот аргумент определяет, следует ли создавать шаблоны исключений или включать их в XML. Если для этого аргумента задано значение **TRUE**, `GenerateDocPatterns` функция создает шаблоны include, и функция должна быть добавлена `<include>` в элемент . При изменении этого аргумента на **FALSE** создаются шаблоны исключения, и функция должна быть добавлена `<exclude>` в элемент .

  Значение по умолчанию: True

- `SystemDrive`: этот аргумент определяет, следует ли создавать шаблоны для всех фиксированных дисков или только для системного диска. При изменении этого аргумента на **TRUE** все шаблоны ограничиваются системным диском.

  Значение по умолчанию: False

Употребление:

Командная строка Windows

```
MigXmlHelper.GenerateDocPatterns ("<ScanProgramFiles>", "<IncludePatterns>",
"<SystemDrive>")
```

Чтобы создать шаблоны данных только для системного диска, выполните следующие действия:

XML

```
<include filter='MigXmlHelper.IgnoreIrrelevantLinks()'>
     <objectSet>
        <script>MigXmlHelper.GenerateDocPatterns ("FALSE","TRUE","TRUE")
</script>
     </objectSet>
</include>
```

Чтобы создать правило включения для сбора файлов для зарегистрированных расширений из каталога %PROGRAMFILES%, выполните следующие действия:

```xml
<include filter='MigXmlHelper.IgnoreIrrelevantLinks()'>
     <objectSet>
        <script>MigXmlHelper.GenerateDocPatterns ("TRUE","TRUE","FALSE")
</script>
     </objectSet>
</include>
```

Чтобы создать шаблоны данных исключения, выполните приведенные далее действия.

```xml
<exclude filter='MigXmlHelper.IgnoreIrrelevantLinks()'>
     <objectSet>
        <script>MigXmlHelper.GenerateDocPatterns ("FALSE","FALSE","FALSE")
</script>
     </objectSet>
</exclude>
```

Общие сведения о системном и пользовательском контексте

XML-файлы миграции содержат два <компонента> с разными параметрами **контекста** :

- Системный контекст применяется к файлам на компьютере, которые не хранятся в каталоге профилей пользователей.
- Контекст пользователя применяется к файлам, которые относятся к конкретному пользователю.

Контекст системы

Системный контекст включает правила для данных за пределами каталога профилей пользователей. Например, при вызове в системном контексте в `MigDocs.xml` файле `GenerateDocPatterns` функция создает шаблоны для всех общих папок оболочки, файлов в корневом каталоге жестких дисков и папок, расположенных в корне жестких дисков. В состав входят следующие папки:

- CSIDL_COMMON_DESKTOPDIRECTORY

- CSIDL_COMMON_FAVORITES
- CSIDL_COMMON_DOCUMENTS
- CSIDL_COMMON_MUSIC
- CSIDL_COMMON_PICTURES
- CSIDL_COMMON_VIDEO
- FOLDERID_PublicDownloads

Контекст пользователя

Контекст пользователя содержит правила для данных в каталоге Профилей пользователей. При вызове в контексте пользователя в `MigDocs.xml` файле `GenerateDocPatterns` функция создает шаблоны для всех папок оболочки пользователя, файлов, расположенных в корне профиля, и папок, расположенных в корне профиля. В состав входят следующие папки:

- CSIDL_MYDOCUMENTS
- CSIDL_MYPICTURES
- FOLDERID_OriginalImages
- CSIDL_MYMUSIC
- CSIDL_MYVIDEO
- CSIDL_FAVORITES
- CSIDL_DESKTOP
- CSIDL_QUICKLAUNCH
- FOLDERID_Contacts
- FOLDERID_Libraries
- FOLDERID_Downloads
- FOLDERID_SavedGames
- FOLDERID_RecordedTV

Примечание

Правила, содержащиеся в компоненте, которому назначен контекст пользователя выполняется для каждого профиля пользователя на компьютере. Файлы, которые сканируются несколько раз файлами `MigDocs.xml` , копируются в хранилище миграции только один раз. Однако большое количество правил в контексте пользователя может замедлить миграцию. Используйте системный контекст, если это применимо.

Примеры правил миграции для настраиваемых версий XML-файлов

Совет

Рекомендации и требования к настраиваемым XML-файлам в USMT см. в статье **Настройка XML-файлов USMT** и **общих соглашений**.

Примеры использования правил исключения

В следующих примерах исходный компьютер содержит **файл.txt** `new text document` в каталоге с именем `new folder`. Поведение по умолчанию `MigDocs.xml` переносит новый текстовый `document.txt` файл и все файлы, содержащиеся в каталоге `new folder` . Правила, создаваемые функцией:

Развернуть таблицу

Правило	Синтаксис
Правило 1	`<pattern type="File">d:\new folder[new text document.txt]</pattern>`
Правило 2	`<pattern type="File">d:\new folder[]</pattern>`

Чтобы исключить новый текстовый `document.txt` файл и все **файлы.txt** в `new folder`, можно внести следующие изменения:

Пример 1. Исключение всех .txt файлов в папке

Чтобы исключить правило 1, должно быть точное совпадение имени файла. Однако для правила 2 можно создать шаблон для исключения файлов с помощью расширения имени файла.

XML

```
<exclude>
     <objectSet>
        <pattern type="File">D:\Newfolder\[new text document.txt]</pattern>
         <pattern type="File">D:\New folder\*[*.txt]</pattern>
     </objectSet>
</exclude>
```

Пример 2. Использование элемента UnconditionalExclude для предоставления правилу приоритета над правилами включения

Если имя файла или расположение файла неизвестно, но расширение имени файла известно, можно использовать функцию `GenerateDrivePatterns` . Однако правило менее специфично, чем правило включения по умолчанию, созданное файлом `MigDocs.xml` , поэтому оно не имеет приоритета. Элемент <UnconditionalExclude> должен использоваться для предоставления этому правилу приоритета над правилом включения по умолчанию. Дополнительные сведения о порядке приоритета для правил миграции XML см. в разделе Конфликты и приоритет.

XML

```
<unconditionalExclude>
     <objectSet>
        <script>MigXmlHelper.GenerateDrivePatterns ("*[*.txt]", "Fixed")
</script>
     </objectSet>
</unconditionalExclude>
```

Пример 3. Использование компонента контекста UserandSystem для выполнения правил в обоих контекстах

Чтобы применить **<элемент UnconditionalExclude>** как к системе, так и к контексту пользователя, можно создать третий компонент с помощью контекста **UserandSystem** . Правила в этом компоненте выполняются в обоих контекстах.

XML

```
<component type="Documents" context="UserandSystem">
   <displayName>MigDocExcludes</displayName>
   <role role="Data">
     <rules>
       <unconditionalExclude>
         <objectSet>
                <script>MigXmlHelper.GenerateDrivePatterns ("*[*.txt]",
```

```
"Fixed")</script>
         </objectSet>
       </unconditionalExclude>
     </rules>
   </role>
</component>
```

Дополнительные примеры правил исключения, которые можно использовать в XML-файлах пользовательской миграции, см. в разделе Исключение файлов и параметров.

Включение примеров использования правил

Каталог данных приложения — это наиболее распространенное расположение, в которое необходимо добавить правило включения. Функция `GenerateDocPatterns` по умолчанию исключает это расположение. Если организация использует приложение, которое сохраняет важные данные в этом расположении, можно создать правила включения для переноса данных. Например, по умолчанию **для PST-файлов** используется расположение: `%CSIDL_LOCAL_APPDATA%\Microsoft\Outlook`. Файл `MigApp.xml` содержит правила миграции для перемещения только тех **PST-файлов** , которые связаны с Microsoft Outlook. Чтобы включить **PST-файлы** , которые не связаны, можно внести следующее изменение:

Пример 1. Включение расширения имени файла в папку известного пользователя

Это правило включает **PST-файлы** , которые находятся в расположении по умолчанию, но не связаны с Microsoft Outlook. Используйте контекст пользователя, чтобы запустить это правило для каждого пользователя на компьютере.

XML

```
<include filter='MigXmlHelper.IgnoreIrrelevantLinks()'>
     <objectSet>
        <pattern type="File">%CSIDL_LOCAL_APPDATA%\Microsoft\Outlook\*
[*.pst]</pattern>
     </objectSet>
</include>
```

Пример 2. Включение расширения имени файла в Program Files

Для расположений за пределами профиля пользователя, таких как папка Program Files, правило можно добавить в компонент контекста системы.

XML

```
<include filter='MigXmlHelper.IgnoreIrrelevantLinks()'>
     <objectSet>
        <pattern type="File">%CSIDL_PROGRAM_FILES%\*[*.pst]</pattern>
     </objectSet>
</include>
```

Дополнительные примеры правил включения, которые можно использовать в XML-файлах пользовательской миграции, см. в разделе Включение файлов и параметров.

Совет

Дополнительные сведения о порядке приоритета для правил миграции XML см. в разделе **Конфликты и приоритет**.

Дальнейшие действия

Дополнительные правила для миграции можно включить в `MigDocs.xml` файл или другие XML-файлы миграции. Например, элемент можно использовать для перемещения файлов из папки, `<locationModify>` в которой они были собраны, в другую папку при их применении к конечному компьютеру.

Xml-файл схемы (`MigXML.xsd`) можно использовать для проверки синтаксиса настраиваемых XML-файлов. Дополнительные сведения см. в разделе Ресурсы USMT.

Связанные статьи

- Исключите файлы и параметры.
- Включите файлы и параметры.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Файл Config.xml

Статья • 29.01.2025 • Применяется к: ✅ Windows 11, ✅ Windows 10

Этот `Config.xml` файл является необязательным файлом средства миграции пользовательской среды (USMT), который можно создать с помощью `/genconfig` параметра с помощью средства **ScanState** . Если необходимо включить все компоненты по умолчанию и не нужно вносить изменения в поведение создания хранилища или миграции профилей `Config.xml` по умолчанию, файл создавать не нужно.

Однако если поведение миграции по умолчанию, определенное `MigApp.xml` в файлах , `MigUser.xml` и `MigDocs.xml` является удовлетворительным, но некоторые компоненты необходимо исключить, файл можно создать и изменить, `Config.xml` оставив остальные **файлы.xml** без изменений. Например, необходимо создать файл, `Config.xml` чтобы исключить какие-либо из перенесенных параметров операционной системы. Необходимо создать и изменить файл, `Config.xml` чтобы изменить поведение по умолчанию для создания хранилища или миграции профилей.

Формат `Config.xml` файла отличается от формата других **файлов.xml** миграции, так как он не содержит никаких правил миграции. Он содержит только список компонентов операционной системы, приложений, документов пользователей, которые можно перенести, а также политики профилей пользователей и политики управления ошибками. По этой причине исключить компоненты, использующие `Config.xml` файл, проще, чем **изменять.xmlфайлы** миграции, так как знакомство с правилами миграции и синтаксисом не требуется. Однако в этом файле нельзя использовать подстановочные знаки.

Дополнительные сведения об использовании `Config.xml` файла с другими файлами миграции, такими как файлы и `MigApps.xml`, см. в `MigDocs.xml` разделе Общие сведения о XML-файлах миграции.

> ⓘ **Примечание**
>
> Чтобы исключить компонент из `Config.xml` файла, задайте для **параметра миграции** значение **нет**. Удаление XML-тега компонента из `Config.xml` файла не исключает компонент из миграции.

Политики миграции

В USMT есть политики миграции, которые можно настроить в `Config.xml` файле. Например, <**можно настроить параметры ErrorControl**>, <**ProfileControl**> и <**HardLinkStoreControl**> . Следующие элементы и параметры предназначены только для использования в `Config.xml` файле.

<Политики>

Элемент <**Policies**> содержит элементы, описывающие политики, которым следует USMT при создании хранилища миграции. Допустимыми дочерними элементами <**элемента Policies**> являются <**ErrorControl**> и <**HardLinkStoreControl**>. Элемент <**Policies**> является дочерним элементом <**Configuration**>.

Синтаксис:

```
XML

<Policies> </Policies>
```

<ErrorControl>

Элемент <**ErrorControl**> является необязательным элементом, который можно настроить в `Config.xml` файле. Настраиваемые <**правила ErrorControl**> поддерживают только переменные среды для работающей операционной системы и пользователя, вошедшего в систему. В качестве обходного решения путь можно указать с помощью подстановочного знака (*).

- **Количество вхождений**: один раз для каждого компонента
- **Родительские элементы**: элемент **Policies**<>
- **Дочерние<элементы: элемент fileError**> и <**registryError**>

Синтаксис:

```
XML

<ErrorControl> </ErrorControl>
```

В следующем примере указывается, что все заблокированные файлы, независимо от их расположения (включая файлы в C:\Users), следует игнорировать. Однако

миграция завершается ошибкой, если не удается получить доступ к файлу в C:\Users по какой-либо другой причине. В следующем примере элемент **ErrorControl> игнорирует все проблемы при переносе разделов реестра,<** которые соответствуют предоставленному шаблону, и устраняет их в ошибке **"Отказано в доступе**".

Кроме того, порядок в **<разделе ErrorControl>** подразумевает приоритет. В этом примере первый **<тег nonFatal>** имеет приоритет над вторым **<неустраним>** . Этот приоритет применяется независимо от того, сколько тегов в списке.

XML

```xml
<ErrorControl>
  <fileError>
    <nonFatal errorCode="33">* [*]</nonFatal>
    <fatal errorCode="any">C:\Users\* [*]</fatal>
  </fileError>
  <registryError>
    <nonFatal errorCode="5">HKCU\SOFTWARE\Microsoft\* [*]</nonFatal>
  </registryError>
</ErrorControl>
```

ⓘ Важно!

Настраиваемые **<правила ErrorControl>** поддерживают только переменные среды для работающей операционной системы и пользователя, вошедшего в систему. В качестве обходного решения можно указать путь, использующий подстановочный знак (*).

<роковой>

Неустранимый<> элемент не требуется.

- **Количество вхождений**: один раз для каждого компонента
- **Родительские элементы**: **<fileError>** и **<registryError>**
- **Дочерние элементы**: None.

Синтаксис:

XML

```xml
<fatal errorCode="any"> <specify pattern here> </fatal>
```

Развернуть таблицу

Параметр	Обязательный	Значение
errorCode	Нет	"any" или "*укажите системное сообщение об ошибке здесь*"

Неустранимый<> элемент можно использовать для указания того, что ошибки, соответствующие определенному шаблону, должны привести к остановке миграции USMT.

<fileError>

Элемент <**fileError**> не требуется.

- **Количество вхождений**: один раз для каждого компонента
- **Родительские элементы**: <**ErrorControl**>
- **Дочерние элементы**: <**nonFatal**> и <**fatal**>

Синтаксис:

```
XML

<fileError> </fileError>
```

Элемент <**fileError**> можно использовать для представления поведения, связанного с ошибками файла.

<NonFatal>

Элемент <**nonFatal**> не требуется.

- **Количество вхождений**: один раз для каждого компонента
- **Родительские элементы**: элементы <**fileError**> и <**registryError**> .
- **Дочерние элементы**: None.

Синтаксис:

```
XML

<nonfatal errorCode="any"> <specify pattern here> </nonFatal>
```

Развернуть таблицу

Параметр	Обязательный	Значение
<errorCode>	Нет	"any" или "*укажите системное сообщение об ошибке*". Если системные сообщения об ошибках не указаны, поведение по умолчанию применяет параметр ко всем сообщениям системных ошибок.

Элемент **<nonFatal>** можно использовать для указания того, что ошибки, соответствующие определенному шаблону, не должны приводить к остановке миграции USMT.

<registryError>

Элемент **<registryError>** не требуется.

- **Количество вхождений**: один раз для каждого компонента
- **Родительские элементы**: **<ErrorControl>**
- **Дочерние элементы**: **<нефатальный и неустранимый>><**

Синтаксис:

```
XML
<registryError errorcode="any"> </registryError>
```

Развернуть таблицу

Параметр	Обязательный	Значение
<errorCode>	Нет	"any" или "*укажите системное сообщение об ошибке здесь*". Если системные сообщения об ошибках не указаны, поведение по умолчанию применяет параметр ко всем сообщениям системных ошибок.

Элемент **<registryError>** можно использовать, чтобы указать, что ошибки, соответствующие определенному шаблону, не должны приводить к остановке миграции USMT.

<HardLinkStoreControl>

Элемент **<HardLinkStoreControl>** содержит элементы, описывающие обработку файлов во время создания хранилища миграции с жесткой компоновкой. Его единственным допустимым дочерним элементом является **<fileLocked>**.

Синтаксис:

```
XML

<HardLinkStoreControl> </HardLinkStoreControl>
```

- **Количество вхождений**: один раз для каждого компонента
- **Родительские элементы**: **<Политики>**
- **Дочерние элементы**: **<fileLocked>**

Синтаксис:

```
XML

<HardLinkStoreControl> </HardLinkStoreControl>
```

В следующем **<примере кода HardLinkStoreControl>** указано, что жесткие ссылки на заблокированные файлы можно создавать только в том случае, если заблокированный файл находится где-то в папке C:\Users\. В противном случае ошибка доступа к файлу возникает при обнаружении заблокированного файла, который не удается скопировать, даже если это технически возможно для создания ссылки.

> ⓘ **Важно!**
>
> Раздел **<ErrorControl>** можно настроить так, чтобы условно игнорировать ошибки доступа к файлам в зависимости от расположения файла.

```
XML

<Policy>
   <HardLinkStoreControl>
      <fileLocked>
         <createHardLink>C:\Users\*</createHardLink>
         <errorHardLink>C:\*</errorHardLink>
      </fileLocked>
   </HardLinkStoreControl>
   <ErrorControl>
      […]
```

```
    </ErrorControl>
</Policy>
```

<fileLocked>

Элемент **<fileLocked>** содержит элементы, описывающие обработку файлов, заблокированных для редактирования. Правила, определенные элементом **<fileLocked>** , обрабатываются в том порядке, в котором они отображаются в XML-файле.

Синтаксис:

```
XML

<fileLocked> </fileLocked>
```

<createHardLink>

Элемент **<createHardLink>** определяет стандартный шаблон MigXML, описывающий пути к файлам, в которых должны создаваться жесткие ссылки, даже если файл заблокирован для редактирования другим приложением.

Синтаксис:

```
XML

<createHardLink> <specify pattern here> </createHardLink>
```

<errorHardLink>

Элемент **<errorHardLink>** определяет стандартный шаблон MigXML, описывающий пути к файлам, в которых не следует создавать жесткие ссылки, если файл заблокирован для редактирования другим приложением. USMT пытается скопировать файлы по этим путям в хранилище миграции. Однако если это невозможно, **возникает Error_Locked** . Эта ошибка представляет собой стандартную ошибку API Для Windows, которая может быть записана **<в разделе ErrorControl>** , чтобы привести к тому, что USMT пропустит файл или прервать миграцию.

Синтаксис:

```
```

XML

```
<errorHardLink> <specify pattern here> </errorHardLink>
```

<ProfileControl>

Этот элемент используется для хранения других элементов, устанавливающих правила для миграции профилей, пользователей и политик в отношении членства в локальных группах во время миграции. **<ProfileMigration>** является дочерним **<элементом Configuration>**.

Синтаксис:

XML

```
<ProfileControl> </ProfileControl>
```

<localGroups>

Этот элемент используется для хранения других элементов, устанавливающих правила миграции локальных групп. **<localGroups>** является дочерним **<элементом ProfileControl>**.

Синтаксис:

XML

```
<localGroups> </localGroups>
```

<Сопоставления>

Этот элемент используется для хранения других элементов, которые устанавливают сопоставления между группами.

Синтаксис:

XML

```
<mappings> </mappings>
```

<changeGroup>

Этот элемент описывает исходные и целевые группы для изменения членства в локальной группе во время миграции. Это дочерний элемент **<localGroups>**. Определяются следующие параметры:

Развернуть таблицу

Параметр	Обязательный	Значение
Исходная версия	Да	Допустимая локальная группа на исходном компьютере, содержащая пользователей, выбранных для миграции в командной строке.
Результат	Да	Локальная группа, в которую будут перемещены пользователи во время миграции.
appliesTo	Да	nonmigratedUsers, migratedUsers, AllUsers. Это значение определяет пользователей, к которым должна применяться операция группы изменений.

Допустимые и обязательные дочерние элементы **<changeGroup>включаются> и исключаются<>.<** Хотя оба могут быть дочерними одновременно, требуется только один.

Синтаксис:

```
XML
<changeGroup From="Group1" To= "Group2"> </changeGroup>
```

<include>

Этот элемент указывает, что его обязательный дочерний элемент, *<шаблон>*, должен быть включен в миграцию.

Синтаксис:

```
XML
<include> </include>
```

<exclude>

Этот элемент указывает, что его обязательный дочерний элемент, *<шаблон>*, должен быть исключен из миграции.

Синтаксис:

XML

```
<exclude> </exclude>
```

Пример файла Config.xml

В следующем примере `Config.xml` файла содержатся подробные примеры элементов, которые можно исключить из миграции.

▼ Разверните для примера файла Config.xml:

XML

```
<?xml version="1.0" encoding="UTF-8"?>
<Configuration>
  <Applications/>
  <Documents/>
  <WindowsComponents>
    <component displayname="Tablet PC Settings" migrate="yes"
ID="tablet_pc_settings">
      <component displayname="Accessories" migrate="yes"
ID="tablet_pc_settings\tablet_pc_accessories">
        <component displayname="Microsoft-Windows-TabletPC-StickyNotes"
migrate="yes"
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
tabletpc-stickynotes/microsoft-windows-tabletpc-stickynotes/settings"/>
        <component displayname="Microsoft-Windows-TabletPC-SnippingTool"
migrate="yes"
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
tabletpc-snippingtool/microsoft-windows-tabletpc-snippingtool/settings"/>
        <component displayname="Microsoft-Windows-TabletPC-Journal"
migrate="yes"
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
tabletpc-journal/microsoft-windows-tabletpc-journal/settings"/>
      </component>
      <component displayname="Input Panel" migrate="yes"
ID="tablet_pc_settings\tablet_pc_input_panel">
        <component displayname="Microsoft-Windows-TabletPC-InputPanel"
migrate="yes"
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
tabletpc-inputpanel/microsoft-windows-tabletpc-inputpanel/settings"/>
      </component>
      <component displayname="General Options" migrate="yes"
ID="tablet_pc_settings\tablet_pc_general_options">
        <component displayname="Microsoft-Windows-TabletPC-UIHub"
migrate="yes"
```

```
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
tabletpc-uihub/microsoft-windows-tabletpc-uihub/settings"/>
        <component displayname="Microsoft-Windows-TabletPC-Platform-Input-
Core" migrate="yes"
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
tabletpc-platform-input-core/microsoft-windows-tabletpc-platform-input-
core/settings"/>
      </component>
      <component displayname="Handwriting Recognition" migrate="yes"
ID="tablet_pc_settings\handwriting_recognition">
        <component displayname="Microsoft-Windows-TabletPC-
InputPersonalization" migrate="yes"
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
tabletpc-inputpersonalization/microsoft-windows-tabletpc-
inputpersonalization/settings"/>
      </component>
    </component>
    <component displayname="Sound and Speech Recognition" migrate="yes"
ID="sound_and_speech_recognition">
      <component displayname="Speech Recognition" migrate="yes"
ID="sound_and_speech_recognition\speech_recognition">
        <component displayname="Microsoft-Windows-SpeechCommon"
migrate="yes"
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
speechcommon/microsoft-windows-speechcommon/settings"/>
      </component>
    </component>
    <component displayname="Hardware" migrate="yes" ID="hardware">
      <component displayname="Phone and Modem" migrate="yes"
ID="hardware\phone_and_modem">
        <component displayname="Microsoft-Windows-TapiSetup" migrate="yes"
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
tapisetup/microsoft-windows-tapisetup/settings"/>
      </component>
      <component displayname="Printers and Faxes" migrate="yes"
ID="hardware\printers_and_faxes">
        <component displayname="Microsoft-Windows-Printing-Spooler-Core"
migrate="yes"
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
printing-spooler-core/microsoft-windows-printing-spooler-core/settings"/>
        <component displayname="Microsoft-Windows-Printing-Spooler-
Networkclient" migrate="yes"
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
printing-spooler-networkclient/microsoft-windows-printing-spooler-
networkclient/settings"/>
        <component displayname="Microsoft-Windows-Printing-Spooler-Core-
Localspl" migrate="yes"
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
printing-spooler-core-localspl/microsoft-windows-printing-spooler-core-
localspl/settings"/>
      </component>
    </component>
    <component displayname="Programs" migrate="yes" ID="programs">
      <component displayname="Media Player Settings" migrate="yes"
ID="programs\media_player_settings">
```

```
        <component displayname="Microsoft-Windows-MediaPlayer-Migration"
migrate="yes"
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
mediaplayer-migration/microsoft-windows-mediaplayer-migration/settings"/>
      </component>
    </component>
    <component displayname="Communications and Sync" migrate="yes"
ID="communications_and_sync">
      <component displayname="Windows Mail" migrate="yes"
ID="communications_and_sync\windows_mail">
        <component displayname="Microsoft-Windows-WAB" migrate="yes"
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
wab/microsoft-windows-wab/settings"/>
        <component displayname="Microsoft-Windows-Mail" migrate="yes"
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
mail/microsoft-windows-mail/settings"/>
      </component>
    </component>
    <component displayname="Microsoft-Windows-Migration-DisplayGroups"
migrate="yes"
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
migration-displaygroups/microsoft-windows-migration-
displaygroups/settings"/>
    <component displayname="Performance and Maintenance" migrate="yes"
ID="performance_and_maintenance">
      <component displayname="Diagnostics" migrate="yes"
ID="performance_and_maintenance\diagnostics">
        <component displayname="Microsoft-Windows-RemoteAssistance-Exe"
migrate="yes"
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
remoteassistance-exe/microsoft-windows-remoteassistance-exe/settings"/>
        <component displayname="Microsoft-Windows-Feedback-Service"
migrate="yes"
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
feedback-service/microsoft-windows-feedback-service/settings"/>
      </component>
      <component displayname="Error Reporting" migrate="yes"
ID="performance_and_maintenance\error_reporting">
        <component displayname="Microsoft-Windows-ErrorReportingCore"
migrate="yes"
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
errorreportingcore/microsoft-windows-errorreportingcore/settings"/>
      </component>
    </component>
    <component displayname="Network and Internet" migrate="yes"
ID="network_and_internet">
      <component displayname="Offline Files" migrate="yes"
ID="network_and_internet\offline_files">
        <component displayname="Microsoft-Windows-OfflineFiles-Core"
migrate="yes"
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
offlinefiles-core/microsoft-windows-offlinefiles-core/settings"/>
      </component>
      <component displayname="Internet Options" migrate="yes"
ID="network_and_internet\internet_options">
```

```
        <component displayname="Microsoft-Windows-ieframe" migrate="yes"
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
ieframe/microsoft-windows-ieframe/settings"/>
        <component displayname="Microsoft-Windows-IE-InternetExplorer"
migrate="yes"
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
ie-internetexplorer/microsoft-windows-ie-internetexplorer/settings"/>
        <component displayname="Microsoft-Windows-IE-Feeds-Platform"
migrate="yes"
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
ie-feeds-platform/microsoft-windows-ie-feeds-platform/settings"/>
        <component displayname="Microsoft-Windows-IE-
ClientNetworkProtocolImplementation" migrate="yes"
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
ie-clientnetworkprotocolimplementation/microsoft-windows-ie-
clientnetworkprotocolimplementation/settings"/>
      </component>
      <component displayname="Networking Connections" migrate="yes"
ID="network_and_internet\networking_connections">
        <component displayname="Microsoft-Windows-Wlansvc" migrate="yes"
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
wlansvc/microsoft-windows-wlansvc/settings"/>
        <component displayname="Microsoft-Windows-RasConnectionManager"
migrate="yes"
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
rasconnectionmanager/microsoft-windows-rasconnectionmanager/settings"/>
        <component displayname="Microsoft-Windows-RasApi" migrate="yes"
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
rasapi/microsoft-windows-rasapi/settings"/>
        <component displayname="Microsoft-Windows-PeerToPeerCollab"
migrate="yes"
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
peertopeercollab/microsoft-windows-peertopeercollab/settings"/>
        <component displayname="Microsoft-Windows-MPR" migrate="yes"
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
mpr/microsoft-windows-mpr/settings"/>
        <component displayname="Microsoft-Windows-Dot3svc" migrate="yes"
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
dot3svc/microsoft-windows-dot3svc/settings"/>
      </component>
    </component>
    <component displayname="Date, Time, Language and Region" migrate="yes"
ID="date_time_language_and_region">
      <component displayname="Regional Language Options" migrate="yes"
ID="date_time_language_and_region\regional_language_options">
        <component displayname="Microsoft-Windows-TableDrivenTextService-
Migration" migrate="yes"
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
tabledriventextservice-migration/microsoft-windows-tabledriventextservice-
migration/settings"/>
        <component displayname="Microsoft-Windows-TextServicesFramework-
Migration" migrate="yes"
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
textservicesframework-migration/microsoft-windows-textservicesframework-
migration/settings"/>
```

```
        <component displayname="Microsoft-Windows-MUI-Settings"
migrate="yes"
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
mui-settings/microsoft-windows-mui-settings/settings"/>
        <component displayname="Microsoft-Windows-International-Core"
migrate="yes"
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
international-core/microsoft-windows-international-core/settings"/>
        <component displayname="Microsoft-Windows-IME-Traditional-Chinese-
Core" migrate="yes"
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
ime-traditional-chinese-core/microsoft-windows-ime-traditional-chinese-
core/settings"/>
        <component displayname="Microsoft-Windows-IME-Simplified-Chinese-
Core" migrate="yes"
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
ime-simplified-chinese-core/microsoft-windows-ime-simplified-chinese-
core/settings"/>
        <component displayname="Microsoft-Windows-Desktop_Technologies-
Text_Input_Services-IME-Japanese-Core" migrate="yes"
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
desktop_technologies-text_input_services-ime-japanese-core/microsoft-
windows-desktop_technologies-text_input_services-ime-japanese-
core/settings"/>
      </component>
    </component>
    <component displayname="Security" migrate="yes" ID="security">
      <component displayname="Microsoft-Windows-Rights-Management-Client-v1-
API" migrate="yes"
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
rights-management-client-v1-api/microsoft-windows-rights-management-client-
v1-api/settings"/>
      <component displayname="Security Options" migrate="yes"
ID="security\security_options">
        <component displayname="Microsoft-Windows-Credential-Manager"
migrate="yes"
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
credential-manager/microsoft-windows-credential-manager/settings"/>
      </component>
    </component>
    <component displayname="Appearance and Display" migrate="yes"
ID="appearance_and_display">
      <component displayname="Windows Games Settings" migrate="yes"
ID="appearance_and_display\windows_games_settings">
        <component displayname="Microsoft-Windows-GameExplorer"
migrate="yes"
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
gameexplorer/microsoft-windows-gameexplorer/settings"/>
      </component>
      <component displayname="Taskbar and Start Menu" migrate="yes"
ID="appearance_and_display\taskbar_and_start_menu">
        <component displayname="Microsoft-Windows-stobject" migrate="yes"
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
stobject/microsoft-windows-stobject/settings"/>
        <component displayname="Microsoft-Windows-explorer" migrate="yes"
```

```
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
explorer/microsoft-windows-explorer/settings"/>
      </component>
      <component displayname="Personalized Settings" migrate="yes"
ID="appearance_and_display\personalized_settings">
        <component displayname="Microsoft-Windows-uxtheme" migrate="yes"
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
uxtheme/microsoft-windows-uxtheme/settings"/>
        <component displayname="Microsoft-Windows-themeui" migrate="yes"
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
themeui/microsoft-windows-themeui/settings"/>
        <component displayname="Microsoft-Windows-shmig" migrate="yes"
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
shmig/microsoft-windows-shmig/settings"/>
        <component displayname="Microsoft-Windows-shell32" migrate="yes"
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
shell32/microsoft-windows-shell32/settings"/>
        <component displayname="Microsoft-Windows-CommandPrompt"
migrate="yes"
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
commandprompt/microsoft-windows-commandprompt/settings"/>
      </component>
    </component>
    <component displayname="Additional Options" migrate="yes"
ID="additional_options">
      <component displayname="Help Settings" migrate="yes"
ID="additional_options\help_settings">
        <component displayname="Microsoft-Windows-Help-Client" migrate="yes"
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
help-client/microsoft-windows-help-client/settings"/>
      </component>
      <component displayname="Windows Core Settings" migrate="yes"
ID="additional_options\windows_core_settings">
        <component displayname="Microsoft-Windows-Win32k-Settings"
migrate="yes"
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
win32k-settings/microsoft-windows-win32k-settings/settings"/>
        <component displayname="Microsoft-Windows-Web-Services-for-
Management-Core" migrate="yes"
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
web-services-for-management-core/microsoft-windows-web-services-for-
management-core/settings"/>
        <component displayname="Microsoft-Windows-UPnPSSDP" migrate="yes"
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
upnpssdp/microsoft-windows-upnpssdp/settings"/>
        <component displayname="Microsoft-Windows-UPnPDeviceHost"
migrate="yes"
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
upnpdevicehost/microsoft-windows-upnpdevicehost/settings"/>
        <component displayname="Microsoft-Windows-UPnPControlPoint"
migrate="yes"
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
upnpcontrolpoint/microsoft-windows-upnpcontrolpoint/settings"/>
        <component displayname="Microsoft-Windows-TerminalServices-
RemoteConnectionManager" migrate="yes"
```

```
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
terminalservices-remoteconnectionmanager/microsoft-windows-terminalservices-
remoteconnectionmanager/settings"/>
        <component displayname="Microsoft-Windows-TerminalServices-Drivers"
migrate="yes"
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
terminalservices-drivers/microsoft-windows-terminalservices-
drivers/settings"/>
        <component displayname="Microsoft-Windows-SQMApi" migrate="yes"
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
sqmapi/microsoft-windows-sqmapi/settings"/>
        <component displayname="Microsoft-Windows-RPC-Remote" migrate="yes"
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
rpc-remote/microsoft-windows-rpc-remote/settings"/>
        <component displayname="Microsoft-Windows-RPC-Local" migrate="yes"
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
rpc-local/microsoft-windows-rpc-local/settings"/>
        <component displayname="Microsoft-Windows-RPC-HTTP" migrate="yes"
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
rpc-http/microsoft-windows-rpc-http/settings"/>
        <component displayname="Microsoft-Windows-Rasppp" migrate="yes"
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
rasppp/microsoft-windows-rasppp/settings"/>
        <component displayname="Microsoft-Windows-RasMprDdm" migrate="yes"
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
rasmprddm/microsoft-windows-rasmprddm/settings"/>
        <component displayname="Microsoft-Windows-RasBase" migrate="yes"
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
rasbase/microsoft-windows-rasbase/settings"/>
        <component displayname="Microsoft-Windows-Microsoft-Data-Access-
Components-(MDAC)-ODBC-DriverManager-Dll" migrate="yes"
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
microsoft-data-access-components-(mdac)-odbc-drivermanager-dll/microsoft-
windows-microsoft-data-access-components-(mdac)-odbc-drivermanager-
dll/settings"/>
        <component displayname="Microsoft-Windows-ICM-Profiles"
migrate="yes"
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
icm-profiles/microsoft-windows-icm-profiles/settings"/>
        <component displayname="Microsoft-Windows-feclient" migrate="yes"
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
feclient/microsoft-windows-feclient/settings"/>
        <component displayname="Microsoft-Windows-dpapi-keys" migrate="yes"
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
dpapi-keys/microsoft-windows-dpapi-keys/settings"/>
        <component displayname="Microsoft-Windows-Crypto-keys" migrate="yes"
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
crypto-keys/microsoft-windows-crypto-keys/settings"/>
        <component displayname="Microsoft-Windows-COM-DTC-Setup"
migrate="yes"
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
com-dtc-setup/microsoft-windows-com-dtc-setup/settings"/>
        <component displayname="Microsoft-Windows-COM-ComPlus-Setup"
migrate="yes"
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
```

```
com-complus-setup/microsoft-windows-com-complus-setup/settings"/>
        <component displayname="Microsoft-Windows-COM-Base" migrate="yes"
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
com-base/microsoft-windows-com-base/settings"/>
        <component displayname="Microsoft-Windows-CAPI2-certs" migrate="yes"
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
capi2-certs/microsoft-windows-capi2-certs/settings"/>
      </component>
    </component>
    <component displayname="Accessibility" migrate="yes" ID="accessibility">
      <component displayname="Accessibility Settings" migrate="yes"
ID="accessibility\accessibility_settings">
        <component displayname="Microsoft-Windows-accessibilitycpl"
migrate="yes"
ID="http://www.microsoft.com/migration/1.0/migxmlext/cmi/microsoft-windows-
accessibilitycpl/microsoft-windows-accessibilitycpl/settings"/>
      </component>
    </component>
  </WindowsComponents>
  <Policies>
    <ErrorControl>
      <!--   Example:

          <fileError>
            <nonFatal errorCode="33">* [*]</nonFatal>
            <fatal errorCode="any">C:\Users\* [*]</fatal>
          </fileError>
          <registryError>
            <nonFatal errorCode="5">* [*]</nonFatal>
          </registryError>
      -->
    </ErrorControl>
    <HardLinkStoreControl>
      <!--   Example:

          <fileLocked>
            <createHardLink>c:\Users\* [*]</createHardLink>
            <errorHardLink>C:\* [*]</errorHardLink>
          </fileLocked>
      -->
    </HardLinkStoreControl>
  </Policies>
  <ProfileControl>
    <!--   Example:

          <localGroups>
            <mappings>
              <changeGroup from="Administrators" to="Users"
appliesTo="MigratedUsers">
                <include>
                  <pattern>DomainName1\Username</pattern>
                </include>
                <exclude>
                  <pattern>DomainName2\Username</pattern>
                </exclude>
```

```
            </changeGroup>
          </mappings>
        </localGroups>

      -->
  </ProfileControl>
</Configuration>
```

Связанные статьи

- Справочник по XML-файлу USMT.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Настройка XML-файлов USMT

Статья • 29.01.2025 • Применяется к: ✅ Windows 11, ✅ Windows 10

Обзор

Чтобы использовать любой из **файлов.xml** миграции со средствами **ScanState** и **LoadState** , укажите эти файлы в командной строке `/i` с помощью параметра . Так как **средствам ScanState** и **LoadState** требуются **файлы.xml** для управления миграцией, укажите один и тот же набор **файлов.xml** для `ScanState.exe` команд и `LoadState.exe` . Тем не менее, `Config.xml` файл с параметром `/config` указывать не нужно, если только некоторые из перенесенных файлов и параметров из хранилища не должны быть исключены. Например, чтобы перенести папку **Documents** в хранилище, но не на конечный компьютер. Чтобы реализовать этот сценарий, измените `Config.xml` файл и укажите обновленный файл с помощью `LoadState.exe` команды . Затем `LoadState.exe` команда переносит только нужные файлы и параметры.

Если **.xml** файл отсутствует из `LoadState.exe` команды, переносятся все данные в хранилище, перенесенные с отсутствующими **файлами.xml** . Однако правила миграции, указанные `ScanState.exe` с помощью команды , не применяются. Например, если **файл.xml** отсутствует и содержит правило перенаправки, например:

```
MigsysHelperFunction.RelativeMove("c:\data", "%CSIDL_PERSONAL%")
```

USMT не перенаправляет файлы, и они переносятся в `C:\data`.

Чтобы изменить миграцию, выполните одно или несколько из следующих действий.

- **Измените файлы .xml миграции.** Чтобы исключить часть компонента, измените **файлы.xml** . Например, для переноса C:\, но исключения всех **.mp3** файлов или для перемещения данных в новое расположение на конечном компьютере. Чтобы изменить эти файлы, необходимо ознакомиться с правилами и синтаксисом миграции. Чтобы использовать эти файлы **в ScanState** и **LoadState** , укажите их в командной строке при вводе каждой команды.
- **Создайте пользовательский файл .xml.** Можно также создать пользовательский **файл.xml** , чтобы перенести параметры для другого

приложения или изменить поведение миграции в соответствии с потребностями организации. Чтобы использовать этот файл **в ScanState** и **LoadState** , укажите их в обеих командных строках.

- **Создайте и измените файл Config.xml.** Создайте и измените файл, `Config.xml` чтобы исключить весь компонент из миграции. Например, `Config.xml` файл можно использовать для исключения всей папки **Documents** или исключения параметров приложения. Исключить компоненты с помощью `Config.xml` файла проще, чем изменить **.xml** файлов миграции, так как знание правил и синтаксиса миграции не требуется. Кроме того, использование `Config.xml` файла — единственный способ исключить параметры операционной системы из переноса.

Дополнительные сведения об исключении данных см. в статье Исключение файлов и параметров .

Перенос файлов .xml

В этом разделе описывается **миграция.xml** файлов, включенных в USMT. Каждый файл содержит правила миграции, определяющие, какие компоненты переносятся и куда переносятся на конечном компьютере.

> ⓘ **Примечание**
>
> В каждом из этих файлов можно использовать подстановочный знак звездочки (*). Однако вопросительный знак (?) нельзя использовать в качестве подстановочного знака.

- **Файл MigApp.xml.** Укажите этот файл с помощью `ScanState.exe` команд и `LoadState.exe` для переноса параметров приложения.

- **Файл MigDocs.xml.** Укажите этот файл с помощью средств **ScanState** и **LoadState** , чтобы перенести все пользовательские папки и файлы, найденные вспомогательной функцией **MigXmlHelper.GenerateDocPatterns** . Эта вспомогающая функция находит данные пользователя, которые находятся в корне любого диска и в каталоге Users. Однако он не находит и не переносит данные приложения, файлы программ или файлы в каталоге Windows. Файл `MigDocs.xml` можно изменить.

- **Файл MigUser.xml.** Укажите этот файл с помощью `ScanState.exe` команд и `LoadState.exe` для переноса пользовательских папок, файлов и типов файлов.

Файл `MigUser.xml` можно изменить. Этот файл не содержит правил для переноса определенных учетных записей пользователей. Единственный способ указать, какие учетные записи пользователей следует перенести, — в командной строке с помощью параметров ScanState User и LoadState User.

> ⓘ **Примечание**
>
> Не используйте `MigUser.xml` файлы и `MigDocs.xml` вместе. Дополнительные сведения см. в статьях **Определение типов файлов, файлов и папок ирекомендаций по USMT** .

Пользовательские файлы .xml

Пользовательские.xml файлы можно создать, чтобы настроить миграцию в соответствии с уникальными потребностями организации. Например, можно создать пользовательский **файл.xml** , чтобы перенести бизнес-приложение или изменить поведение миграции по умолчанию. `LoadState.exe` Чтобы `ScanState.exe` использовать этот файл, укажите его с помощью обеих команд. Дополнительные сведения см. в статье Примеры пользовательских XML-файлов .

Файл Config.xml

Файл `Config.xml` является необязательным файлом, который создается с помощью `/genconfig` параметра с командой `ScanState.exe` . Этот файл необходимо создать и изменить, чтобы исключить определенные компоненты из миграции. Кроме того, этот файл необходимо создать и изменить, чтобы исключить какие-либо параметры операционной системы из переноса. Формат `Config.xml` файла отличается от **формата.xmlфайлов** миграции, так как он не содержит никаких правил миграции. Он содержит только список компонентов операционной системы, приложений и пользовательских документов, которые можно перенести. Пример см. в статье файлConfig.xml . По этой причине исключить компоненты, использующие `Config.xml` файл, проще, чем изменить миграцию **.xml** файлов. В , `Config.xml` знакомство с правилами миграции и синтаксисом не является. Однако подстановочные знаки нельзя использовать в `Config.xml` файле.

Чтобы включить все компоненты по умолчанию, `Config.xml` не нужно создавать файл. Кроме того, если поведение миграции по умолчанию, определенное `MigApp.xml` в файлах , `MigDocs.xml` и `MigUser.xml` , является удовлетворительным и

необходимо исключить только некоторые компоненты, `Config.xml` можно создать файл. Другие **.xml** файлы можно оставить в исходном состоянии.

При выполнении `ScanState.exe` команды с параметром `/genconfig` считывает другие **.xml** файлы, `ScanState.exe` указанные с помощью `/i` параметра , чтобы создать настраиваемый список компонентов, которые можно перенести с компьютера. Этот файл содержит только компоненты операционной системы, приложения и разделы пользовательского документа, которые находятся в обоих **файлах.xml** и устанавливаются на компьютере при выполнении `ScanState.exe` команды с параметром `/genconfig` . Таким образом, этот файл должен быть создан на исходном компьютере, который содержит все компоненты, приложения и параметры, которые присутствуют на конечных компьютерах. Создание файла на исходном компьютере гарантирует, что этот файл содержит все компоненты, которые можно перенести. Компоненты организованы по разделам: <Приложения>, <Компоненты Windows> и <Документы>. Чтобы не переносить компонент, измените его запись на `migrate="no"`.

После создания этого файла его необходимо указать только с `ScanState.exe` помощью команды с помощью `/Config` параметра , чтобы повлиять на миграцию. Однако если необходимо исключить дополнительные данные, перенесенные в хранилище, измените `Config.xml` файл и укажите обновленный файл с помощью `LoadState.exe` команды . Например, если папка **Documents** собирается в хранилище, но не требуется переносить папку **Documents** на конечный компьютер, файл можно изменить, `Config.xml` чтобы указать `migrate="no"` перед выполнением `LoadState.exe` команды, и файл не будет перенесен. Дополнительные сведения о приоритете, который имеет место при исключении данных, см. в статье Исключение файлов и параметров .

Кроме того, обратите внимание на следующие функциональные возможности файла `Config.xml` :

- Если родительский компонент удаляется из миграции в `Config.xml` файле путем указания `migrate="no"`, все его дочерние компоненты автоматически удаляются из миграции, даже если для дочернего компонента задано значение `migrate="yes"`.

- Если по ошибке для одного компонента существуют две строки кода, где одна строка указывает `migrate="no"` , а другая — `migrate="yes"`, компонент переносится.

- В USMT существует несколько политик миграции, которые можно настроить в `Config.xml` файле. Например, можно настроить дополнительные **<параметры ErrorControl>**, **<ProfileControl>** и **<HardLinkStoreControl>** . Дополнительные сведения см. в статье файлConfig.xml .

> ⓘ **Примечание**
>
> Чтобы исключить компонент из `Config.xml` файла, задайте для **параметра миграции** значение **"нет"**. Удаление XML-тега компонента из `Config.xml` файла не исключает компонент из миграции.

Примеры:

- Следующая команда создает `Config.xml` файл в текущем каталоге, но не создает хранилище:

  ```
  ScanState.exe /i:MigApp.xml /i:MigDocs.xml /genconfig:Config.xml /v:5
  ```

- Следующая команда создает зашифрованное хранилище с помощью `Config.xml` файла и миграции по умолчанию **.xml** файлов:

  ```
  ScanState.exe \\server\share\migration\mystore /i:MigApp.xml /i:MigDocs.xml /o
  /config:Config.xml /v:5 /encrypt /key:"mykey"
  ```

- Следующая команда расшифровывает хранилище и переносит файлы и параметры:

  ```
  LoadState.exe \\server\share\migration\mystore /i:MigApp.xml /i:MigDocs.xml
  /v:5 /decrypt /key:"mykey"
  ```

Дополнительные сведения

- Дополнительные сведения об изменении файлов и параметров, которые переносятся, см. в статьях о средстве миграции пользовательской среды (USMT).
- Дополнительные сведения о каждом **.xml** элементе см. в статье библиотека XML-элементов .
- Ответы на распространенные вопросы см. в разделе ".xml файлов" статьи Часто задаваемые вопросы .

Связанные статьи

- Синтаксис командной строки средства миграции пользовательской среды (USMT).
- Ресурсы USMT.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Примеры пользовательских файлов XML

Статья • 29.01.2025 • Применяется к: ✅ Windows 11, ✅ Windows 10

Пример 1. Перенос неподдерживаемого приложения

Следующий шаблон является шаблоном для разделов, необходимых для миграции приложений. Шаблон не работает сам по себе, но его можно использовать для записи **пользовательских.xml** файла.

Шаблон

▼ Разверните, чтобы отобразить пример **1** шаблона приложения:

XML

```
<migration
urlid="http://www.microsoft.com/migration/1.0/migxmlext/migtestapp">
  <component type="Application">
    <!-- Name of the application -->
    <displayName>Some Application</displayName>
    <!-- Specify whether the environment variables exist in the context of
user or system or both -->
    <environment context="System">
      <!-- Create the environment variables -->
      <variable name="myVar1">
        <!-- Simple text value assignment to a variable -->
        <text>value</text>
      </variable>
      <variable name="myAppExePath">
        <!-- Make a call to in-built helper function to get a value from a
reg key and assign that value to the variable -->

<script>MigXMLHelper.GetStringContent("Registry","HKLM\Software\MyApp\Instal
ler [EXEPATH]")</script>
      </variable>
    </environment>
    <role role="Settings">
      <detects>
        <!-- All of these checks must be true for the component to be
detected -->
        <detect>
          <!-- Make a call to in-built helper function to check if an object
exists or not -->

<condition>MigXMLHelper.DoesObjectExist("Registry","HKLM\Software\MyApp
[win32_version]")</condition>
```

```
        </detect>
        <detect>
          <!-- Either of these checks must be true for the component to be
detected -->
          <!-- Make a call to in-built helper function to check if a file
version matches or not -->

<condition>MigXMLHelper.DoesFileVersionMatch("%MyAppExePath%","ProductVersio
n","8.*")</condition>

<condition>MigXMLHelper.DoesFileVersionMatch("%MyAppExePath%","ProductVersio
n","9.*")</condition>
        </detect>
      </detects>
      <!-- Describe the rules that will be executed during migration of this
component and the context, whether user, system or both -->
      <rules context="User">
        <!-- Delete objects specified in the object set on the destination
computer before applying source objects -->
        <destinationCleanup>
          <!-- Describe the pattern for the list of objects to be deleted --
>
          <objectSet>
            <pattern type="Registry">HKCU\Software\MyApp\Toolbar\* [*]
</pattern>
            <pattern type="Registry">HKCU\Software\MyApp\ListView\* [*]
</pattern>
            <pattern type="Registry">HKCU\Software\MyApp [ShowTips]
</pattern>
          </objectSet>
        </destinationCleanup>
        <!-- Specify which set of objects should be migrated -->
        <include>
          <!-- Describe the pattern for the list of objects to be included -
->
          <objectSet>
            <pattern type="Registry">HKCU\Software\MyApp\Toolbar\* [*]
</pattern>
            <pattern type="Registry">HKCU\Software\MyApp\ListView\* [*]
</pattern>
            <pattern type="Registry">HKCU\Software\MyApp [ShowTips]
</pattern>
          </objectSet>
        </include>
        <!-- Specify which set of objects should not be migrated -->
        <exclude>
          <!-- Describe the pattern for the list of objects to be excluded
from migration -->
          <objectSet>
            <pattern type="Registry">HKCU\Software\MyApp [Display]</pattern>
          </objectSet>
        </exclude>
      </rules>
    </role>
```

```
  </component>
</migration>
```

Пример 2. Перенос папки "Мои видео"

В следующем примере приведен пользовательский **файл** `CustomFile.xml`.xml, который переносит папку **Видео** для всех пользователей, если папка существует на исходном компьютере.

- **Пример условия**: проверяет, существует ли папка **Videos** на исходном компьютере:

  `<condition>MigXmlHelper.DoesObjectExist("File","%CSIDL_MYVIDEO%")</condition>`

- **Пример фильтра**: фильтрует ярлыки в папке **Видео** , которые не разрешаются на конечном компьютере:

  `<include filter='MigXmlHelper.IgnoreIrrelevantLinks()'>`

  Этот фильтр не влияет на файлы, которые не являются ярлыками. Например, если в папке **Видео** на исходном компьютере есть ярлык, указывающий `C:\Folder1` на , это ярлык переносится только в том случае, если `C:\Folder1` он существует на конечном компьютере. Однако все остальные файлы, например **файлы.mp3** , переносятся без фильтрации.

- **Пример шаблона**. Переносит папку **Видео** для всех пользователей:

  `<pattern type="File">%CSIDL_MYVIDEO%* [*]</pattern>`

XML-файл

▼ Разверните, чтобы отобразить XML-файл **примера 2** :

XML

```
<?xml version="1.0" encoding="UTF-8"?>
<migration
urlid="http://www.microsoft.com/migration/1.0/migxmlext/CustomFile">
<component type="Documents" context="User">
        <displayName>My Video</displayName>
        <role role="Data">
            <detects>
                <detect>

<condition>MigXmlHelper.DoesObjectExist("File","%CSIDL_MYVIDEO%")
</condition>
                </detect>
```

```
            </detects>
            <rules>
                <include filter='MigXmlHelper.IgnoreIrrelevantLinks()'>
                    <objectSet>
                        <pattern type="File">%CSIDL_MYVIDEO%\* [*]</pattern>
                    </objectSet>
                </include>
            </rules>
        </role>
    </component>
</migration>
```

Пример 3. Перенос файлов и разделов реестра

Примеры шаблонов описывают поведение в следующем примере **.xml** файла.

- **Пример шаблона**. Переносит все экземпляры файла `Usmttestfile.txt` из всех подкаталогов в :`%ProgramFiles%\USMTTestFolder`

  `<pattern type="File">%ProgramFiles%\USMTTestFolder* [USMTTestFile.txt] </pattern>`

- **Пример шаблона**. Переносит весь каталог в `%ProgramFiles%\USMTDIRTestFolder`:

  `<pattern type="File">%ProgramFiles%\USMTDIRTestFolder* []</pattern>`

- **Пример шаблона**. Переносит все экземпляры MyKey в :`HKCU\Software\USMTTESTKEY`

  `<pattern type="Registry">HKCU\Software\USMTTESTKEY* [MyKey]</pattern>`

- **Пример шаблона**: переносит весь куст реестра в :`HKLM\Software\USMTTESTKEY`

  `<pattern type="Registry">HKLM\Software\USMTTESTKEY* []</pattern>`

XML-файл

▼ Разверните, чтобы отобразить XML-файл **примера 3** :

XML

```
<migration
urlid="http://www.microsoft.com/migration/1.0/migxmlext/testfilemig">
  <component type="Application" context="System">
   <displayName>File Migration Test</displayName>
   <role role="Data">
```

```
    <rules context="System">
     <include>
      <objectSet>
        <pattern type="File">%ProgramFiles%\USMTTestFolder\*
[USMTTestFile.txt]</pattern>
        <pattern type="File">%ProgramFiles%\USMTDIRTestFolder\* [*]
</pattern>
      </objectSet>
    </include>
   </rules>
  </role>
</component>
<component type="System">
  <displayName>Registry Migration Test</displayName>
  <role role="Settings">
   <rules context="UserAndSystem">
     <include>
      <objectSet>
          <pattern type="Registry">HKCU\Software\USMTTESTKEY\* [MyKey]
</pattern>
          <pattern type="Registry">HKLM\Software\USMTTESTKEY\* [*]</pattern>
      </objectSet>
     </include>
   </rules>
  </role>
 </component>
</migration>
```

Пример 4. Перенос определенных папок из различных расположений

Поведение этого настраиваемого **файла.xml** описано в `<displayName>` тегах в коде.

XML-файл

▼ Разверните, чтобы отобразить XML-файл **примера 4** :

XML

```
<migration urlid="http://www.microsoft.com/migration/1.0/migxmlext/test">

<component type="Documents" context="System">
  <displayName>Component to migrate all Engineering Drafts subfolders
without documents in this folder </displayName>
  <role role="Data">
    <rules>
        <include>
          <objectSet>
              <pattern type="File"> C:\EngineeringDrafts\* [*]</pattern>
          </objectSet>
         </include>
```

```
          <exclude>
             <objectSet>
                  <pattern type="File"> C:\EngineeringDrafts\ [*]</pattern>
             </objectSet>
          </exclude>
    </rules>
  </role>
</component>

<component type="Documents" context="System">
  <displayName>Component to migrate all user documents except
Sample.doc</displayName>
  <role role="Data">
    <rules>
          <include>
            <objectSet>
                  <pattern type="File"> C:\UserDocuments\* [*]</pattern>
            </objectSet>
          </include>
          <exclude>
             <objectSet>
                  <pattern type="File"> C:\UserDocuments\ [Sample.doc]
</pattern>
              </objectSet>
          </exclude>
    </rules>
  </role>
</component>

<component type="Documents" context="System">
  <displayName>Component to migrate all Requests folders on any drive on the
computer </displayName>
  <role role="Data">
    <rules>
          <include>
             <objectSet>
                  <script>MigXmlHelper.GenerateDrivePatterns ("\Requests\*
[*] ", "Fixed")</script>
                  <script>MigXmlHelper.GenerateDrivePatterns ("*\Requests\*
[*] ", "Fixed")</script>
             </objectSet>
           </include>
    </rules>
  </role>
</component>

<component type="Documents" context="System">
  <displayName>Component to migrate all Presentations folder from any
location on the C: drive </displayName>
  <role role="Data">
    <rules>
          <include>
             <objectSet>
                  <pattern type="File"> C:\*\Presentations\* [*]</pattern>
                  <pattern type="File"> C:\Presentations\* [*]</pattern>
```

```
            </objectSet>
          </include>
    </rules>
  </role>
</component>
</migration>
```

Связанные статьи

- Справочник по XML-файлу USMT.
- Настройка XML-файлов USMT.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Конфликты и приоритет

Статья • 29.01.2025 • Применяется к: ✅ Windows 11, ✅ Windows 10

При включении, исключении и изменении перенаправления файлов и параметров важно знать, как средство миграции пользовательской среды (USMT) справляется с конфликтами и приоритетом. Ниже приведены наиболее важные конфликты и рекомендации по приоритету, которые следует учитывать при работе с USMT.

- **Если в компоненте есть конфликтующие правила, применяется наиболее конкретное правило.** Однако правило **безусловного< исключения> является** исключением, так как оно имеет приоритет над всеми остальными. Имена каталогов имеют приоритет над расширениями файлов. Примеры см. в разделе Что происходит при наличии конфликтующих <правил включения> и <исключения>? и первый пример в <примерах приоритета правил включения> и <исключения> далее в этой статье.

- **Только правила внутри одного компонента могут влиять друг на друга в зависимости от специфики.** Правила, которые находятся в разных компонентах, не влияют друг на друга, за исключением правила **безусловного< исключения>.**

- **Если правила одинаково специфичны, <исключение> имеет приоритет над <включением>.** Например, если **<правило исключения>** используется для исключения файла, а **<правило включения>** используется для включения одного и того же файла, файл исключается.

- **Порядок компонентов не имеет значения.** Не имеет значения, какие компоненты перечислены в каком **.xml** файле, так как каждый компонент обрабатывается независимо от других компонентов во всех **.xml** файлах.

- **Порядок <правил включения> и <исключения> в компоненте не имеет значения.**

- **Элемент <unconditionalExclude> можно использовать для глобального исключения данных.** Этот элемент исключает объекты, независимо от других **<правил включения>** , которые находятся в **файлах.xml** . Например, **<элемент unconditionalExclude>** можно использовать для исключения всех MP3-файлов на компьютере или для исключения всех файлов из `C:\UserData`.

Общее

Какова связь между правилами, расположенными в разных компонентах?

Только правила внутри одного компонента могут влиять друг на друга в зависимости от специфики, за исключением правила **безусловного< включения>**. Правила, которые находятся в разных компонентах, не влияют друг на друга. При наличии **<правила включения>** в одном компоненте и идентичного **<правила исключения>** в другом компоненте данные переносятся, так как эти два правила не зависят друг от друга.

<Если правило включения> находится в одном компоненте**<, а правило locationModify>** находится в другом компоненте для того же файла, файл переносится в обоих местах. То есть файл включается на **<основе правила включения>** , а файл переносится на **<основе правила locationModify>** .

Следующий **файл.xml** переносит все файлы из C:\Userdocs, включая **файлы.mp3** , так как **<правило исключения>** указывается в отдельном компоненте.

XML

```
<migration
urlid="http://www.microsoft.com/migration/1.0/migxmlext/UserDocs">
<component type="Documents" context="System">
<displayName>User Documents</displayName>
        <role role="Data">
            <rules>
                <exclude>
                    <objectSet>
                        <pattern type="File">C:\Userdocs\* [*.mp3]</pattern>
                    </objectSet>
                </exclude>
          </rules>
        </role>
</component>

<component type="Documents" context="System">
<displayName> User documents to include </displayName>
        <role role="Data">
            <rules>
                <include>
                    <objectSet>
                        <pattern type="File"> C:\Userdocs\ [*]</pattern>
                    </objectSet>
                </include>
          </rules>
        </role>
</component>
</migration>
```

Как приоритет работает с файлом Config.xml?

Указание `migrate="no"` в `Config.xml` файле аналогично удалению соответствующего компонента из файла **.xml** миграции. Однако если `migrate="no"` для папки **Документы** задано правило, аналогичное следующему, существует в файле **миграции.xml** (который содержит все **.doc** файлы из папки **Документы**), то переносятся только **файлы.doc** , а все остальные файлы исключаются:

XML

```
<include>
   <objectSet>
      <pattern type="File">%CSIDL_PERSONAL%\* [*.doc] </pattern>
   </objectSet>
</include>
```

Как USMT обрабатывает каждый компонент в файле .xml с несколькими компонентами?

Порядок компонентов не имеет значения. Каждый компонент обрабатывается независимо от других компонентов. Например, если **<правило включения>** находится в одном компоненте, а **<правило locationModify>** находится в другом компоненте для того же файла, файл переносится в обоих местах. То есть файл включается на **<основе правила включения>** , а файл переносится на **<основе правила locationModify>** .

Как обрабатываются правила?

Существует две широкие категории правил.

- **Правила, влияющие на поведение средств ScanState и LoadState**. Например, **<правила include>**, **<exclude>** и **<unconditionalExclude>** обрабатываются для каждого компонента в **файлах.xml** . Для каждого компонента USMT создает список включения и список исключений. Некоторые правила в компоненте могут быть отменены из-за специфики, но все остальные правила обрабатываются. Для каждого **<правила включения>** USMT выполняет итерацию по элементам, чтобы узнать, нужно ли исключить какое-либо из расположений. USMT перечисляет все объекты и создает список объектов, которые он собирается собрать для каждого пользователя. После завершения списка каждый из объектов сохраняется или переносится на конечный компьютер.

- **Правила, влияющие на поведение только средства LoadState**. Например, **<правила locationModify>**, **<contentModify>** и **<destinationCleanup>** не влияют на ScanState. Они обрабатываются только с помощью LoadState. Во-первых, средство **LoadState** определяет содержимое и расположение каждого компонента на **<основе правил locationModify>** и **<contentModify>** . Затем **LoadState** обрабатывает все **<правила destinationCleanup>** и удаляет данные с конечного компьютера. Наконец, **LoadState** применяет компоненты к компьютеру.

Как USMT объединяет все .xml файлы, указанные в командной строке?

USMT не различает **файлы.xml** по их имени или содержимому. Каждый компонент в файлах обрабатывается отдельно. USMT поддерживает несколько **файлов.xml** только для упрощения обслуживания и организации компонентов в них. Так как USMT использует urlid для отличия каждого компонента от других, убедитесь, что каждый **.xml** файл, указанный в командной строке, имеет уникальный URL-код миграции.

Правила <включения> и <исключения>

Что происходит при наличии конфликтующих <правил включения> и <исключения> ?

Если в компоненте есть конфликтующие правила, применяется наиболее конкретное правило, за исключением правила **безусловного< исключения>,** которое имеет приоритет над всеми другими правилами. Если правила одинаково специфичны, данные не переносятся. Например, если один и тот же файл исключен и включен, файл не переносится. Если в разных компонентах есть конфликтующие правила, они не влияют друг на друга, так как каждый компонент обрабатывается независимо.

В следующем примере mp3-файлы не исключаются из миграции. Mp3-файлы не исключаются, так как имена каталогов имеют приоритет над расширениями файлов.

XML

```
<include>
     <objectSet>
          <pattern type="File">C:\Data\* [*]</pattern>
```

```
      </objectSet>
</include>
<exclude>
      <objectSet>
           <pattern type="File"> C:\* [*.mp3]</pattern>
      </objectSet>
</exclude>
```

<Примеры приоритета правил включения> и <исключения>

В этих примерах объясняется, как USMT работает с **<правилами включения>** и **<исключения>** . Если правила находятся в разных компонентах, результирующее поведение будет одинаковым независимо от того, находятся ли компоненты в одном или в разных **файлах.xmlмиграции** .

- Включение и исключение файлов
- Включение и исключение объектов реестра

Включение и исключение файлов

Развернуть таблицу

Если следующий код существует в том же компоненте	Результирующее поведение	Объяснение
• Включить правило: <pattern type="File">C:\Dir1* [] </pattern> • Правило исключения: <pattern type="File">C:* [.txt] </pattern>	Переносит все файлы и вложенные папки в Dir1 (включая все **.txt** файлы в C:).	Правило **<исключения>** не влияет на миграцию, так как **<правило включения>** является более конкретным.
• Включить правило: <pattern type="File">C:\Dir1* [] </pattern> • Правило исключения: <pattern type="File">C:\Dir1\Dir2* [.txt]</pattern>	Переносит все файлы и вложенные папки в C:\Dir1, за исключением **.txt** файлов в C:\Dir1\Dir2 и его вложенных папок.	Оба правила обрабатываются по назначению.
• Включить правило: <pattern type="File">C:\Dir1* []	Переносит все файлы и вложенные папки в C:\Dir1,	Оба правила обрабатываются по

Если следующий код существует в том же компоненте	Результирующее поведение	Объяснение
</pattern> • Правило исключения: <pattern type="File">C:\Dir1\ * [.txt]</pattern>	за исключением **.txt** файлов в C:\Dir1 и его вложенных папок.	назначению.
• Включить правило: <pattern type="File">C:\Dir1\Dir2* [.txt]</pattern> • Правило исключения: <pattern type="File">C:\Dir1\Dir2* [.txt]</pattern>	Ничего не переносится.	Правила одинаково специфичны, поэтому **<правило исключения>** имеет приоритет над правилом **<включения>** .
• Включить правило: C:\Dir1* [.txt] • Правило исключения: C:\Dir1\Dir2* []	Переносит **файлы.txt** в Dir1 и **файлы.txt** из вложенных папок, отличных от Dir2. Файлы не переносятся из Dir2 или его вложенных папок.	Оба правила обрабатываются по назначению.
• Включить правило: C:\Dir1\Dir2* [] • Правило исключения: C:\Dir1* [.txt]	Переносит все файлы и вложенные папки Dir2, за исключением **.txt** файлов из Dir1 и всех вложенных папок Dir1 (включая Dir2).	Оба правила обрабатываются по назначению.

Развернуть таблицу

Если следующий код существует в разных компонентах	Результирующее поведение	Объяснение
Компонент 1. • Включить правило: <pattern type="File">C:\Dir1* [] </pattern> • Правило исключения: <pattern type="File">C:\Dir1\Dir2* [.txt]</pattern> Компонент 2.	Переносит все файлы и вложенные папки C:\Dir1\ (включая C:\Dir1\Dir2).	Правила, которые находятся в разных компонентах, не влияют друг на друга, за исключением правила **безусловного< исключения>.** Таким образом, в этом примере, хотя некоторые **.txt** файлы были исключены при обработке компонента 1, они были включены при обработке компонента 2.

Если следующий код существует в разных компонентах	Результирующее поведение	Объяснение
• Включить правило: <pattern type="File">C:\Dir1\Dir2* [.txt]</pattern> • Правило исключения: <pattern type="File">C:\Dir1* [] </pattern>		
Компонент 1. • Включить правило: C:\Dir1\Dir2* [] Компонент 2. • Правило исключения: C:\Dir1* [.txt]	Переносит все файлы и вложенные папки из Dir2, кроме **файлов.txt** в C:\Dir1 и его вложенных папок.	Оба правила обрабатываются по назначению.
Компонент 1. • Правило исключения: C:\Dir1\Dir2* [] Компонент 2. • Включить правило: C:\Dir1* [.txt]	Переносит все **.txt** файлы в Dir1 и все вложенные папки.	Компонент 1 не содержит **<правила включения>** , поэтому **<правило исключения>** не обрабатывается.

Включение и исключение объектов реестра

Развернуть таблицу

Если следующий код существует в том же компоненте	Результирующее поведение	Объяснение
• Включить правило: HKLM\Software\Microsoft\Command Processor* [] • Правило исключения: HKLM\Software\Microsoft\Command Processor [DefaultColor]	Переносит все ключи в HKLM\Software\Microsoft\Command Processor, кроме DefaultColor.	Оба правила обрабатываются по назначению.

Если следующий код существует в том же компоненте	Результирующее поведение	Объяснение
• Включить правило: HKLM\Software\Microsoft\Command Processor [DefaultColor] • Правило исключения: HKLM\Software\Microsoft\Command Processor* []	Переносит только DefaultColor в HKLM\Software\Microsoft\Command Processor.	DefaultColor переносится, так как **<правило включения>** является более конкретным, чем **<правило исключения>** .
• Включить правило: HKLM\Software\Microsoft\Command Processor [DefaultColor] • Правило исключения: HKLM\Software\Microsoft\Command Processor [DefaultColor]	Не переносит DefaultColor.	Правила одинаково специфичны, поэтому **<правило исключения>** имеет приоритет над правилом <включения> .

Развернуть таблицу

Если следующий код существует в разных компонентах	Результирующее поведение	Объяснение
Компонент 1. • Включить правило: HKLM\Software\Microsoft\Command Processor [DefaultColor] • Правило исключения: HKLM\Software\Microsoft\Command Processor* [] Компонент 2. • Включить правило: HKLM\Software\Microsoft\Command Processor* [] • Правило исключения: HKLM\Software\Microsoft\Command Processor [DefaultColor]	Переносит все ключи и значения в HKLM\Software\Microsoft\Command Processor.	Правила, которые находятся в разных компонентах, не влияют друг на друга, за исключением правила **безусловного< исключения>.** В этом примере объекты, исключенные при обработке компонента 1, были включены при

Если следующий код существует в разных компонентах	Результирующее поведение	Объяснение
		обработке компонента 2.

Конфликты файлов

Каково поведение по умолчанию при возникновении конфликтов файлов?

Если правила **слияния> нет<**, по умолчанию для реестра источник перезаписывает назначение. Поведение по умолчанию для файлов — постепенное переименование источника: например, OriginalFileName(1). OriginalExtension, OriginalFileName(2). OriginalExtension и т. д.

Как работает <правило слияния> при наличии конфликтов файлов?

При обнаружении конфликта USMT выбирает наиболее конкретное **<правило слияния>** и применяет его для разрешения конфликта. Например, если **для C:* [*]** существует правило **слияния>, для параметра sourcePriority(), а другое правило слияния для C:\subfolder* [*] — destinationPriority(), то USMT использует правило destinationPriority(), так как оно является наиболее конкретным.< <>**

Пример сценария

Исходный компьютер содержит следующие файлы:

- `C:\Data\SampleA.txt`
- `C:\Data\SampleB.txt`
- `C:\Data\Folder\SampleB.txt`

Конечный компьютер содержит следующие файлы:

- `C:\Data\SampleB.txt`
- `C:\Data\SampleB.txt`

Пользовательский **файл.xml** содержит следующий код:

XML

```
<include>
   <objectSet>
      <pattern type="File">c:\data\* [*]</pattern>
   </objectSet>
</include>
```

В этом примере следующие сведения описывают результирующее поведение при добавлении кода в пользовательский **файл.xml** .

Пример 1

XML

```
<merge script="MigXmlHelper.DestinationPriority()">
        <objectSet>
                <pattern type="File">c:\data* []</pattern>
        </objectSet>
</merge>
```

Результат. Во время ScanState все файлы добавляются в хранилище. Во время LoadState восстанавливается только `C:\Data\SampleA.txt` .

Пример 2

XML

```
<merge script="MigXmlHelper.SourcePriority()">
        <objectSet>
                <pattern type="File">c:\data* []</pattern>
        </objectSet>
</merge>
```

Результат. Во время ScanState все файлы добавляются в хранилище. Во время LoadState все файлы восстанавливаются, перезаписав существующие файлы на конечном компьютере.

Пример 3

XML

```
<merge script="MigXmlHelper.SourcePriority()">
        <objectSet>
```

```
                <pattern type="File">c:\data\ [*]</pattern>
        </objectSet>
</merge>
```

Результат. Во время ScanState все файлы добавляются в хранилище. Во время LoadState выполняются следующие действия:

- `C:\Data\SampleA.txt` восстанавливается.
- `C:\Data\SampleB.txt` восстанавливается, перезаписывается существующий файл на конечном компьютере.
- `C:\Data\Folder\SampleB.txt` не восстанавливаются.

Связанные статьи

Справочник по XML-файлу USMT.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Общие соглашения

Статья • 29.01.2025 • Применяется к: ✅ Windows 11, ✅ Windows 10

В этой статье описаны вспомогательные функции XML.

Общие рекомендации по XML

Перед изменением файлов **.xml** ознакомьтесь со следующими рекомендациями:

- **Схема XML.**

  Схема `MigXML.xsd` XML средства миграции пользовательской среды (USMT) может использоваться для записи и проверки файлов миграции **.xml** .

- **Конфликтов.**

  Как правило, при наличии конфликтов в схеме XML приоритет имеет наиболее конкретный шаблон. Дополнительные сведения см. в разделе Конфликты и приоритет.

- **Обязательные элементы.**

  Обязательными **элементами для** .xmlфайла **миграции являются< миграция>**, **<компонент>**, **<роль>** и **<правила>**.

- **Обязательные дочерние элементы.**

  - USMT не завершается ошибкой, если не указаны необходимые дочерние элементы. Однако для родительского элемента необходимо указать необходимые дочерние элементы, чтобы повлиять на миграцию.

  - Обязательные дочерние элементы применяются только к первому определению элемента. Если эти элементы определены, а затем ссылаются на них с помощью их имени, необходимые дочерние элементы не применяются. Например, если `<detects name="Example">` задано в **<namedElements>** и `<detects name="Example"/>` указано в **<компоненте>** для ссылки на этот элемент, определение внутри **<namedElements>** должно содержать обязательные дочерние элементы, но **<элемент компонента>** не должен содержать необходимые дочерние элементы.

- **Имена файлов в квадратных скобках.**

Если файл с символом в скобках ([или]) в имени файла переносится, необходимо вставить символ карата (^). Символ в каратах (^) должен находиться непосредственно перед скобкой, чтобы символ скобки был допустимым. Например, если есть файл с именем **file].txt**, `<pattern type="File">c:\documents\mydocs [file^].txt]</pattern>` должен быть указан вместо `<pattern type="File">c:\documents\mydocs [file].txt]</pattern>`.

- **Использование кавычек.**

  Если код заключен в кавычки, можно использовать двойные ("") или одиночные (') кавычки.

Вспомогательные функции

Вспомогательные функции XML в библиотеке XML-элементов можно использовать для изменения поведения миграции. Прежде чем использовать эти функции в **файле.xml** , обратите внимание на следующие элементы:

- **Все параметры являются строками.**
- **Параметры NULL можно оставить пустыми.**

  Как и в случае с параметрами с соглашением о значении по умолчанию, если в конце списка есть параметр NULL, его можно исключить. Например, следующая функция:

  Командная строка Windows

  ```
  SomeFunction("My String argument",NULL,NULL)
  ```

  эквивалентен:

  Командная строка Windows

  ```
  SomeFunction("My String argument")
  ```

- **Закодированное расположение, используемое во всех вспомогательных функциях, является однозначным строковым представлением для имени объекта.**

Закодированное расположение состоит из части узла, за которой при необходимости следует конечный элемент, заключенный в квадратные скобки. В этом формате делается четкое различие между узлами и листьями.

Например, укажите файл

`C:\Windows\Notepad.exe`

as

c:\Windows[Notepad.exe]

Аналогичным образом укажите каталог

`C:\Windows\System32`

as

c:\Windows\System32

Обратите внимание на отсутствие символов **[]** во втором примере.

Реестр представлен аналогичным образом. Значение по умолчанию раздела реестра представлено в виде пустой конструкции **[]** . Например, значение по умолчанию для `HKLM\SOFTWARE\MyKey` раздела реестра — **HKLM\SOFTWARE\MyKey[]**.

- **Шаблон расположения указывается таким образом, как указано фактическое расположение.**

  Исключение заключается в том, что и узел, и конечная часть принимают шаблоны. Однако шаблон из узла не распространяется на конечный элемент.

  Например, шаблон **c:\Windows*** соответствует каталогу `\Windows` и всем подкаталогам, но не соответствует ни одному из файлов в этих каталогах. Чтобы также соответствовать файлам, необходимо указать **c:\Windows*[*]** .

Связанные статьи

- Справочник по XML-файлу USMT.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Требования к XML-файлам

Статья • 29.01.2025 • Применяется к: ✅ Windows 11, ✅ Windows 10

При создании **пользовательских файлов.xml** обратите внимание на следующие требования.

- **Файл должен быть в формате преобразования Юникода 8 (UTF-8).** Сохраните файл в этом формате, и в начале каждого **файла.xml** должен быть указан следующий синтаксис:

  ```
  XML
  ```

  ```xml
  <?xml version="1.0" encoding="UTF-8"?>
  ```

- **Файл должен иметь уникальный URL-адрес миграции**. URL-адрес каждого файла, указанного в командной строке, должен отличаться. Если два файла **миграции.xml** имеют одинаковый URL-адрес, второй **.xml** файл, указанный в командной строке, не обрабатывается. Второй файл не обрабатывается, так как USMT использует идентификатор URL-адреса для определения компонентов в файле. Например, в начале каждого файла необходимо указать следующий синтаксис:

  ```
  XML
  ```

  ```xml
  <?xml version="1.0" encoding="UTF-8"?>
  <migration
  urlid="http://www.microsoft.com/migration/1.0/migxmlext/<CustomFileName
  >">
  ```

- **Каждый компонент в файле должен иметь отображаемое имя, чтобы он отображалось в файле Config.xml.** Это условие связано с тем, `Config.xml` что файл определяет компоненты с помощью отображаемого имени и идентификатора URL-адреса миграции. Например, укажите следующий синтаксис:

  ```
  XML
  ```

  ```xml
  <displayName>My Application</displayName>
  ```

Примеры пользовательских **файлов.xml** см. в разделе Примеры пользовательских XML-файлов.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Распознанные переменные среды

Статья • 29.01.2025 • Применяется к: ✅ Windows 11, ✅ Windows 10

При использовании XML-файлов `MigDocs.xml`, `MigApp.xml`, и `MigUser.xml` переменные среды можно использовать для идентификации папок, которые могут отличаться на разных компьютерах. Значения списка специальных постоянных элементов (CSIDL) позволяют определить папки, которые приложения часто используют, но могут иметь разные имена или расположения на любом компьютере. Например, папка "**Документы**" может находиться `C:\Users\<Username>\Documents` на одном компьютере, а `C:\Users\<Username>\My Documents` на другом. Подстановочный знак звездочки (*) можно использовать в файлах `MigUser.xml`, `MigApp.xml` и `MigDoc.xml` . Однако подстановочный знак звездочки (*) нельзя использовать в `Config.xml` файле.

Переменные, обрабатываемые для операционной системы и в контексте каждого пользователя

Эти переменные можно использовать в разделах **в файлах.xml** с `context=UserAndSystem`, `context=User` и `context=System`.

Развернуть таблицу

Переменная	Объяснение
ALLUSERSAPPDATA	То же, **что и CSIDL_COMMON_APPDATA**.
ALLUSERSPROFILE	Ссылается на `%PROFILESFOLDER%\Public` или `%PROFILESFOLDER%\all users`.
COMMONPROGRAMFILES	То же, **что и CSIDL_PROGRAM_FILES_COMMON**.
COMMONPROGRAMFILES(X86)	Ссылается на папку в `C:\Program Files (x86)\Common Files` 64-разрядных системах.
CSIDL_COMMON_ADMINTOOLS	Версия 10.0. Каталог файловой системы, содержащий средства администрирования для всех пользователей компьютера.
CSIDL_COMMON_ALTSTARTUP	Каталог файловой системы, соответствующий нелокализованной группе программы запуска для всех пользователей.

Переменная	Объяснение
CSIDL_COMMON_APPDATA	Каталог файловой системы, содержащий данные приложения для всех пользователей. Типичный путь Windows — `C:\ProgramData`.
CSIDL_COMMON_DESKTOPDIRECTORY	Каталог файловой системы, содержащий файлы и папки, которые отображаются на рабочем столе для всех пользователей. Типичный путь — `C:\Users\Public\Desktop`.
CSIDL_COMMON_DOCUMENTS	Каталог файловой системы, содержащий общие для всех пользователей документы. Типичный путь — `C:\Users\Public\Documents`.
CSIDL_COMMON_FAVORITES	Каталог файловой системы, который служит общим репозиторием для избранного, общего для всех пользователей. Типичный путь — C:\Users\Public\Favorites.
CSIDL_COMMON_MUSIC	Каталог файловой системы, который служит репозиторием для музыкальных файлов, общих для всех пользователей. Типичный путь — `C:\Users\Public\Music`.
CSIDL_COMMON_PICTURES	Каталог файловой системы, который служит репозиторием для файлов образов, общих для всех пользователей. Типичный путь — `C:\Users\Public\Pictures`.
CSIDL_COMMON_PROGRAMS	Каталог файловой системы, содержащий каталоги для общих групп программ, которые отображаются в меню **Пуск** для всех пользователей. Типичный путь — `C:\ProgramData\Microsoft\Windows\Start Menu\Programs`.
CSIDL_COMMON_STARTMENU	Каталог файловой системы, содержащий программы и папки, которые отображаются в меню **Пуск** для всех пользователей. Типичный путь в Windows — `C:\ProgramData\Microsoft\Windows\Start Menu`.
CSIDL_COMMON_STARTUP	Каталог файловой системы, содержащий программы, которые отображаются в папке Startup для всех пользователей. Типичный путь — `C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup`.
CSIDL_COMMON_TEMPLATES	Каталог файловой системы, содержащий шаблоны, доступные всем пользователям. Типичный путь — `C:\ProgramData\Microsoft\Windows\Templates`.

Переменная	Объяснение
CSIDL_COMMON_VIDEO	Каталог файловой системы, который служит репозиторием для видеофайлов, общих для всех пользователей. Типичный путь — `C:\Users\Public\Videos`.
CSIDL_DEFAULT_APPDATA	Ссылается на папку внутри `Appdata` `%DEFAULTUSERPROFILE%`.
C SIDL_DEFAULT_LOCAL_APPDATA	Ссылается на локальную `Appdata` папку внутри `%DEFAULTUSERPROFILE%`.
CSIDL_DEFAULT_COOKIES	Ссылается на папку Cookie внутри `%DEFAULTUSERPROFILE%`.
CSIDL_DEFAULT_CONTACTS	Ссылается на папку "Контакты" внутри `%DEFAULTUSERPROFILE%`.
CSIDL_DEFAULT_DESKTOP	Ссылается на папку Desktop внутри `%DEFAULTUSERPROFILE%`.
CSIDL_DEFAULT_DOWNLOADS	Ссылается на папку Загрузки внутри `%DEFAULTUSERPROFILE%`.
CSIDL_DEFAULT_FAVORITES	Ссылается на папку Избранное внутри `%DEFAULTUSERPROFILE%`.
CSIDL_DEFAULT_HISTORY	Ссылается на папку History внутри `%DEFAULTUSERPROFILE%`.
CSIDL_DEFAULT_INTERNET_CACHE	Ссылается на папку интернет-кэша внутри `%DEFAULTUSERPROFILE%`.
CSIDL_DEFAULT_PERSONAL	Ссылается на личную папку внутри `%DEFAULTUSERPROFILE%`.
CSIDL_DEFAULT_MYDOCUMENTS	Ссылается на папку Documents внутри `%DEFAULTUSERPROFILE%`.
CSIDL_DEFAULT_MYPICTURES	Ссылается на папку Рисунки внутри `%DEFAULTUSERPROFILE%`.
CSIDL_DEFAULT_MYMUSIC	Ссылается на папку Music внутри `%DEFAULTUSERPROFILE%`.
CSIDL_DEFAULT_MYVIDEO	Ссылается на папку Видео внутри `%DEFAULTUSERPROFILE%`.
CSIDL_DEFAULT_RECENT	Ссылается на папку Recent внутри `%DEFAULTUSERPROFILE%`.

Переменная	Объяснение
CSIDL_DEFAULT_SENDTO	Ссылается на папку Send To внутри `%DEFAULTUSERPROFILE%`.
CSIDL_DEFAULT_STARTMENU	Ссылается на папку меню "Пуск" внутри `%DEFAULTUSERPROFILE%`.
CSIDL_DEFAULT_PROGRAMS	Ссылается на папку Programs внутри `%DEFAULTUSERPROFILE%`.
CSIDL_DEFAULT_STARTUP	Ссылается на папку Startup внутри `%DEFAULTUSERPROFILE%`.
CSIDL_DEFAULT_TEMPLATES	Ссылается на папку Templates внутри `%DEFAULTUSERPROFILE%`.
CSIDL_DEFAULT_QUICKLAUNCH	Ссылается на папку быстрого запуска внутри `%DEFAULTUSERPROFILE%`.
CSIDL_FONTS	Виртуальная папка, содержащая шрифты. Типичный путь — `C:\Windows\Fonts`.
CSIDL_PROGRAM_FILESX86	Папка Program Files в 64-разрядных системах. Типичный путь — `C:\Program Files (x86)`.
CSIDL_PROGRAM_FILES_COMMONX86	Папка для компонентов, которые совместно используются в приложениях в 64-разрядных системах. Типичный путь — `C:\Program Files (x86)\Common`.
CSIDL_PROGRAM_FILES	Папка Program Files. Типичный путь — `C:\Program Files`.
CSIDL_PROGRAM_FILES_COMMON	Папка для компонентов, которые совместно используются в приложениях. Типичный путь — `C:\Program Files\Common`.
CSIDL_RESOURCES	Каталог файловой системы, содержащий данные ресурсов. Типичный путь — `C:\Windows\Resources`.
CSIDL_SYSTEM	Системная папка Windows. Типичный путь — `C:\Windows\System32`.
CSIDL_WINDOWS	Каталог Windows или корневой путь к системе. Это значение соответствует `%WINDIR%` переменным среды или `%SYSTEMROOT%` . Типичный путь — `C:\Windows`.
DEFAULTUSERPROFILE	Ссылается на значение в `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList [DefaultUserProfile]`.

Переменная	Объяснение
PROFILESFOLDER	Ссылается на значение в `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList [ProfilesDirectory]`.
PROGRAMFILES	То же, что **и CSIDL_PROGRAM_FILES**.
PROGRAMFILES(X86)	Ссылается на папку в `C:\Program Files (x86)` 64-разрядных системах.
СИСТЕМА	Ссылается на `%WINDIR%\system32`.
SYSTEM16	Ссылается на `%WINDIR%\system`.
SYSTEM32	Ссылается на `%WINDIR%\system32`.
SYSTEMDRIVE	Диск, на котором хранится папка Windows. Это значение является именем диска, а не именем папки (`C:` не `C:\`).
SYSTEMPROFILE	Ссылается на значение в `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-18 [ProfileImagePath]`.
SYSTEMROOT	То же, что **и WINDIR**.
WINDIR	Ссылается на папку Windows, расположенную на системном диске.

Переменные, распознаваемые только в контексте пользователя

Эти переменные можно использовать в **файлах.xml** в разделах с `context=User` и `context=UserAndSystem`.

Развернуть таблицу

Переменная	Объяснение
APPDATA	То же, **что и CSIDL_APPDATA**.
CSIDL_ADMINTOOLS	Каталог файловой системы, используемый для хранения средств администрирования для отдельного пользователя. Консоль управления (MMC) сохраняет настраиваемые консоли в этом

Переменная	Объяснение
	каталоге, который перемещается вместе с профилем пользователя.
CSIDL_ALTSTARTUP	Каталог файловой системы, соответствующий нелокализованной группе программы запуска пользователя.
CSIDL_APPDATA	Каталог файловой системы, который служит общим репозиторием для данных конкретного приложения. Типичный путь — `C:\Users\<username>\AppData\Roaming`.
CSIDL_BITBUCKET	Виртуальная папка, содержащая объекты в корзине пользователя.
CSIDL_CDBURN_AREA	Каталог файловой системы, выступающий в качестве промежуточной области для файлов, ожидающих записи на компакт-диск. Типичный путь — `C:\Users\<username>\AppData\Local\Microsoft\Windows\MasteredBurning\Disc Burning`.
CSIDL_CONNECTIONS	Виртуальная папка, представляющая сетевую Connections, которая содержит сетевые подключения и подключения удаленного доступа.
CSIDL_CONTACTS	Это значение ссылается на папку Контакты в %**CSIDL_PROFILE**%.
CSIDL_CONTROLS	Виртуальная папка, содержащая значки для элементов панель управления.
CSIDL_COOKIES	Каталог файловой системы, который служит общим репозиторием для файлов cookie Интернета. Типичный путь — `C:\Users\<username>\AppData\Roaming\Microsoft\Windows\Cookies`.
CSIDL_DESKTOP	Виртуальная папка, представляющая рабочий стол Windows.
CSIDL_DESKTOPDIRECTORY	Каталог файловой системы, используемый для физического хранения файловых объектов на рабочем столе, который не следует путать с самой папкой рабочего стола. Типичный путь — `C:\Users\<username>\Desktop`.
CSIDL_DRIVES	Виртуальная папка , представляющая **этот компьютер**, которая содержит все на локальном компьютере: запоминающие устройства, принтеры и панель управления. Папка также может содержать сопоставленные сетевые диски.
CSIDL_FAVORITES	Каталог файловой системы, который служит общим репозиторием для избранного пользователя. Типичный путь — `C:\Users\<username>\Favorites`.
CSIDL_HISTORY	Каталог файловой системы, который служит общим

Переменная	Объяснение
	репозиторием для элементов журнала Интернета.
CSIDL_INTERNET	Виртуальная папка для интернет-Обозреватель.
CSIDL_INTERNET_CACHE	Каталог файловой системы, который служит общим репозиторием для временных файлов в Интернете. Типичный путь : `C:\Users\<username>\AppData\Local\Microsoft\Windows\Temporary Internet Files`
CSIDL_LOCAL_APPDATA	Каталог файловой системы, который служит репозиторием данных для локальных, не перемещаемых приложений. Типичный путь — `C:\Users\<username>\AppData\Local`.
CSIDL_MYDOCUMENTS	Виртуальная папка, представляющая папку **Documents** . Типичный путь — `C:\Users\<username>\Documents`.
CSIDL_MYMUSIC	Каталог файловой системы, который служит общим репозиторием для музыкальных файлов. Типичный путь — `C:\Users\<username>\Music`.
CSIDL_MYPICTURES	Каталог файловой системы, который служит общим репозиторием для файлов изображений. Типичный путь — `C:\Users\<username>\Pictures`.
CSIDL_MYVIDEO	Каталог файловой системы, который служит общим репозиторием для видеофайлов. Типичный путь — `C:\Users\<username>\Videos`.
CSIDL_NETHOOD	Каталог файловой системы, содержащий объекты связи, которые могут существовать в виртуальной папке **Network** . Это не то же самое, что *CSIDL_NETWORK*, который представляет корневой каталог сетевого пространства имен. Типичный путь — `C:\Users\<username>\AppData\Roaming\Microsoft\Windows\Network Shortcuts`.
CSIDL_NETWORK	Виртуальная папка, представляющая элемент **сетевого** рабочего стола, корневой каталог иерархии сетевого пространства имен.
CSIDL_PERSONAL	Виртуальная папка, представляющая **<элемент рабочего стола Пользователя>** . Это значение эквивалентно **CSIDL_MYDOCUMENTS**. Типичный путь — `C:\User\<username>\Documents`.
CSIDL_PLAYLISTS	Виртуальная папка, используемая для хранения альбомов воспроизведения, обычно .`C:\Users\<username>\Music\Playlists`
CSIDL_PRINTERS	Виртуальная папка, содержащая установленные принтеры.

Переменная	Объяснение
CSIDL_PRINTHOOD	Каталог файловой системы, содержащий объекты связи, которые могут существовать в виртуальной папке Принтеры. Типичный путь — `C:\Users\<username>\AppData\Roaming\Microsoft\Windows\Printer Shortcuts`.
CSIDL_PROFILE	Папка профиля пользователя. Типичный путь — `C:\Users\<username>`.
CSIDL_PROGRAMS	Каталог файловой системы, содержащий группы программ пользователя, которые сами являются каталогами файловой системы. Типичный путь — `C:\Users\<username>\AppData\Roaming\Microsoft\Windows\Start Menu\Programs`.
CSIDL_RECENT	Каталог файловой системы, содержащий ярлыки для последних использованных документов пользователя. Типичный путь — `C:\Users\<username>\AppData\Roaming\Microsoft\Windows\Recent`.
CSIDL_SENDTO	Каталог файловой системы, содержащий пункты меню "**Отправить** ". Типичный путь — `C:\Users\<username>\AppData\Roaming\Microsoft\Windows\SendTo`.
CSIDL_STARTMENU	Каталог файловой системы, содержащий элементы меню "**Пуск** ". Типичный путь — `C:\Users\<username>\AppData\Roaming\Microsoft\Windows\Start Menu`.
CSIDL_STARTUP	Каталог файловой системы, соответствующий группе программы запуска пользователя. Типичный путь — `C:\Users\<username>\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup`.
CSIDL_TEMPLATES	Каталог файловой системы, который служит общим репозиторием для шаблонов документов. Типичный путь — `C:\Users\<username>\AppData\Roaming\Microsoft\Windows\Templates`.
HOMEPATH	То же, что и стандартная переменная среды.
TEMP	Временная папка на компьютере. Типичный путь — `%USERPROFILE%\AppData\Local\Temp`.
TMP	Временная папка на компьютере. Типичный путь — `%USERPROFILE%\AppData\Local\Temp`.
USERPROFILE	То же, **что и CSIDL_PROFILE**.
USERSID	Представляет текущий идентификатор безопасности (SID) учетной записи пользователя. Например, `S-1-5-21-1714567821-`

Переменная	Объяснение
	`1326601894-715345443-1026`.

Связанные статьи

Справочник по XML-файлу USMT

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Библиотека XML-элементов

Статья • 29.01.2025 • Применяется к: ✅ Windows 11, ✅ Windows 10

В этой статье описываются XML-элементы и вспомогательные функции, которые можно использовать для создания миграции **.xml** файлов для использования с помощью средства миграции пользовательской среды (USMT). В этой статье предполагается базовое знание XML.

В дополнение к XML-элементам и вспомогательным функциям, эта статья:

- Описывается указание закодированных расположений и шаблонов расположений.
- Функции, которые предназначены только для внутреннего USMT, используются только.
- Теги версий, которые можно использовать со вспомогательными функциями.

Элементы и вспомогательные функции

В следующей таблице описаны XML-элементы и вспомогательные функции, которые можно использовать с USMT.

Развернуть таблицу

Элементы A–K	Элементы L–Z	Вспомогательные функции
<addObjects>	<библиотека>	<Функции условий>
<Атрибуты>	<местоположение>	<функции содержимого>
<Байт>	<locationModify>	<функции contentModify>
<commandLine>	<_locDefinition>	<включить> и <исключить> функции фильтрации
<компонент>	<изготовитель>	
<состояние>	<сливать>	<Функции locationModify>
<условия>	<миграция>	<Функции слияния>
<содержание>	<namedElements>	<функции скрипта>
<contentModify>	<объект>	Внутренние функции USMT
<описание>	<objectSet>	
<destinationCleanup>	<путь>	
<обнаруживать>	<Пути>	
<Обнаруживает>	<шаблон>	
<обнаружение>	<обработка>	
<displayName>	<подключаемый модуль>	
<окружающая среда>	<роль>	
<исключать>	<Правила>	
<excludeAttributes>	<сценарий>	

Элементы A–K	Элементы L–Z	Вспомогательные функции
<Расширения>	<CMC>	
<расширение>	<unconditionalExclude>	
<externalProcess>	<переменная>	
<icon>	<Версия>	
<include>	<windowsObjects>	
<includeAttribute>		

<addObjects>

Элемент **<addObjects>** имитирует существование одного или нескольких объектов на исходном компьютере. Дочерние **<элементы объекта>** предоставляют сведения о эмулированных объектах. Если содержимое является элементом **<скрипта>** , результатом вызова является массив объектов.

- **Число вхождений:** не ограничено
- **Родительские элементы:**<правила>
- **Обязательные дочерние элементы:**<object> . Кроме того, <расположение> и <атрибут> должны быть указаны в качестве дочерних элементов этого **<элемента объекта>** .
- **Необязательные дочерние элементы:**<условия>, <условие>, <скрипт>

Синтаксис:

XML

```
<addObjects>
</addObjects>
```

Следующий пример из `MigApp.xml` файла:

XML

```
<addObjects>
   <object>
      <location
type="Registry">%HklmWowSoftware%\Microsoft\Office\16.0\Common\Migration\Off
ice [UpgradeVersion]</location>
      <attributes>DWORD</attributes>
      <bytes>0B000000</bytes>
   </object>
   <object>
      <location
```

```
type="Registry">%HklmWowSoftware%\Microsoft\Office\16.0\Common\Migration\Off
ice [Lang]</location>
      <attributes>DWORD</attributes>
      <bytes>00000000</bytes>
   </object>
</addObjects>
```

<Атрибуты>

Элемент **<attributes>** определяет атрибуты для раздела реестра или файла.

- **Количество вхождений:** один раз для каждого <объекта>
- **Родительские элементы:**<object>
- **Дочерние элементы:** none

Синтаксис:

XML

```
<attributes>Content</attributes>
```

Развернуть таблицу

Параметр	Обязательно?	Значение

Содержимое	Да	Содержимое зависит от типа указанного объекта.
		• Для файлов содержимое может быть строкой, содержащей любой из следующих атрибутов, разделенных запятыми:
		  ◦ Archive
		  ◦ Только чтение
		  ◦ System
		  ◦ Hidden (Скрыто)
		• Для разделов реестра содержимое может быть одного из следующих типов:
		  ◦ Нет
		  ◦ Строка
		  ◦ ExpandString
		  ◦ Двоичный
		  ◦ Dword
		  ◦ REG_SZ

Следующий пример из `MigApp.xml` файла:

XML

```xml
<object>
   <location
type="Registry">%HklmWowSoftware%\Microsoft\Office\16.0\Common\Migration\Off
ice [Lang]</location>
   <attributes>DWORD</attributes>
   <bytes>00000000</bytes>
</object>
```

<Байт>

Элемент **<bytes>** можно указать только для файлов, так как если **<расположение>** соответствует разделу реестра или каталогу, **<байты>** игнорируются.

- **Количество вхождений:** ноль или одно
- **Родительские элементы:**<object>
- **Дочерние элементы:** none

Синтаксис:

XML

```xml
<bytes string="Yes|No" expand="Yes|No">Content</bytes>
```

Развернуть таблицу

Параметр	Обязательно?	Значение
string	Нет, по умолчанию — Нет.	Определяет, следует ли интерпретировать *содержимое* как строку или как байт.
expand	Нет (по умолчанию = Да	Если параметр expand имеет значение **Да**, содержимое **<элемента bytes>** сначала разворачивается в контексте исходного компьютера, а затем интерпретируется.
Содержимое	Да	Зависит от значения строки. • Если строка имеет значение **Да**, содержимое **<элемента bytes>** интерпретируется как строка. • Если строка имеет значение **No**, содержимое **<элемента bytes>** интерпретируется как байт. Каждые два символа представляют шестнадцатеричное значение байта. Например, `616263` является представлением для `abc` строки ANSI.

Параметр	Обязательно?	Значение
		Полное представление строки `abc` ЮНИКОДа, включая терминатор строки, будет следующим: `6100620063000000`.

Следующий пример из `MigApp.xml` файла:

XML

```
<object>
   <location
type="Registry">%HklmWowSoftware%\Microsoft\Office\16.0\Common\Migration\Off
ice [Lang]</location>
   <attributes>DWORD</attributes>
   <bytes>00000000</bytes>
</object>
```

<commandLine>

Элемент **<commandLine>** можно использовать для запуска или остановки службы или приложения до или после запуска средств **ScanState** и **LoadState** .

- **Число вхождений:** не ограничено
- **Родительские элементы:** <externalProcess>
- **Дочерние элементы:** none

Синтаксис:

XML

```
<commandLine>CommandLineString</commandLine>
```

Развернуть таблицу

Параметр	Обязательно?	Значение
CommandLineString	Да	Допустимая командная строка.

<компонент>

Элемент **<компонента>** является обязательным в пользовательском **.xml** файле. Этот элемент определяет основную конструкцию файла **.xmlмиграции** . Например, в `MigApp.xml` файле **Microsoft Office 2016** является компонентом, который содержит другой компонент, **Microsoft Office Access 2016**. Для определения компонента можно использовать дочерние элементы.

Компонент может быть вложен в другой компонент; то есть **<элемент компонента>** может быть дочерним элементом **<элемента роли>** в элементе **<компонента>** в двух случаях:

1. Когда родительский **<элемент компонента>** является контейнером
2. Значение , если дочерний **<элемент компонента>** имеет ту же роль, что и родительский **<элемент компонента>** .

- **Количество вхождений:** Неограниченный
- **Родительские элементы:**<миграция>, <роль>
- **Обязательные дочерние элементы:**<role>, <displayName>
- **Необязательные дочерние элементы:**<производитель>, <версия>, <описание>, <пути>, <значок>, <среда>, <расширения>

Синтаксис:

XML

```
<component type="System|Application|Device|Documents"
context="User|System|UserAndSystem" defaultSupported="TRUE|FALSE|YES|NO"
hidden="Yes|No">
</component>
```

Развернуть таблицу

Параметр	Обязательно?	Значение
type	Да	Следующие элементы можно использовать для группировки параметров и определения типа компонента. • **Система:** Параметры операционной системы. Все компоненты Windows определяются этим типом. Если **type="System"** и **defaultSupported="FALSE"**, параметры не переносятся, если в **файлах.xml** нет эквивалентного компонента, указанного в командной `LoadState.exe` строке. Например, файл по умолчанию `MigSys.xml` содержит компоненты

Параметр	Обязательно?	Значение
		с **type="System"** и **defaultSupported="FALSE"**. Если этот файл указан в командной строке `ScanState.exe` , он также должен быть указан в командной `LoadState.exe` строке для переноса параметров. Файл должен быть указан, `LoadState.exe` так как средство должно обнаружить эквивалентный компонент. То есть компонент должен иметь одинаковый URL-адрес миграции **файла.xml** и идентичное отображаемое имя. В противном случае средство **LoadState** не переносит эти параметры из хранилища. Этот параметр полезен, так как хранилище можно использовать для конечных компьютеров, которые имеют ту же или другую версию Windows, что и исходный компьютер. • **Приложение:** Параметры приложения. • **Устройство:** Параметры устройства. • **Документы:** Указывает файлы.
контекст	Нет По умолчанию = UserAndSystem	Определяет область этого параметра, т. е. следует ли обрабатывать этот компонент в контексте конкретного пользователя, во всей операционной системе или в обоих случаях. Наибольший возможный область задается элементом **<компонента>**. Например, если **<элемент компонента>** имеет контекст **User** , а **<элемент rules>** имеет контекст **UserAndSystem**, элемент **<rules>** будет действовать так, как будто он имеет контекст **User**. Если элемент **rules> имеет контекст System, он будет действовать так, как будто элемента rules**<>< нет. • **Пользователь**: вычисляет компонент для каждого пользователя. • **Система**. Оценивает компонент только один раз для системы. • **UserAndSystem**: оценивает компонент для всей операционной системы и каждого пользователя.
defaultSupported	Нет (по умолчанию = TRUE)	Может иметь значение **TRUE**, **FALSE**, **ДА** или **НЕТ**. Если этот параметр имеет значение **FALSE** (или **NO**), компонент не переносится, если на целевом компьютере нет эквивалентного компонента. Если **type="System"** и **defaultSupported="FALSE"**, параметры не переносятся, если в **.xml** файлах, указанных `LoadState.exe` в командной строке, нет эквивалентного компонента. Например, файл по умолчанию `MigSys.xml` содержит компоненты с

Параметр	Обязательно?	Значение
		type="System" и **defaultSupported="FALSE".** Если этот файл указан в командной строке `ScanState.exe` , он также должен быть указан в командной `LoadState.exe` строке для переноса параметров. Файл должен быть указан в обеих командных строках, так как средство **LoadState** должно обнаружить эквивалентный компонент. То есть компонент должен иметь тот же URL-адрес миграции **файла.xml** и идентичное отображаемое имя, иначе средство **LoadState** не переносит эти параметры из хранилища. Этот параметр полезен, так как хранилище можно использовать для конечных компьютеров, которые имеют ту же или другую версию Windows, что и исходный компьютер.
скрытый		Этот параметр предназначен только для внутреннего использования USMT.

Пример см. в любом из файлов **миграции** по умолчанию.xml.

<состояние>

<**Хотя элемент condition**> в <**элементах detect**>, <**objectSet**> и <**addObjects**> по-прежнему поддерживается, корпорация Майкрософт рекомендует больше не использовать <**элемент condition**>, так как он может быть нерекомендуем в будущих версиях USMT. <**Если элемент condition**> является устаревшим, потребуется перезаписать все скрипты, использующие <**элемент condition**>. Вместо этого, если условие необходимо использовать в <**элементах objectSet**> и <**addObjects**> , корпорация Майкрософт рекомендует использовать более мощный <элемент conditions> . Элемент <**conditions**> позволяет формулировать сложные логические инструкции.

Элемент <**condition**> имеет логический результат. Этот элемент можно использовать для указания условий, в которых вычисляется родительский элемент. Если какое-либо из указанных условий возвращает **значение FALSE**, родительский элемент не вычисляется.

- **Число вхождений:** неограниченно.
- **Родительские элементы:**<conditions>, <detect>, <objectSet>, <addObjects>
- **Дочерние элементы:** none

- **Вспомогательные функции:** С этим элементом можно использовать следующие <функции условия>: `DoesOSMatch`, , `IsNative64Bit()`, `IsOSLaterThan`, `IsOSEarlierThan` `DoesObjectExist`, `DoesFileVersionMatch`, `IsFileVersionAbove`, , `IsFileVersionBelow`, `IsSystemContext`, `DoesStringContentEqual`, `DoesStringContentContain`, `IsSameObject`, `IsSameContent` и `IsSameStringContent`.

Синтаксис:

XML

```
<condition negation="Yes|No">ScriptName</condition>
```

Развернуть таблицу

Параметр	Обязательно?	Значение
отрицание	Нет По умолчанию = Нет	**Значение "Да"** отменяет значение True или False условия.
ScriptName	Да	Скрипт, определенный в этом разделе миграции.

Например, в следующем примере **<кода элементы условия>A** и **B** объединяются оператором **AND** , так как находятся в отдельных **<разделах условий>** :

XML

```
<detection>
   <conditions>
      <condition>A</condition>
   </conditions>
   <conditions operation="AND">
      <condition>B</condition>
   </conditions>
</detection>
```

Однако в следующем примере **<кода элементы условия>A** и **B** объединяются оператором **OR** , так как находятся в одном **<разделе условий>** .

XML

```
<detection>
   <conditions>
      <condition>A</condition>
      <condition>B</condition>
```

```
    </conditions>
</detection>
```

<Функции условий>

Функции **<условия>** возвращают логическое значение. Эти элементы можно использовать в **<условиях addObjects>** .

- Функции версии операционной системы
- Функции содержимого объектов

Функции версии операционной системы

- **DoesOSMatch**

  Все совпадения не учитывают регистр.

  Синтаксис: `DoesOSMatch("OSType","OSVersion")`

  Развернуть таблицу

Параметр	Обязательно?	Значение
OSType	Да	Единственное допустимое значение для этого параметра — **NT**. Однако этот параметр необходимо задать, чтобы функции **условий> работали<** правильно.
OSVersion	Да	Основная версия, дополнительная версия, номер сборки и исправленная версия дискеты службы разделены точками. Например, `5.0.2600.Service Pack 1`. Частичная спецификация версии также может быть указана с помощью шаблона, `5.0.*`например .

  Пример

```
XML
<condition>MigXmlHelper.DoesOSMatch("NT","\*")</condition>
```

- **IsNative64Bit**

  Функция **IsNative64Bit** возвращает **значение TRUE** , если процесс миграции выполняется как собственный 64-разрядный процесс; то есть процесс,

выполняемый в 64-разрядной системе без Windows в Windows (WOW). В противном случае возвращается **значение FALSE**.

- **IsOSLaterThan**

  Все сравнения не учитывают регистр.

  Синтаксис: `IsOSLaterThan("OSType","OSVersion")`

  Развернуть таблицу

Параметр	Обязательно?	Значение
OSType	Да	Может быть **9x** или **NT**. Если *ТИП OSType* не соответствует типу текущей операционной системы, возвращается **значение FALSE**. Например, если текущая операционная система основана на Windows NT, а *osType* — **"9x"**, результатом будет **ЛОЖЬ**.
OSVersion	Да	Основная версия, дополнительная версия, номер сборки и исправленная версия дискеты службы разделены точками. Например, `5.0.2600.Service Pack 1`. Можно также указать частичную спецификацию версии, но шаблон не допускается, например `5.0`. Функция **IsOSLaterThan** возвращает **значение TRUE** , если текущая операционная система позже *или равна OSVersion*.

  Пример

```
XML
```

```xml
<condition negation="Yes">MigXmlHelper.IsOSLaterThan("NT","6.0")
</condition>
```

- **IsOSEarlierThan**

  Все сравнения не учитывают регистр.

  Синтаксис: `IsOSEarlierThan("OSType","OSVersion")`

  Развернуть таблицу

Параметр	Обязательно?	Значение
OSType	Да	Может быть **9x** или **NT**. Если *ТИП OSType* не соответствует типу текущей операционной системы, возвращается **значение FALSE**. Например, если текущая операционная система основана на Windows NT, а *OSType* — **"9x"**, результатом будет **FALSE**.
OSVersion	Да	Основная версия, дополнительная версия, номер сборки и исправленная версия дискеты службы разделены точками. Например, `5.0.2600.Service Pack 1`. Можно также указать частичную спецификацию версии, но шаблон не допускается, например `5.0`. Функция **IsOSEarlierThan** возвращает **значение TRUE** , если текущая операционная система находится раньше , *чем OSVersion*.

Функции содержимого объектов

- **DoesObjectExist**

  Функция DoesObjectExist возвращает **значение TRUE** , если существует какой-либо объект, соответствующий шаблону расположения. В противном случае возвращается **значение FALSE**. Шаблон расположения развертывается перед попыткой перечисления.

  Синтаксис: `DoesObjectExist("ObjectType","EncodedLocationPattern")`

  Развернуть таблицу

Параметр	Обязательно?	Значение
ObjectType	Да	Определяет тип объекта. Может быть файлом или реестром.
EncodedLocationPattern	Да	Шаблон расположения. Переменные среды разрешены.

  Пример этого элемента см. в `MigApp.xml` файле .

- **DoesFileVersionMatch**

  Шаблон проверка не учитывает регистр.

Синтаксис:

`DoesFileVersionMatch("EncodedFileLocation","VersionTag","VersionValue")`

Развернуть таблицу

Параметр	Обязательно?	Значение
EncodedFileLocation	Да	Шаблон расположения для проверяемого файла. Переменные среды разрешены.
VersionTag	Да	Значение тега версии , которое проверяется.
VersionValue	Да	Шаблон строки. Например, "Microsoft*".

Пример:

XML

```
<condition>MigXmlHelper.DoesFileVersionMatch("%MSNMessengerInstPath%\\msnmsgr.exe","ProductVersion","6.\*")</condition>
<condition>MigXmlHelper.DoesFileVersionMatch("%MSNMessengerInstPath%\\msnmsgr.exe","ProductVersion","7.\*")</condition>
```

- **IsFileVersionAbove**

  Функция **IsFileVersionAbove** возвращает **значение TRUE** , если версия файла выше *VersionValue*.

  Синтаксис:

  `IsFileVersionAbove("EncodedFileLocation","VersionTag","VersionValue")`

  Развернуть таблицу

Параметр	Обязательно?	Значение
EncodedFileLocation	Да	Шаблон расположения для проверяемого файла. Переменные среды разрешены.
VersionTag	Да	Значение тега версии , которое проверяется.
VersionValue	Да	Сравниваемое значение. Невозможно указать шаблон.

- **IsFileVersionBelow**

  Синтаксис:

  `IsFileVersionBelow("EncodedFileLocation","VersionTag","VersionValue")`

Развернуть таблицу

Параметр	Обязательно?	Значение
EncodedFileLocation	Да	Шаблон расположения для проверяемого файла. Переменные среды разрешены.
VersionTag	Да	Значение тега версии , которое проверяется.
VersionValue	Да	Сравниваемое значение. Невозможно указать шаблон.

- **IsSystemContext**

  Функция **IsSystemContext** возвращает **значение TRUE** , если текущий контекст имеет значение **System**. В противном случае возвращается **значение FALSE**.

  Синтаксис: `IsSystemContext()`

- **DoesStringContentEqual**

  Функция **DoesStringContentEqual** возвращает **значение TRUE** , если строковое представление данного объекта идентично `StringContent`.

  Синтаксис:
  `DoesStringContentEqual("ObjectType","EncodedLocation","StringContent")`

Развернуть таблицу

Параметр	Обязательно?	Значение
ObjectType	Да	Определяет тип объекта . Может быть файлом или реестром.
EncodedLocationPattern	Да	Закодированное расположение проверяемого объекта. Переменные среды можно указать.
StringContent	Да	Строка, с которым выполняется проверка.

Пример

XML

```
<condition
negation="Yes">MigXmlHelper.DoesStringContentEqual("File","%USERNAME%",
"")</condition>
```

- **DoesStringContentContain**

  Функция **DoesStringContentContain** возвращает **значение TRUE** , если в строковом представлении объекта имеется хотя бы одно вхождение *StrToFind* .

  Синтаксис:
  `DoesStringContentContain("ObjectType","EncodedLocation","StrToFind")`

  Развернуть таблицу

Параметр	Обязательно?	Значение
ObjectType	Да	Определяет тип объекта . Может быть файлом или реестром.
EncodedLocationPattern	Да	Закодированное расположение проверяемого объекта. Переменные среды можно указать.
StrToFind	Да	Строка, которая выполняется в содержимом заданного объекта.

- **IsSameObject**

  Функция **IsSameObject** возвращает **значение TRUE** , если заданные закодированные расположения разрешаются в один и тот же физический объект. В противном случае возвращается **значение FALSE**.

  Синтаксис: `IsSameObject("ObjectType","EncodedLocation1","EncodedLocation2")`

  Развернуть таблицу

Параметр	Обязательно?	Значение
ObjectType	Да	Определяет тип объекта . Может быть файлом или реестром.
EncodedLocation1	Да	Закодированное расположение для первого объекта. Переменные среды можно указать.
EncodedLocation2	Да	Закодированное расположение для второго объекта. Переменные среды можно указать.

  Пример:

```
XML
```

```
<objectSet>
   <condition
negation="Yes">MigXmlHelper.IsSameObject("File","%CSIDL_FAVORITES%","%C
SIDL_COMMON_FAVORITES%")</condition>
   <pattern type="File">%CSIDL_FAVORITES%\* [*]</pattern>
</objectSet>
```

- **IsSameContent**

  Функция **IsSameContent** возвращает **значение TRUE** , если заданные объекты имеют одинаковое содержимое. В противном случае возвращается **значение FALSE**. Содержимое сравнивается по байтам.

  Синтаксис:
  `IsSameContent("ObjectType1","EncodedLocation1","ObjectType2","EncodedLocation2")`

  Развернуть таблицу

Параметр	Обязательно?	Значение
ObjectType1	Да	Определяет тип первого объекта. Может быть файлом или реестром.
EncodedLocation1	Да	Закодированное расположение для первого объекта. Переменные среды можно указать.
ObjectType2	Да	Определяет тип второго объекта. Может быть файлом или реестром.
EncodedLocation2	Да	Закодированное расположение для второго объекта. Переменные среды можно указать.

- **IsSameStringContent**

  Функция **IsSameStringContent** возвращает **значение TRUE** , если заданные объекты имеют одинаковое содержимое. В противном случае возвращается **значение FALSE**. Содержимое интерпретируется как строка.

  Синтаксис:
  `IsSameStringContent("ObjectType1","EncodedLocation1","ObjectType2","EncodedLocation2")`

  Развернуть таблицу

Параметр	Обязательно?	Значение
ObjectType1	Да	Определяет тип первого объекта. Может быть файлом или реестром.
EncodedLocation1	Да	**Закодированное расположение** для первого объекта. Переменные среды можно указать.
ObjectType2	Да	Определяет тип второго объекта. Может быть файлом или реестром.
EncodedLocation2	Да	**Закодированное расположение** для второго объекта. Переменные среды можно указать.

<условия>

Элемент **<conditions>** возвращает логический результат, который используется для указания условий, в которых вычисляется родительский элемент. USMT оценивает дочерние элементы, а затем объединяет их результаты с помощью операторов **AND** или **OR** в соответствии с параметром операции.

- **Количество вхождений:** Неограниченный внутри другого **<элемента условий>** . Ограничено одним вхождением в <обнаружении>, <правилах>, <addObjects> и <objectSet>
- **Родительские элементы:**<условия>, <обнаружение>, <среда>, <правила>, <addObjects> и <objectSet>
- **Дочерние элементы:**<условия>, <условие>

Синтаксис:

```xml
<conditions operation="AND|OR">
</conditions>
```

Развернуть таблицу

Параметр	Обязательно?	Значение
операция	Нет, по умолчанию = AND	Определяет логическую операцию, выполняемую с результатами, полученными из дочерних элементов.

Следующий пример из `MigApp.xml` файла:

XML

```
<environment name="GlobalEnv">
   <conditions>
      <condition negation="Yes">MigXmlHelper.IsNative64Bit()</condition>
   </conditions>
   <variable name="HklmWowSoftware">
   <text>HKLM\Software</text>
   </variable>
</environment>
```

<содержание>

Элемент **<content>** можно использовать для указания списка шаблонов объектов для получения набора объектов с исходного компьютера. Вычисляется каждый **<objectSet>** в элементе **<содержимого>** . Для каждого результирующего списка шаблонов объектов перечисляются соответствующие ему объекты, а их содержимое фильтруется по параметру фильтра. Результирующий строковый массив является выходными данными для элемента **содержимого<>**. Скрипт фильтра возвращает массив расположений. Родительский **<элемент objectSet>** может содержать несколько дочерних **<элементов содержимого>** .

- **Число вхождений:** не ограничено
- **Родительские элементы:**<objectSet>
- **Дочерние элементы:**<objectSet>
- **Вспомогательные функции:** С этим элементом можно использовать следующие <функции содержимого>: `ExtractSingleFile`, `ExtractMultipleFiles` и `ExtractDirectory`.

Синтаксис:

XML

```
<content filter="ScriptInvocation">
</content>
```

Развернуть таблицу

Параметр	Обязательно?	Значение
filter	Да	Скрипт, за которым следует любое количество строковых аргументов, разделенных запятой и заключенных в круглые

Параметр	Обязательно?	Значение
		скобки. Например, `MyScripts.AScript ("Arg1","Arg2")`. Скрипт вызывается для каждого объекта, который перечисляется наборами объектов в правиле **<включения>** . Скрипт фильтра возвращает логическое значение. Если возвращаемое значение равно **TRUE**, объект переносится. Если имеет значение **FALSE**, он не переносится.

<функции содержимого>

Следующие функции создают шаблоны из содержимого объекта . Эти функции вызываются для каждого объекта, перечисляемого родительским **<элементом ObjectSet>** .

- **ExtractSingleFile**

  Если значение реестра — **MULTI-SZ**, обрабатывается только первый сегмент. Возвращаемый шаблон — это закодированное расположение для файла, который должен существовать в системе. Если спецификация указана правильно в значении реестра, но файл не существует, эта функция возвращает **значение NULL**.

  Синтаксис: `ExtractSingleFile(Separators,PathHints)`

  Развернуть таблицу

Параметр	Обязательно?	Значение
Разделители	Да	Список возможных разделителей, которые могут соответствовать спецификации файла в этом имени значения реестра. Например, если содержимое — **"C:\Windows\Notepad.exe-2"**, разделитель — запятая. Можно указать **значение NULL**.
PathHints	Да	Список дополнительных путей, разделенных двоеточием (`;`), где функция ищет файл, соответствующий текущему содержимому. Например, если содержимое — **"Notepad.exe"**, а путь — это переменная среды **%Path%,** функция находит **Notepad.exe** в `%windir%` и возвращает **"c:\Windows [Notepad.exe]".** Можно указать **значение NULL**.

  Пример:

  ```
  XML
  ```

```
<content filter="MigXmlHelper.ExtractSingleFile(',','%system%')">
```

и

```
XML

<content
filter="MigXmlHelper.ExtractSingleFile(NULL,'%CSIDL_COMMON_FONTS%')">
```

- **ExtractMultipleFiles**

  Функция **ExtractMultipleFiles** возвращает несколько шаблонов, по одному для каждого файла, который находится в содержимом заданного значения реестра. Если значение реестра — **MULTI-SZ**, разделитель **MULTI-SZ** по умолчанию считается разделителем. Поэтому для **MULTI-SZ<аргумент Разделители>** должен иметь значение **NULL**.

  Возвращаемые шаблоны — это закодированные расположения для файлов, которые должны существовать на исходном компьютере. Если спецификация указана правильно в значении реестра, но файл не существует, она не включается в результирующий список.

  Синтаксис: `ExtractMultipleFiles(Separators,PathHints)`

  Развернуть таблицу

Параметр	Обязательно?	Значение
Разделители	Да	Список возможных разделителей, которые могут соответствовать спецификации файла в этом имени значения реестра. Например, если содержимое — **"C:\Windows\Notepad.exe-2"**, разделитель — запятая. Этот параметр должен иметь значение NULL при обработке **значений реестра MULTI-SZ** .
PathHints	Да	Список дополнительных путей, разделенных двоеточием (`;`), где функция ищет файл, соответствующий текущему содержимому. Например, если содержимое — **"Notepad.exe"**, а путь — это переменная среды **%Path%,** функция находит **Notepad.exe** в `%windir%` и возвращает **"c:\Windows [Notepad.exe]"**. Можно указать **значение NULL**.

- **ExtractDirectory**

Функция **ExtractDirectory** возвращает шаблон, который является закодированным расположением для каталога, который должен существовать на исходном компьютере. Если спецификация указана правильно в значении реестра, но каталог не существует, эта функция возвращает **значение NULL**. При обработке значения реестра, которое является **MULTI-SZ**, обрабатывается только первый сегмент.

Синтаксис: `ExtractDirectory(Separators,LevelsToTrim,PatternSuffix)`

Развернуть таблицу

Параметр	Обязательно?	Значение
Разделители	Нет	Список возможных разделителей, которые могут соответствовать спецификации файла в этом имени значения реестра. Например, если содержимое — **"C:\Windows\Notepad.exe-2"**, разделитель — запятая. При обработке значений реестра **MULTI-SZ** необходимо указать **значение NULL**.
LevelsToTrim	Да	Количество уровней, удаляемых из конца спецификации каталога. Используйте эту функцию для извлечения корневого каталога при наличии значения реестра, указывающего внутри этого корневого каталога в известном расположении.
PatternSuffix	Да	Шаблон, добавляемый в спецификацию каталога. Например, `* [*]`.

Пример:

XML

```
<objectSet>
   <content filter='MigXmlHelper.ExtractDirectory (NULL, "1")'>
        <objectSet>
             <pattern
type="Registry">%HklmWowSoftware%\Classes\Software\RealNetworks\Prefere
nces\DT_Common []</pattern>
        </objectSet>
   </content>
</objectSet>
```

<contentModify>

Элемент **<contentModify>** изменяет содержимое объекта перед записью объекта на целевой компьютер. Для каждого **<элемента contentModify>** может быть несколько **<элементов objectSet>** . Этот элемент возвращает новое содержимое обрабатываемого объекта.

- **Количество вхождений:** Неограниченный
- **Родительские элементы:**<правила>
- **Обязательные дочерние элементы:**<objectSet>
- **Вспомогательные функции**. С этим элементом можно использовать следующие <функции contentModify>: **ConvertToDWORD**, **ConvertToString**, **ConvertToBinary**, **KeepExisting**, **OffsetValue**, **SetValueByTable**, **MergeMultiSzContent** и **MergeDelimitedContent**.

Синтаксис:

```xml
<contentModify script="ScriptInvocation">
</contentModify>
```

Развернуть таблицу

Параметр	Обязательно?	Значение
сценарий	Да	Скрипт, за которым следует любое количество строковых аргументов, разделенных запятой и заключенных в круглые скобки. Например `MyScripts.AScript ("Arg1","Arg2").` Скрипт вызывается для каждого объекта, который перечисляется наборами объектов в правиле включения. Скрипт фильтра возвращает логическое значение. Если возвращаемое значение равно **TRUE**, объект переносится. Если имеет значение **FALSE**, он не переносится.

<функции contentModify>

Следующие функции изменяют содержимое объектов по мере их переноса. Эти функции вызываются для каждого объекта, перечисляемого родительским **<элементом ObjectSet>** .

- **ConvertToDWORD**

Функция **ConvertToDWORD** преобразует содержимое значений реестра, перечисляемых родительским **<элементом ObjectSet>** , в DWORD. Например, **ConvertToDWORD** преобразует строку `"1"` в DWORD `0x00000001`. Если преобразование завершается ошибкой, применяется значение **DefaultValueOnError** .

Синтаксис: `ConvertToDWORD(DefaultValueOnError)`

Развернуть таблицу

Параметр	Обязательно?	Значение
DefaultValueOnError	Нет	Значение, которое записывается в имя значения в случае сбоя преобразования. **Значение NULL** можно указать, и `0` записывается в случае сбоя преобразования.

- **ConvertToString**

Функция **ConvertToString** преобразует содержимое значений реестра, которые соответствуют родительскому **<элементу ObjectSet>** , в строку. Например, он преобразует DWORD `0x00000001` в строку **"1".** Если преобразование завершается ошибкой, применяется значение **DefaultValueOnError** .

Синтаксис: `ConvertToString(DefaultValueOnError)`

Развернуть таблицу

Параметр	Обязательно?	Значение
DefaultValueOnError	Нет	Значение, которое записывается в имя значения в случае сбоя преобразования. **Значение NULL** можно указать, и `0` записывается в случае сбоя преобразования.

Пример:

XML

```
<contentModify script="MigXmlHelper.ConvertToString('1')">
   <objectSet>
        <pattern type="Registry">HKCU\Control Panel\Desktop
[ScreenSaveUsePassword]</pattern>
```

```
    </objectSet>
  </contentModify>
```

- **ConvertToBinary**

  Функция **ConvertToBinary** преобразует содержимое значений реестра, которые соответствуют родительскому **<элементу ObjectSet>** , в двоичный тип.

  Синтаксис: `ConvertToBinary ()`

- **OffsetValue**

  Функция **OffsetValue** добавляет значение или вычитает *значение* из значения перенесенного объекта, а затем записывает результат обратно в значение реестра на конечном компьютере. Например, если перенесенный объект является DWORD со значением `14`, а *значение* — **"-2"**, значение реестра будет находиться `12` на конечном компьютере.

  Синтаксис: `OffsetValue(Value)`

Развернуть таблицу

Параметр	Обязательно?	Значение
Ценность	Да	Строковое представление числового значения. Он может быть положительным или отрицательным. Например, `OffsetValue(2)`.

- **SetValueByTable**

  Функция **SetValueByTable** сопоставляет значение исходного компьютера с исходной таблицей. Если значение имеется, применяется эквивалентное значение в целевой таблице. Если значение отсутствует или целевая таблица не имеет эквивалентного значения, применяется *значение DefaultValueOnError* .

  Синтаксис: `SetValueByTable(SourceTable,DestinationTable,DefaultValueOnError)`

Развернуть таблицу

Параметр	Обязательно?	Значение
SourceTable	Да	Список значений, разделенных запятыми, которые возможны для исходных значений

Параметр	Обязательно?	Значение
		реестра.
DestinationTable	Нет	Список переведенных значений, разделенных запятыми.
DefaultValueOnError	Нет	Значение, применяемое к конечному компьютеру, если 1. Значение исходного компьютера не совпадает с *SourceTable*. 2. *DestinationTable* не имеет эквивалентного значения. Если **defaultValueOnError** имеет **значение NULL**, значение не изменяется на конечном компьютере.

- **KeepExisting**

  Функцию **KeepExisting** можно использовать при возникновении конфликтов на конечном компьютере. Эта функция сохраняет (не перезаписывает) указанные атрибуты для объекта, который находится на конечном компьютере.

  Синтаксис: `KeepExisting("OptionString","OptionString","OptionString",…)`

  Развернуть таблицу

Параметр	Обязательно?	Значение
OptionString	Да	*OptionString* может иметь значение **Security**, **TimeFields** или **FileAttrib**:*Letter*. Можно указать один из каждого типа *OptionStrings* . Не указывайте несколько *OptionStrings* с одинаковым значением. Если указано несколько *объектов OptionStrings* с одинаковым значением, сохраняется самый правый параметр этого типа. Например, не указывайте **("FileAttrib:H", "FileAttrib:R"),** так как вычисляется только для чтения. Вместо этого укажите **("FileAttrib:HR"),** а на конечном компьютере хранятся как скрытые, так и только для чтения атрибуты. ◦ **Безопасность**: сохраняет дескриптор безопасности целевого объекта, если он существует. ◦ **TimeFields**: сохраняет метки времени целевого объекта. Этот параметр предназначен только для файлов.

Параметр	Обязательно?	Значение
		◦ **FileAttrib:<Letter>**: сохраняет значение атрибута целевого объекта (**ON** или **OFF**) для указанного набора атрибутов файла. Этот параметр предназначен только для файлов. Ниже приведены значения без учета регистра, но USMT игнорирует все значения, которые являются недопустимыми, повторяющимися или если после **FileAttrib:**есть пробел. Можно указать любое сочетание следующих атрибутов: ◦ **A** = Archive ◦ **C** = сжатый ◦ **E** = Зашифровано ◦ **H** = скрытый ◦ **I** = не индексировано содержимого ◦ **O** = в автономном режиме ◦ **R** = Read-Only ◦ **S** = System ◦ **T** = временный

- **MergeMultiSzContent**

  Функция **MergeMultiSzContent** объединяет содержимое **MULTI-SZ** значений реестра, перечисляемых родительским **<элементом ObjectSet>** , с содержимым эквивалентных значений реестра, которые уже существуют на конечном компьютере. `Instruction` и `String` либо удалить, либо добавить содержимое в результирующий **MULTI-SZ**. Повторяющиеся элементы удаляются.

  Синтаксис: `MergeMultiSzContent (Instruction,String,Instruction,String,…)`

  Развернуть таблицу

Параметр	Обязательно?	Значение
Инструкция	Да	Может иметь одно из следующих значений: ◦ **Добавить**. Добавляет соответствующую строку в результирующий объект MULTI-SZ, если его еще нет. ◦ **Удалить**. Удаляет соответствующую строку из результирующего MULTI-SZ.
Строка	Да	Добавляемая или удаляемая строка.

- **MergeDelimitedContent**

Функция **MergeDelimitedContent** объединяет содержимое значений реестра, перечисленных родительским **<элементом ObjectSet>** , с содержимым эквивалентных значений реестра, которые уже существуют на конечном компьютере. Содержимое считается списком элементов, разделенных одним из символов в параметре Разделители. Повторяющиеся элементы удаляются.

Синтаксис: `MergeDelimitedContent(Delimiters,Instruction,String,…)`

Развернуть таблицу

Параметр	Обязательно?	Значение
Разделители	Да	Один символ, используемый для разделения содержимого обрабатываемого объекта. Содержимое рассматривается как список элементов, разделенных *разделителями*. Например, `"."` разделяет строку на основе точки.
Инструкция	Да	Может иметь одно из следующих значений: ◦ **Добавить**: добавляет *string* в результирующий MULTI-SZ, если он еще не существует. ◦ **Удалить**. Удаляет *строку* из полученного multi-SZ.
Строка	Да	Добавляемая или удаляемая строка.

<описание>

Элемент **<description>** определяет описание компонента, но не влияет на миграцию.

- **Количество вхождений:** ноль или одно
- **Родительские элементы:**<component>
- **Дочерние элементы:** none

Синтаксис:

```
XML
<description>ComponentDescription</description>
```

Развернуть таблицу

Параметр	Обязательно?	Значение
ComponentDescription	Да	Описание компонента.

В следующем примере кода показано, как <элемент description> определяет описание "Мой настраиваемый компонент".

XML

```
<description>My custom component<description>
```

<destinationCleanup>

Элемент **<destinationCleanup>** удаляет объекты, такие как файлы и разделы реестра, с конечного компьютера перед применением объектов с исходного компьютера. Этот элемент вычисляется только при запуске средства **LoadState** на конечном компьютере. То есть этот элемент игнорируется средством **ScanState** .

> ⓘ **Важно!**
>
> Используйте этот параметр с особой осторожностью, так как он удалит объекты с конечного компьютера.

Для каждого **<элемента destinationCleanup>** может быть несколько **<элементов objectSet>** . Обычно этот элемент используется, если на исходном компьютере отсутствует раздел реестра, но компонент по-прежнему требуется перенести. В этом случае все разделы реестра компонента можно удалить перед переносом исходных разделов реестра. Удаление всех разделов реестра компонента гарантирует, что если на исходном компьютере отсутствует ключ, он также будет отсутствовать на конечном компьютере.

- **Количество вхождений:** Неограниченный
- **Родительские элементы:** <правила>
- **Дочерние элементы:** <objectSet> (конечный компьютер удаляет все дочерние элементы.)

Синтаксис:

XML

```
<destinationCleanup filter=ScriptInvocation>
</destinationCleanup>
```

Развернуть таблицу

Параметр	Обязательно?	Значение
filter	Да	Скрипт, за которым следует любое количество строковых аргументов, разделенных запятой и заключенных в круглые скобки. Например, `MyScripts.AScript ("Arg1","Arg2")`. Скрипт вызывается для каждого объекта, который перечисляется наборами объектов в правиле включения. Скрипт фильтра возвращает логическое значение. Если возвращаемое значение равно **TRUE**, объект переносится. Если имеет значение **FALSE**, он не переносится.

Пример:

XML

```
<destinationCleanup>
   <objectSet>
      <pattern type="Registry">HKCU\Software\Lotus\123\99.0\DDE
Preferences\* [*]</pattern>
      <pattern type="Registry">HKCU\Software\Lotus\123\99.0\Find
Preferences\* [*]</pattern>
   </objectSet>
</destinationCleanup>
```

<обнаруживать>

Хотя элемент **detect> по-прежнему<** поддерживается, корпорация Майкрософт рекомендует больше не использовать **<элемент detect>**, так как он может быть нерекомендуем в будущих версиях USMT. **<Если элемент detect>** является устаревшим, потребуется перезаписать все скрипты, использующие **<элемент detect>**. Вместо этого корпорация Майкрософт рекомендует использовать **<элемент обнаружения>** . Элемент **<обнаружения>** позволяет более четко сформулировать сложные логические инструкции.

Элемент **<detect>** можно использовать для определения наличия компонента в системе. Если все дочерние **<элементы обнаружения>** в элементе **<обнаружения>** разрешаются в **TRUE**, то **<элемент detect>** разрешается в **TRUE**. Если какие-либо дочерние **<элементы обнаружения>** разрешаются в **FALSE**, то их

родительский **<элемент обнаружения>** разрешается в **FALSE**. Если раздел **элемента обнаружения> отсутствует**<, USMT предполагает наличие компонента.

Для каждого **<элемента обнаружения>** может быть несколько дочерних **<элементов условия>** или **<objectSet>** , которые логически соединены оператором **OR** . Если хотя бы один **<элемент condition>** или **<objectSet>** имеет значение **TRUE**, то **<элемент detect>** будет иметь значение **TRUE**.

- **Число вхождений:** не ограничено
- **Родительские элементы:**<detects>, <namedElements>
- **Обязательные дочерние элементы:**<condition>
- **Необязательные дочерние элементы:**<objectSet>

Синтаксис:

XML

```
<detect name="ID" context="User|System|UserAndSystem">
</detect>
```

Развернуть таблицу

Параметр	Обязательно?	Значение
name	Да, если **<свойство detect>** является дочерним элементом **для< именованныхЭлементов>** Нет, если **<обнаружение>** является дочерним объектом для <обнаружения>	Если указан *идентификатор* , все дочерние элементы не обрабатываются. Вместо этого обрабатываются любые другие **<элементы обнаружения>** с тем же именем, объявленные в элементе **<namedElements>** .
контекст	Нет (по умолчанию = UserAndSystem)	Определяет область этого параметра, который определяет, следует ли обрабатывать этот компонент в контексте конкретного пользователя, во всей операционной системе или в обоих случаях. Наибольший возможный область задается элементом компонента. Например, если **<элемент компонента>** имеет контекст **User**, а **<элемент rules>** имеет контекст **UserAndSystem**, то **<элемент rules>** будет действовать так, как если бы он имел контекст **User**. Если элемент **rules> имеет контекст**

Параметр	Обязательно?	Значение
		System, он будет действовать так, как если бы элемента rules не< было.>< • **Пользователь**: вычисляет переменные для каждого пользователя. • **Система**. Оценивает переменные только один раз для системы. • **UserAndSystem**: вычисляет переменные для всей операционной системы и каждого пользователя.

Примеры см. в примерах для <обнаружения>.

<Обнаруживает>

Хотя элемент **detects> по-прежнему**< поддерживается, корпорация Майкрософт рекомендует больше не использовать **<элемент detects>**, так как он может быть нерекомендуем в будущих версиях USMT. **<Если элемент detects>** является устаревшим, потребуется перезаписать все скрипты, использующие **<элемент detects>**. Вместо этого корпорация Майкрософт рекомендует использовать **<элемент обнаружения>** , если родительский элемент является **<role>** или **<namedElements>**, или использовать **<элемент conditions>** , если родительский элемент является **<rules>**. Элемент **<обнаружения>** позволяет более четко формулировать сложные логические инструкции, а **<элемент conditions>** позволяет формулировать сложные логические инструкции.

Элемент **<detects>** — это контейнер для одного или нескольких **<элементов обнаружения>** . Если все дочерние **<элементы обнаружения>** в **элементе< detect разрешаются>** в **TRUE**, то **<обнаруживает>** разрешение в **TRUE**. Если какой-либо из дочерних **<элементов обнаружения>** разрешается в **FALSE**, то **<обнаруживает>** значение **FALSE**. Чтобы предотвратить **<запись элемента detects>** в компоненте, создайте **<элемент detects>** в элементе **<namedElements>** , а затем сослаться на него. Если раздел элемента **detects> отсутствует**<, USMT предполагает наличие компонента. Результаты каждого **<элемента detects>** объединяются оператором **OR** для формирования правила, используемого для обнаружения родительского элемента.

Синтаксис:

```
XML
```

```
<detects name="ID" context="User|System|UserAndSystem">
</detects>
```

- **Количество вхождений:** Неограниченный.
- **Родительские элементы:**<role>, <rules>, <namedElements>
- **Обязательные дочерние элементы:**<detect>

Развернуть таблицу

Параметр	Обязательно?	Значение
name	Да, если <определяет> является дочерним элементом **для<** **namedElements>** Нет, если <определяет> является дочерним элементом **роли<>** или **<правил>**	При *указании идентификатора* дочерние **<элементы обнаружения>** не обрабатываются. Вместо этого обрабатываются любые другие **<элементы обнаружения>** с тем же именем, объявленные в элементе **<namedElements>** .
контекст	Нет (по умолчанию = UserAndSystem)	Определяет область этого параметра: следует ли обрабатывать этот компонент в контексте конкретного пользователя, во всей операционной системе или в обоих случаях. Наибольший возможный область задается **элементом<> компонента**. Например, если **<элемент компонента>** имеет контекст **User** , а **<элемент rules>** имеет контекст **UserAndSystem**, то **<элемент rules>** будет действовать так, как если бы он имел контекст **User**. Если элемент **rules> имеет контекст System, он будет действовать так, как если бы элемента rules не<** было.> • **Пользователь**: вычисляет переменные для каждого пользователя. • **Система**. Оценивает переменные только один раз для системы. • **UserAndSystem**: вычисляет переменные для всей операционной системы и каждого пользователя. Параметр контекста игнорируется для **<обнаружения>** элементов, которые находятся внутри **<элементов правил>** .

Следующий пример из `MigApp.xml` файла.

```xml
<detects>
   <detect>

<condition>MigXmlHelper.DoesFileVersionMatch("%Lotus123InstPath%\123w.exe","
ProductVersion","9.*")</condition>
   </detect>
   <detect>

<condition>MigXmlHelper.DoesFileVersionMatch("%SmartSuiteInstPath%\smartctr.
exe","ProductVersion","99.*")</condition>
   </detect>
</detects>
```

<обнаружение>

Элемент **<обнаружения>** является контейнером для одного **<элемента условий>** . Результат дочерних **<элементов условия>** , расположенных под элементом **<conditions>** , определяет результат этого элемента. Например, если все дочерние **<элементы>** в элементе **<обнаружения>** разрешаются в **TRUE**, то **<элемент обнаружения>** разрешается в **TRUE**. Если какой-либо из **дочерних< элементов условий>** разрешается в **FALSE**, то **<элемент обнаружения>** разрешается в **FALSE**.

Кроме того, результаты каждого **<раздела обнаружения>** в элементе **<role>** объединяются оператором **OR** для формирования правила обнаружения родительского элемента. То есть, если один из **<разделов обнаружения>** разрешается в **TRUE**, то **<обрабатывается элемент role>** . В противном **<случае элемент role>** не обрабатывается.

<Используйте элемент обнаружения> в элементе **<namedElements>**, чтобы не записывать данные в компоненте. Затем добавьте раздел **обнаружения> соответствия<** в **<элемент роли>**, чтобы определить, переносится ли компонент. Если для компонента нет **<раздела обнаружения>** , USMT предполагает наличие компонента.

- **Количество вхождений:** Неограниченный.
- **Родительские элементы:**<role>, <namedElements>
- **Дочерние элементы:**<условия>

Синтаксис:

XML

```
<detection name="ID" context="User|System|UserAndSystem">
</detection>
```

Развернуть таблицу

Параметр	Обязательно?	Значение
name	• Да, при **объявлении<обнаружения>** в **именованныхЭлементах<>** • Необязательный параметр при объявлении в **роли<>**	При объявлении содержимое **<элемента обнаружения>** игнорируется, а содержимое **<элемента обнаружения>** с тем же именем, которое объявлено в элементе **<namedElements>** , оценивается.
контекст	Нет, по умолчанию = UserAndSystem	Определяет область этого параметра: следует ли обрабатывать этот компонент в контексте конкретного пользователя, во всей операционной системе или в обоих случаях. • **Пользователь**: вычисляет компонент для каждого пользователя. • **Система**. Оценивает компонент только один раз для системы. • **UserAndSystem**: оценивает компонент для всей операционной системы и каждого пользователя.

Пример:

XML

```
<detection name="AdobePhotoshopCS">
   <conditions>

<condition>MigXmlHelper.DoesObjectExist("Registry","HKCU\Software\Adobe\Phot
oshop\8.0")</condition>

<condition>MigXmlHelper.DoesFileVersionMatch("%PhotoshopSuite8Path%\Photosho
p.exe","FileVersion","8.*")</condition>
   </conditions>
</detection>
```

и

XML

```
<role role="Settings">
   <detection>
      <conditions>

<condition>MigXmlHelper.DoesFileVersionMatch("%QuickTime5Exe%","ProductVersi
on","QuickTime 5.*")</condition>

<condition>MigXmlHelper.DoesFileVersionMatch("%QuickTime5Exe%","ProductVersi
on","QuickTime 6.*")</condition>
      </conditions>
   </detection>
```

<displayName>

Элемент **<displayName>** является обязательным полем в каждом **<элементе компонента>** .

- **Количество вхождений:** один раз для каждого компонента
- **Родительские элементы:** <component>
- **Дочерние элементы:** none

Синтаксис:

XML

```
<displayName _locID="ID">ComponentName</displayName>
```

Развернуть таблицу

Параметр	Обязательно?	Значение
locID	Нет	Этот параметр предназначен для внутреннего использования USMT. Не используйте этот параметр.
Имя компонента	Да	Имя компонента.

Пример:

XML

```
<displayName>Command Prompt settings</displayName>
```

<окружающая среда>

Элемент **<среды>** — это контейнер для **<переменных>** элементов, в котором переменные могут быть определены для использования в **файле.xml** . Все переменные среды, определенные таким образом, являются закрытыми. То есть они доступны только для своих дочерних компонентов и компонента, в котором они были определены. Два примера сценариев см. в разделе Примеры.

- **Число вхождений:** не ограничено
- **Родительские элементы:**<role>, <component>, <namedElements>
- **Обязательные дочерние элементы:**<переменная>
- **Необязательные дочерние элементы:**<conditions>

Синтаксис:

XML

```
<environment name="ID" context="User|System|UserAndSystem">
</environment>
```

Развернуть таблицу

Параметр	Обязательно?	Значение
name	Да, если **<среда>** является дочерним элементом **<объекта namedElements>** Нет, если **<среда>** является дочерним **<элементом роли>** или **<компонента>**	При объявлении в качестве дочернего **<элемента роли>** или **<компонента>** , если объявлен *идентификатор* , USMT игнорирует содержимое **<элемента среды>** и обрабатывается содержимое **<элемента среды>** с тем же именем, объявленным в **<элементе nameElements>** .
контекст	Нет (по умолчанию = UserAndSystem)	Определяет область этого параметра: следует ли обрабатывать этот компонент в контексте конкретного пользователя, во всей операционной системе или в обоих случаях. Наибольший возможный область задается элементом **<компонента>**. Например, если **<элемент компонента>** имеет контекст **User** , а **<элемент rules>** имеет контекст **UserAndSystem**, то **<элемент rules>** будет действовать так, как если бы он имел контекст **User**. Если бы элемент **rules> имел контекст System, он действовал бы так, как будто правил там< нет.><**

Параметр	Обязательно?	Значение
		• **Пользователь**: вычисляет переменные для каждого пользователя. • **Система**. Оценивает переменные только один раз для системы. • **UserAndSystem**: вычисляет переменные для всей операционной системы и каждого пользователя.

Примеры:

Пример сценария 1

В этом сценарии создайте расположение объектов во время выполнения в зависимости от конфигурации конечного компьютера. Например, если приложение записывает данные в каталог, в котором установлено приложение, и пользователи могут установить приложение в любом месте компьютера. Если приложение записывает значение `hklm\software\companyname\install [path\]` реестра, а затем обновляет это значение с указанием расположения, в котором установлено приложение, то единственный способ правильно перенести необходимые данные — определить переменную среды. Пример:

XML

```
<environment>
   <variable name="INSTALLPATH">

<script>MigXmlHelper.GetStringContent("Registry","\software\companyname\inst
all [path]")</script>
   </variable>
</environment>
```

Затем правило включения можно использовать следующим образом. Для выполнения аналогичных задач можно использовать любую из функций скрипта>.
<

XML

```
<include>
   <objectSet>
      <pattern type="File">%INSTALLPATH%\ [*.xyz]</pattern>
```

```
   </objectSet>
</include>
```

Во-вторых, значения реестра можно отфильтровать, чтобы они содержали необходимые данные. В следующем примере первая строка (перед разделителем "`,`") извлекается из значения реестра `Hklm\software\companyname\application\ [Path\]`.

XML

```
<environment>
   <variable name="APPPATH">
        <objectSet>
           <content filter='MigXmlHelper.ExtractDirectory (",", "1")'>
             <objectSet>
                <pattern
type="Registry">Hklm\software\companyname\application\ [Path]</pattern>
              </objectSet>
            </content>
        </objectSet>
    </variable>
</environment>
```

Пример сценария 2

В этом сценарии пять файлов с именем `File1.txt`, `File2.txt` и т. д. необходимо перенести из `%SYSTEMDRIVE%\data\userdata\dir1\dir2\`. Чтобы перенести эти файлы, в файле **.xml** должно быть следующее **<правило включения>**:

XML

```
<include>
   <objectSet>
      <pattern type="File">%SYSTEMDRIVE%\data\userdata\dir1\dir2 [File1.txt]
</pattern>
      <pattern type="File">%SYSTEMDRIVE%\data\userdata\dir1\dir2 [File2.txt]
</pattern>
      <pattern type="File">%SYSTEMDRIVE%\data\userdata\dir1\dir2 [File3.txt]
</pattern>
      <pattern type="File">%SYSTEMDRIVE%\data\userdata\dir1\dir2 [File4.txt]
</pattern>
      <pattern type="File">%SYSTEMDRIVE%\data\userdata\dir1\dir2 [File5.txt]
</pattern>
   </objectSet>
</include>
```

Вместо того чтобы вводить путь пять раз, создайте переменную для расположения следующим образом:

XML

```
<environment>
   <variable name="DATAPATH">
      <text>%SYSTEMDRIVE%\data\userdata\dir1\dir2 </text>
      </variable>
</environment>
```

Затем укажите переменную в правиле **<включения>** следующим образом:

XML

```
<include>
   <objectSet>
      <pattern type="File">%DATAPATH% [File1.txt]</pattern>
      <pattern type="File">%DATAPATH% [File2.txt]</pattern>
      <pattern type="File">%DATAPATH% [File3.txt]</pattern>
      <pattern type="File">%DATAPATH% [File4.txt]</pattern>
      <pattern type="File">%DATAPATH% [File5.txt]</pattern>
   </objectSet>
</include>
```

<exclude>

Элемент **<exclude>** определяет, какие объекты не переносятся, если нет более конкретного **<элемента include>** , который переносит объект. Если для одного и того же объекта есть **<элемент include>** и **<exclude>** , объект включается. Для каждого **<элемента exclude>** может быть несколько дочерних **<элементов objectSet>** .

- **Количество вхождений:** Неограниченный
- **Родительские элементы:** <правила>
- **Дочерние элементы:** <objectSet>
- **Вспомогательные функции:** С этим элементом можно использовать следующие <функции фильтра exclude>: `CompareStringContent`, `IgnoreIrrelevantLinks`, `AnswerNo`, `NeverRestore` и `SameRegContent`.

Синтаксис:

XML

```
<exclude filter="ScriptInvocation">
</exclude>
```

Развернуть таблицу

Параметр	Обязательно?	Значение
filter	Нет (по умолчанию = Нет)	Скрипт, за которым следует любое количество строковых аргументов, разделенных запятой и заключенных в круглые скобки. Например, `MyScripts.AScript ("Arg1","Arg2")`. Скрипт вызывается для каждого объекта, который перечисляется наборами объектов в правиле включения. Скрипт фильтра возвращает логическое значение. Если возвращаемое значение равно **TRUE**, объект переносится. Если имеет значение **FALSE**, он не переносится.

Например, из `MigUser.xml` файла:

XML

```
<exclude>
   <objectSet>
      <pattern type="File">%CSIDL_MYMUSIC%\* [*]</pattern>
      <pattern type="File">%CSIDL_MYPICTURES%\* [*]</pattern>
      <pattern type="File">%CSIDL_MYVIDEO%\* [*]</pattern>
   </objectSet>
</exclude>
```

<excludeAttributes>

Элемент **<excludeAttributes>** можно использовать, чтобы определить, какие параметры, связанные с объектом, не переносятся. При наличии конфликтов между элементами **<includeAttributes>** и **<excludeAttributes>** наиболее конкретный шаблон определяет шаблоны, которые не переносятся. Если у объекта нет **<элемента includeAttributes>** или **<excludeAttributes>** , переносятся все его параметры.

- **Количество вхождений:** Неограниченный
- **Родительские элементы:** <правила>
- **Дочерние элементы:** <objectSet>

Синтаксис:

XML

```
<excludeAttributes attributes="Security|TimeFields|Security,TimeFields">
</excludeAttributes>
```

Развернуть таблицу

Параметр	Обязательно?	Значение
Атрибуты	Да	Указывает атрибуты, которые необходимо исключить. Можно указать один из следующих вариантов или оба варианта. При указании обоих значений они должны быть разделены кавычками. Например, `"Security","TimeFields"`: • Безопасность может быть владельцем, группой, DACL или SACL. • TimeFields может быть одним из элементов CreationTime, LastAccessTime и LastWrittenTime.

Пример.

XML

```
<migration urlid="http://www.microsoft.com/migration/1.0/migxmlext/miguser">
<!-- This component migrates the files in the Video folder -->
   <component type="System" context="System">
      <displayName>System Data</displayName>
         <role role="Data">
            <rules>
<!-- Include all of the text files, which are immediately in the drive where
the operating system is installed -->
               <include>
                  <objectSet>
                     <pattern type="File">%SYSTEMDRIVE%\ [*.txt]</pattern>
                  </objectSet>
               </include>
<!-- Exclude the time stamps from the text file starting with the letter a -
->
               <excludeAttributes attributes="TimeFields">
                  <objectSet>
                     <pattern type="File">%SYSTEMDRIVE%\ [a*.txt]</pattern>
                  </objectSet>
               </excludeAttributes>
<!-- include the time stamps from the text file aa.txt -->
               <includeAttributes attributes="TimeFields">
                  <objectSet>
                     <pattern type="File">%SYSTEMDRIVE%\ [aa.txt]</pattern>
                  </objectSet>
               </includeAttributes>
<!-- Logoff the user after LoadState successfully completed. -->
```

```
                <externalProcess when="post-apply">
                   <commandLine>
                      logoff
                   </commandLine>
                </externalProcess>
             </rules>
   </role>
<!-- Migrate
   all doc files from the system
   all power point files
   all visio design files
   all my c++ program files -->
   <extensions>
      <extension>DOC</extension>
      <extension>PPT</extension>
      <extension>VXD</extension>
      <extension>PST</extension>
      <extension>CPP</extension>
   </extensions>
</component>
</migration>
```

<Расширения>

Элемент <extensions> — это контейнер для одного или нескольких <элементов расширения> .

- **Количество вхождений:** ноль или одно
- **Родительские элементы:**<component>
- **Обязательные дочерние элементы:**<extension>

Синтаксис:

XML

```
<extensions>
</extensions>
```

<расширение>

Элемент <extension> можно использовать для указания документов определенного расширения.

- **Число вхождений:** не ограничено

- **Родительские элементы:** <расширения>
- **Дочерние элементы:** none

Синтаксис:

```
XML

<extension>FilenameExtension</extension>
```

Развернуть таблицу

Параметр	Обязательно?	Значение
FilenameExtension	Да	Расширение имени файла.

Например, чтобы перенести все файлы *.doc с исходного компьютера, указав следующий код в элементе **<компонента>** :

```
XML

<extensions>
        <extension>doc</extension>
<extensions>
```

аналогично указанию следующего кода под элементом **<rules>** :

```
XML

<include>
        <objectSet>
                <script>MigXmlHelper.GenerateDrivePatterns ("* [*.doc]",
"Fixed")</script>
        </objectSet>
</include>
```

Еще один пример использования <элемента расширения> см. в примере для <excludeAttributes>.

<externalProcess>

Элемент <externalProcess> можно использовать для запуска командной строки во время процесса миграции. Например, после завершения процесса **LoadState** может потребоваться выполнить команду.

- **Количество вхождений:** Неограниченный
- **Родительские элементы:**<правила>
- **Обязательные дочерние элементы:**<commandLine>

Синтаксис:

```
XML
<externalProcess when="pre-scan|scan-success|post-scan|pre-apply|apply-success|post-apply">
</externalProcess>
```

Развернуть таблицу

Параметр	Обязательно?	Значение
когда	Да	Указывает, когда следует запустить командную строку. Это значение может быть одним из следующих значений: • **предварительная проверка** перед началом процесса сканирования. • **Проверка успешно** завершена после успешного завершения процесса сканирования. • **после завершения** сканирования, независимо от того, успешно ли это было выполнено. • **предварительно примените перед** началом процесса применения. • **успешное применение** после успешного завершения процесса применения. • **после применения** после завершения процесса применения, независимо от того, был ли он успешным или нет.

Пример использования <элемента externalProcess> см. в примере для <excludeAttributes>.

<icon>

Этот элемент является внутренним элементом USMT. Не используйте этот элемент.

<include>

Элемент **<include>** определяет, что следует перенести, если нет более конкретного <правила исключения> . Можно указать скрипт, чтобы он был более конкретным, чтобы расширить определение того, что требуется собрать. Для каждого **<элемента include>** может быть несколько **<элементов objectSet>** .

- **Количество вхождений:** Неограниченный
- **Родительские элементы:**<правила>
- **Обязательный дочерний элемент:**<objectSet>
- **Вспомогательные функции:** С этим элементом можно использовать следующие <> функции фильтра: `CompareStringContent`, `IgnoreIrrelevantLinks`, `AnswerNo`, и `NeverRestore`.

Синтаксис:

XML

```xml
<include filter="ScriptInvocation">
</include>
```

Развернуть таблицу

Параметр	Обязательно?	Значение
filter	Нет. Если этот параметр не указан, обрабатываются все шаблоны, которые находятся внутри дочернего **<элемента objectSet>** .	Скрипт, за которым следует любое количество строковых аргументов, разделенных запятой и заключенных в круглые скобки. Например, `MyScripts.AScript ("Arg1","Arg2")`. Скрипт вызывается для каждого объекта, который перечисляется наборами объектов в правиле **<включения>** . Скрипт фильтра возвращает логическое значение. Если возвращаемое значение равно **TRUE**, объект переносится. Если имеет значение **FALSE**, он не переносится.

Следующий пример из `MigUser.xml` файла:

XML

```xml
<component type="Documents" context="User">
   <displayName _locID="miguser.myvideo">My Video</displayName>
      <paths>
         <path type="File">%CSIDL_MYVIDEO%</path>
      </paths>
```

```
      <role role="Data">
         <detects>
            <detect>

<condition>MigXmlHelper.DoesObjectExist("File","%CSIDL_MYVIDEO%")
</condition>
            </detect>
         </detects>
         <rules>
               <include filter='MigXmlHelper.IgnoreIrrelevantLinks()'>
                  <objectSet>
                     <pattern type="File">%CSIDL_MYVIDEO%\* [*]</pattern>
                  </objectSet>
               </include>
               <merge script="MigXmlHelper.DestinationPriority()">
                  <objectSet>
                     <pattern type="File">%CSIDL_MYVIDEO% [desktop.ini]
</pattern>
                  </objectSet>
            </merge>
         </rules>
      </role>
    </component>
```

<включить> и <исключить> функции фильтрации

Следующие функции возвращают логическое значение. Их можно использовать для переноса определенных объектов в зависимости от того, когда выполняются определенные условия.

- **AnswerNo**

  Этот фильтр всегда возвращает **значение FALSE**.

  Синтаксис: `AnswerNo ()`

- **CompareStringContent**

  Синтаксис: `CompareStringContent("StringContent","CompareType")`

Развернуть таблицу

Параметр	Обязательно?	Значение
StringContent	Да	Строка для проверка.
CompareType	Да	Строка. Используйте одно из следующих значений: ○ **Равно** (без учета регистра). Функция возвращает **значение TRUE** , если строковое представление

Параметр	Обязательно?	Значение
		текущего объекта, обрабатываемого подсистемой миграции, идентично `StringContent`. ○ **NULLили любое другое значение**. Функция возвращает **значение TRUE** , если строковое представление текущего объекта, обрабатываемого подсистемой миграции, не соответствует `StringContent`.

- **IgnoreIrrelevantLinks**

  Этот фильтр отображает **файлы .lnk** , указывающие на недопустимый объект на конечном компьютере. Проверка выполняется на конечном компьютере, поэтому все **.lnk** файлы сохраняются в хранилище во время **ScanState**. Затем они отображаются при запуске средства **LoadState** .

  Синтаксис: `IgnoreIrrelevantLinks ()`

  Пример:

  XML

```
<include filter='MigXmlHelper.IgnoreIrrelevantLinks()'>
     <objectSet>
          <pattern type="File">%CSIDL_COMMON_VIDEO%\* [*]</pattern>
     </objectSet>
</include>
```

- **NeverRestore**

  Эту функцию можно использовать для сбора указанных объектов с исходного компьютера, но затем не переносить объекты на конечный компьютер. При запуске с помощью средства **ScanState** эта функция принимает значение **TRUE**. При запуске с помощью средства **LoadState** эта функция принимает значение **FALSE**. Эта функция может использоваться для проверка значения объекта на конечном компьютере, но перенос объекта в целевой объект не имеет намерения.

  Синтаксис: `NeverRestore()`

  В следующем примере HKCU\панель управления\International [locale] включен в хранилище, но не переносится на конечный компьютер:

  XML

```
<include filter="MigXmlHelper.NeverRestore()">
   <objectSet>
      <pattern type="Registry">HKCU\Control Panel\International
[Locale]</pattern>
   </objectSet>
</include>
```

<includeAttributes>

Элемент **<includeAttributes>** можно использовать для определения того, переносятся ли определенные параметры, связанные с объектом, вместе с самим объектом. При наличии конфликтов между элементами **<includeAttributes>** и **<excludeAttributes>** наиболее конкретный шаблон определяет, какие параметры переносятся. Если у объекта нет **<элемента includeAttributes>** или **<excludeAttributes>** , переносятся все его параметры.

- **Число вхождений:** не ограничено
- **Родительские элементы:** <правила>
- **Дочерние элементы:** <objectSet>

Синтаксис:

XML

```
<includeAttributes attributes="Security|TimeFields|Security,TimeFields">
</includeAttributes>
```

Развернуть таблицу

Параметр	Обязательно?	Значение

Атрибуты	Да	Указывает атрибуты, которые будут включены в перенесенный объект. Можно указать один из следующих вариантов или оба варианта. При указании обоих значений они должны быть разделены кавычками. Например, `"Security","TimeFields"`:
		• Безопасность может иметь одно из следующих значений:
		  ◦ **Владелец**: владелец объекта (SID).
		  ◦ **Группа**: основная группа для объекта (SID).
		  ◦ **DACL** (дискреционный список управления доступом). Список управления доступом, контролируемый владельцем объекта и указывающий, какой доступ к

Параметр	Обязательно?	Значение
		объекту могут иметь определенные пользователи или группы. ○ **SACL** (список управления доступом системы). Список ACL, который управляет созданием сообщений аудита для попыток доступа к защищаемому объекту. Возможность получения или задания SACL объекта контролируется привилегией, обычно предоставляемой только системными администраторами. • TimeFields может иметь одно из следующих значений: ○ **CreationTime**: указывает, когда был создан файл или каталог. ○ **LastAccessTime**: указывает, когда файл в последний раз считывается, записывается в или для исполняемых файлов выполняется. ○ **LastWrittenTime**: указывает, когда файл записывается в последний раз, усечен или перезаписан.

Пример использования **<элемента includeAttributes>** см. в примере для< excludeAttributes>.

<библиотека>

Этот элемент является внутренним элементом USMT. Не используйте этот элемент.

<местоположение>

Элемент **<location>** определяет расположение **<элемента объекта>** .

- **Количество вхождений:** один раз для каждого **<объекта>**
- **Родительские элементы:**<object>
- **Дочерние элементы:**<script>

Синтаксис:

XML

```
<location type="typeID">ObjectLocation</location>
```

Развернуть таблицу

Параметр	Обязательно?	Значение
type	Да	*TypeID* может быть реестром или файлом.
Объектолокация	Да	Расположение объекта.

Следующий пример из `MigApp.xml` файла:

XML

```
<addObjects>
   <object>
      <location
type="Registry">%HklmWowSoftware%\Microsoft\Office\16.0\Common\Migration\Off
ice [UpgradeVersion]</location>
      <attributes>DWORD</attributes>
      <bytes>0B000000</bytes>
   </object>
   <object>
      <location
type="Registry">%HklmWowSoftware%\Microsoft\Office\16.0\Common\Migration\Off
ice [Lang]</location>
      <attributes>DWORD</attributes>
      <bytes>00000000</bytes>
   </object>
</addObjects>
```

<locationModify>

Элемент **<locationModify>** можно использовать для изменения расположения и имени объекта перед переносом объекта на целевой компьютер. Элемент **<locationModify>** обрабатывается только при запуске средства **LoadState** на конечном компьютере. Другими словами, этот элемент игнорируется средством **ScanState** . Элемент **<locationModify>** создает соответствующую папку на конечном компьютере, если он еще не существует.

Количество вхождений: Неограниченный

- **Родительские элементы:** <правила>
- **Обязательный дочерний элемент:** <objectSet>
- **Вспомогательные функции:** С этим элементом можно использовать следующие <функции locationModify>: `ExactMove`, `RelativeMove` и `Move`.

Синтаксис:

XML

```
<locationModify script="ScriptInvocation">
</locationModify>
```

Развернуть таблицу

Параметр	Обязательно?	Значение
сценарий	Да	Скрипт, за которым следует любое количество строковых аргументов, разделенных запятой и заключенных в круглые скобки. Например, `MyScripts.AScript ("Arg1","Arg2")`. Скрипт вызывается для каждого объекта, который перечисляется наборами объектов в правиле включения. Скрипт фильтра возвращает логическое значение. Если возвращаемое значение равно **TRUE**, объект переносится. Если имеет значение **FALSE**, он не переносится.

Следующий пример из `MigApp.xml` файла:

XML

```
<locationModify
script="MigXmlHelper.RelativeMove('%CSIDL_APPDATA%\Microsoft\Office','%CSIDL
_APPDATA%')">
   <objectSet>
      <pattern type="File">%CSIDL_APPDATA%\Microsoft\Office\ [Access10.pip]
</pattern>
   </objectSet>
</locationModify>
```

<Функции locationModify>

Следующие функции изменяют расположение объектов при их переносе **<при использовании элемента locationModify>** . Эти функции вызываются для каждого объекта, перечисляемого родительским **<элементом objectSet>** . Элемент **<locationModify>** создает соответствующую папку на конечном компьютере, если он еще не существует.

- **ExactMove**

  Функция ExactMove перемещает все объекты, соответствующие родительскому **<элементу objectSet>** , в заданное *объект ObjectEncodedLocation*. Эту функцию можно использовать для перемещения

одного файла в другое расположение на конечном компьютере. Если конечным расположением является узел, все соответствующие исходные объекты записываются в узел без подкаталогов. Если целевое расположение является конечным, подсистема миграции переносит все соответствующие исходные объекты в одно и то же расположение. Если возникает конфликт, применяются обычные алгоритмы.

Синтаксис: `ExactMove(ObjectEncodedLocation)`

Развернуть таблицу

Параметр	Обязательно?	Значение
ObjectEncodedLocation	Да	Целевое расположение для всех исходных объектов.

Пример:

XML

```
<locationModify script="MigXmlHelper.ExactMove('HKCU\Keyboard
Layout\Toggle [HotKey]')">
   <objectSet>
        <pattern type="Registry">HKCU\Keyboard Layout\Toggle []
</pattern>
   </objectSet>
</locationModify>
```

- **Двигаться**

  Функция Переместить перемещает объекты в другое расположение на конечном компьютере. Кроме того, эта функция создает подкаталоги, которые были выше самого длинного CSIDL в имени исходного объекта.

  Синтаксис: `Move(DestinationRoot)`

  Развернуть таблицу

Параметр	Обязательно?	Значение
DestinationRoot	Да	Расположение, в котором перемещаются исходные объекты. При необходимости эта функция создает все подкаталоги, которые были выше самого длинного CSIDL в имени исходного объекта.

- **RelativeMove**

Функцию RelativeMove можно использовать для сбора и перемещения данных. Переменные среды можно использовать в исходных и целевых корнях, но они могут быть определены по-разному на исходном и целевом компьютерах.

Синтаксис: `RelativeMove(SourceRoot,DestinationRoot)`

Развернуть таблицу

Параметр	Обязательно?	Значение
SourceRoot	Да	Расположение, из которого перемещаются объекты. Все исходные объекты, перечисляемые родительским **<элементом objectSet>** , которые не находятся в этом расположении, не перемещаются.
DestinationRoot	Да	Расположение, куда перемещаются исходные объекты на конечном компьютере. При необходимости эта функция создает все подкаталоги, которые были выше *SourceRoot*.

Пример:

XML

```
<include>
   <objectSet>
      <pattern type="File">%CSIDL_COMMON_FAVORITES%\* [*]</pattern>
   <objectSet>
</include>
<locationModify
script="MigXmlHelper.RelativeMove('%CSIDL_COMMON_FAVORITES%','%CSIDL_COMMON_
FAVORITES%')">
     <objectSet>
          <pattern type="File">%CSIDL_COMMON_FAVORITES%\* [*]</pattern>
     </objectSet>
</locationModify>
```

<_locDefinition>

Этот элемент является внутренним элементом USMT. Не используйте этот элемент.

<изготовитель>

Элемент <**manufacturer**> определяет производителя компонента, но не влияет на миграцию.

- **Количество вхождений:** ноль или одно
- **Родительские элементы:**<component>
- **Дочерние элементы:** none

Синтаксис:

```xml
<manufacturer>Name</manufacturer>
```

Развернуть таблицу

Параметр	Обязательно?	Значение
Имя	Да	Имя производителя компонента.

<сливать>

Элемент <**merge**> определяет, что происходит при столкновении. Конфликт возникает, когда переносимый объект уже присутствует на конечном компьютере. Если этот элемент не указан, по умолчанию для реестра исходный объект перезаписывает целевой объект. Поведение по умолчанию для файлов — переименование исходного файла в `OriginalFileName(1).OriginalExtension`. Этот элемент указывает только то, что следует сделать при возникновении конфликта. Он не включает объекты. Поэтому для миграции <**объектов необходимо указать правила включения**> вместе с элементом <**merge**> . При обработке объекта и обнаружении конфликта USMT выбирает наиболее конкретное правило слияния. Затем он применяет правило для разрешения конфликта. Например, если <**для правила слияния**> **задано** значение <**sourcePriority**>, а <**для правила слияния**> — <**destinationPriority**>, USMT будет использовать <**правило destinationPriority**>, так как оно является более конкретным.`C:\subfolder\* [*] C:\* [*]`

Пример этого элемента см. в разделе Конфликты и приоритет.

- **Количество вхождений:** Неограниченный
- **Родительские элементы:**<правила>
- **Обязательный дочерний элемент:**<objectSet>

- **Вспомогательные функции:** С этим элементом можно использовать следующие <функции слияния>: `SourcePriority`, , `DestinationPriority`, `FindFilePlaceByPattern` `LeafPattern`, `NewestVersion`, `HigherValue()` и `LowerValue()`.

Синтаксис:

XML

```
<merge script="ScriptInvocation">
</merge>
```

Развернуть таблицу

Параметр	Обязательно?	Значение
сценарий	Да	Скрипт, за которым следует любое количество строковых аргументов, разделенных запятой и заключенных в круглые скобки. Например, `MyScripts.AScript ("Arg1","Arg2")`. Скрипт вызывается для каждого объекта, который перечисляется наборами объектов в правиле **<включения>** . Скрипт фильтра возвращает логическое значение. Если возвращаемое значение равно **TRUE**, объект переносится. Если имеет значение **FALSE**, он не переносится.

Следующий пример из `MigUser.xml` файла:

XML

```
<rules>
   <include filter='MigXmlHelper.IgnoreIrrelevantLinks()'>
      <objectSet>
         <pattern type="File">%CSIDL_MYVIDEO%\* [*]</pattern>
      </objectSet>
   </include>
   <merge script="MigXmlHelper.DestinationPriority()">
      <objectSet>
         <pattern type="File">%CSIDL_MYVIDEO% [desktop.ini]</pattern>
      </objectSet>
   </merge>
</rules>
```

<Функции слияния>

Эти функции управляют разрешением конфликтов.

- **DestinationPriority**

  Указывает, что объект, который находится на конечном компьютере, не переносится с исходного компьютера.

  Пример:

  ```
  XML
  ```

  ```xml
  <merge script="MigXmlHelper.DestinationPriority()">
       <objectSet>
            <pattern
  type="Registry">HKCU\Software\Microsoft\Office\16.0\PhotoDraw\
  [MyPictures]</pattern>
            <pattern
  type="Registry">HKCU\Software\Microsoft\Office\16.0\PhotoDraw\Settings\
  [PicturesPath]</pattern>
            <pattern
  type="Registry">HKCU\Software\Microsoft\Office\16.0\PhotoDraw\Settings\
  [AdditionalPlugInPath]</pattern>
       </objectSet>
  </merge>
  ```

- **FindFilePlaceByPattern**

  Функция FindFilePlaceByPattern сохраняет файлы с добавочным счетчиком при возникновении конфликта. Это строка, которая содержит одну из каждой конструкции: **<F>**, **<E>**, **<N>** в любом порядке.

  Синтаксис: `FindFilePlaceByPattern(FilePattern)`

  Развернуть таблицу

Параметр	Обязательно?	Значение
FilePattern	Да	◦ **<F>** заменяется исходным именем файла. ◦ **<N>** заменяется добавочным счетчиком до тех пор, пока не будет конфликтов с объектами на конечном компьютере. ◦ **<E>** заменяется исходным расширением имени файла. Например, `<F> (<N>).<E>` измените исходный файл `MyDocument.doc` `MyDocument (1).doc` на на целевом компьютере.

- **NewestVersion**

Функция NewestVersion разрешает конфликты на конечном компьютере в зависимости от версии файла.

Синтаксис: `NewestVersion(VersionTag)`

Развернуть таблицу

Параметр	Обязательно?	Значение
VersionTag	Да	Поле версии, которое проверяется. Это поле может быть `FileVersion` или `ProductVersion`. Файл с наивысшей версией *VersionTag* определяет, какие конфликты разрешаются на основе версии файла. Например, если `Myfile.txt` содержит FileVersion 1 и тот же файл на конечном компьютере содержит FileVersion 2, файл на целевом компьютере остается.

- **HigherValue()**

  Эту функцию можно использовать для объединения значений реестра. Значения реестра оцениваются как числовые, а значения с более высоким значением определяют, какие значения реестра объединяются.

- **LowerValue()**

  Эту функцию можно использовать для объединения значений реестра. Значения реестра оцениваются как числовые значения, а одно с меньшим значением определяет, какие значения реестра объединяются.

- **SourcePriority**

  Указывает для переноса объекта с исходного компьютера и удаления объекта, который находится на конечном компьютере.

  Пример:

```
XML
```

```xml
<merge script="MigXmlHelper.SourcePriority()">
 <objectSet>
   <pattern
type="Registry">%HklmWowSoftware%\Microsoft\Office\14.0\Common\Migratio
n\Publisher [UpgradeVersion]</pattern>
   <pattern
type="Registry">%HklmWowSoftware%\Microsoft\Office\15.0\Common\Migratio
n\Publisher [UpgradeVersion]</pattern>
   <pattern
type="Registry">%HklmWowSoftware%\Microsoft\Office\16.0\Common\Migratio
```

```
n\Publisher [UpgradeVersion]</pattern>
 </objectSet>
</merge>
```

<миграция>

Элемент <**миграции**> является единственным корневым элементом файла **.xml** миграции и является обязательным. Каждый **файл.xml** должен иметь уникальный URL-адрес миграции. URL-идентификатор каждого файла, указанного в командной строке, должен быть уникальным. URL-идентификаторы должны быть уникальными, так как USMT использует urlid для определения компонентов в файле.

- **Количество вхождений:** один
- **Родительские элементы:** none
- **Обязательные дочерние элементы:**<component>
- **Необязательные дочерние элементы:**<library>, <namedElements>

Синтаксис:

XML

```
<migration urlid="*UrlID/*Name">
</migration>
```

Развернуть таблицу

Параметр	Обязательно?	Значение
urlid	Да	*UrlID* — это строковый идентификатор, который однозначно идентифицирует этот **.xml** файл. Этот параметр должен быть без двоеточия, как определено в спецификации пространств имен XML. Каждый **файл.xml** миграции должен иметь уникальный url-идентификатор. Если два файла **миграции.xml** имеют одинаковый urlid, второй **.xml** файл, указанный в командной строке, не обрабатывается. Дополнительные сведения о пространствах имен XML см. в разделе Использование пространств имен XML.
Имя	Нет	Хотя это не обязательно, рекомендуется использовать имя **.xml** файла.

Следующий пример из `MigApp.xml` файла:

XML

```
<migration urlid="http://www.microsoft.com/migration/1.0/migxmlext/migapp">
</migration>
```

MigXMLHelper.FileProperties

Эту вспомогательную функцию фильтра можно использовать для фильтрации миграции файлов по размеру файла и атрибутам даты.

Развернуть таблицу

Вспомогаемая функция	**MigXMLHelper.FileProperties (property, operator, valueToCompare)**
Свойство	filesize, dateCreated, dateModified, dateAccessed
Оператор	range, neq, lte, lt, eq, gte, gt
valueToCompare	Сравниваемое значение. Пример: Дата: "2023/05/15-2020/05/17", "2023/05/15" Размер: число с В, КБ, МБ или ГБ в конце. "5 ГБ", "1 КБ-1 МБ"

XML

```
<component context="System"  type="Application">
<displayName>File_size</displayName>
<role role="Data">

   <rules>
        <include
filter='MigXmlHelper.FileProperties("dateAccessed","range","2023/05/15-
2020/05/17")'>
         <objectSet>
         <pattern type="File">%SYSTEMDRIVE%\DOCS\* [*]</pattern>
         </objectSet>
      </include>
   </rules>
</role>
</component>
```

<namedElements>

Элемент **<namedElements>** можно использовать для определения именованных элементов. Эти элементы можно использовать в любом компоненте **в файле.xml** . Пример использования этого элемента см. в `MigApp.xml` файле .

Синтаксис:

```
XML

<namedElements>
</namedElements>
```

- **Количество вхождений:** Неограниченный
- **Родительские элементы:**<миграция>
- **Дочерние элементы:**<среда>, <правила>, <условия>, <обнаружение>, <обнаружение, обнаружение>, <обнаружение>

Пример этого элемента см. в `MigApp.xml` файле .

<объект>

Элемент **<object>** представляет файл или раздел реестра.

- **Количество вхождений:** Неограниченный
- **Родительские элементы:**<addObjects>
- **Обязательные дочерние элементы:**<location>, <атрибуты>
- **Необязательные дочерние элементы:**<байты>

Синтаксис:

```
XML

<object>
</object>
```

Следующий пример из `MigApp.xml` файла:

```
XML

<addObjects>
   <object>
      <location
```

```
type="Registry">%HklmWowSoftware%\Microsoft\Office\16.0\Common\Migration\Off
ice [UpgradeVersion]</location>
      <attributes>DWORD</attributes>
      <bytes>0B000000</bytes>
   </object>
   <object>
      <location
type="Registry">%HklmWowSoftware%\Microsoft\Office\16.0\Common\Migration\Off
ice [Lang]</location>
      <attributes>DWORD</attributes>
      <bytes>00000000</bytes>
      </object>
</addObjects>
```

<objectSet>

Элемент **<objectSet>** содержит список шаблонов объектов, например пути к файлам, расположения реестра и т. д. Все дочерние **<элементы условий>** оцениваются в первую очередь. Если все **дочерние< элементы условий>** возвращают **значение FALSE**, **<элемент objectSet>** вычисляется как пустой набор. Для каждого родительского элемента может быть только несколько **<элементов objectSet>** .

- **Количество вхождений:** Неограниченный
- **Родительские элементы:**<переменная>, <содержимое>, <include>, <exclude>, <merge>, <contentModify>, <locationModify>, <destinationCleanup>, <includeAttributes>, <excludeAttributes>, <unconditionalExclude>, <detect>
- **Обязательные дочерние**<элементы: скрипт> или <шаблон>
- **Необязательные дочерние элементы:**<содержимое>, <условия>, <условие>

Синтаксис:

XML

```
<objectSet>
</objectSet>
```

Следующий пример из `MigUser.xml` файла:

XML

```
<component type="Documents" context="User">
   <displayName _locID="miguser.mymusic">My Music</displayName>
      <paths>
         <path type="File">%CSIDL_MYMUSIC%</path>
      </paths>
   <role role="Data">
      <detects>
      <detect>
         <condition>MigXmlHelper.DoesObjectExist("File","%CSIDL_MYMUSIC%")
</condition>
      </detect>
   </detects>
   <rules>
      <include filter='MigXmlHelper.IgnoreIrrelevantLinks()'>
         <objectSet>
            <pattern type="File">%CSIDL_MYMUSIC%\* [*]</pattern>
         </objectSet>
      </include>
      <merge script="MigXmlHelper.DestinationPriority()">
         <objectSet>
            <pattern type="File">%CSIDL_MYMUSIC%\ [desktop.ini]</pattern>
         </objectSet>
      </merge>
   </rules>
   </role>
</component>
```

<path>

Этот элемент является внутренним элементом USMT. Не используйте этот элемент.

<Пути>

Этот элемент является внутренним элементом USMT. Не используйте этот элемент.

<шаблон>

Этот элемент можно использовать для указания нескольких объектов. Для каждого **<элемента objectSet>** можно использовать несколько **<элементов шаблона>**, и они объединяются. При указании файлов корпорация Майкрософт рекомендует использовать `GenerateDrivePatterns` вместо этого **со< скриптом>**.

`GenerateDrivePatterns` в основном то же самое, что **<и правило шаблона>** , без спецификации букв диска. Например, следующие две строки кода похожи:

```
XML
```

```
<pattern type="File">C:\Folder\* [Sample.doc]</pattern>
<script>MigXmlHelper.GenerateDrivePatterns("\Folder\* [Sample.doc]","Fixed"
</script>
```

- **Количество вхождений:** Неограниченный
- **Родительские элементы:** <objectSet>
- **Дочерние элементы:** только *Path* [*объект*] должен быть допустимым.

Синтаксис:

XML

```
<pattern type="typeID">Path [object]</pattern>
```

Развернуть таблицу

Параметр	Обязательно?	Значение
type	Да	*typeID* может иметь значение Registry, File или Ini. Если *typeId* имеет значение Ini, пробел между *Path* и *объектом* не допускается. Например, следующий формат является правильным, если type="Ini": **<pattern type="Ini">%WinAmp5InstPath%\Winamp.ini|WinAmp[keeponscreen]</pattern>**
Путь [*объект*]	Да	Допустимый шаблон реестра или пути к файлу, за которым следует по крайней мере один пробел, а затем скобки [], содержащие переносимый объект. • *Путь* может содержать подстановочный знак звездочки (`*`) или быть распознаваемыми переменными среды. Вопросительный знак нельзя использовать в качестве подстановочного знака. `HKCU` и `HKLM` можно использовать для ссылки на `HKEY_CURRENT_USER` и `HKEY_LOCAL_MACHINE` соответственно. • *Объект* может содержать подстановочный знак звездочки (`*`). Однако вопросительный знак нельзя использовать в качестве подстановочного знака. Пример **`C:\Folder\ [*]`** перечисляет все файлы в `C:\Folder` , но не содержит вложенных `C:\Folder` папок . **`C:\Folder* [*]`** перечисляет все файлы и вложенные папки .`C:\Folder` **`C:\Folder\ [*.mp3]`** перечисляет все `.mp3` файлы в `C:\Folder`. **`C:\Folder\ [Sample.doc]`** перечисляет только файл, расположенный `Sample.doc` в папке C:\Folder.

Параметр	Обязательно?	Значение
		Примечание При переносе файла с символом квадратной скобки ([или]) в имени файла, символ моркови (^) должен быть вставлен непосредственно перед скобкой, чтобы он был действителен. Например, если есть файл с именем "file].txt", `<pattern type="File">c:\documents\mydocs [file^].txt]</pattern>` его необходимо указать вместо `<pattern type="File">c:\documents\mydocs [file].txt]</pattern>`.

Пример

- Чтобы перенести один раздел реестра, выполните следующие действия:

```
XML

<pattern
type="Registry">HKLM\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\Cache [Persistent]</pattern>
```

- Чтобы перенести папку `C:\EngineeringDrafts` и все вложенные папки с диска C::

```
XML

<pattern type="File">C:\EngineeringDrafts\* [*]</pattern>
```

- Чтобы перенести с диска C: только `C:\EngineeringDrafts` папку, за исключением всех вложенных папок, выполните следующие действия.

  Перенаправка файлов и параметров

- `Sample.doc` Перенос файла из `C:\EngineeringDrafts`:

```
XML

<pattern type="File"> C:\EngineeringDrafts\ [Sample.doc]</pattern>
```

- Чтобы перенести `Sample.doc` файл из места, где он существует на диске C:, используйте шаблон следующим образом. Если на диске C: существует несколько файлов с одинаковыми именами, все эти файлы переносятся.

  XML

  ```
  <pattern type="File"> C:\* [Sample.doc] </pattern>
  ```

- Дополнительные примеры использования этого элемента см. в разделах Исключение файлов и параметров, Перенаправка файлов и параметров, Включение файлов и параметров и Пользовательские примеры XML.

<обработка>

Этот элемент можно использовать для выполнения скрипта в определенной точке процесса миграции. Возвращаемые значения не ожидаются от указанных скриптов. Если есть возвращаемые значения, они игнорируются.

- **Число вхождений:** не ограничено
- **Родительские элементы:** <правила>
- **Обязательный дочерний элемент:** <script>

Синтаксис:

XML

```
<processing when="pre-scan|scan-success|post-scan|pre-apply|apply-
success|post-apply">
</processing>
```

Развернуть таблицу

Параметр	Обязательно?	Значение
когда	Да	Указывает, когда должен выполняться скрипт. Это значение может быть одним из следующих значений: • **Предварительная проверка** означает до начала процесса сканирования. • **Успешное сканирование** означает успешное завершение процесса сканирования. • **post-scan** означает, что после завершения процесса сканирования, независимо от того, был ли он успешным или нет.

Параметр	Обязательно?	Значение
		• **Предварительное применение** означает до начала процесса применения. • **Apply-success** означает, что после успешного завершения процесса применения. • **post-apply** означает, что после завершения процесса применения, независимо от того, был ли он успешным или нет.

<подключаемый модуль>

Этот элемент является внутренним элементом USMT. Не используйте этот элемент.

<роль>

Элемент **<role>** является обязательным в пользовательском **файле.xml** . При указании **<элемента роли>** можно создать конкретный компонент. Компонент определяется параметрами, указанными на **<уровне компонента>** , и ролью, указанной здесь.

- **Количество вхождений:** Каждый **<компонент>** может содержать один, два или три дочерних **<элемента роли>** .
- **Родительские элементы:** <компонент>, <роль>
- **Обязательные дочерние элементы:** <rules>
- **Необязательные дочерние элементы:** <среда>, <обнаружение>, <компонент>, <роль>, <обнаружения>, <подключаемый модуль>

Синтаксис:

XML

```
<role role="Container|Binaries|Settings|Data">
</role>
```

Развернуть таблицу

Параметр	Обязательно?	Значение
роль	Да	Определяет роль для компонента. Роль может быть одной из следующих:

Параметр	Обязательно?	Значение

		• **Контейнер**
		• **Двоичные файлы**
		• **Параметры**
		• **Данные**
		
		Можно указать один из следующих элементов:
		
		1. До трех **<элементов роли>** в **компоненте<>** — один элемент роли Binaries, один элемент роли Settings и один элемент роли Data. Эти параметры не изменяют поведение миграции. Их единственная цель — помочь классифицировать переносимые параметры. Эти **<элементы роли>** могут быть вложенными, но каждый вложенный элемент должен иметь один и тот же параметр роли.
		2. Один элемент **роли> Container<** в **элементе< компонента>**. В этом случае нельзя указать какие-либо дочерние **<элементы правил>** , а только другие **<элементы компонента>** . И каждый дочерний **<элемент компонента>** должен иметь тот же тип, что и у родительского **<элемента компонента>** . Пример:
		
		`<component context="UserAndSystem" type="Application">`
		
		`<displayName _locID="migapp.msoffice2016">Microsoft Office 2016</displayName>`
		
		`<имя среды="GlobalEnv" />`
		
		`<role="Container">`
		
		`<detection name="AnyOffice2016Version" />`
		
		`<detection name="Word2016" />`
		
		`<!--`
		`Общие параметры Office 2016`
		`-->`
		`<component context="UserAndSystem" type="Application">`

Следующий пример из `MigUser.xml` файла. Дополнительные примеры см. в `MigApp.xml` файле:

XML

```
<component type="System" context="User">
   <displayName _locID="miguser.startmenu">Start Menu</displayName>
   <paths>
      <path type="File">%CSIDL_STARTMENU%</path>
   </paths>
   <role role="Settings">
      <detects>
         <detect>

<condition>MigXmlHelper.DoesObjectExist("File","%CSIDL_STARTMENU%")
</condition>
         </detect>
      </detects>
   <rules>
      <include filter='MigXmlHelper.IgnoreIrrelevantLinks()'>
         <objectSet>
            <pattern type="File">%CSIDL_STARTMENU%\* [*]</pattern>
         </objectSet>
      </include>
      <merge script="MigXmlHelper.DestinationPriority()">
         <objectSet>
            <pattern type="File">%CSIDL_STARTMENU% [desktop.ini]</pattern>
            <pattern type="File">%CSIDL_STARTMENU%\* [*]</pattern>
         </objectSet>
      </merge>
   </rules>
   </role>
</component>
```

<правила>

Элемент **<rules>** является обязательным в пользовательском **файле.xml** . Этот элемент содержит правила, которые выполняются во время миграции, если выбран родительский **<элемент компонента>** , если дочерний **<элемент условий>** (если он имеется) не будет иметь значение **FALSE**. Для каждого **<элемента rules>** может быть несколько дочерних **<элементов правил>** .

- **Число вхождений:** не ограничено
- **Родительские элементы:**<role>, <rules>, <namedElements>
- **Обязательные дочерние элементы:**<include>

- **Необязательные дочерние элементы:** <rules>, <exclude>, <unconditionalExclude>, <merge>, <contentModify>, <locationModify>, <destinationCleanup>, <addObjects>, <externalProcess>, <processing>, <includeAttributes>, <excludeAttributes>, условия, <обнаружения>

Синтаксис:

```xml
<rules name="ID" context="User|System|UserAndSystem">
</rules>
```

Развернуть таблицу

Параметр	Обязательно?	Значение
name	Да, если **<правила>** являются дочерними для **<именованныхЭлементов>** Нет, если **<правила>** являются дочерними для любого другого элемента	Если указан *идентификатор* , все дочерние элементы не обрабатываются. Вместо этого обрабатываются все другие **<элементы правил>** с тем же именем, объявленные в **<nameElements>** .
контекст	Нет (по умолчанию = UserAndSystem)	Определяет область этого параметра: следует ли обрабатывать этот компонент в контексте конкретного пользователя, во всей операционной системе или в обоих случаях. Наибольший возможный область задается элементом компонента. Например, если **<элемент компонента>** имеет контекст **User** , а **<элемент rules>** имеет контекст **UserAndSystem**, элемент **<rules>** будет действовать так, как будто он имеет контекст **User**. Если **<бы правила>** имели контекст **System**, он действовал бы так, как будто **<правил>** не было. • **Пользователь**: вычисляет переменные для каждого пользователя. • **Система**. Оценивает переменные только один раз для системы. • **UserAndSystem**: вычисляет переменные для всей операционной системы и каждого пользователя.

Следующий пример из `MigUser.xml` файла:

XML

```
<component type="Documents" context="User">
   <displayName _locID="miguser.mymusic">My Music</displayName>
      <paths>
         <path type="File">%CSIDL_MYMUSIC%</path>
      </paths>
   <role role="Data">
      <detects>
      <detect>
         <condition>MigXmlHelper.DoesObjectExist("File","%CSIDL_MYMUSIC%")
</condition>
      </detect>
   </detects>
   <rules>
      <include filter='MigXmlHelper.IgnoreIrrelevantLinks()'>
         <objectSet>
            <pattern type="File">%CSIDL_MYMUSIC%\* [*]</pattern>
         </objectSet>
      </include>
      <merge script="MigXmlHelper.DestinationPriority()">
         <objectSet>
            <pattern type="File">%CSIDL_MYMUSIC%\ [desktop.ini]</pattern>
         </objectSet>
      </merge>
   </rules>
   </role>
</component>
```

<сценарий>

Возвращаемое значение, необходимое **для скрипта<>**, зависит от родительского элемента.

Количество вхождений: Один раз для <переменной>, неограниченно для <objectSet> и <обработки>

Родительские элементы:<objectSet>, <переменная>, <обработка>

Дочерние элементы: none

Синтаксис и вспомогательные функции:

- Общий синтаксис: `<script>ScriptWithArguments</script>`
- Метод GetStringContent можно использовать, если **<скрипт>** находится в **переменной<>**.

Синтаксис:
`<script>MigXmlHelper.GetStringContent("ObjectType","EncodedLocationPattern", "ExpandContent")</script>`

Пример:
`<script>MigXMLHelper.GetStringContent("Registry","HKLM\Software\MyApp\Installe r [EXEPATH]")</script>`

- GenerateUserPatterns можно использовать, если **<скрипт>** находится в **objectSet<>**.

  Синтаксис:
  `<script>MigXmlHelper.GenerateUserPatterns("ObjectType","EncodedLocationPattern ","ProcessCurrentUser")</script>`

  Пример: `<script>MigXmlHelper.GenerateUserPatterns ("File","%USERPROFILE%\* [*.doc]", "FALSE")</script>`

- GenerateDrivePatterns можно использовать, если **<скрипт>** находится в **<objectSet>**.

  Синтаксис:
  `<script>MigXmlHelper.GenerateDrivePatterns("PatternSegment","DriveType") </script>`

  Пример: `<script>MigXmlHelper.GenerateDrivePatterns("* [sample.doc]", "Fixed") </script>`

- Простые исполняемые скрипты можно использовать с **<элементами скриптов>**, которые находятся в **<элементах обработки>**: AskForLogoff, ConvertToShortFileName, KillExplorer, RemoveEmptyDirectories, RestartExplorer, RegisterFonts, StartService, StopService, SyncSCM.

  Синтаксис: `<script>MigXmlHelper.ExecutingScript</script>`

  Пример: `<script>MigXmlHelper.KillExplorer()</script>`

Развернуть таблицу

Параметр	Обязательно?	Значение
ScriptWithArguments	Да	Скрипт, за которым следует любое количество строковых аргументов, разделенных запятой и заключенных в круглые скобки. Например, `MyScripts.AScript ("Arg1","Arg2")`.

Параметр	Обязательно?	Значение
		Скрипт вызывается для каждого объекта, который перечисляется наборами объектов в правиле **<включения>** . Скрипт фильтра возвращает логическое значение. Если возвращаемое значение равно **TRUE**, объект переносится. Если имеет значение **FALSE**, он не переносится. Возвращаемое значение, необходимое **для скрипта<>**, зависит от родительского элемента. • При использовании в **<переменной>** возвращаемое значение должно быть строковым. • При использовании в **<objectSet>** возвращаемое значение должно быть двумерным массивом строк. • При использовании в **расположении<>** возвращаемое значение должно быть допустимым расположением, которое соответствует атрибуту **<типа location>**. Например, если <location type="File">, дочерний элемент скрипта, если он указан, должен быть допустимым расположением файла. **Примечание** При переносе файла с символом скобки ([или]) в имени файла вставьте символ моркови (^) непосредственно перед скобкой, чтобы он был действителен. Например, если есть файл с именем "file].txt", укажите `<pattern type="File">c:\documents\mydocs[file^].txt]</pattern>` вместо `<pattern type="File">c:\documents\mydocs[file].txt]</pattern>`.

Примеры:

Чтобы перенести файл Sample.doc с любого диска на исходном компьютере, используйте **<сценарий>** , как показано ниже. Если существует несколько файлов с одинаковыми именами, все эти файлы переносятся.

XML

```
<script>MigXmlHelper.GenerateDrivePatterns("* [sample.doc]", "Fixed")
</script>
```

Дополнительные примеры использования этого элемента см. в разделах Исключение файлов и параметров, Перенаправка файлов и параметров и Пользовательские примеры XML.

<функции скрипта>

Следующие функции можно использовать с элементом **<script>** .

- Функции создания строк и шаблонов
- Простое выполнение скриптов

Функции создания строк и шаблонов

Эти функции возвращают строку или шаблон.

- **GetStringContent**

  Метод GetStringContent можно использовать с **<элементами скрипта>** , которые находятся в **<переменных>** элементах. По возможности эта функция возвращает строковое представление заданного объекта. В противном случае возвращается **значение NULL**. Для файлового объекта эта функция всегда возвращает **значение NULL**.

  Синтаксис: `GetStringContent("ObjectType","EncodedLocationPattern", "ExpandContent")`

  Развернуть таблицу

Параметр	Обязательно?	Значение
ObjectType	Да	Тип объекта . Может иметь значение Registry или Ini (для **файла.ini**).
EncodedLocationPattern	Да	◦ Если тип объекта — Registry, encodedLocationPattern должен быть допустимым путем к реестру. Например, `HKLM\SOFTWARE\MyKey[]`. ◦ Если тип объекта — Ini, то encodedLocationPattern должен иметь

Параметр	Обязательно?	Значение
		следующий формат: **IniFilePath|SectionName[SettingName]**
ExpandContent	Нет (default=TRUE)	Может иметь значение **TRUE** или **FALSE**. Если **значение FALSE**, указанное расположение не разворачивается перед возвратом.

Пример

XML

```
<variable name="MSNMessengerInstPath">
<script>MigXmlHelper.GetStringContent("Registry","%HklmWowSoftware%\Mic
rosoft\MSNMessenger [InstallationDirectory]")</script>
</variable>
```

- **GenerateDrivePatterns**

Функция `GenerateDrivePatterns` выполняет итерацию всех доступных дисков и выбирает те, которые соответствуют требуемому типу диска. Затем он объединяет выбранные диски с конечной частью *PatternSegment* , чтобы сформировать полнокодированный шаблон файла. Например, если *PatternSegment* имеет значение `Path [file.txt]` , а *DriveType* — `Fixed`, то функция создает `C:\Path [file.txt]` и другие шаблоны, если есть фиксированные диски, отличные от C:. Переменные среды нельзя указать с помощью этой функции. `GenerateDrivePatterns` может использоваться с **<элементами скрипта>** , которые находятся в <objectSet> и находятся в **<include>/<exclude>**.

Синтаксис: `GenerateDrivePatterns("PatternSegment","DriveType")`

Развернуть таблицу

Параметр	Обязательно?	Значение
PatternSegment	Да	Суффикс закодированного шаблона. Значение объединяется со спецификацией диска, например "c:", чтобы сформировать полный шаблон закодированного файла. Например, "* [*.doc]". *PatternSegment* не может быть переменной среды.
DriveType	Да	Тип диска, для которого должны быть созданы шаблоны. Можно указать один из следующих элементов:

Параметр	Обязательно?	Значение
		◦ Фиксированная ◦ CDROM ◦ Сменный ◦ Удаленный

Пример этого элемента см. в последнем компоненте `MigUser.xml` в файле.

- **GenerateUserPatterns**

  Функция `GenerateUserPatterns` выполняет итерацию по всем пользователям, которые переносятся, за исключением текущего обработанного пользователя, если <**ProcessCurrentUser**> имеет **значение FALSE**, и расширяет указанный шаблон в контексте каждого пользователя. Например, если пользователи A, B и C имеют профили в `C:\Users`, вызывая `GenerateUserPattens('File','%userprofile% [*.doc]','TRUE')`, вспомогательная функция создает следующие три шаблона:

  ◦ "C:\Users\A* [*.doc]"

  ◦ "C:\Users\B* [*.doc]"

  ◦ "C:\Users\C* [*.doc]"

  Синтаксис: `GenerateUserPatterns("ObjectType","EncodedLocationPattern","ProcessCurrentUser")`

  Развернуть таблицу

Параметр	Обязательно?	Значение
ObjectType	Да	Определяет тип объекта. Может быть файлом или реестром.
EncodedLocationPattern	Да	Шаблон расположения. Переменные среды разрешены.
ProcessCurrentUser	Да	Может иметь значение **TRUE** или **FALSE**. Указывает, должны ли быть созданы шаблоны для текущего пользователя.

Пример.

Если `GenerateUserPattens('File','%userprofile% [*.doc]','FALSE')` вызывается, когда USMT обрабатывает пользователя A, то эта функция создает шаблоны только для пользователей B и C. Эту вспомогательную функцию можно использовать для создания сложных правил. Например, чтобы перенести все `.doc` файлы с исходного компьютера, но если пользователь X не перенесен, не переносите файлы `.doc` из профиля пользователя X.

В следующем примере приведен пример кода для этого сценария. Первый **<элемент rules>** переносит все `.doc` файлы на исходном компьютере, за исключением файлов внутри `C:\Users`. Вторые **<элементы правил>** переносятся из всех `.doc` файлов `C:\Users` , `.doc` за исключением файлов в профилях других пользователей. Поскольку второй **<элемент rules>** обрабатывается в каждом контексте перенесенного пользователя, конечным результатом является требуемое поведение. Конечный результат — тот, который мы ожидали.

XML

```
<rules context="System">
  <include>
    <objectSet>
      <script>MigXmlHelper.GenerateDrivePatterns ("* [*.doc]", "Fixed")
</script>
    </objectSet>
  </include>
  <exclude>
    <objectSet>
      <pattern type="File">%ProfilesFolder%\* [*.doc]</pattern>
    </objectSet>
  </exclude>
</rules>
<rules context="User">
  <include>
    <objectSet>
      <pattern type="File">%ProfilesFolder%\* [*.doc]</pattern>
    </objectSet>
  </include>
  <exclude>
    <objectSet>
      <script>MigXmlHelper.GenerateUserPatterns ("File","%userprofile%\*
[*.doc]", "FALSE")</script>
    </objectSet>
  </exclude>
</rules>
```

MigXmlHelper.GenerateDocPatterns

Вспомогающая `MigXmlHelper.GenerateDocPatterns` функция вызывает средство поиска документов для проверки системы на наличие всех файлов, которые можно перенести. Его можно вызвать в контексте **system** или **user** для фокусировки сканирования.

Развернуть таблицу

Параметр	Обязательно?	Значение
ScanProgramFiles	Нет (по умолчанию = FALSE)	Может иметь значение **TRUE** или **FALSE**. Параметр *ScanProgramFiles* определяет, сканирует ли средство поиска документов каталог **Program Files** для сбора зарегистрированных расширений файлов для известных приложений. Например, если задано значение **TRUE** , он обнаруживает и переносит **.jpg** файлы в каталог Photoshop, если `.jpg` это расширение файла, зарегистрированное в Photoshop.
IncludePatterns	Нет (по умолчанию = TRUE)	Может иметь значение **TRUE** или **FALSE**. **Значение TRUE** создает шаблоны включения и может быть добавлено в **<элемент include>** . **FALSE** создает шаблоны исключений и может быть добавлен в **<элемент exclude>** .
SystemDrive	Нет (по умолчанию = FALSE)	Может иметь значение **TRUE** или **FALSE**. Если **задано значение TRUE**, все шаблоны ограничиваются системным диском.

XML

```
 <!-- This component migrates data in user context -->
  <component type="Documents" context="User">
    <displayName>MigDocUser</displayName>
    <role role="Data">
      <rules>
        <include filter='MigXmlHelper.IgnoreIrrelevantLinks()'>
          <objectSet>
            <script>MigXmlHelper.GenerateDocPatterns ("false")</script>
          </objectSet>
        </include>
        <exclude>
          <objectSet>
           <script>MigXmlHelper.GenerateDocPatterns ("false", "false",
"false")</script>
          </objectSet>
        </exclude>
      </rules>
    </role>
  </component>
```

Простое выполнение скриптов

Следующие скрипты не имеют возвращаемого значения. Следующие ошибки можно использовать с **<элементами скрипта>**, которые находятся в **элементах< обработки>**

- **AskForLogoff()**. Запросы пользователя выйти из службы в конце миграции. Пример

  ```
  XML

  <processing when="apply-success">
    <script>MigXmlHelper.AskForLogoff()</script>
  </processing>
  ```

- **ConvertToShortFileName(RegistryEncodedLocation).** Если *RegistryEncodedLocation* — это полный путь к существующему файлу, эта функция преобразует файл в его короткое имя, а затем обновляет значение реестра.

- **KillExplorer()**. Останавливает Explorer.exe для текущего контекста пользователя. Остановка Explorer.exe позволяет получить доступ к определенным ключам и файлам, которые сохраняются открытыми при выполнении Explorer.exe. Пример:

  ```
  XML

  <processing when="pre-apply">
    <script>MigXmlHelper.KillExplorer()</script>
  </processing>
  ```

- **RegisterFonts(FileEncodedLocation).** Регистрирует заданный шрифт или все шрифты в заданном каталоге. Пример

```
XML

<processing when="apply-success">
  <script>MigXmlHelper.RegisterFonts("%CSIDL_COMMON_FONTS%")</script>
</processing>
```

- **RemoveEmptyDirectories (DirectoryEncodedPattern).** Удаляет все пустые каталоги, соответствующие *DirectoryEncodedPattern* на конечном компьютере.

- **RestartExplorer().** Перезапускает Explorer.exe в конце миграции. Пример:

```xml
<processing when="post-apply">
  <script>MigXmlHelper.RestartExplorer()</script>
</processing>
```

- **StartService (ServiceName, OptionalParam1, OptionalParam2,...).** Запускает службу, определяемую *с помощью ServiceName*. *ServiceName* — это подраздел в `HKLM\System\CurrentControlSet\Services` , который содержит данные для данной службы. Необязательные параметры, если таковые есть, передаются в API StartService. Дополнительные сведения см. в статье о функции StartServiceA (winsvc.h).

- **StopService (ServiceName)**. Останавливает службу, определяемую *serviceName*. *ServiceName* — это подраздел в `HKLM\System\CurrentControlSet\Services` , который содержит данные для данной службы.

- **SyncSCM(ServiceShortName).** Считывает значение начального типа из реестра `(HKLM\System\CurrentControlSet\Services\ServiceShortName [Start])` после изменения значения подсистемой миграции, а затем синхронизирует Service Control Manager (SCM) с новым значением.

<CMC>

Текстовый<> элемент можно использовать для задания значения для любых переменных среды, которые находятся в одном из **файлов миграции.xml**.

- **Количество вхождений:** Один раз в каждом <элементе переменной> .

- **Родительские элементы:**<переменная>

- **Дочерние элементы:** Никакой.

Синтаксис:

```xml
<text>NormalText</text>
```

Развернуть таблицу

Параметр	Значение
NormalText	Этот текст интерпретируется как обычный текст.

Пример

```
XML
<variable name="QuickTime5or6DataSys">
  <text>%CSIDL_COMMON_APPDATA%\QuickTime</text>
</variable>
```

<unconditionalExclude>

Элемент **<unconditionalExclude>** исключает указанные файлы и значения реестра из миграции, независимо от других правил включения в любом из **файлов.xml** миграции `Config.xml` или в файле. Объекты, объявленные здесь, не переносятся, так как этот элемент имеет приоритет над всеми другими правилами. Например, даже если существуют явные **<правила включения> файлов**, если они исключены с помощью этого параметра, они не переносятся. `.mp3`

Используйте этот элемент для исключения всех `.mp3` файлов с исходного компьютера. Кроме того, при резервном копировании `C:\UserData` с помощью другого метода можно исключить всю папку из миграции. Используйте этот элемент с осторожностью. Если приложению требуется исключенный файл, приложение может работать неправильно на конечном компьютере.

- **Количество вхождений:** Неограниченный.
- **Родительские элементы:** <правила>
- **Дочерние элементы:** <objectSet>

Синтаксис:

```
XML
<unconditionalExclude></unconditionalExclude>
```

Следующий **файл.xml** исключает все `.mp3` файлы из миграции. Дополнительные примеры использования этого элемента см. в разделе Исключение файлов и параметров.

XML

```
<migration
urlid="http://www.microsoft.com/migration/1.0/migxmlext/excludefiles">
  <component context="System" type="Documents">
        <displayName>Test</displayName>
        <role role="Data">
            <rules>
             <unconditionalExclude>
                        <objectSet>
    <script>MigXmlHelper.GenerateDrivePatterns ("* [*.mp3]", "Fixed")
</script>
                        </objectSet>
             </unconditionalExclude>
            </rules>
        </role>
    </component>
</migration>
```

<переменная>

Элемент **<переменной>** является обязательным в элементе **<среды>** . Для каждого **<элемента переменной>** должен быть один **<objectSet>**, **<скрипт>** или **<текстовый>** элемент. Содержимое элемента **переменной<>** присваивает текстовое значение переменной среды. Этот элемент имеет следующие три варианта:

1. Если элемент **переменной<>** содержит **текстовый<>** элемент, значение элемента переменной является значением **текстового<>** элемента.

2. Если элемент **переменной<><содержит элемент script>**, а вызов скрипта создает строку, не содержащую null, то значение элемента **переменной<>** является результатом вызова скрипта.

3. Если элемент **переменной<>** содержит **<элемент objectSet>** и при вычислении **<элемента objectSet>** создается по крайней мере один шаблон объекта, то значение первого объекта, соответствующего результирующему шаблону объекта, является значением элемента переменной.

- **Количество вхождений:** Неограниченный
- **Родительские элементы:**<среда>
- **Обязательные дочерние**<элементы: text>, <script> или <objectSet>

Синтаксис:

XML

```
<variable name="ID" remap=TRUE|FALSE>
</variable>
```

Развернуть таблицу

Параметр	Обязательно?	Значение
name	Да	*Id* — это строковое значение, которое является именем, используемым для ссылки на переменную среды. Корпорация Майкрософт рекомендует начинать *идентификатор* с имени компонента, чтобы избежать конфликтов пространства имен. Например, если имя компонента — MyComponent и требуется переменная, которая является путем установки компонента, `MyComponent.InstallPath` можно указать.
Переназначить	Нет, по умолчанию = FALSE	Указывает, следует ли оценивать эту переменную среды как переменную среды для повторного сопоставления. Объекты, расположенные по пути, который находится под значением этой переменной среды, автоматически перемещаются в место, где переменная среды указывает на целевой компьютер.

Следующий пример из `MigApp.xml` файла:

XML

```
<environment>
   <variable name="HklmWowSoftware">
      <text>HKLM\Software</text>
   </variable>
   <variable name="WinZip8or9or10Exe">

<script>MigXmlHelper.GetStringContent("Registry","%HklmWowSoftware%\Microsoft\Windows\CurrentVersion\App Paths\winzip32.exe []")</script>
   </variable>
</environment>
```

<version>

Элемент <**version**> определяет версию компонента, но не влияет на миграцию.

- **Количество вхождений:** ноль или одно
- **Родительские элементы:** <component>

- **Дочерние элементы:** none

Синтаксис:

```
XML

<version>ComponentVersion</version>
```

Развернуть таблицу

Параметр	Обязательно?	Значение
ComponentVersion	Да	Версия компонента, которая может содержать шаблоны.

Пример:

```
XML

<version>4.*</version>
```

<windowsObjects>

Элемент <**windowsObjects**> предназначен только для внутреннего использования USMT. Не используйте этот элемент.

Приложение

Указание расположений

- **Указание закодированных расположений**. Закодированное расположение, используемое во всех вспомогательных функциях, является однозначным строковым представлением для имени объекта. Закодированное расположение состоит из части узла, за которой при необходимости следует конечный элемент, заключенный в квадратные скобки. В этом формате делается четкое различие между узлами и листьями.

  Например, укажите файл `C:\Windows\Notepad.exe` следующим образом: `c:\Windows[Notepad.exe]`. Аналогичным образом укажите каталог `C:\Windows\System32` следующим образом: `c:\Windows\System32`. (Обратите внимание на отсутствие `[]` конструкции.)

Представляет реестр аналогично. Значение по умолчанию раздела реестра представлено в виде пустой `[]` конструкции. Например, значение по умолчанию для `HKLM\SOFTWARE\MyKey` раздела реестра — `HKLM\SOFTWARE\MyKey[]`.

- **Указание шаблонов расположения**. Указание шаблона расположения аналогично указанию фактического расположения. Исключение заключается в том, что и узел, и конечная часть принимают шаблоны. Однако шаблон из узла не распространяется на конечный элемент.

  Например, шаблон `c:\Windows\*` соответствует каталогу Windows и всем подкаталогам, но не соответствует ни одному из файлов в этих каталогах. Чтобы также соответствовать файлам, `c:\Windows\*[*]` необходимо указать значение .

Внутренние функции USMT

Следующие функции предназначены только для внутреннего использования USMT. Не используйте их в **файле.xml** .

- *AntiAlias*
- *ConvertScreenSaver*
- *ConvertShowIEOnDesktop*
- *ConvertToOfficeLangID*
- *MigrateActiveDesktop*
- *MigrateAppearanceUPM*
- *MigrateDisplayCS*
- *MigrateDisplayss*
- *MigrateIEAutoSearch*
- *MigrateMouseUPM*
- *MigrateSoundSysTray*
- *MigrateTaskBarss*
- *SetPstPathInMapiStruc*

Допустимые теги версий

Следующие теги версий можно использовать с различными вспомогательными функциями:

- "CompanyName"
- "FileDescription"
- FileVersion
- InternalName
- "LegalCopyright"
- "OriginalFilename"
- "ProductName"
- "ProductVersion"

Следующие теги версий содержат значения, которые можно сравнить:

- FileVersion
- "ProductVersion"

Связанные статьи

- Справочник по XML-файлу USMT.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Справочные материалы по автономному переносу

Статья • 29.01.2025 • Применяется к: ✅ Windows 11, ✅ Windows 10

Автономная миграция позволяет средству **ScanState** выполняться в операционной системе Windows, отличной от операционной системы Windows, из которой **ScanState** собирает файлы и параметры. Существует два основных сценария автономного использования:

- **Среда предустановки Windows.** Средство **ScanState** можно запускать из среды предустановки Windows, собирая файлы и параметры из автономной операционной системы Windows на этом компьютере.
- **Windows.old.** Средство **ScanState** может собирать файлы и параметры из каталога **Windows.old** . Каталог **Windows.old** создается во время установки Windows в секции, содержащей предыдущую установку Windows. Например, средство **ScanState** может запускаться в Windows, собирая файлы из предыдущей установки Windows, содержащейся в каталоге **Windows.old** .

При использовании средства миграции пользовательской среды (USMT) для сбора и восстановления пользовательского состояния автономная миграция снижает затраты на развертывание за счет:

- **Снижение сложности.** В сценариях обновления компьютера миграция из каталога **Windows.old** снижает сложность, устраняя необходимость запуска средства **ScanState** перед развертыванием операционной системы. Кроме того, миграция из каталога **Windows.old** позволяет последовательно выполнять **ScanState** и **LoadState** .
- **Повышение производительности.** При запуске USMT в автономной среде предустановки Windows (WinPE) он имеет лучший доступ к аппаратным ресурсам. Запуск USMT в WinPE может повысить производительность на старых компьютерах с ограниченными аппаратными ресурсами и множеством установленных программных приложений.
- **Новый сценарий восстановления.** В сценариях, когда компьютер больше не перезагружается должным образом, можно собрать состояние пользователя с помощью средства **ScanState** из WinPE.

Что переносится в автономном режиме?

Следующие пользовательские данные и параметры переносятся в автономном режиме, как в режиме онлайн:

- Разделы данных и реестра, указанные в MigXML.
- Учетные записи пользователей.
- Параметры приложения.
- Ограниченный набор параметров операционной системы.
- ФАЙЛЫ EFS.
- Избранное.

Исключения, которые могут быть перенесены в автономном режиме, см. в статье Что такое миграция USMT?

Какие автономные среды поддерживаются?

Все поддерживаемые в настоящее время

В следующей таблице определяется поддерживаемая комбинация сетевых и автономных операционных систем в USMT.

Развернуть таблицу

Запуск операционной системы	Автономная операционная система
Поддерживаемая в настоящее время версия WinPE с библиотекой MSXML	Windows 7, Windows 8, Windows 10, Windows 11
Windows 10, Windows 11	Каталог **Windows.old**

> **Примечание**
>
> Средство **ScanState** можно запустить, пока диск остается зашифрованным, приостановив шифрование диска Windows BitLocker перед загрузкой в WinPE. Дополнительные сведения см. в разделе Руководство по операциям BitLocker: Приостановка и возобновление работы. При использовании Microsoft Configuration Manager последовательности задач см. раздел Шаги последовательности задач: отключение BitLocker.

Управление членством в группах пользователей и профилем

Членство в группах пользователей не сохраняется во время автономной миграции. Раздел **<ProfileControl>** должен быть настроен в `Config.xml` файле, чтобы указать группы, членами которыми должны быть перенесенные пользователи. В следующем примере все перенесенные пользователи помещаются в группу Пользователи:

XML

```
<Configuration>
<ProfileControl>
    <localGroups>
      <mappings>
         <changeGroup from="*" to="Users" appliesTo="MigratedUsers">
            <include>
            <pattern>*</pattern>
            </include>
         </changeGroup>
      </mappings>
   </localGroups>
  </ProfileControl>
</Configuration>
```

Сведения о формате `Config.xml` файла см. в разделе файлConfig.xml.

Параметры командной строки

Автономную миграцию можно включить с помощью файла конфигурации в командной строке или с помощью одного из следующих параметров командной строки:

Развернуть таблицу

Компонент	Параметр	Описание
ScanState.exe	**/offline:***<path to Offline.xml>*	Этот параметр командной строки включает режим автономной миграции и требует пути к файлу конфигурации Offline.xml.
ScanState.exe	**/offlineWinDir:** *<каталог> Windows*	Этот параметр командной строки включает режим автономной миграции и запускает миграцию из указанного расположения. Он предназначен только для

Компонент	Параметр	Описание
		использования в автономных сценариях WinPE, где миграция выполняется из каталога Windows.
ScanState.exe	**Каталог /OfflineWinOld:** *<Windows.old>*	Этот параметр командной строки включает режим автономной миграции и запускает миграцию из указанного расположения. Используйте только в сценариях миграции **Windows.old** , когда миграция происходит из каталога **Windows.old** .

Одновременно можно использовать только один из `/offline` параметров командной строки , `/offlineWinDir` или `/OfflineWinOld` . USMT не поддерживает совместное использование нескольких элементов.

Переменные среды

Системные переменные среды необходимы в сценариях, описанных в следующей таблице:

Развернуть таблицу

Переменная	Значение	Сценарий
USMT_WORKING_DIR	Полный путь к рабочему каталогу	Требуется, если двоичные файлы USMT находятся на носителе только для чтения, который не поддерживает создание файлов журнала или временного хранилища. Чтобы задать системную переменную среды, в командной строке введите следующую команду: `Set USMT_WORKING_DIR=<path to working directory>`
MIG_OFFLINE_PLATFORM_ARCH	32 или 64	При работе в автономном режиме эта переменная среды определяет архитектуру автономной системы, если система не соответствует WinPE и `ScanState.exe` архитектуре. Эта переменная среды позволяет 32-разрядному приложению **ScanState** собирать данные с компьютера с 64-разрядной архитектурой или 64-разрядное приложение **ScanState** для сбора данных с компьютера с 32-разрядной архитектурой. Если автоматическое обнаружение автономной архитектуры не

Переменная	Значение	Сценарий
		работает должным образом, необходимо указать архитектуру. Например, чтобы задать эту системную переменную среды для 32-разрядной архитектуры, в командной строке введите следующую команду: `Set MIG_OFFLINE_PLATFORM_ARCH=32`

элементы Offline.xml

`Offline.xml` Используйте файл при запуске средства **ScanState** на компьютере с несколькими каталогами Windows. Файл `Offline.xml` указывает, какие каталоги следует проверять на наличие файлов Windows. Файл `Offline.xml` можно использовать с параметром в `/offline` качестве альтернативы указанию одного пути к каталогу Windows с параметром `/offlineDir` .

<автономный>

Этот элемент содержит другие элементы, определяющие способ выполнения автономной миграции.

Синтаксис:

```
XML

<offline> </offline>
```

<winDir>

Этот элемент является обязательным дочерним элементом **автономного<>** режима и содержит сведения о том, как можно выбрать автономный том. Миграция выполняется из первого элемента **<winDir>** , содержащего допустимый системный том Windows.

Синтаксис:

```
XML

<winDir> </winDir>
```

<path>

Этот элемент является обязательным дочерним **<элементом winDir>** и содержит путь к файлу, указывающий на допустимый каталог Windows. Относительные пути интерпретируются из рабочего каталога средства **ScanState** .

Синтаксис:

```
XML

<path> C:\Windows </path>
```

или при использовании с элементом **<mappings>** :

Синтаксис:

```
XML

<path> C:\, D:\ </path>
```

<Сопоставления>

Этот элемент является необязательным дочерним элементом **в автономном режиме<>**. Если этот параметр указан, **<элемент mappings>** переопределяет автоматически обнаруженные сопоставления дисков WinPE. Каждый дочерний **<элемент пути>** обеспечивает сопоставление из одного системного тома в другой. Кроме того, можно предоставить сопоставления между папками, так как к определенной папке можно подключить весь том.

Синтаксис:

```
XML

<mappings> </mappings>
```

<failOnMultipleWinDir>

Этот элемент является необязательным дочерним элементом **в автономном режиме<>**. Элемент **<failOnMultipleWinDir>** позволяет пользователю указать, что миграция должна завершиться ошибкой, когда USMT обнаруживает наличие нескольких экземпляров Windows, установленных на исходном компьютере. **<Если**

элемент failOnMultipleWinDir> отсутствует, по умолчанию миграция не завершается ошибкой.

Синтаксис:

```
XML

<failOnMultipleWinDir>1</failOnMultipleWinDir>
```

или

Синтаксис:

```
XML

<failOnMultipleWinDir>0</failOnMultipleWinDir>
```

Пример автономного .xml

В следующем примере XML показаны некоторые элементы, рассмотренные ранее в этой статье.

```
XML

<offline>
     <winDir>
          <path>C:\Windows</path>
          <path>D:\Windows</path>
          <path>E:\</path>
     </winDir>
     <failOnMultipleWinDir>1</failOnMultipleWinDir>
</offline>
```

Связанные статьи

- Планирование миграции.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Устранение неполадок средства миграции пользовательской среды (USMT)

Статья • 29.01.2025 • Применяется к: ✅ Windows 11, ✅ Windows 10

В следующей таблице описаны статьи, в которые рассматриваются распространенные проблемы и вопросы средства миграции пользовательской среды (USMT). В этих статьях описаны средства, которые можно использовать для устранения неполадок, возникающих во время миграции.

В этом разделе

Развернуть таблицу

Ссылка	Описание
Общие проблемы	Найдите решения для устранения распространенных проблем в USMT.
Часто задаваемые вопросы	Найдите ответы на вопросы об использовании USMT.
Файлы журнала	Узнайте, как включить ведение журнала для устранения неполадок в USMT.
Коды возврата	Узнайте, как использовать коды возврата для выявления проблем в USMT.
Ресурсы средства миграции пользовательской среды	Дополнительные сведения и поддержка использования USMT.

Связанные статьи

- Рекомендации по USMT.
- Обзор средства миграции пользовательской среды (USMT).
- Статьи с инструкциями по средству миграции пользовательской среды (USMT).
- Справочник по набору средств миграции пользовательской среды (USMT).

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Распространенные проблемы с инструментом миграции пользовательского состояния (USMT)

15.01.2025Применяется к: Supported versions of Windows Client

В следующих разделах рассматриваются распространенные проблемы, которые могут возникнуть при запуске средств USMT 10.0. USMT создает файлы журналов, описывающие дополнительные сведения о любых ошибках, возникших во время процесса миграции. Эти журналы можно использовать для устранения сбоев миграции.

Общие рекомендации по выявлению проблем миграции

При возникновении проблемы или сообщения об ошибке во время миграции можно использовать следующие общие рекомендации, которые помогут определить источник проблемы:

- **Проверьте журналы ScanState, LoadState** и UsmtUtils, чтобы получить точные сообщения об ошибках USMT и сообщения об ошибках интерфейса программирования приложений Windows® (API). Дополнительные сведения о кодах возврата USMT и сообщениях об ошибках см. в разделе "Коды возврата". Дополнительные сведения о любых перечисленных системных **кодах ошибок Windows** можно получить, введя в окне `net.exe helpmsg <error_number>` командной строки, где *<error_number>* номер кода ошибки, созданный сообщением об ошибке. Дополнительные сведения о системных кодах ошибок см. в разделе Системные коды ошибок (0–499).

  В большинстве случаев **журналы ScanState и LoadState** указывают, почему миграция USMT завершается сбоем. Рекомендуется использовать `/v:5` этот параметр при тестировании миграции. Этот уровень детализации можно изменить в рабочей миграции; однако снижение уровня детализации может оказаться более сложным для диагностики сбоев, возникающих во время миграции рабочей среды. Вы можете использовать уровень детализации выше 5, если вы хотите, чтобы выходные данные файлов журнала отправились в отладчик.

  > ⓘ **Примечание**

Запуск средств ScanState и LoadState с `/v:5` параметром создает подробный файл журнала. Хотя этот параметр делает файл журнала большим, дополнительные сведения помогут определить, где произошли ошибки миграции.

- `/Verify` Используйте параметр с инструментом UsmtUtils, чтобы определить, повреждены ли файлы в сжатом хранилище миграции. Дополнительные сведения см. в разделе "Проверка состояния сжатого хранилища миграции".
- `/Extract` Используйте параметр с инструментом UsmtUtils для извлечения файлов из сжатого хранилища миграции. Дополнительные сведения см. в статье "Извлечение файлов из сжатого хранилища миграции USMT".
- Создайте журнал хода выполнения с помощью `/Progress` параметра для мониторинга миграции.
- Для исходных и конечных компьютеров получите сведения об операционной системе и версии приложений, таких как Internet Explorer и любые другие соответствующие программы. Затем проверьте точные шаги, необходимые для воспроизведения проблемы. Эти сведения помогут вам понять, что не так, и воспроизвести проблему в тестовой среде.
- Выйдите из программы LoadState после запуска **средства LoadState** . Некоторые параметры, такие как шрифты, фон рабочего стола и параметры с сохранением экрана, не будут входить в силу до следующего входа пользователя.
- Закройте все приложения перед запуском **средств ScanState или LoadState**. Если некоторые приложения выполняются во время **процесса ScanState или LoadState**, USMT может не перенести некоторые данные. Например, если Microsoft Outlook® открыт, USMT может не перенести PST-файлы.

> ⓘ **Примечание**
>
> USMT завершится ошибкой, если он не может перенести файл или параметр, если вы не укажете `/c` этот параметр. При указании `/c` параметра USMT игнорирует ошибки. Однако он регистрирует ошибку при обнаружении файла, который используется, который не переносится.

Проблемы с учетной записью пользователя

В следующих разделах описаны распространенные проблемы с учетной записью пользователя. Разверните раздел, чтобы просмотреть рекомендуемые решения.

У меня возникли проблемы с созданием локальных учетных записей на конечном компьютере

Разрешение. Дополнительные сведения о создании учетных записей и переносе локальных учетных записей см. в разделе "Миграция учетных записей пользователей".

Не все учетные записи пользователей были перенесены на конечный компьютер.

Причины и разрешения существуют две возможные причины этой проблемы:

При запуске **средств ScanState и LoadState** в Windows 7, Windows 8 или Windows 10 необходимо запустить их в режиме администратора из учетной записи с учетными данными администратора, чтобы обеспечить перенос всех указанных пользователей. Выполнение в режиме администратора:

1. Выберите "**Пуск>всех программ>" Аксессуары.**
2. Щелкните правой кнопкой мыши **командную строку**.
3. Выберите **"Запуск от имени администратора**".
4. *Укажите команду LoadState.exe или ScanState.exe*.

Если вы не запускаете USMT в режиме администратора, в миграцию будет включен только профиль пользователя, вошедший в систему.

Никакие учетные записи пользователей на компьютере, который не использовался, не будут перенесены. Например, если вы добавляете User1 на компьютер, но User1 никогда не входит в систему, USMT не переносит учетную запись User1.

Учетные записи пользователей, которые я исключил, были перенесены на конечный компьютер.

Причина: указанная команда могла иметь конфликтующие `ui` параметры и `/ue` параметры. Если пользователь указан с `/ui` параметром и параметрами `/ue` `/uel` одновременно, он будет включен в миграцию. Например, если указать `/ui:domain1\*` `/ue:domain1\user1`, пользователь1 будет перенесен, так как параметр `/ui` имеет приоритет.

Разрешение. Дополнительные сведения об использовании `/ui` и `/ue` параметрах см. в примерах в статье "Синтаксис ScanState".

Я использую параметр /uel, но многие учетные записи по-прежнему включены в миграцию

Причина. Параметр `/uel` зависит от последней измененной даты NTUser.dat файла пользователей. Существуют сценарии, в которых дата последнего изменения может не соответствовать дате последнего входа пользователей.

Разрешение. Это ограничение `/uel` параметра. Возможно, вам потребуется вручную исключить этих пользователей `/ue` с помощью параметра.

Средство LoadState сообщает об ошибке в виде возвращаемого кода 71 и не может восстановить профиль пользователя во время теста миграции.

Причина. Во время теста миграции, если вы запускаете **средство ScanState на тестовом компьютере, а затем удаляете профили пользователей, чтобы проверить средство LoadState** на том же компьютере, у вас может быть конфликтующий ключ в реестре. **Команда net use** для удаления профиля пользователя удаляет папки и файлы, связанные с этим профилем, но не удаляет раздел реестра.

Разрешение. Чтобы удалить профиль пользователя, используйте **элемент "Учетные** записи пользователей" в панель управления. Чтобы исправить неполное удаление профиля пользователя:

1. Откройте редактор реестра, введя *regedit.exe* в командной строке с повышенными привилегиями.
2. Перейдите к `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList`.

   Каждый профиль пользователя хранится в разделе " `ProfileList`Системный идентификатор".
3. Удалите ключ для профиля пользователя, который вы пытаетесь удалить.

Файлы, которые не были зашифрованы до миграции, теперь шифруются с учетной записью, используемой для запуска средства LoadState

Причина. Средство **ScanState** было запущено с помощью `/EFS:copyraw` параметра для переноса зашифрованных файлов и сертификатов файловой системы шифрования (EFS). Атрибут шифрования был установлен в папке, перенесенной, но атрибут был удален из содержимого файла этой папки до миграции.

Разрешение. Перед использованием **средства ScanState** для миграции, включающей зашифрованные файлы и сертификаты EFS, можно запустить средство шифра в командной строке, чтобы просмотреть и изменить параметры шифрования файлов и папок. Атрибут шифрования необходимо удалить из папок, содержащих незашифрованные файлы, или зашифровать содержимое всех файлов в зашифрованной папке.

Чтобы удалить шифрование из файлов, которые уже перенесены неправильно, необходимо войти на компьютер с учетной записью, которая использовалась для запуска **средства LoadState** , а затем удалить шифрование из затронутых файлов.

Средство LoadState сообщает об ошибке в виде возвращаемого кода 71 и ошибки Windows 2202 в файле журнала

Причина. Имя компьютера было изменено во время автономной миграции локального профиля пользователя.

Разрешение. При запуске **средства LoadState** можно использовать `/mu` этот параметр, чтобы указать новое имя пользователя. Например,

Командная строка Windows

```
LoadState.exe  /i:MigApp.xml /i:MigDocs.xml \\server\share\migration\mystore
/progress:Progress.log /l:LoadState.log /mu:fareast\user1:farwest\user1
```

Проблемы с командной строкой

В следующих разделах описываются распространенные проблемы командной строки. Разверните раздел, чтобы просмотреть рекомендуемые решения.

Я получил следующее сообщение об ошибке : "Ошибка использования: невозможно указать путь к файлу с любым из параметров командной строки, превышающих 256 символов".

Причина. Это сообщение об ошибке может возникать в некоторых случаях, даже если вы не указываете длинный путь к хранилищу или файлу, так как длина пути вычисляется на основе абсолютного пути. Например, если выполнить `**ScanState**.exe /o store` команду из *C:\Program Files\USMT40*, каждый символ в *C:\Program Files\USMT40* будет добавлен в длину хранилища, чтобы получить длину пути.

Разрешение. Убедитесь, что общая длина пути не превышает 256 символов. Общая длина пути включает путь к хранилищу и текущий каталог.

Я получил следующее сообщение об ошибке: "USMT не удалось создать файл журнала. Убедитесь, что у вас есть доступ на запись к каталогу журнала".

Причина. Если вы используете **средства ScanState или LoadState** из общего сетевого ресурса, вы получите это сообщение об ошибке, если не указать `/l`.

Решение. Чтобы устранить эту проблему в этом сценарии, укажите `/l:ScanState.log` или `/l:LoadState.log` параметр.

Проблемы с XML-файлом

В следующих разделах описываются распространенные проблемы с XML-файлом. Разверните раздел, чтобы просмотреть рекомендуемые решения.

Я использовал `/genconfig` параметр для создания файла Config.xml, но я вижу только несколько приложений и компонентов, которые находятся в MigApp.xml. Почему Config.xml не содержит все одно и то же приложение?

Причина: *Config.xml* будут содержать только компоненты операционной системы, приложения и разделы пользовательского документа, которые находятся в обоих .xml файлах и устанавливаются на компьютере при запуске `/genconfig` параметра. В противном случае эти приложения и компоненты не будут отображаться в *файле Config.xml* .

Решение. Установите все необходимые приложения на компьютере перед запуском `/genconfig` параметра. Затем запустите *ScanState.exe* со всеми файлами .xml. Например, выполните следующую команду:

Командная строка Windows

```
ScanState.exe /genconfig:Config.xml /i:MigDocs.xml /i:MigApp.xml /v:5
/l:ScanState.log
```

У меня возникли проблемы с пользовательским файлом .xml, который я создал, и я не могу проверить правильность синтаксиса.

Разрешение. Вы можете загрузить XML-файл *схемы MigXML.xsd* в средство разработки XML. *MigXML.xsd* входит в состав USMT. Примеры см. в Центре разработки Visual Studio. Затем загрузите файл .xml в средство разработки, чтобы узнать, есть ли синтаксическая ошибка. Дополнительные сведения об использовании XML-элементов см. в справочнике по XML-коду USMT.

Я использую вспомогательные функции MigXML, но миграция не работает так, как я ожидал его. Разделы справки устранить эту проблему?

Причина. Как правило, эта проблема вызвана неправильным синтаксисом, используемым в вспомогательной функции. Вы получаете код возврата успешно, но файлы, которые вы хотите перенести, не были собраны или применены, или не были собраны или применены таким образом, как вы ожидали.

Разрешение. Вы должны искать **в журнале ScanState или LoadState** имя компонента, содержащее вспомогающую функцию MigXML, или заголовок вспомогательной функции MigXML, чтобы найти соответствующее предупреждение в файле журнала.

Проблемы с миграцией

В следующих разделах описываются распространенные проблемы миграции. Разверните раздел, чтобы просмотреть рекомендуемые решения.

Файлы, указанные для исключения, по-прежнему переносятся

Причина: может быть другое правило, включающее файлы. Если существует более конкретное правило или конфликтующее правило, файлы будут включены в миграцию.

Разрешение. Дополнительные сведения см. в разделе "Конфликты и приоритет " и раздел журнала диагностики в файлах журналов.

Я указал правила для перемещения папки в определенное расположение на целевом компьютере, но он не перенесен правильно.

Причина: в синтаксисе XML может возникнуть ошибка.

Решение. Для записи и проверки файлов .xml миграции можно использовать схему XML USMT (*MigXML.xsd*). Также см. примеры XML в следующих статьях:

Конфликты и приоритет

Исключение файлов и параметров

Перенаправка файлов и параметров

Включение файлов и параметров

Пользовательские XML-примеры

После завершения LoadState новый фон рабочего стола не отображается на целевом компьютере

Существует три типичных причины этой проблемы.

Причина. Некоторые параметры, такие как шрифты, фон рабочего стола и параметры сохранения экрана, не применяются **LoadState** до перезапуска целевого компьютера.

Решение. Чтобы устранить эту проблему, выйдите из системы, а затем войдите в систему, чтобы просмотреть перенесенный фон рабочего стола.

В миграцию включены MigApp.xml, но некоторые PST-файлы не переносятся

Причина. Файл *MigApp.xml* переносит только PST-файлы, связанные с профилями Outlook.

Разрешение. Чтобы перенести PST-файлы, которые не связаны с профилями Outlook, необходимо создать отдельное правило миграции для записи этих файлов.

USMT не переносит макет "Пуск"

Описание. Вы используете USMT для переноса профилей из одной установки Windows 10 в другую установку Windows 10 на другом оборудовании. После миграции пользователь

войдет на новое устройство и не имеет макета меню , который он ранее настроил.

Причина. Изменение кода в меню "Пуск" с Windows 10 версии 1607 и более поздних версий несовместимо с этой функцией USMT.

Решение. Доступно следующее обходное решение:

1. При входе пользователя создайте резервную копию макета "Пуск" с помощью следующей команды Windows PowerShell. При желании можно указать другой путь:

   ```
   PowerShell
   ```

   ```
   Export-StartLayout -Path "C:\Layout\user1.xml"
   ```

2. Перенос профиля пользователя с помощью USMT.

3. Прежде чем пользователь войдет на новое устройство, импортируйте макет start с помощью следующей команды Windows PowerShell:

   ```
   PowerShell
   ```

   ```
   Import-StartLayout -LayoutPath "C:\Layout\user1.xml" -MountPath %systemdrive%
   ```

Это обходное решение изменяет макет начального запуска пользователя по умолчанию. Решение не масштабируется до массовых миграций или многопользовательских устройств, но может потенциально разблокировать некоторые сценарии. Если другие пользователи будут входить на устройство, необходимо удалить layoutmodification.xml из профиля пользователя по умолчанию. В противном случае все пользователи, которые войдут на это устройство, будут использовать импортированный макет запуска.

Проблемы автономной миграции

В следующих разделах описываются распространенные проблемы автономной миграции. Разверните раздел, чтобы просмотреть рекомендуемые решения.

Некоторые из моих параметров системы не переносятся в автономной миграции

Причина. Некоторые системные параметры, такие как фон рабочего стола и сетевые принтеры, не поддерживаются в автономной миграции. Дополнительные сведения см. в разделе "Что выполняет миграция USMT"?

Разрешение. При автономной миграции эти параметры системы должны быть восстановлены вручную.

Средство ScanState завершается сбоем с кодом возврата 26

Причина: распространенная причина возврата кода 26 заключается в том, что временный профиль активен на исходном компьютере. Этот профиль сопоставляется с c:\users\temp. В журнале ScanState **отображается исключение MigStartupOfflineCaught, включающее повторяющуюся ошибку SID профиля пользователя.**

Разрешение. Вы можете перезагрузить компьютер, чтобы избавиться от профиля temp или задать **MIG_FAIL_ON_PROFILE_ERROR=0** , чтобы пропустить ошибку и исключить временный профиль.

Правила включения и исключения для переноса профилей пользователей не работают в автономном режиме, как и в Интернете

Причина. При автономном режиме DNS-сервер не может запрашиваться для разрешения имени пользователя и сопоставления идентификаторов безопасности.

Разрешение. Используйте идентификатор безопасности (SID), чтобы включить пользователя при запуске **средства ScanState** . Например:

Командная строка Windows

```
ScanState.exe /ui:S1-5-21-124525095-708259637-1543119021*
```

Подстановочная карточка (*) в конце идентификатора безопасности будет переносить *ключ SID*_Classes также.

Вы также можете использовать шаблоны для идентификаторов SID, определяющих универсальных пользователей или групп. Например, можно использовать `/ue:*-500` параметр, чтобы исключить учетные записи локального администратора. Дополнительные сведения о идентификаторах WINDOWS см. в разделе "Идентификаторы безопасности".

Мой сценарий для очистки диска завершается сбоем после запуска средства ScanState в 64-разрядной системе.

Причина. Куст реестра HKLM не выгружается после **завершения работы средства ScanState** .

Разрешение. Перезагрузите компьютер или выгрузите куст реестра в командной строке после **завершения работы средства ScanState** . Например, в командной строке введите:

Командная строка Windows

```
reg.exe unload hklm\$dest$software
```

Проблемы с миграцией с жесткой связью

В следующих разделах описаны распространенные проблемы миграции с жесткой связью. Разверните раздел, чтобы просмотреть рекомендуемые решения.

Файлы EFS не восстанавливаются в новом разделе

Причина. Файлы EFS нельзя переместить в новую секцию с жесткой ссылкой. Параметр `/efs:hardlink` командной строки применим только к файлам, перенесенным в той же секции.

Разрешение. Используйте `/efs:copyraw` параметр командной строки для копирования файлов EFS во время миграции вместо создания жестких ссылок или вручную скопируйте файлы EFS из хранилища жесткой связи.

Средство ScanState не может удалить предыдущее хранилище миграции с жесткой связью

Причина. Хранилище миграции содержит жесткие ссылки на заблокированные файлы.

Разрешение. Используйте средство UsmtUtils для удаления хранилища или изменения имени хранилища. Например, в командной строке введите:

Командная строка Windows

```
UsmtUtils.exe /rd <storedir>
```

Вы также должны перезагрузить компьютер.

Сбор данных

Если вам нужна помощь службы поддержки Microsoft, мы рекомендуем собирать информацию путем выполнения действий, описанных в разделе Сбор информации с помощью TSS для решения проблем, связанных с развертыванием.

Связанные статьи

Устранение неполадок средства миграции пользовательского состояния (USMT)

Часто задаваемые вопросы по Аналитике компьютеров

Коды возврата

Синтаксис UsmtUtils

Часто задаваемые вопросы

Относится к:

- Windows 11
- Windows 10

В следующих разделах приводятся часто задаваемые вопросы и рекомендуемые решения для миграции с помощью средства миграции пользовательской среды (USMT).

Общее

Сколько места требуется на конечном компьютере?

Целевому компьютеру требуется достаточно свободного места для следующих элементов:

- Операционная система
- Приложения
- Несжатый магазин

Можно ли хранить файлы и параметры непосредственно на конечном компьютере или требуется сервер?

Файлы не нужно сохранять на сервере. При перемещении пользовательского состояния на новый компьютер хранилище можно создать на:

- Общая папка.
- На съемных носителях, таких как USB-устройство флэш-памяти (UFD).
- Непосредственно на конечном компьютере.

Чтобы сохранить его непосредственно на конечном компьютере, выполните следующие действия:

1. Создайте каталог `C:\store` и поделитесь им на конечном компьютере.
2. Запустите средство **ScanState** на исходном компьютере и сохраните файлы и параметры в `\\<DestinationComputerName>\store`

3. Запустите средство **LoadState** на конечном компьютере и укажите `C:\store` в качестве расположения хранилища.

Можно ли переносить данные между операционными системами с разными языками?

Нет. USMT не поддерживает перенос данных между операционными системами с разными языками; язык операционной системы исходного компьютера должен соответствовать языку операционной системы конечного компьютера.

Можно ли изменить расположение временного каталога на конечном компьютере?

Да. Переменную `USMT\_WORKING\_DIR` среды можно изменить на альтернативный временный каталог. Существуют некоторые сценарии автономной миграции, в которых необходимо изменить временный каталог, например, если двоичные файлы USMT находятся на загрузочном носителе среды предустановки Windows (WinPE) только для чтения.

Как устанавливается USMT?

Так как USMT входит в комплект средств оценки и развертывания Windows (Windows ADK), пакет Windows ADK необходимо установить по крайней мере на одном компьютере в среде. Затем двоичные файлы USMT можно скопировать из каталога USMT, расположенного на исходном компьютере, на котором был установлен Windows ADK, на дополнительные клиентские компьютеры.

Как удаляется USMT?

Для компьютеров, на которых установлен Windows ADK, при удалении Windows ADK с компьютера удаляется USMT. Для клиентских компьютеров, на которых не установлена Windows ADK, каталог USMT можно удалить, чтобы удалить USMT.

Файлы и параметры

Как исключить папку или файл определенного типа из миграции?

Элемент <**unconditionalExclude**> можно использовать для глобального исключения данных из миграции. Например, этот элемент можно использовать для исключения всех MP3-файлов на компьютере или для исключения всех файлов из `C:\UserData`. Этот элемент исключает объекты независимо от других <**правил включения**> , которые находятся в **файлах.xml** . Пример см. в статье <**О безусловном исключении**>файлов и параметров . Синтаксис этого элемента см. в разделе Библиотека XML-элементов.

Что происходит с файлами, расположенными на диске, которые не существуют на конечном компьютере?

USMT переносит файлы в , `%SystemDrive%` сохраняя правильную иерархию папок. Пример:

- `E:\data\File.pst` находится на исходном компьютере.
- На конечном компьютере нет диска E:\.
- C:\ — системный диск на конечном компьютере.

файл переносится в `C:\data\File.pst`. Это поведение действует, даже если <**правила locationModify**> пытаются переместить данные на диск, который не существует на конечном компьютере.

Файлы .xml USMT

Где есть примеры файлов USMT **.xml**?

В следующих статьях приведены примеры файлов **.xml** USMT:

- Исключение файлов и параметров
- Перенаправка файлов и параметров
- Включение файлов и параметров
- Пользовательские примеры XML

Можно ли использовать пользовательские файлы **.xml**, написанные для USMT 5.0?

Да. Пользовательские **.xml** файлы, написанные для USMT 5.0, можно использовать с более новыми версиями USMT. Тем не менее, чтобы использовать новые функции USMT,

пользовательские файлы USMT должны быть пересмотрены и обновлены, чтобы включить новые параметры командной строки и XML-элементы.

Как проверить файлы **.xml**?

Xml-схема USMT (`MigXML.xsd`) может использоваться для записи и проверки файлов миграции **.xml** .

Почему файлы **.xml** должны быть включены в команды 'ScanState.exe' и 'LoadState.exe' ?

Файлы **.xml** не копируются в хранилище, как в предыдущих версиях USMT. Так как **средствам ScanState** и **LoadState** требуются **файлы.xml** для управления миграцией, для команд и `LoadState.exe` должен быть указан `ScanState.exe` один и тот же набор **.xml** файлов. Если в **средстве ScanState** использовался определенный набор файлов mig*.xml, вызываемых с помощью `/auto` параметра или по `/i` отдельности, то тот же параметр следует использовать для вызова тех же файлов mig*.xml в **средстве LoadState** . `Config.xml` Однако указывать файл не требуется, если только файлы и параметры, перенесенные в хранилище, не должны быть исключены. Например, папку **Документы** можно перенести в хранилище, но не на конечный компьютер. Чтобы выполнить миграцию этого типа, измените `Config.xml` файл и укажите обновленный файл с помощью `LoadState.exe` команды . **LoadState** переносит только нужные файлы и параметры.

Если **файл.xml** исключен из `LoadState.exe` команды, то переносятся все данные в хранилище, которое было перенесено с отсутствующими **файлами.xml** . Однако правила миграции, указанные `ScanState.exe` для команды, не применяются. Например, если `MigApp.xml` файл с правилом перенаправки, например `MigsysHelperFunction.RelativeMove("c:\data", "%CSIDL_PERSONAL%")` , исключен, USMT не перенаправляет файлы. Вместо этого они переносятся в `C:\data`.

Какие файлы можно изменить и указать в командной строке?

Файлы `MigUser.xml`, `MigApp.xml` и `MigDocs.xml` можно указать в командной строке. Каждый из этих файлов можно изменить. Манифесты управляют переносом параметров операционной системы. Манифесты нельзя изменить. Чтобы исключить определенные параметры операционной системы или любые другие компоненты, создайте и измените `Config.xml` файл.

Что произойдет, если файлы **.xml** не указаны в командной строке?

- **Scanstate**

  Если с помощью команды не указаны `ScanState.exe` файлы, переносятся все учетные записи пользователей и компоненты операционной системы по умолчанию.

- **Loadstate**

  Если с помощью команды не указаны `LoadState.exe` файлы, переносятся все данные, которые находятся в хранилище. Однако все правила миграции, относящиеся к целевому объекту, указанные в **.xml** файлах с `ScanState.exe` помощью команды , не применяются. Например, если `MigApp.xml` файл с правилом перенаправки, например `MigsysHelperFunction.RelativeMove("c:\data", "%CSIDL_PERSONAL%")` , исключен, USMT не перенаправляет файлы. Вместо этого они переносятся в `C:\data`.

Конфликты и приоритет

Что происходит при наличии конфликтующих правил XML или конфликтующих объектов на конечном компьютере?

Дополнительные сведения см. в разделе Конфликты и приоритет.

Связанные темы

- Устранение неполадок средства миграции пользовательской среды (USMT).
- Извлеките файлы из сжатого хранилища миграции USMT.
- Проверьте состояние сжатого хранилища миграции.

Файлы журнала USMT

Статья • 29.01.2025 • Применяется к: ✅ Windows 11, ✅ Windows 10

Журналы средства миграции пользовательской среды (USMT) можно использовать для мониторинга миграции и устранения ошибок и неудачных миграций. В этой статье описываются доступные параметры командной строки для включения журналов USMT. В ней также описываются новые XML-элементы, которые можно использовать для настройки:

- Какие типы ошибок являются неустранимыми и должны остановить миграцию.
- Какие типы не являются неустранимыми и должны быть пропущены, чтобы продолжить миграцию.

Параметры командной строки журнала

В следующей таблице описаны все параметры командной строки, связанные с журналами, а также имя журнала и описание типа информации, содержащейся в каждом журнале.

Развернуть таблицу

Параметр командной строки	Имя файла	Описание
/l:"*[путь]Имя_файла*	`ScanState.exe.log` или `LoadState.log`	Указывает путь и имя файла журнала **ScanState** или **LoadState** .
/progress: *[Path]Имя_файла*	Указывает путь и имя файла журнала хода выполнения.	Предоставляет сведения о состоянии миграции по проценту завершения.
/v:*[VerbosityLevel]*	Неприменимо	См . раздел Параметры мониторинга в синтаксисе ScanState.
/listfiles: *[путь]Имя_файла*	Указывает путь и имя файла журнала Listfiles.	Предоставляет список перенесенных файлов.
Задайте **для переменной среды MIG_ENABLE_DIAG** путь к XML-файлу.	`USMTDiag.xml`	Журнал диагностики содержит подробные сведения о системной среде, сведения о пользовательской среде, а также сведения о собираемых

Параметр командной строки	Имя файла	Описание
		единицах миграции (migunits) и их содержимом.

> **Примечание**
>
> Файлы журнала не могут храниться в *StorePath*. Если файлы журнала хранятся в *StorePath*, файлы журнала перезаписываются при запуске USMT.

Журналы ScanState и LoadState

Журналы **ScanState** и **LoadState** — это текстовые файлы, которые создаются при запуске средств **ScanState** и **LoadState**. Эти журналы можно использовать для мониторинга миграции. Содержимое журнала зависит от используемых параметров командной строки и заданного уровня детализации. Дополнительные сведения об уровнях детализации см. в разделе Параметры мониторинга в синтаксисе ScanState.

Журнал выполнения

Журнал выполнения можно создать с помощью `/progress` параметра . Внешние средства, такие как Microsoft System Center Operations Manager, могут анализировать журнал выполнения для обновления систем мониторинга. Первые три поля в каждой строке фиксируются следующим образом:

- **Дата:** Date в формате *dayshortNameOfTheMonthyear*. Например: 08 июня 2023 г.
- **Местное время:** Время в формате *hrs:minutes:seconds* (с использованием 24-часовых часов). Например: 13:49:13.
- **Время миграции:** Продолжительность выполнения USMT в формате *hrs:minutes:seconds*. Например: 00:00:20.

Остальные поля являются парами "ключ-значение", как показано в следующей таблице.

Развернуть таблицу

Раздел	Значение
программа	`ScanState.exe` или `LoadState.exe`.
productVersion	Полный номер версии продукта USMT.
computerName	Имя исходного или целевого компьютера, на котором был запущен USMT.
commandLine	Полная команда, используемая для запуска USMT.
ФАЗА	Сообщает о начале нового этапа миграции. Этот ключ может быть одним из следующих значений: • Инициализации • Сканирование • Собирание • Спасительный • Оценки • Применение
detectedUser	• Для средства **ScanState** этот ключ представляет собой определяемый пользователем USMT на исходном компьютере, который можно перенести. • Для средства **LoadState** этот ключ — это определяемые пользователем USMT в хранилище, которое можно перенести.
includedInMigration	Определяет, включен ли профиль пользователя или компонент для миграции. Допустимые значения: **Да** или **Нет**.
forUser	Задает одно из следующих значений: • Переносимое состояние пользователя. • *Это компьютер*, то есть файлы и параметры, которые не связаны с пользователем.
detectedComponent	Указывает компонент, обнаруженный с помощью USMT. • Для *ScanState* этот ключ является компонентом или приложением, установленным на исходном компьютере. • Для **LoadState** этот ключ является компонентом или приложением, обнаруженным в хранилище.
totalSizeInMBToTransfer	Общий размер файлов и параметров для миграции в мегабайтах (МБ).
totalPercentageCompleted	Общий процент миграции, завершенной **с помощью ScanState** или **LoadState**.

Раздел	Значение
collectingUser	Указывает, для какого пользователя **ScanState** собирает файлы и параметры.
totalMinutesRemaining	Оценка времени (в минутах) для завершения миграции.
ошибка	Тип неустранимой ошибки. Этот ключ может быть одним из следующих значений: • **Не удается** скопировать хранилище, так как диск, на котором находится хранилище, заполнен. • **Не удается** открыть файл для миграции, так как файл открыт в другом приложении или службе в режиме без общего доступа. • **UnableToCopyCatalog**: не удается скопировать, так как хранилище повреждено. • **UnableToAccessDevice**: не удается получить доступ к устройству. • **Не удается** применить параметр к конечному компьютеру.
objectName	Имя файла или параметра, вызвавшего неустранимую ошибку.
действие	Действие, выполняемое USMT для неустранимой ошибки. Ниже приведены следующие значения: • **Игнорировать**: неустранимая ошибка игнорируется и миграция продолжается, так как параметр **/c** был указан в командной строке. • **Прерывание**: миграция остановлена, так как параметр **/c** не указан.
errorCode	Значение errorCode или возвращаемое значение.
numberOfIgnoredErrors	Общее количество неустранимых ошибок, пропущенных USMT.
*Сообщение**	Сообщение, соответствующее errorCode.

Журнал файлов списка

Журнал списка файлов (`Listfiles.txt`) содержит список перенесенных файлов. Этот список можно использовать для устранения проблем с XML или сохранить в виде записи файлов, собранных в хранилище миграции. Журнал файлов списка доступен только для `ScanState.exe`.

Журнал диагностики

Журнал диагностики можно получить, задав **переменную среды MIG_ENABLE_DIAG** пути к XML-файлу.

Журнал диагностики содержит:

- Подробные сведения о системной среде.
- Подробные сведения о пользовательской среде.
- Сведения о собираемых единицах миграции (migunits) и их содержимом.

Использование журнала диагностики

Журнал диагностики по сути представляет собой отчет обо всех единицах миграции (мигунитах), включенных в миграцию. Migunit — это коллекция данных. В XML-файлах компонент определяет migunit, с которым связан migunit. Хранилище миграции состоит из всех migunits в миграции. Журнал диагностики можно использовать для проверки того, какие migunitы были включены в миграцию, а также для устранения неполадок при создании XML-файлов миграции.

В следующих примерах описаны распространенные сценарии, в которых можно использовать журнал диагностики.

Почему этот файл не переносится, когда я создал для него правило включения?

Предположим, что у нас есть следующая структура каталогов и что мы хотим, чтобы каталог **данных** был включен в миграцию вместе с файлом **New Text Document.txt** в **новой папке**. Каталог `C:\data` содержит:

Командная строка Windows

```
12/21/2023  01:08 PM    <DIR>          .
12/21/2023  01:08 PM    <DIR>          ..
12/21/2023  01:08 PM    <DIR>          New Folder
12/21/2023  01:19 PM                13 test (1).txt
12/21/2023  01:19 PM                13 test.txt
               2 File(s)             26 bytes
```

Каталог `C:\data\New Folder` содержит:

Командная строка Windows

```
12/21/2023  01:08 PM    <DIR>          .
12/21/2023  01:08 PM    <DIR>          ..
```

```
12/21/2023  01:08 PM                 0 New Text Document.txt
               1 File(s)              0 bytes
```

Для переноса этих файлов создается следующий XML-код миграции:

XML

```xml
<?xml version="1.0" encoding="UTF-8"?>
<migration urlid="http://www.microsoft.com/migration/1.0/TestSuite_BUGFIX">

<component context="System"  type="Application">
  <displayName>DATA1</displayName>
  <role role="Data">
    <rules>
      <include>
        <objectSet>
          <pattern type="File">c:\data\ [*]</pattern>
        </objectSet>
      </include>

    </rules>
  </role>
</component>
</migration>
```

Однако при тестировании миграции файл **new text Document.txt** замечается, что он не был включен в миграцию. Чтобы устранить эту ошибку, миграцию можно повторить с переменной среды , **MIG_ENABLE_DIAG** задать таким образом, чтобы был создан журнал диагностики. При поиске компонента **DATA1** в журнале диагностики отображается следующий раздел XML:

XML

```xml
<MigUnitList>
  <MigUnit Name="\<System\>\DATA1 (CMXEAgent)" Context="System"
ConfidenceLevel="100" Group="Applications" Role="UserData" Agent="CMXEAgent"
Selected="true" Supported="true">
    <Patterns Type="Include">
      <Pattern Type="File" Path="C:\data [*]"/>
    </Patterns>
  </MigUnit>
</MigUnitList>
<Perform Name="Gather" User="System">
  <MigUnit Name="\<System\>\DATA1 (CMXEAgent)">
    <Operation Name="Store" Type="File" Path="C:\data" SimObj="false"
Success="true"/>
    <Operation Name="Store" Type="File" Path="C:\data [test (1).txt]"
SimObj="false" Success="true"/>
    <Operation Name="Store" Type="File" Path="C:\data [test.txt]"
SimObj="false" Success="true"/>
```

```
  </MigUnit>
</Perform>
```

Анализ этого раздела XML показывает migunit, созданный при обработке правила миграции. В **<разделе Выполнение>** подробно описаны фактические файлы, которые были запланированы для сбора, и результат операции сбора. Файл **New Text Document.txt** не отображается в этом разделе, что подтверждает неправильное создание правила миграции.

Анализ справочной статьи по библиотеке XML-элементов показывает, что **<тег шаблона>** необходимо изменить следующим образом:

XML

```
<pattern type="File">c:\data\* [*]</pattern>
```

При повторном выполнении миграции с измененным тегом журнал диагностики отображает следующие сведения:

XML

```
<MigUnitList>
  <MigUnit Name="\<System\>\DATA1 (CMXEAgent)" Context="System"
ConfidenceLevel="100" Group="Applications" Role="UserData" Agent="CMXEAgent"
Selected="true" Supported="true">
    <Patterns Type="Include">
      <Pattern Type="File" Path="C:\data\* [*]"/>
    </Patterns>
  </MigUnit>
</MigUnitList>
<Perform Name="Gather" User="System">
  <MigUnit Name="\<System\>\DATA1 (CMXEAgent)">
    <Operation Name="Store" Type="File" Path="C:\data" SimObj="false"
Success="true"/>
    <Operation Name="Store" Type="File" Path="C:\data [test (1).txt]"
SimObj="false" Success="true"/>
    <Operation Name="Store" Type="File" Path="C:\data [test.txt]"
SimObj="false" Success="true"/>
    <Operation Name="Store" Type="File" Path="C:\data\New Folder"
SimObj="false" Success="true"/>
    <Operation Name="Store" Type="File" Path="C:\data\New Folder [New Text
Document.txt]" SimObj="false" Success="true"/>
  </MigUnit>
</Perform>
```

Этот журнал диагностики подтверждает, что измененное **<значение шаблона>** позволяет перенести файл.

Почему этот файл переносится, когда я создал правило исключения, исключающее его?

В этом сценарии существует следующая структура каталогов, и все файлы в каталоге **Данных** должны быть перенесены, за исключением текстовых файлов. Папка `C:\Data` содержит:

Командная строка Windows

```
Directory of C:\Data

12/21/2023  01:08 PM    <DIR>          .
12/21/2023  01:08 PM    <DIR>          ..
12/21/2023  01:08 PM    <DIR>          New Folder
12/21/2023  01:19 PM                13 test (1).txt
12/21/2023  01:19 PM                13 test.txt
               2 File(s)             26 bytes
```

Содержит `C:\Data\New Folder\` :

Командная строка Windows

```
12/21/2023  01:08 PM    <DIR>          .
12/21/2023  01:08 PM    <DIR>          ..
12/21/2023  01:08 PM                 0 New Text Document.txt
               1 File(s)              0 bytes
```

Создается следующий XML-код миграции:

XML

```xml
<?xml version="1.0" encoding="UTF-8"?>
<migration urlid="http://www.microsoft.com/migration/1.0/TestSuite_BUGFIX">

<component context="System"  type="Application">
  <displayName>DATA1</displayName>
  <role role="Data">
    <rules>
      <include>
        <objectSet>
          <pattern type="File">c:\data\* [*]</pattern>
        </objectSet>
      </include>
    </rules>
    <rules>
      <exclude>
        <objectSet>
          <pattern type="File">c:\* [*.txt]</pattern>
        </objectSet>
```

```
      </exclude>

    </rules>
  </role>
</component>
```

Однако при тестировании миграции все текстовые файлы замечаются, что они по-прежнему включены в миграцию. Чтобы устранить эту проблему, миграцию можно выполнить с переменной среды , **MIG_ENABLE_DIAG** задать для создания журнала диагностики. При поиске компонента **DATA1** в журнале диагностики отображается следующий раздел XML:

XML

```
<MigUnitList>
  <MigUnit Name="\<System\>\DATA1 (CMXEAgent)" Context="System"
ConfidenceLevel="100" Group="Applications" Role="UserData" Agent="CMXEAgent"
Selected="true" Supported="true">
    <Patterns Type="Include">
      <Pattern Type="File" Path="C:\data\* [*]"/>
    </Patterns>
    <Patterns Type="Exclude">
      <Pattern Type="File" Path="C:\* [*.txt]"/>
    </Patterns>
  </MigUnit>
</MigUnitList>
<Perform Name="Gather" User="System">
  <MigUnit Name="\<System\>\DATA1 (CMXEAgent)">
    <Operation Name="Store" Type="File" Path="C:\data" SimObj="false"
Success="true"/>
    <Operation Name="Store" Type="File" Path="C:\data [test (1).txt]"
SimObj="false" Success="true"/>
    <Operation Name="Store" Type="File" Path="C:\data [test.docx]"
SimObj="false" Success="true"/>
    <Operation Name="Store" Type="File" Path="C:\data [test.txt]"
SimObj="false" Success="true"/>
    <Operation Name="Store" Type="File" Path="C:\data\New Folder"
SimObj="false" Success="true"/>
    <Operation Name="Store" Type="File" Path="C:\data\New Folder [New Text
Document.txt]" SimObj="false" Success="true"/>
    <Operation Name="Store" Type="File" Path="C:\data\New Folder
[test.docx]" SimObj="false" Success="true"/>
  </MigUnit>
</Perform>
```

При проверке журнала диагностики подтверждается, что файлы по-прежнему переносятся, и что это проблема с созданным правилом XML миграции. Для XML-скрипта миграции создается обновление следующим образом:

XML

```
<?xml version="1.0" encoding="UTF-8"?>
<migration urlid="http://www.microsoft.com/migration/1.0/TestSuite_BUGFIX">

<component context="System"  type="Application">
  <displayName>DATA1</displayName>
  <role role="Data">
    <rules>
      <include>
        <objectSet>
          <pattern type="File">c:\data\* [*]</pattern>
        </objectSet>
      </include>
    </rules>
    <rules>
      <exclude>
        <objectSet>
          <pattern type="File">c:\data\* [*.txt]</pattern>
        </objectSet>
      </exclude>

    </rules>
  </role>
</component>


</migration>
```

Измененный XML-скрипт миграции исключает файлы из миграции, как указано в журнале диагностики:

XML

```
<MigUnitList>
  <MigUnit Name="\<System\>\DATA1 (CMXEAgent)" Context="System"
ConfidenceLevel="100" Group="Applications" Role="UserData" Agent="CMXEAgent"
Selected="true" Supported="true">
    <Patterns Type="Include">
      <Pattern Type="File" Path="C:\data\* [*]"/>
    </Patterns>
    <Patterns Type="Exclude">
      <Pattern Type="File" Path="C:\data\* [*.txt]"/>
    </Patterns>
  </MigUnit>
</MigUnitList>
<Perform Name="Gather" User="System">
  <MigUnit Name="\<System\>\DATA1 (CMXEAgent)">
    <Operation Name="Store" Type="File" Path="C:\data" SimObj="false"
Success="true"/>
    <Operation Name="Store" Type="File" Path="C:\data [test.docx]"
SimObj="false" Success="true"/>
    <Operation Name="Store" Type="File" Path="C:\data\New Folder"
SimObj="false" Success="true"/>
```

```
    <Operation Name="Store" Type="File" Path="C:\data\New Folder
[test.docx]" SimObj="false" Success="true"/>
  </MigUnit>
</Perform>
```

Связанные статьи

- Библиотека XML-элементов.
- Синтаксис ScanState.
- Синтаксис LoadState.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Коды возврата средства миграции пользовательского состояния (USMT)

15.01.2025Применяется к: Supported versions of Windows Client

В этой статье описаны коды возврата и сообщения об ошибках USMT 10.0. Также включена таблица с описанием кодов возврата USMT со связанными шагами по устранению рисков. Кроме того, в этой статье содержатся советы по использованию файлов журнала, чтобы определить, почему вы получили ошибку.

Понимание требований к запуску USMT может помочь свести к минимуму ошибки в миграции USMT. Дополнительные сведения см. в разделе "Требования USMT".

Коды возврата, используемые USMT

При возникновении ошибки при миграции USMT можно использовать коды возврата и более конкретную информацию, указанную в связанных сообщениях об ошибках USMT, чтобы устранить проблему и определить шаги по устранению рисков.

Коды возврата группируются в следующие широкие категории, описывающие их область отчетов об ошибках:

- Успешное выполнение или отмена пользователей
- Недопустимые командные строки
- Настройка и инициализация
- Неустранимая ошибка
- Неустранимая ошибка

Рекомендуется задать уровень детализации 5, `v:5` на *ScanState.exe*, *LoadState.exe u UsmtUtils.exe* команд, чтобы наиболее подробные отчеты были доступны в соответствующих журналах USMT. Вы можете использовать более высокий уровень детализации, если вы хотите, чтобы выходные данные файлов журналов пошли в отладчик.

Сообщения об ошибках USMT

Сообщения об ошибках предоставляют более подробные сведения о проблеме миграции, чем связанный код возврата. Например, **средство ScanState, LoadState** или

UsmtUtils может возвращать код **11** (для **USMT_INVALID_PARAMETERS**) и связанное сообщение об ошибке, которое считывает **/key и /keyfile оба указанных**. Сообщение об ошибке отображается в командной строке и определяется в **файлах журнала ScanState, LoadState** или **UsmtUtils**, чтобы определить, почему получен код возврата.

Дополнительные сведения о любых перечисленных системных **кодах ошибок Windows** можно получить, введя в окне `net.exe helpmsg <error_number>` командной строки, где *<error_number>* номер кода ошибки, созданный сообщением об ошибке. Дополнительные сведения о системных кодах ошибок см. в разделе Системные коды ошибок (0–499).

Устранение неполадок с кодами возврата и сообщениями об ошибках

Следующая информация содержит список каждого возвращаемого кода по числовым значениям, а также связанных сообщений об ошибках и предлагаемых действий по устранению неполадок.

0: USMT_SUCCESS

- **Категория**: успешное или пользовательское отмена

Развернуть таблицу

Сообщение об ошибке	Устранение неполадок, устранение рисков, обходные пути
Успешное выполнение	Неприменимо

1: USMT_DISPLAY_HELP

- **Категория**: успешное или пользовательское отмена

Развернуть таблицу

Сообщение об ошибке	Устранение неполадок, устранение рисков, обходные пути
Запрошенная справка по командной строке	Неприменимо

2: USMT_STATUS_CANCELED

- **Категория**: успешное или пользовательское отмена

Развернуть таблицу

Сообщение об ошибке	Устранение неполадок, устранение рисков, обходные пути
Сбор был прерван из-за файла EFS	Неприменимо
Пользователь решил отменить (например, нажатие клавиш CTRL+C)	Неприменимо

3: USMT_WOULD_HAVE_FAILED

- **Категория:**

Развернуть таблицу

Сообщение об ошибке	Устранение неполадок, устранение рисков, обходные пути
По крайней мере одна ошибка пропущена в результате /c.	Дополнительные сведения об ошибках командной строки см. в журнале ScanState, LoadState или UsmtUtils.

11: USMT_INVALID_PARAMETERS

- **Категория**: недопустимые командные строки

Развернуть таблицу

Сообщение об ошибке	Устранение неполадок, устранение рисков, обходные пути
/all конфликтует с /ui, /ue или /uel	Дополнительные сведения об ошибках командной строки см. в журнале ScanState или журнале LoadState.
/auto ожидает необязательный параметр для папки скрипта	Дополнительные сведения об ошибках командной строки см. в журнале ScanState или журнале LoadState.
Не удается использовать /nocompress /encrypt	Дополнительные сведения об ошибках командной строки см. в журнале ScanState или журнале LoadState.

Сообщение об ошибке	Устранение неполадок, устранение рисков, обходные пути
/encrypt требует /key или /keyfile	Дополнительные сведения об ошибках командной строки см. в журнале ScanState или журнале LoadState.
Не удается использовать /genconfig с большинством других параметров	Дополнительные сведения об ошибках командной строки см. в журнале ScanState или журнале LoadState.
Не удается использовать /genmigxml с большинством других параметров	Дополнительные сведения об ошибках командной строки см. в журнале ScanState или журнале LoadState.
/hardlink требует /nocompress	Дополнительные сведения об ошибках командной строки см. в журнале ScanState или журнале LoadState.
/key и /keyfile оба указанных	Дополнительные сведения об ошибках командной строки см. в журнале ScanState или журнале LoadState.
/key или /keyfile, используемые без включения шифрования	Дополнительные сведения об ошибках командной строки см. в журнале ScanState или журнале LoadState.
/lae используется только с /lac	Дополнительные сведения об ошибках командной строки см. в журнале ScanState или журнале LoadState.
/listfiles нельзя использовать с /p	Дополнительные сведения об ошибках командной строки см. в журнале ScanState или журнале LoadState.
Для /offline требуется допустимый путь к XML-файлу, описывающий автономные пути.	Дополнительные сведения об ошибках командной строки см. в журнале ScanState или журнале LoadState.
/offlinewindir требует допустимого пути к автономной папке Windows	Дополнительные сведения об ошибках командной строки см. в журнале ScanState или журнале LoadState.
Для /offlinewinold требуется допустимый путь к автономной папке Windows	Дополнительные сведения об ошибках командной строки см. в журнале ScanState или журнале LoadState.
Команда уже указана	Убедитесь в правильности синтаксиса командной строки и отсутствии повторяющихся команд.
Отсутствует аргумент параметра	Дополнительные сведения об ошибках командной строки см. в журнале ScanState или журнале

Сообщение об ошибке	Устранение неполадок, устранение рисков, обходные пути
	LoadState.
Параметр указывается несколько раз и неоднозначно	Дополнительные сведения об ошибках командной строки см. в журнале ScanState или журнале LoadState.
По умолчанию /auto выбирает всех пользователей и использует самый высокий уровень детализации журнала. Переключатели, такие как /all, /ui, /ue, /v, не допускаются.	Дополнительные сведения об ошибках командной строки см. в журнале ScanState или журнале LoadState.
Обязательные аргументы командной строки. Уточнять/? для параметров.	Дополнительные сведения об ошибках командной строки см. в журнале ScanState или журнале LoadState.
Недопустимый параметр командной строки	Дополнительные сведения об ошибках командной строки см. в журнале ScanState или журнале LoadState.
Указанный параметр EFS недопустим для /efs	Дополнительные сведения об ошибках командной строки см. в журнале ScanState или журнале LoadState.
Недопустимый аргумент файла для /genconfig	Дополнительные сведения об ошибках командной строки см. в журнале ScanState или журнале LoadState.
Недопустимый аргумент файла для /genmigxml	Дополнительные сведения об ошибках командной строки см. в журнале ScanState или журнале LoadState.
Недопустимый путь оценки пространства. Проверка параметров и (или) разрешений файловой системы	Дополнительные сведения об ошибках командной строки см. в журнале ScanState или журнале LoadState.
Аргумент пути к файлу списка недопустим для /listfiles	Дополнительные сведения об ошибках командной строки см. в журнале ScanState или журнале LoadState.
Аргумент повторных попыток должен быть целым числом	Дополнительные сведения об ошибках командной строки см. в журнале ScanState или журнале LoadState.
Указанный аргумент хранилища параметров недопустим	Дополнительные сведения об ошибках командной строки см. в журнале ScanState или журнале LoadState. Убедитесь, что путь к хранилищу

Сообщение об ошибке	Устранение неполадок, устранение рисков, обходные пути
	доступен и заданы соответствующие уровни разрешений.
Указанный алгоритм шифрования не поддерживается	Дополнительные сведения об ошибках командной строки см. в журнале ScanState или журнале LoadState.
Для /efs:hardlink требуется /hardlink	Дополнительные сведения об ошибках командной строки см. в журнале ScanState или журнале LoadState.
Параметр /targetWindows7 доступен только для Windows XP, Windows Vista и Windows 7	Дополнительные сведения об ошибках командной строки см. в журнале ScanState или журнале LoadState.
Параметр хранилища является обязательным, но не указан	Дополнительные сведения об ошибках командной строки см. в журнале ScanState или журнале LoadState.
Сопоставление доменов с исходным кодом недопустимо для /md	Дополнительные сведения об ошибках командной строки см. в журнале ScanState или журнале LoadState.
Сопоставление учетных записей пользователей источника к целевому объекту недопустимо для /mu	Дополнительные сведения об ошибках командной строки см. в журнале ScanState или журнале LoadState.
Параметр неопределенной или неполной командной строки	Дополнительные сведения об ошибках командной строки см. в журнале ScanState или журнале LoadState.
Используйте /nocompress или укажите путь к XML-файлу с помощью /p"pathtoafile", чтобы получить оценку размера сжатого хранилища	Дополнительные сведения об ошибках командной строки см. в журнале ScanState или журнале LoadState.
Недопустимый аргумент исключения пользователя	Дополнительные сведения об ошибках командной строки см. в журнале ScanState или журнале LoadState.
Уровень детализации должен быть указан в виде суммы требуемых параметров журнала: Подробные (0x01), Объекты записи (0x04), Эхо для отладки порта (0x08)	Дополнительные сведения об ошибках командной строки см. в журнале ScanState или журнале LoadState.
Функция теневого копирования томов не поддерживается в хранилище жесткой связи	Дополнительные сведения об ошибках командной строки см. в журнале ScanState или журнале LoadState.

Сообщение об ошибке	Устранение неполадок, устранение рисков, обходные пути
Аргумент задержки ожидания должен быть целым числом	Дополнительные сведения об ошибках командной строки см. в журнале ScanState или журнале LoadState.

12: USMT_ERROR_OPTION_PARAM_TOO_LARGE

- **Категория**: недопустимые командные строки

Развернуть таблицу

Сообщение об ошибке	Устранение неполадок, устранение рисков, обходные пути
Аргументы командной строки не могут превышать 256 символов	Дополнительные сведения об ошибках командной строки см. в журнале ScanState или журнале LoadState.
Указанный путь к хранилищу параметров превышает максимальную допустимую длину 256 символов.	Дополнительные сведения об ошибках командной строки см. в журнале ScanState или журнале LoadState.

13: USMT_INIT_LOGFILE_FAILED

- **Категория**: недопустимые командные строки

Развернуть таблицу

Сообщение об ошибке	Устранение неполадок, устранение рисков, обходные пути
Недопустимый аргумент пути журнала для /l	При `/l` указании в командной строке ScanState USMT проверяет путь. Убедитесь, что диск и другие сведения, например символы файловой системы, верны.

14: USMT_ERROR_USE_LAC

- **Категория**: недопустимые командные строки

Развернуть таблицу

Сообщение об ошибке	Устранение неполадок, устранение рисков, обходные пути
Не удалось создать локальную учетную запись, так как /lac не указан	При создании локальных учетных записей параметры командной строки `/lac` и `/lae` их следует использовать.

26: USMT_INIT_ERROR

- **Категория**: настройка и инициализация

Развернуть таблицу

Сообщение об ошибке	Устранение неполадок, устранение рисков, обходные пути
Найдено несколько установок Windows	Listfiles.txt не удалось создать. Убедитесь, что расположение, указанное для создания этого файла, является допустимым.
Ошибка программного обеспечения или неизвестное исключение	Проверьте все загруженные .xml файлы ошибок, распространенные ошибки при загрузке `/i` *файла Config.xml* .
Не удается найти допустимый каталог Windows для продолжения запрошенной автономной операции; Проверьте наличие автономного входного файла и наличие допустимых записей	Убедитесь, что автономный входной файл присутствует и имеет допустимые записи. USMT не удалось найти допустимую автономную операционную систему. Проверьте сопоставление автономных каталогов.

27: USMT_INVALID_STORE_LOCATION

- **Категория**: настройка и инициализация

Развернуть таблицу

Сообщение об ошибке	Устранение неполадок, устранение рисков, обходные пути
Путь к хранилищу нельзя использовать, так как существующее хранилище существует; укажите /o для перезаписи	Укажите `/o` для перезаписи существующего промежуточного или хранилища миграции.
Путь к хранилищу отсутствует или имеет неполные данные	Убедитесь, что путь к хранилищу доступен и заданы соответствующие уровни разрешений.

Сообщение об ошибке	Устранение неполадок, устранение рисков, обходные пути
Произошла ошибка во время создания хранилища	Убедитесь, что путь к хранилищу доступен и заданы соответствующие уровни разрешений. Укажите `/o` для перезаписи существующего промежуточного или хранилища миграции.
Неуместным устройством, например диском floppy, было указано для хранилища.	Убедитесь, что путь к хранилищу доступен и заданы соответствующие уровни разрешений.
Недопустимый путь к хранилищу; Проверьте параметры хранилища и (или) разрешения файловой системы	Недопустимый путь к хранилищу; Проверьте параметры хранилища и /или разрешения файловой системы.
Макет файла и (или) содержимое файла не распознается как допустимое хранилище.	Убедитесь, что путь к хранилищу доступен и заданы соответствующие уровни разрешений. Укажите `/o` для перезаписи существующего промежуточного или хранилища миграции.
Путь к хранилищу содержит хранилище, несовместимое с текущей версией USMT	Убедитесь, что путь к хранилищу доступен и заданы соответствующие уровни разрешений.
Расположение сохранения хранилища доступно только для чтения или не поддерживает запрошенный вариант хранения.	Убедитесь, что путь к хранилищу доступен и заданы соответствующие уровни разрешений.

28: USMT_UNABLE_GET_SCRIPTFILES

- **Категория**: настройка и инициализация

Развернуть таблицу

Сообщение об ошибке	Устранение неполадок, устранение рисков, обходные пути
Файл скрипта недопустим для /i	Проверьте все указанные файлы миграции .xml для ошибок. Эта ошибка распространена при `/i` загрузке *файла Config.xml* .
Не удается найти файл скрипта, указанный в /i	Проверьте расположение файлов скриптов и убедитесь, что параметры командной строки верны.

29: USMT_FAILED_MIGSTARTUP

- **Категория**: настройка и инициализация

Развернуть таблицу

Сообщение об ошибке	Устранение неполадок, устранение рисков, обходные пути
Для временных файлов требуется не менее 250 МБ свободного места	Убедитесь, что система соответствует минимальному требованию временного места на диске 250 МБ. В качестве обходного решения можно задать переменную `USMT_WORKING_DIR=<path>` среды для перенаправления временного каталога файлов.
Другой процесс — предотвращение миграции; Одновременно может выполняться только одно средство миграции.	Проверьте файл журнала ScanState для ошибок при миграции .xml файлов.
Не удалось запустить основную обработку, найти в журнале системные ошибки или проверить установку	Проверьте файл журнала ScanState для ошибок при миграции .xml файлов.
Сбой миграции из-за ошибки XML; поиск в журнале для конкретных сведений	Проверьте файл журнала ScanState для ошибок при миграции .xml файлов.
Не удается автоматически сопоставить буквы диска с макетом букв в сети; Использование /offline для предоставления таблицы сопоставления	Проверьте файл журнала ScanState для ошибок при миграции .xml файлов.

31: USMT_UNABLE_FINDMIGUNITS

- **Категория**: настройка и инициализация

Развернуть таблицу

Сообщение об ошибке	Устранение неполадок, устранение рисков, обходные пути
Ошибка произошла во время этапа обнаружения; В журнале должны быть более конкретные сведения	Проверьте файл журнала ScanState для ошибок при миграции .xml файлов.

32: USMT_FAILED_SETMIGRATIONTYPE

- **Категория**: настройка и инициализация

Развернуть таблицу

Сообщение об ошибке	Устранение неполадок, устранение рисков, обходные пути
Произошла ошибка при обработке системы миграции	Проверьте файл журнала ScanState для миграции .xml ошибок в файле или используйте веб-справку, введя `/?` в командной строке.

33: USMT_UNABLE_READKEY

- **Категория**: настройка и инициализация

Развернуть таблицу

Сообщение об ошибке	Устранение неполадок, устранение рисков, обходные пути
Ошибка доступа к файлу, указанному параметром /keyfile	Проверьте файл журнала ScanState для миграции .xml ошибок в файле или используйте веб-справку, введя `/?` в командной строке.
Ключ шифрования должен иметь по крайней мере один символ	Проверьте файл журнала ScanState для миграции .xml ошибок в файле или используйте веб-справку, введя `/?` в командной строке.

34: USMT_ERROR_INSUFFICIENT_RIGHTS

- **Категория**: настройка и инициализация

Развернуть таблицу

Сообщение об ошибке	Устранение неполадок, устранение рисков, обходные пути
Удаление каталога требует повышенных привилегий	Войдите от имени администратора и запустите с повышенными привилегиями.
Нет прав на создание профилей пользователей; войдите в систему с правами администратора; выполнение с повышенными привилегиями	Войдите от имени администратора и запустите с повышенными привилегиями.
Нет прав на чтение или удаление профилей пользователей; Войдите в систему от имени администратора, запустите с повышенными привилегиями	Войдите от имени администратора и запустите с повышенными привилегиями.

35: USMT_UNABLE_DELETE_STORE

- **Категория**: настройка и инициализация

Развернуть таблицу

Сообщение об ошибке	Устранение неполадок, устранение рисков, обходные пути
Перезагрузка требуется для удаления хранилища	Перезагрузите все файлы, которые не удалось удалить при выполнении команды.
Не удается использовать путь к хранилищу, так как он содержит данные, которые не могут быть перезаписаны	Не удалось удалить хранилище миграции. Если вы используете хранилище миграции с жесткой связью, в нем может быть заблокирован файл. Необходимо вручную удалить хранилище или использовать `UsmtUtils.exe /rd` команду для удаления хранилища.
Произошла ошибка при удалении хранилища	Дополнительные сведения об ошибках командной строки см. в журнале ScanState или журнале LoadState.

36: USMT_ERROR_UNSUPPORTED_PLATFORM

- **Категория**: настройка и инициализация

Развернуть таблицу

Сообщение об ошибке	Устранение неполадок, устранение рисков, обходные пути
Сбой проверки соответствия требованиям; Проверьте журналы для получения сведений	Проверьте, существует ли активный временный профиль в системе.
Использование /offline не поддерживается во время применения	Команда `/offline` не использовалась при выполнении в среде предварительной установки Windows (WinPE).
Использование /offline для сбора данных на этой платформе	Команда `/offline` не использовалась при выполнении в WinPE.

37: USMT_ERROR_NO_INVALID_KEY

- **Категория**: настройка и инициализация

Развернуть таблицу

Сообщение об ошибке	Устранение неполадок, устранение рисков, обходные пути
Хранилище содержит зашифрованные данные, но правильный ключ шифрования не был предоставлен.	Убедитесь, что правильный ключ шифрования или файл ключа был включен в `/key` параметр или `/keyfile` параметр.

38: USMT_ERROR_CORRUPTED_NOTENCRYPTED_STORE

- **Категория**: настройка и инициализация

Развернуть таблицу

Сообщение об ошибке	Устранение неполадок, устранение рисков, обходные пути
Произошла ошибка во время доступа к хранилищу	Дополнительные сведения об ошибках командной строки см. в журнале ScanState или журнале LoadState. Убедитесь, что путь к хранилищу доступен и заданы соответствующие уровни разрешений.

39: USMT_UNABLE_TO_READ_CONFIG_FILE

- **Категория**: настройка и инициализация

Развернуть таблицу

Сообщение об ошибке	Устранение неполадок, устранение рисков, обходные пути
Ошибка чтения Config.xml	Дополнительные сведения об ошибках командной *строки в файле Config.xml* см. в журнале ScanState или журнале LoadState.
Недопустимый аргумент файла для /config	Проверьте командную строку, используемую *для загрузки файла Config.xml* . Вы можете использовать веб-справку, введя `/?` в командной строке.

40: USMT_ERROR_UNABLE_CREATE_PROGRESS_LOG

- **Категория**: настройка и инициализация

Развернуть таблицу

Сообщение об ошибке	Устранение неполадок, устранение рисков, обходные пути
Ошибка записи в журнал хода выполнения	Не удалось создать журнал хода выполнения. Убедитесь, что расположение является допустимым и у вас есть доступ на

Сообщение об ошибке	Устранение неполадок, устранение рисков, обходные пути
	запись.
Недопустимый аргумент журнала выполнения для /progress	Не удалось создать журнал хода выполнения. Убедитесь, что расположение является допустимым и у вас есть доступ на запись.

41: USMT_PREFLIGHT_FILE_CREATION_FAILED

- **Категория**: настройка и инициализация

Развернуть таблицу

Сообщение об ошибке	Устранение неполадок, устранение рисков, обходные пути
Не удается перезаписать существующий файл	Не удалось создать журнал хода выполнения. Убедитесь, что расположение является допустимым и у вас есть доступ на запись.
Недопустимый путь оценки пространства. Проверка параметров и (или) разрешений файловой системы	Дополнительные сведения об ошибках командной строки см. в журнале ScanState или журнале LoadState.

42: USMT_ERROR_CORRUPTED_STORE

- **Категория:**

Развернуть таблицу

Сообщение об ошибке	Хранилище содержит один или несколько поврежденных файлов.
Хранилище содержит зашифрованные данные, но правильный ключ шифрования не был предоставлен.	Дополнительные сведения о поврежденных файлах см. в журнале UsmtUtils. Сведения о том, как извлечь файлы, которые не повреждены, см. в статье "Извлечение файлов из сжатого хранилища миграции USMT".

61: USMT_MIGRATION_STOPPED_NONFATAL

- **Категория**: неустранимая ошибка

Развернуть таблицу

Сообщение об ошибке	Хранилище содержит один или несколько поврежденных файлов.
Обработка остановлена из-за ошибки ввода-вывода	USMT завершил работу, но может продолжить работу с `/c` параметром командной строки с дополнительным **<настраиваемым разделом ErrorControl>** или с помощью параметра командной `/vsc` строки.

71: USMT_INIT_OPERATING_ENVIRONMENT_FAILED

- **Категория**: неустранимая ошибка

Развернуть таблицу

Сообщение об ошибке	Устранение неполадок, устранение рисков, обходные пути
Произошла ошибка API Windows Win32	Передача данных началась, и во время создания хранилища миграции или во время применения произошла ошибка. Дополнительные сведения см. в журнале ScanState или журнале LoadState.
Ошибка при попытке инициализации механизмов диагностики, таких как журнал	Передача данных началась, и во время создания хранилища миграции или во время применения произошла ошибка. Дополнительные сведения см. в журнале ScanState или журнале LoadState.
Не удалось записать диагностические сведения	Передача данных началась, и во время создания хранилища миграции или во время применения произошла ошибка. Дополнительные сведения см. в журнале ScanState или журнале LoadState.
Не удается запустить. Убедитесь, что вы используете USMT с повышенными привилегиями	Выйдите из USMT и снова войдите с повышенными привилегиями.

72: USMT_UNABLE_DOMIGRATION

- **Категория**: неустранимая ошибка

Развернуть таблицу

Сообщение об ошибке	Устранение неполадок, устранение рисков, обходные пути
Произошла ошибка при закрытии хранилища	Передача данных началась и произошла ошибка во время создания хранилища миграции или на этапе применения. Дополнительные сведения см. в журнале ScanState или журнале LoadState.

Сообщение об ошибке	Устранение неполадок, устранение рисков, обходные пути
Произошла ошибка в процессе применения	Передача данных началась и произошла ошибка во время создания хранилища миграции или на этапе применения. Дополнительные сведения см. в журнале ScanState или журнале LoadState.
Произошла ошибка в процессе сбора	Передача данных началась и произошла ошибка во время создания хранилища миграции или на этапе применения. Дополнительные сведения см. в журнале ScanState или журнале LoadState.
Свободное место на диске при записи хранилища	Передача данных началась и произошла ошибка во время создания хранилища миграции или на этапе применения. Дополнительные сведения см. в журнале ScanState или журнале LoadState.
Вне временного места на диске локальной системы	Передача данных началась и произошла ошибка во время создания хранилища миграции или на этапе применения. Дополнительные сведения см. в журнале ScanState или журнале LoadState.

Сбор данных

Если вам нужна помощь службы поддержки Microsoft, мы рекомендуем собирать информацию путем выполнения действий, описанных в разделе Сбор информации с помощью TSS для решения проблем, связанных с развертыванием.

Связанные статьи

Устранение неполадок средства миграции пользовательского состояния (USMT)

Файлы журнала USMT

Ресурсы USMT

Статья • 29.01.2025 • Применяется к: ✅ Windows 11, ✅ Windows 10

Веб-ресурсы USMT

- Заметки о выпуске ADK.
- Microsoft Visual Studio
  - Схему XML средства миграции пользовательской среды (USMT) (`MigXML.xsd` файл) можно использовать для **проверки.xmlфайлов** миграции с помощью средства разработки XML, например Microsoft Visual Studio.

    Дополнительные сведения об использовании схемы со средой разработки XML см. в документации по среде.
- Обратитесь к блогу группы по службам каталогов.
- Форумах:
  - Форум по набору средств развертывания Майкрософт.
  - Configuration Manager форуме по развертыванию операционной системы.

Связанные статьи

Обзор средства миграции пользовательской среды (USMT).

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте