Оставьте отзыв о скачивании PDF-файла.

Документация по Windows 365 Корпоративная

Техническая документация по официальному продукту Windows 365 Корпоративная

ОБЗОР
Что такое Windows 365 Корпоративн...

ОБЗОР
Что нового в Windows 365 Корпоративн...

ОБЗОР
Функции в разработке

НАЧАЛО...
Планирование развертывания Windows 365

ПРАКТИЧЕС...
Требования

ОБЗОР
Что такое подготовка?

Планирование

- Руководство по планированию
- Требования
- Управление доступом на основе ролей
- Рекомендации о размере облачного компьютера

Посмотреть больше >

Настройка Windows 365

- Действия по развертыванию
- Назначение лицензий пользователям
- Создать сетевое подключение Azure
- Добавление изображений устройства

Посмотреть больше >

Подготовка облачных компьютеров

- Создание политики подготовки
- Этапы автоматической подготовки

Посмотреть больше >

Безопасность Windows 365

- Рекомендации по безопасности

Приложения в Windows 365

- Обзор приложений
- Назначение приложений облачным компьютерам

Управление устройствами Windows 365

- Обзор управления устройствами

Развертывание базовой конфигурации безопасности

Настройка политик условного доступа

Посмотреть больше

Microsoft Teams на обласном компьютере

Посмотреть больше

Дистанционное управление устройствами с Windows 365

Повторное предоставление облачного компьютера

Посмотреть больше

Дополнительные ресурсы, связанные с Windows 365

Клиент Windows для ИТ-специалистов

Документация по клиенту Windows для ИТ-специалистов

Развертывание и обновление клиента Windows

Настройка клиента Windows

Блоги о Windows

семейство продуктов Microsoft Intune

документация по семейству продуктов Microsoft Intune

Общие сведения о семье Microsoft Intune

блог Microsoft Intune

Microsoft 365

Ознакомьтесь с Microsoft 365, полным решением, в которое входит Intune

Документация по Microsoft 365 корпоративный

Базовая инфраструктура Microsoft 365 корпоративный

Управление облачными компьютерами в Microsoft 365 Lighthouse для поставщиков управляемых услуг (MSP)

Microsoft Entra ID

Документация по управлению пользователями

Документация по проверке подлинности

Документация по удостоверениям устройств

Документация по гибридным удостоверениям

Что такое Windows 365 Корпоративная?

Статья • 31.01.2025

Windows 365 Корпоративная — это облачная служба, которая автоматически создает новый тип виртуальной машины Windows (Облачные компьютеры) для конечных пользователей. Она предоставляет реализованные в Microsoft 365 преимущества повышения производительности, обеспечения безопасности и совместной работы. Windows 365 Корпоративная использует:

- Microsoft Intune для управления облачными компьютерами.
- Microsoft Entra ID для управления удостоверениями и доступом.
- Виртуальный рабочий стол Azure для удаленного подключения.

Каждый облачный компьютер назначается отдельному пользователю и является его выделенным устройством Windows. Назначение пользователю Облачного компьютера аналогично назначению почтового ящика Exchange Online. При назначении лицензии Windows 365 пользователю:

- Автоматически начинается подготовка нового облачного компьютера.
- Облачный компьютер зарегистрирован в Microsoft Intune.

С помощью службы Windows 365 можно выполнять следующие задачи:

- Автоматически подготавливать облачные компьютеры с Windows Корпоративная по запросу пользователей. Подготовка — это автоматическое создание облачных компьютеров для конечных пользователей. После настройки поддержки облачных компьютеров в Microsoft Intune облачный компьютер автоматически подготавливается при назначении пользователя с лицензией на облачный компьютер соответствующей группе Microsoft Entra пользователей. Для настройки поддержки облачного компьютера выполняются следующие действия.
  - [Необязательно] Создание сетевых подключений Azure , которые являются связями между облачными компьютерами и вашими локальными ресурсами.
  - Выбор встроенного оптимизированного образа Windows (или создание собственного), который будет использоваться в качестве основы для каждого облачного компьютера.

- Управляйте облачными компьютерами, как и другими устройствами вашей организации в Microsoft Intune. В зависимости от вашей конфигурации

облачные компьютеры:

  - Присоединено к корпоративному домену Active Directory и синхронизировано с Microsoft Entra ID.
  - Непосредственно присоединено к Microsoft Entra ID.

  Независимо от типа соединения облачные компьютеры полностью управляются Microsoft Intune. Windows 365 полностью интегрирован в Центр администрирования Microsoft Intune. Облачные компьютеры легко управляются на Microsoft Intune, как и любое другое поддерживаемое устройство, включая конфигурацию, приложения и обновления.

- Настраивать политики подготовки для создания пользовательских конфигураций облачных компьютеров.

- Использовать группы устройств, политики и базовые показатели безопасности для настройки конфигураций облачных компьютеров для поддержки различных потребностей пользователей.

- Предварительно установите приложения в пользовательском образе облачного компьютера и отправьте к ним другие приложения через Microsoft Intune.

Другие версии Windows 365

Существуют и другие версии, доступные для Windows 365. Дополнительные сведения см. в статье Что такое Windows 365?.

Что такое Облачный компьютер?

Облачный компьютер — это высокодоступная, оптимизированная и масштабируемая виртуальная машина, предоставляющая пользователям широкие возможности рабочего стола Windows. Он размещается в службе Windows 365 и доступен из любого места на любом устройстве.

Между конечным пользователем и Облачным компьютером действует отношение 1 : 1. Это собственный персональный компьютер пользователя в облаке. Пользователи могут подключаться к своим облачным компьютерам, используя сайт windows365.microsoft.com. Для устройств Windows, Mac, iOS и Android действует доступ через браузер и доступ на основе приложений. Пользователи на базе стола также могут использовать Windows 365 Link для безопасного подключения к Облачный компьютер Windows 365 за считанные секунды.

Создание Облачного компьютера

Облачные компьютеры автоматически создаются службой Windows 365, когда конечному пользователю в соответствующей группе пользователей Microsoft Entra назначается лицензия на Windows 365.

Администраторы не создают Облачные компьютеры вручную.

Выставление счетов

Счета за облачные компьютеры выставляются по модели "на пользователя в месяц". Эта модель означает, что организации не нужно управлять изменениями стоимости вычислений и хранения данных, характерными для традиционной модели размещенного рабочего стола.

По умолчанию облачные компьютеры присоединяются к корпоративному домену Active Directory, синхронизируются с Microsoft Entra ID и полностью управляются Microsoft Intune.

Microsoft 365 Lighthouse

Поставщики управляемых серверов (MSP) могут управлять облачными компьютерами для арендаторов своих клиентов в Microsoft 365 Lighthouse. Дополнительные сведения см. в статье Обзор страницы Windows 365 (облачные компьютеры).

Дальнейшие действия

Запланируйте развертывание Облачного компьютера.

Если вам нужна документация по Windows 365 для бизнеса, см. статью Начало работы с Windows 365 для бизнеса и облачными компьютерами.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Что нового в Windows 365 Enterprise

05.08.2025

Узнайте о новых возможностях в Windows 365 Enterprise.

> ⓘ **Примечание**
>
> Каждое ежемесячное обновление может быть развернуто в течение нескольких недель и может быть доступно не сразу для всех клиентов.

Сведения о Windows App и его функциях см. в статье Новые возможности Windows App.

Дополнительные сведения об элементах общедоступной предварительной версии см. в разделе Общедоступная предварительная версия в Windows 365.

Неделя с 4 августа 2025 г.

Управление устройствами

Восстановление Windows 365 Корпоративная облачных компьютеров, которые были отменены из-за истечения срока действия лицензии (предварительная версия)

Теперь вы можете восстановить облачные компьютеры с Windows 365 Enterprise, которые были отменены из-за истечения срока действия лицензии. После повторного выкупа просроченных лицензий и соблюдения предварительных требований вы можете использовать snapshot хранения для восстановления облачного компьютера для конечного пользователя. Дополнительные сведения см. в статье Восстановление до состояния на определенный момент времени для Windows 365 Корпоративная.

Безопасность устройства

Выбор перенаправлений, отключенных для недавно подготовленных и повторно подготовленных облачных компьютеров

Windows 365 повышает безопасность облачных компьютеров, так как буфер обмена, диск, непрозрачные низкоуровневые USB-подключения и перенаправления принтеров

отключены по умолчанию для всех вновь подготовленных и повторно подготовленных облачных компьютеров. Это изменение сводит к минимуму риск кражи данных и внедрения вредоносных программ, что обеспечивает более безопасный интерфейс и соответствует принципу Microsoft Secure Future Initiative (SFI) и включает и применяет защиту безопасности по умолчанию.

Дополнительные сведения см. в разделе Управление перенаправлениями устройств RDP для облачных компьютеров.

Неделя с 30 июня 2025 г. (выпуск службы 2506)

Управление устройствами

Два новых языковых пакета интерфейса для облачных компьютеров

Английский (Ирландия) и английский (Австралия) теперь доступны в качестве языковых пакетов, которые можно использовать в политиках подготовки для настройки языка интерфейса по умолчанию для облачных компьютеров. Дополнительные сведения см. в статье Использование политики подготовки для настройки языка интерфейса по умолчанию на облачных компьютерах.

Windows 365 Frontline

Интеллектуальный предварительный запуск для Windows 365 Frontline в выделенном режиме (предварительная версия)

Windows 365 Frontline облачные компьютеры могут прогнозировать, когда пользователь подключается и предварительно запускает облачный компьютер перед подключением . Этот прогноз повышает время подключения для облачных компьютеров таких пользователей. Дополнительные сведения см. в разделе Интеллектуальный предварительный запуск для Windows 365 Frontline в выделенном режиме.

Настройка часовых поясов, отличных от UTC, для массовой повторной подготовки для Windows 365 Frontline облачных компьютеров в общем режиме

Теперь можно настроить часовые пояса, отличные от UTC, при планировании массовой повторной подготовки для Windows 365 Frontline облачных компьютеров в общем

режиме. Дополнительные сведения см. в статье Планирование массовой повторной подготовки облачных компьютеров Frontline в общем режиме.

Неделя с 23 июня 2025 г.

Управление устройствами

Аварийное восстановление между регионами для Windows 365 Frontline в выделенном режиме (предварительная версия)

Windows 365 Frontline в выделенном режиме теперь поддерживает аварийное восстановление между регионами. Дополнительные сведения см. в разделе Аварийное восстановление между регионами в Windows 365.

Неделя с 2 июня 2025 г.

Управление устройствами

Поддержка аппаратного ускорения видео с высокой эффективностью (H.265)

Windows 365 SKU Super и Max с поддержкой GPU теперь поддерживают ускорение графического модуля обработки (GPU) для кодирования кадров с помощью HEVC/H.265. Ускорение GPU улучшает графические возможности при использовании протокола удаленного рабочего стола (RDP) с совместимыми облачными компьютерами с поддержкой GPU.

Дополнительные сведения см. в разделах Облачные компьютеры GPU в Windows 365 и Включение ускорения GPU для Виртуального рабочего стола Azure.

Windows 365 Frontline управление параллелизмом в выделенном режиме теперь общедоступно

Windows 365 Frontline управления параллелизмом выделенного режима вышел из предварительной версии и стал общедоступным. Дополнительные сведения см. в разделе Управление параллелизмом.

Поддержка Teams VDI 1.0 в iOS (предварительная версия)

Windows 365 теперь поддерживает Teams VDI 1.0 в iOS. Дополнительные сведения см. в статье Microsoft Teams на облачном компьютере.

Неделя с 28 мая 2025 г. (выпуск службы 2505)

Управление и устранение неполадок

Отчет об использовании облачных компьютеров: новые параметры агрегированного времени подключения

Теперь вы можете:

- Выберите интервалы времени в 28, 60 и 90 дней для агрегированных подключенных данных времени.
- См. раздел Облачные компьютеры, к которым еще никто не подключен.

Дополнительные сведения см. в статье Отчет об использовании облачных компьютеров.

Ход выполнения пакетного отчета о состоянии действия облачного компьютера теперь общедоступен

Следующая функция была переведена из предварительной версии и стала общедоступной:

В отчете о состоянии действия облачного компьютера отображаются пакеты устройств, на которых были активированы действия. Вы можете просмотреть текущий ход выполнения пакета. Дополнительные сведения см. в статье Отчет о действиях облачного компьютера.

Работа конечных пользователей

windows365.microsoft.com заменяются Windows App

Портал windows365.microsoft.com конечных пользователей в настоящее время не рекомендуется использовать. Переход к windows365.microsoft.com автоматически перенаправляется в Windows App в Интернете. Прекращение поддержки будет завершено 1 июня 2025 г. (Windows 365 пользователи для государственных организаций по-прежнему могут получать доступ к порталу конечных пользователей.)

Неделя с 28 апреля 2025 г. (выпуск службы 2504)

Управление устройствами

Руководство по размещению облачного компьютера под проверкой

Соблюдайте правило 17a-4 SEC, настроив хранилище BLOB-объектов Azure для неизменяемости. Дополнительные сведения см. в разделах Размещение облачного компьютера под проверкой и Отчет Azure — Cohasset Assessment — WORM Storage (2024).

Изменение размера Windows 365 Frontline облачных компьютеров в указанном режиме (предварительная версия)

Теперь администраторы могут изменять размер Windows 365 Frontline облачных пк в указанном режиме. Дополнительные сведения см. в статье Изменение размера Windows 365 Frontline облачных компьютеров в выделенном режиме.

Безопасность устройств

Credential Guard и HVCI включены по умолчанию

На недавно подготовленных и повторно подготовленных облачных компьютерах, работающих с образом Windows 11 коллекции, по умолчанию включены VBS, HVCI и Credential Guard. Дополнительные сведения см. в статье Безопасность Windows365.

Управление и устранение неполадок

Отчет подключенных облачных компьютеров frontline является общедоступным

Отчет подключенных облачных компьютеров frontline вышел из предварительной версии и стал общедоступным. Дополнительные сведения см. в разделе Отчет подключенных облачных компьютеров Frontline.

Windows App

Защита маркеров (предварительная версия) в Windows App на устройствах Windows

Теперь можно использовать политику условного доступа, чтобы требовать защиту маркеров для маркеров входа (маркеров обновления) на устройствах Windows. Такие политики могут уменьшить количество атак с помощью кражи маркеров, гарантируя, что маркер можно использовать только с предполагаемого устройства. Дополнительные сведения см. в разделе Microsoft Entra защита маркеров условного доступа.

Неделя с 21 апреля 2025 г.

Управление устройствами

Перемещение выбранных облачных компьютеров из одного региона или сетевого подключения Azure в другой

Теперь вы можете перемещать выбранные облачные компьютеры из одного региона или сетевого подключения Azure (ANC) в другой. Дополнительные сведения см. в разделе Перемещение облачного компьютера.

Подготовка устройств

Предупреждение о создании процесса политики подготовки из-за отсутствия лицензий Windows 365 Frontline

При создании политики подготовки для Windows 365 Frontline облачных компьютеров процесс теперь выдает предупреждение, если у клиента нет Windows 365 Frontline лицензий.

Документация

Новая статья документации: Роли и обязанности майкрософт и клиентов для Windows 365

Мы создали новую статью. Дополнительные сведения см. в статье Роли и обязанности майкрософт и клиентов для Windows 365.

Неделя с 14 апреля 2025 г.

Управление устройствами

Состояние работоспособности для точки восстановления облачного компьютера

Теперь вы можете просмотреть состояние работоспособности точек восстановления облачного компьютера, прежде чем принимать решение о начале восстановления. Дополнительные сведения см. в статьях Восстановление одного облачного компьютера до предыдущего состояния и Массовое восстановление нескольких облачных компьютеров.

Управление и устранение неполадок

Оповещение об использовании буфера параллелизма

Вы можете настроить новое оповещение для отслеживания использования буфера параллелизма для Windows 365 Frontline в выделенном режиме.

Обновление отчета о параллелизме облачных компьютеров

В отчете Подключенные облачные компьютеры frontline теперь отображается длина сеанса пользователя. Вы также можете перезапустить Windows 365 Frontline облачных компьютеров из отчета, если достигнут максимальный параллелизм для любых индивидуальных назначений. Дополнительные сведения см. в разделе Отчет подключенных облачных компьютеров Frontline.

Неделя с 7 апреля 2025 г.

правительство Windows 365

поддержка тегов область Windows 365 для государственных организаций

Windows 365 правительство теперь поддерживает теги область.

Неделя с 31 марта 2025 г. (выпуск службы 2503)

Управление устройствами

Каждый раз, когда частота входа теперь становится общедоступной

Параметр "Частота входа каждый раз" вышел из предварительной версии и стал общедоступным. Дополнительные сведения см. в разделе Настройка политик условного доступа.

Изменение параметра производительности визуальных эффектов по умолчанию

Теперь для параметра Производительность визуальных эффектов по умолчанию **выбрано значение Разрешить Windows выбрать оптимальный вариант для моего компьютера**.

Windows 365 варианты аварийного восстановления

Теперь у администраторов есть два варианта аварийного восстановления: существующее аварийное восстановление между регионами и новое аварийное восстановление плюс. Последний выделяет второй облачный компьютер во время настройки, что улучшает RTO. Так как облачный компьютер для восстановления уже существует, на момент сбоя не существует риска емкости. Дополнительные сведения см. в разделе Аварийное восстановление Windows 365.

Подготовка

Диск данных не разрешен для пользовательских образов

Отправка пользовательского образа с подключенными управляемыми дисками данных больше не допускается для Windows 365 пользовательских образов.

Windows 365 Frontline

Windows 365 Frontline облачных компьютеров в режиме общего доступа теперь общедоступен

Windows 365 Frontline облачные компьютеры в режиме общего доступа вышли из предварительной версии и перешли в общедоступную версию. Дополнительные сведения см. в разделе Windows 365 Frontline в режиме общего доступа.

Связывание подготовки устройства Autopilot с Windows 365 Frontline облачными компьютерами в общем режиме

Теперь вы можете связать подготовку устройства Autopilot с Windows 365 Frontline облачными компьютерами в общем режиме. Дополнительные сведения см. в статье Использование подготовки устройства Autopilot на основе политик с Windows 365 компьютеров Front Cloud в общем режиме.

Работа конечных пользователей

Возврат к локальному рабочему столу

В режиме загрузки Windows 365 (только Windows 11) пользователи теперь могут вернуться к физическому рабочему столу устройства с любого из следующих вариантов:

- Экран CTRL-ALT-DEL
- Экраны ошибок облачного компьютера

Администраторы могут настроить эту функцию в интерактивном сценарии загрузки.

Windows App

Доступ к Windows App с помощью Edge на личных устройствах Windows с помощью MAM

Теперь вы можете включить защищенный доступ управления мобильными приложениями (MAM) к Windows App с помощью Microsoft Edge на личных устройствах Windows. Дополнительные сведения см. в статье Требование обеспечения безопасности локального клиентского устройства с помощью Microsoft Intune и условного доступа Microsoft Entra.

Неделя с 17 марта 2025 г.

Управление устройствами

Повышение производительности перенаправления

Теперь администраторы могут настроить повышение производительности для перенаправления дисков Windows App в операционных системах Windows.

Дополнительные сведения см. в статье Настройка перенаправления фиксированных, съемных и сетевых дисков по протоколу удаленного рабочего стола.

Неделя с 10 марта 2025 г.

Подготовка

Windows 365 поддержка центральной Мексики

Windows 365 Корпоративная теперь поддерживает центрально-мексиканский регион в географическом регионе Центральной Америки. Дополнительные сведения см. в статье Поддерживаемые регионы Azure для подготовки облачных компьютеров.

Windows 365 поддержка центральной Испании

Windows 365 Корпоративная теперь поддерживает регион Центральной Испании в географическом регионе Европейского союза. Дополнительные сведения см. в статье Поддерживаемые регионы Azure для подготовки облачных компьютеров.

Неделя с 26 февраля 2025 г. (выпуск службы 2502)

Windows App

Поддержка устройств FIDO и ключей доступа в Android (предварительная версия)

Windows App и приложение удаленного рабочего стола для Android теперь поддерживают устройства FIDO и ключи доступа для Microsoft Entra ID входа на устройствах с брокером и без брокера. Дополнительные сведения см. в статье Сравнение функций Windows App на разных платформах и устройствах.

Intune поддержка управления мобильными приложениями (MAM) на Windows App в Android (предварительная версия) для устройств под управлением Android 15

Intune политики MAM теперь можно применять к Windows App в Android (предварительная версия), когда устройство работает на Android 15. Ранее Windows App могли работать на Android 15, но политики MAM не вступают в силу.

Неделя с 3 февраля 2025 г. (выпуск службы 2501)

Управление устройствами

Выбор уровня доступа к хранилищу при размещении облачного компьютера под проверкой

Чтобы снизить затраты на хранение, теперь можно выбрать горячий, холодный, холодный и архивный уровни при размещении облачного компьютера под проверкой. Для обеспечения соответствия требованиям теперь также можно поместить облачный компьютер под проверку на горячий, холодный и холодный уровни доступа, настроенные с поддержкой неизменяемости.

Фильтр "Новый тип устройства" на странице "Все облачные компьютеры"

Новый фильтр "Тип устройства" на странице "Все облачные компьютеры" позволяет фильтровать результаты по типу облачного компьютера (Enterprise, Frontline, Dev Box, Power Automate).

Подготовка

Windows 365 поддержка Западной Японии

Windows 365 Корпоративная будет поддерживать западный регион Японии в географическом регионе Японии. Дополнительные сведения см. в статье Поддерживаемые регионы Azure для подготовки облачных компьютеров.

Планирование массовой повторной подготовки для Windows 365 Frontline облачных компьютеров в общем режиме

Теперь вы можете запланировать массовую повторную подготовку для Windows 365 Frontline облачных компьютеров в общем режиме. Дополнительные сведения см. в статье

Массовая повторная подготовка Windows 365 Frontline облачных компьютеров в общем режиме.

Windows 365 Frontline

Более точное управление параллелизмом Windows 365 Frontline

Теперь можно выделять параллельные сеансы для Windows 365 Frontline облачных компьютеров в выделенном режиме для каждой группы Microsoft Entra, назначенной в политике подготовки. Это позволяет зарезервировать сеансы для определенных групп, чтобы сеансы не потреблялись другими группами, а также управлять максимальными ограничениями параллелизма.

Неделя с 17 декабря 2024 г.

Управление устройствами

Восстановление, перезапуск и устранение неполадок на облачных компьютерах с недоступными отчетами

Теперь вы можете использовать команду **Массовые действия устройства** на **облачных компьютерах, которые недоступны** отчет, для восстановления, перезапуска и устранения неполадок непосредственно из отчета. Дополнительные сведения см. в статье Облачные компьютеры, которые недоступны в отчете.

Неделя с 9 декабря 2024 г.

Управление устройствами

Перемещение выбранных облачных компьютеров в новый регион

Теперь вы можете переместить выбранные облачные компьютеры в новый регион. Это вместо перемещения всех облачных компьютеров в политику подготовки.

Неделя с 2 декабря 2024 г. (выпуск службы 2411)

Управление устройствами

теги Intune область теперь общедоступны

Windows 365 поддержка тегов Intune область вышла из предварительной версии и стала общедоступной. Дополнительные сведения см. в разделе Теги области.

Создание точек восстановления и совместное использование для 5 000 облачных компьютеров

Теперь можно массово создавать точки восстановления для до 5000 облачных компьютеров. Затем вы можете предоставить доступ к точкам восстановления указанной учетной записи хранения Azure. Дополнительные сведения см. в статье Массовое создание нескольких точек восстановления вручную.

Управление и устранение неполадок

Отчет о выделенных и общих данных на подключенных облачных компьютерах Frontline

В отчете Подключенные облачные компьютеры frontline теперь показано:

- Разделение данных для выделенных и общих облачных компьютеров Frontline.
- Пользователь, который подключен в данный момент, и его продолжительность сеанса
- Возможность перезапуска компьютеров Frontline Cloud для отключения пользователя от сеанса и превышения пороговых значений параллелизма.

Дополнительные сведения см. в разделе Подключенные облачные компьютеры Frontline.

Поддержка отчетов о действиях облачных компьютеров для перемещения облачных компьютеров

Отчет о действиях облачного компьютера можно использовать для просмотра состояния перемещения облачных компьютеров в новые регионы.

Windows 365 для государственных организаций поддерживает массовое устранение неполадок

Удаленное действие "Устранение неполадок" теперь можно использовать в пакетном режиме с Windows 365 для государственных организаций. Дополнительные сведения см. в статье Удаленное управление Windows 365 устройствами.

Подготовка

Увеличено ограничение сетевого подключения Azure

Увеличено ограничение сетевого подключения Azure для каждого клиента. Дополнительные сведения см. в статье Максимальное число сетевых подключений Azure.

Подготовка

Windows 365 теперь поддерживает центральную часть Израиля

Windows 365 Корпоративная теперь поддерживает Центральный регион Израиля в географии Ближнего Востока. Дополнительные сведения см. в статье Поддерживаемые регионы Azure для подготовки облачных компьютеров.

Неделя с 19 ноября 2024 г.

Windows 365 Frontline

Windows 365 Frontline в режиме общего доступа (предварительная версия)

Windows 365 Frontline в режиме общего доступа позволяет подготавливать коллекцию облачных компьютеров, которую можно использовать для нескольких пользователей, сопоставленных с группой Microsoft Entra ID. Для каждой лицензии разрешен один активный облачный компьютер. Дополнительные сведения см. в разделе Windows 365 Frontline в режиме общего доступа.

Управление устройствами

Настройка параметров перенаправления клиентских устройств для Windows App в iOS,iPadOS/Android с помощью Microsoft Intune

Теперь вы можете использовать управление мобильными приложениями Microsoft Intune для проверка для состояния устройств и управления перенаправлениями для Windows App в iOS, iPadOS и Android (предварительная версия). Вы можете использовать Microsoft Intune как на корпоративных управляемых, так и на личных устройствах.

Безопасность устройств

Поддержка устройств FIDO и ключей доступа в macOS и iOS

Windows App и приложение удаленного рабочего стола для macOS и iOS теперь поддерживают устройства FIDO и ключи доступа для Microsoft Entra ID входа на устройствах с брокером и устройствах без брокера. Дополнительные сведения см. в статье Поддержка проверки подлинности FIDO2 с помощью Microsoft Entra ID.

Партнеры

Использование Citrix HDX Plus с Windows 365 Frontline

Теперь вы можете использовать Citrix HDX Plus с Windows 365 Frontline облачными компьютерами.

Неделя с 28 октября 2024 г. (выпуск службы 2410)

Управление устройствами

Массовое устранение неполадок теперь общедоступное действие

Действие "Устранение неполадок" в пакетном режиме перешло из предварительной версии и стало общедоступным.

Дополнительные сведения см. в статье Удаленное управление Windows 365 устройствами.

Удаленный рабочий стол (Майкрософт) клиент iOS теперь поддерживает перенаправление интеллектуальной карта Yubikey

Клиент iOS Удаленный рабочий стол (Майкрософт) теперь поддерживает перенаправление интеллектуального карта для YubiKeys с помощью usb-C или Lightning connector. Это позволяет использовать интеллектуальные карта в сеансе.

Управление и устранение неполадок

Отчет о состоянии действия "Обновление до облачного компьютера"

В отчете о состоянии действия Cloud PC теперь отображаются пакеты устройств, на которых были активированы действия. Вы можете просмотреть текущий ход выполнения пакета. Дополнительные сведения см. в статье Отчет о действиях облачного компьютера .

Неактивное состояние сетевых подключений Azure

Сетевые подключения Azure, удовлетворяющие одно из следующих условий в течение более четырех недель, теперь помечаются как неактивные:

- ANC, которые не связаны с политиками подготовки.
- AnCs с политиками подготовки, с которыми не связаны облачные компьютеры.

Отчет о качестве подключения к облачному компьютеру теперь доступен для Windows 365 государственных организаций

Отчет о качестве подключения к облачному компьютеру теперь доступен для Windows 365 для государственных организаций, облака сообщества государственных организаций (GCC) и GCC-High. Дополнительные сведения см. в разделе Отчет о качестве подключения к облачному компьютеру.

Неделя с 21 октября 2024 г.

Windows 365 поддержка смешанного режима AVC, если MMR не включен (предварительная версия)

Смешанный режим AVC теперь доступен в графическом профиле по умолчанию. Если MMR не включен, AVC/h.264 используется для кодирования обнаруженного содержимого изображения вместо кодировщика изображений RemoteFX. Это повышает производительность при кодировании изображений относительно скорости и частоты кадров в сценариях с ограничением сети.

Неделя с 14 октября 2024 г.

Безопасность устройств

Новая IP-подсеть Windows 365 для подключения по протоколу RDP

Трафик RDP на основе core TCP для подключений к облачному компьютеру использует полное доменное имя (FQDN) с подстановочным знаком *.wvd.microsoft.com. Полное доменное имя остается неизменным, но базовые IP-адреса, связанные с ним, вскоре будут изменены на одну подсеть. Это упростит оптимизацию этого трафика и уменьшит потребность в управлении изменениями в будущем.

Управление устройствами

Перенаправление вызовов

Windows 365 теперь поддерживает перенаправление вызовов мультимедиа. Дополнительные сведения см. в разделе Использование перенаправления мультимедиа.

Партнеры

HP Anyware для Windows 365 теперь общедоступен

HP Anyware для Windows 365 вышел из предварительной версии и стал общедоступным.

Дополнительные сведения см. в статье Настройка HP Anyware для Windows 365 Корпоративная

Неделя с 30 сентября 2024 г. (выпуск службы 2409)

Управление и устранение неполадок

Отчет "Недоступные облачные компьютеры", добавленный на страницу обзора отчетов

Отчет о **недоступных облачных компьютерах** был добавлен на страницу **Обзор облачных компьютеров Отчеты**>.

Подготовка устройств

Windows 11 образы из коллекции облачных компьютеров 24H2

Для подготовки новых устройств доступны последние образы Windows Enterprise 24H2. Вы можете обновить политики подготовки, чтобы использовать любой из следующих образов:

- Windows 11 Корпоративная 24H2
- Windows 11 Корпоративная + Приложения Microsoft 365 24H2

Неделя с 23 сентября 2024 г.

Управление устройствами

облачные компьютеры Windows 11 теперь поддерживают EN-NZ

Windows 365 облачные компьютеры теперь поддерживают EN-NZ для Windows 11.

Неделя с 16 сентября 2024 г.

Управление устройствами

Поддержка симметричного NAT с RDP Shortpath

RDP Shortpath в Windows 365 теперь поддерживает установку непрямого UDP-подключения с помощью обхода с использованием ретрансляторов вокруг NAT (TURN) для симметричного NAT. TURN — это популярный стандарт для сетевых подключений с устройства на устройство с низкой задержкой и высокой пропускной способностью с помощью Службы коммуникации Azure. Дополнительные сведения о TURN и Службы коммуникации Azure см. в разделе Основные понятия обхода сети. Дополнительные сведения о RDP Shortpath см. в статье Использование RDP Shortpath для общедоступных сетей с Windows 365.

Windows 365 поддержка программирования видео HEVC

Windows 365 будет поддерживать аппаратное кодирование видео с высокой эффективностью (HEVC) h.265 4:2:0 на совместимых облачных компьютерах с поддержкой GPU. Дополнительные сведения см. в статье Включение ускорения GPU для Виртуального рабочего стола Azure.

Windows App

Windows App теперь общедоступна

Windows App вышла из предварительной версии и стала общедоступной.

Дополнительные сведения см. в статье Что такое Windows App?

Неделя с 26 августа 2024 г. (выпуск службы 2408)

Приложения

Поддержка Azure Monitor на облачных компьютерах Windows 365

Агент Azure Monitor теперь можно установить на Windows 365 Корпоративная и Windows 365 облачных компьютерах для государственных организаций. Дополнительные сведения см. в статье Общие сведения о службе Azure Monitor.

Безопасность устройств

Настройка функции блокировки сеансов для единого входа

Теперь вы можете настроить функцию удаленной блокировки сеанса, если включен единый вход между поведением отключения по умолчанию и отображением экрана удаленной блокировки. Дополнительные сведения см. в статье Настройка единого входа для Windows 365 с помощью Microsoft Entra проверки подлинности.

Windows 365 поддержка ключа клиента Microsoft Purview теперь общедоступна

Windows 365 поддержка шифрования облачных компьютеров путем настройки ключа клиента Microsoft Purview была переведена из предварительной версии и стала общедоступной. Дополнительные сведения см. в разделе Шифрование служб с помощью ключа клиента Microsoft Purview.

Неделя с 5 августа 2024 г.

Документация

Обновленная статья документации: устойчивость службы Windows 365

Мы создали новую статью, объясняющую устойчивость службы Windows 365. Дополнительные сведения см. в разделе Windows 365 устойчивости службы.

Неделя с 29 июля 2024 г. (выпуск службы 2407)

Управление устройствами

Поддержка однонаправленного буфера обмена теперь общедоступна

Поддержка однонаправленного буфера обмена для облачных компьютеров недоступна и теперь общедоступна. Дополнительные сведения см. в статье Настройка направления передачи буфера обмена и типов данных, которые можно скопировать в Виртуальном рабочем столе Azure.

Закрытие порта 3389 по умолчанию для вновь подготовленных и повторно подготовленных облачных компьютеров

Чтобы защитить среду Windows 365, входящий порт 3389 по умолчанию закрыт.

Windows 365 поддержка смешанного режима AVC, если MMR не включен (предварительная версия)

Windows 365 теперь поддерживает смешанный режим AVC, если MMR не включен.

Безопасность устройств

Windows 365 для государственных организаций теперь поддерживает защищенное хранилище клиентов

Windows 365 для государственных организаций теперь поддерживает microsoft Purview Customer Lockbox.

Дополнительные сведения см. в разделе Microsoft Purview Customer Lockbox.

Управление и устранение неполадок

Новый отчет Intune и действие устройства для аттестации регистрации Windows (общедоступная предварительная версия)

Используйте новый отчет о состоянии аттестации устройств в Microsoft Intune, чтобы узнать, безопасно ли устройство заверяло и зарегистрировалось при аппаратной поддержке. Дополнительные сведения см. в разделе Отчет о состоянии аттестации устройств.

Партнеры

Теперь общедоступна поддержка клиентов Omnissa Horizon и протокола Blast с Windows 365 Корпоративная.

Поддержка клиентов Horizon Omnissa (ранее VMware) и протокола Blast на Windows 365 Корпоративная облачных компьютерах была переведена из предварительной версии и стала общедоступной. Дополнительные сведения см. в статье Настройка Omnissa Horizon для Windows 365 Корпоративная.

Подготовка

Новые предложения GPU для облачных компьютеров стали общедоступными

Новые предложения GPU для облачных компьютеров Windows 365 Enterprise вышли из предварительной версии и стали общедоступными. Дополнительные сведения см. в разделе Облачные компьютеры GPU.

Windows 365 Frontline

Буфер параллелизма Windows 365 Frontline теперь общедоступен.

Буфер параллелизма Windows 365 вышел из предварительной версии и стал общедоступным.

Неделя с 23 июля 2024 г.

Обновлены параметры по умолчанию для Windows 365 базовых показателей безопасности

Несколько значений базовых показателей безопасности Windows 365 изменены по умолчанию. Полный список всех обновленных параметров см. в разделе Список параметров в Облачный компьютер Windows 365 базовых показателей безопасности в Intune.

Неделя с 15 июля 2024 г.

Поддержка облачных компьютеров для устройств FIDO и ключей доступа в macOS и iOS (предварительная версия)

Windows 365 облачные компьютеры теперь поддерживают устройства FIDO и ключи доступа для Microsoft Entra ID входа в macOS и iOS.

Неделя с 8 июля 2024 г.

Управление устройствами

Chroma subsampling по умолчанию изменится на 4:2:0

Чтобы уменьшить проблемы с поддержкой мониторов, служба Windows 365 теперь по умолчанию использует chroma subsampling в 4:2:0. (вместо предыдущего 4:4:4). Дополнительные сведения см. в статье Изменение значения хрома по умолчанию для Windows 365 облачных компьютеров.

Неделя с 1 июля 2024 г.

Приложения

Облачный компьютер Windows 365 образы коллекции используют новый VDI Teams

Облачный компьютер Windows 365 образы коллекции теперь используют новую инфраструктуру виртуализированных рабочих столов (VDI) Teams. Дополнительные сведения см. в разделах Microsoft Teams на облачном компьютере и Новое решение VDI для Teams.

Управление устройствами

Аварийное восстановление между регионами

Windows 365 теперь поддерживает аварийное восстановление между регионами. Дополнительные сведения см. в разделе Аварийное восстановление между регионами в Windows 365.

Неделя с 24 июня 2024 г. (выпуск службы 2406)

Управление устройствами

Windows 365 загрузка и переключение Windows 365 теперь поддерживают перенаправление состояния батареи

Windows 365 загрузка и переключение Windows 365 теперь поддерживают перенаправление состояния батареи. Теперь на облачных компьютерах отображается состояние батареи локального компьютера.

Обновление лицензий Windows 365 в Центре администрирования Майкрософт

Клиенты, у которых есть Современные облачные соглашения Microsoft, могут обновить существующие лицензии на Windows 365 в Центре Администратор Майкрософт.

Безопасность устройств

Изменение проверки подлинности клиентов Windows 365 единого входа

Единый вход для Windows 365 переходит на использование облачного приложения Windows Cloud Login Entra ID для проверка подлинности Windows начиная с Windows и веб-клиентов. Дополнительные сведения см. в разделе Настройка политик условного доступа.

Управление и устранение неполадок

Windows 365 для государственных организаций теперь поддерживает отчет об использовании облачных компьютеров

Windows 365 для государственных организаций теперь поддерживает отчет об использовании облачных компьютеров. Дополнительные сведения см. в статье Отчет об использовании облачных компьютеров.

Отчет о рекомендациях по размеру облачного компьютера теперь общедоступен

Отчет о рекомендациях по размеру облачного компьютера вышел из предварительной версии и теперь является общедоступным. Дополнительные сведения см. в отчете о рекомендациях по облачным компьютерам.

Неделя с 3 июня 2024 г. (выпуск службы 2405)

Безопасность устройств

Windows 365 поддержка судебно-медицинских доказательств Microsoft Purview

Windows 365 теперь поддерживает судебно-медицинские доказательства Microsoft Purview. Дополнительные сведения см. в разделе Настройка судебно-медицинских доказательств.

Управление устройствами

Действие по устранению неполадок теперь поддерживает массовую

Удаленное действие "Устранение неполадок" теперь можно использовать в пакетном режиме. Дополнительные сведения см. в статье Удаленное управление Windows 365 устройствами.

Облако сообщества для государственных организаций

Новые предложения Windows 365 Frontline для GCC

Новые предложения Windows 365 Frontline теперь доступны для клиентов облака сообщества для государственных организаций (GCC), использующих коммерческое облако Azure.

Неделя с 27 мая 2024 г.

Управление устройствами

Новые Облачный компьютер Windows 365 образы, доступные в коллекции

Теперь доступны новые образы из коллекции облачных компьютеров для Windows 10 и Windows 11. Эти улучшенные образы согласованы с Windows 365 образами приложений для улучшения управления политиками:

- Win 10 Enterprise Cloud PC: 21H2, 22H2,
- Win 11 Enterprise Cloud PC: 21H2, 22H2, 23H2

Управление перенаправлениями для облачных компьютеров на устройствах Android

Теперь вы можете использовать Центр администрирования Intune для управления перенаправлениями для пользователей Android, которые получают доступ к своим облачным компьютерам с помощью Удаленный рабочий стол (Майкрософт).

Управление перенаправлениями для облачных компьютеров на устройствах iOS/iPadOS

Теперь вы можете использовать Центр администрирования Intune для управления перенаправлениями для пользователей iOS/iPadOS, которые получают доступ к своим облачным компьютерам с помощью Удаленный рабочий стол (Майкрософт) и Windows App.

Неделя с 20 мая 2024 г.

Управление устройствами

Облачный компьютер Windows 365 образы из коллекции теперь предустановлено новое приложение Microsoft Teams

Образы из коллекции для облачных компьютеров Windows 365 теперь поставляются с новой предустановленной microsoft Teams (не Teams (классическая версия)). Это

относится к Windows Корпоративная 11 23H2 и 22H2. Дополнительные сведения см. в разделе Образы из коллекции.

Неделя с 6 мая 2024 г. (выпуск службы 2404)

Безопасность устройств

Полные доменные имена удалены из списка требований

Многие необходимые полные доменные имена ранее были перемещены в полное доменное имя *.infra.windows365.microsoft.com с подстановочными знаками. Старые полные доменные имена теперь удаляются. Обновленный список полных доменных имен см. в разделе Требования к сети.

Управление и устранение неполадок

Облачные компьютеры с недоступными отчетами теперь стали общедоступными

Отчет о недоступных облачных компьютерах вышел из предварительной версии и стал общедоступным. Дополнительные сведения см. в статье Облачные компьютеры, которые недоступны в отчете.

Управление доступом на основе ролей

теги Intune область (предварительная версия)

Windows 365 теперь поддерживает теги Intune область. Дополнительные сведения см. в разделе Теги области.

Неделя с 10 апреля 2024 г.

Партнеры

Использование HP Anyware для Windows 365 Корпоративная (предварительная версия)

Теперь вы можете использовать HP Anyware для Windows 365 Корпоративная облачных компьютеров. Дополнительные сведения см. в статье Настройка HP Anyware для Windows 365 Корпоративная.

Неделя с 1 апреля 2024 г.

Управление устройствами

Дополнительные лицензии теперь поддерживают хранилище

Для Windows 365 лицензии на расширение теперь поддерживают хранилище. Дополнительные сведения см. в разделе Изменение размера с помощью лицензирования step-up.

Неделя с 26 марта 2024 г. (выпуск службы 2403)

Управление устройствами

Буфер параллелизма для облачных компьютеров Windows 365 Frontline

Новый буфер параллелизма позволяет превысить максимальное число параллелизма в течение ограниченного времени при определенных обстоятельствах, например при смене смены. Дополнительные сведения см. в разделе Буфер параллелизма.

Периоды обслуживания (общедоступная предварительная версия)

Теперь можно задать периоды обслуживания для выполнения удаленных действий на облачных компьютерах. Это будет уведомлять пользователей в сеансе о надвигающемся периоде удаленного действия. Дополнительные сведения см. в разделе Окна обслуживания облачных компьютеров.

Поддержка массовых удаленных действий

Теперь можно использовать массовые действия со следующими удаленными действиями: Восстановление, Перезапуск, Изменение размера и Повторная подготовка. Дополнительные сведения см. в статье Удаленное управление Windows 365 устройствами.

Безопасность устройств

Защита от потери данных Microsoft Purview поддержка Windows 365 Корпоративная

Защита от потери данных Microsoft Purview (DLP) теперь поддерживает Windows 365 Корпоративная. Дополнительные сведения см. в статье Поддержка защиты от потери данных конечных точек для виртуализированных сред.

общий режим загрузки Windows 365 поддерживает FIDO

Windows 365 общий режим загрузки теперь поддерживает FIDO. Дополнительные сведения см. в разделе Практическое руководство. Вход с ключом безопасности FIDO2 без пароля для Windows 10 устройств HAADJ .

Документация

Обновленная статья документации: Известные проблемы

Мы обновили статью Известные проблемы: Windows 365 Корпоративная и Frontline, добавить известную проблему для Teams не принудительного захвата экрана.

Разное

Поддержка API Microsoft Graph для рабочих нагрузок Windows 365 версии 1.0

Помимо рабочих нагрузок бета-версии API Microsoft Graph теперь поддерживают Windows 365 как рабочие нагрузки версии 1.0. Дополнительные сведения см. в статье Использование Microsoft Entra ID для доступа к API Windows 365 в Microsoft Graph.

Управление и устранение неполадок

Дата создания отчета об использовании облачных компьютеров

В отчете об использовании облачных компьютеров теперь отображается дата создания облачного компьютера. Дополнительные сведения см. в статье Отчет об использовании облачных компьютеров.

Отчет о рекомендациях по размеру облачного компьютера (общедоступная предварительная версия)

В новом отчете Центра администрирования Intune рекомендуется подходящий размер для облачных компьютеров, чтобы лучше соответствовать потребностям вашей организации. Дополнительные сведения см. в отчете о рекомендациях по облачным компьютерам.

Улучшения в отчете о качестве подключения к облачному компьютеру стали общедоступными

Улучшения в отчете о качестве подключения к облачному компьютеру вышли из предварительной версии и стали общедоступными. К этим улучшениям относятся:

- более полное представление общей производительности облачных компьютеров.
- более подробное представление устройств, когда они находятся в состоянии низкой производительности из-за большого времени кругового пути.
- Видимость на уровне клиента до последних или текущих для:
  - Время кругового пути.
  - Пропускная способность.
  - Время подключения.
  - Использование UDP.
- Сведения о подключении по IP-адресу клиента и связанному шлюзу CPC.
- Фильтры для всех столбцов.

Дополнительные сведения см. в разделе Отчет о качестве подключения к облачному компьютеру.

Windows 365 Frontline

Windows 365 Frontline поддержка включения и выключения питания в массовом режиме

Теперь вы можете использовать массовые действия для включения и выключения Windows 365 Frontline облачных компьютеров.

Неделя с 11 марта 2024 г.

Документация

Обновлена статья документации: Параметр принудительного входа в браузер для образов из коллекции облачных компьютеров

Мы обновили статью Общие сведения об образах устройств, отметив, что образы из коллекции предварительно применены к принудительному входу в браузер .

Неделя с 4 марта 2024 г. (выпуск службы 2402)

Управление и устранение неполадок

Оповещения для Windows 365 Frontline максимальное количество одновременных облачных компьютеров

Новое оповещение уведомляет администраторов о том, что максимальное количество одновременно работающих облачных компьютеров для Windows 365 Frontline подписок.

Общедоступный отчет об использовании облачных компьютеров

Отчет об **использовании облачных компьютеров** вышел из предварительной версии и стал общедоступным. Дополнительные сведения см. в статье Отчет об использовании облачных компьютеров.

Данные действий устройства хранятся в течение 90 дней

На странице **Обзор** для отдельных облачных компьютеров в **разделе Действия** будут отображаться действия, выполненные за последние 90 дней.

переключатель Windows 365

поддержка Windows 365 переключения для Windows 365 Frontline

Windows 365 Switch теперь поддерживает облачные компьютеры Windows 365 Frontline. Дополнительные сведения см. в разделе Windows 365 Switch.

Управление устройствами

Синхронизация обновлений облачных компьютеров в автономном режиме Windows 365 Frontline

Windows 365 Frontline облачные компьютеры, которые не использовались в течение семи дней, теперь автоматически включены и синхронизированы с клиентский компонент Центра обновления Windows клиентскими политиками.

Администраторы могут удаленно включить и выключить Windows 365 Frontline облачных компьютеров

Теперь администраторы могут включить и выключить Windows 365 Frontline облачных компьютеров с помощью удаленных действий. Дополнительные сведения см. в статье Удаленное управление Windows 365 устройствами.

Поддержка однонаправленного буфера обмена (предварительная версия)

Теперь можно настроить однонаправленный буфер обмена для облачных компьютеров с windows Insider Build 25898 или более поздней версии. Дополнительные сведения см. в статье Настройка направления передачи буфера обмена и типов данных, которые можно скопировать в Виртуальном рабочем столе Azure.

Безопасность устройств

Поддержка защищенного хранилища теперь общедоступна

поддержка Windows 365 Корпоративная и frontline для microsoft Purview Customer Lockbox была переведена из предварительной версии и теперь общедоступна.

Дополнительные сведения см. в разделе Microsoft Purview Customer Lockbox.

Неделя с 26 февраля 2024 г.

Безопасность устройств

Новый параметр более быстрой частоты входа (предварительная версия)

Если единый вход включен, выбор параметра**Частота**> входа сеанса **условного доступа**>>**Каждый раз** обеспечивает более быстрый период повторной проверки подлинности в 5–10 минут в зависимости от используемого клиента. Дополнительные сведения см. в разделе Настройка политик условного доступа.

Загрузка Windows 365

Режимы загрузки общих и выделенных Windows 365 теперь общедоступны

Windows 365 режимы общего и выделенного устройства загрузки вышли из предварительной версии и перешли в общедоступную версию.

Дополнительные сведения см. в разделах Что такое загрузка Windows 365? и Интерактивный сценарий развертывания Windows 365 загрузки на общих физических устройствах.

настройка страницы входа в Windows 365 загрузки теперь общедоступна

Windows 365 поддержка загрузки для настройки страницы входа вышла из предварительной версии и стала общедоступной. Дополнительные сведения см. в статье Интерактивный сценарий развертывания Windows 365 загрузки на общих физических устройствах.

Windows 365 быстрые уведомления о сбое загрузки стали общедоступными

Windows 365 обнаружение загрузки и уведомление о проблемах с настройкой сети или приложения вышли из предварительной версии и перешли в общую доступность.

Управление параметрами локального компьютера с помощью Windows 365 загрузка теперь общедоступна

Управление пользователями параметрами локального компьютера с помощью Windows 365 Загрузочный облачный компьютер вышел из предварительной версии и стал общедоступным.

переключатель Windows 365

идентификаторы Windows 365 переключения рабочих столов стали общедоступными

Идентификаторы представления задач Windows для облачного или локального компьютера были перенесены из предварительной версии и стали общедоступными.

Windows 365 улучшенное отключение переключения теперь общедоступен

Возможность для пользователей без проблем отключиться от облачного компьютера, не выходя из локального рабочего стола, переместилась из предварительной версии и стала общедоступной. Дополнительные сведения см. в разделе Windows 365 Switch.

Windows 365 состояние переключения подключения теперь общедоступен

Сведения о состоянии подключения и времени ожидания на экране подключения для Windows 365 Переключение с Windows 365 Frontline облачных компьютеров вышел из предварительной версии и стал общедоступным.

Неделя с 29 января 2024 г. (выпуск службы 2401)

Безопасность устройств

Изменение требований полного доменного имени

Многие необходимые полные доменные имена были перемещены в полное доменное имя *.infra.windows365.microsoft.com с подстановочными знаками. Это снижает первоначальные требования к конфигурации и частоту изменения требований к подключению. Для Windows 365 правительства полные доменные имена были перемещены в *.infra.windows365.microsoft.us. Чтобы избежать проблем при подготовке новых облачных компьютеров, необходимо убедиться, что *.infra.windows365.microsoft.com* (.infra.windows365.microsoft.us для Windows 365 для государственных организаций) является доступной конечной точкой в списке разрешенных сетей.

Работа конечных пользователей

Конечные пользователи могут перезапустить свой облачный компьютер с Windows с помощью клавиатуры

Для вновь созданных облачных компьютеров конечные пользователи теперь могут перезапустить или завершить работу облачного компьютера с помощью сочетания клавиш CTL+ALT+DEL. Это не относится к облачным компьютерам, созданным до 31.01.2024 г.

Неделя с 15 января 2024 г.

Документация

Обновленная статья документации: Относительная производительность для различных размеров облачных компьютеров

Мы обновили статью и добавили сведения о производительности для дополнительных размеров облачных компьютеров. Дополнительные сведения см. в статье Относительная производительность для разных размеров облачных компьютеров.

Неделя с 8 января 2024 г. (выпуск службы 2312)

Управление и устранение неполадок

Новое правило генерации оповещений: облачные компьютеры, которые недоступны (предварительная версия)

Теперь доступно новое правило генерации оповещений, которое будет уведомлять вас о недоступности облачных компьютеров. Дополнительные сведения об оповещениях в целом см. в разделе Оповещения в Windows 365. Дополнительные сведения об отчете см. в разделе Облачные компьютеры, которые недоступны для отчета. Эта функция пока недоступна для Windows 365 Frontline.

Подготовка

Windows 365 теперь поддерживает Северную Италию и Центральную Польшу

Windows 365 Корпоративная и облачный компьютер Windows 365 Frontline теперь поддерживают регионы Северная Италия и Центральная Польша. Дополнительные сведения см. в статье Поддерживаемые регионы Azure для подготовки облачных компьютеров.

Загрузка Windows 365

Управление параметрами локального компьютера с помощью Windows 365 загрузки (предварительная версия)

Теперь пользователи могут легко получать доступ к параметрам локального компьютера и управлять ими со своего Windows 365 загрузить облачный компьютер. К ним относятся звук, дисплей и другие параметры локального компьютера, относящиеся к устройству. Параметры можно найти, перейдя в **раздел Параметры** запуска > на облачном компьютере.

настройка страницы входа Windows 365 загрузки (предварительная версия)

Windows 365 Boot теперь поддерживает настройку страницы входа в Cloud PC с фирменной символикой логотипа компании для облачных компьютеров в режиме общего компьютера. Дополнительные сведения см. в статье Интерактивный сценарий развертывания Windows 365 загрузки на общих физических устройствах.

Windows 365 режимы загрузки устройства — общий и выделенный (предварительная версия)

Windows 365 Boot теперь поддерживает два режима входа на облачный компьютер с физического устройства:

- Режим общего компьютера. Несколько пользователей могут использовать одно и то же физическое устройство для входа на собственные облачные компьютеры через экран Windows 11 входа.
- (Новое) Режим выделенного компьютера. Физическое устройство назначается конкретному пользователю для входа на свой облачный компьютер через экран Windows 11 входа.

Дополнительные сведения см. в разделах Что такое загрузка Windows 365? и Интерактивный сценарий развертывания Windows 365 загрузки на общих физических устройствах.

быстрые уведомления о Windows 365 загрузки (предварительная версия)

Чтобы ускорить процесс входа, Windows 365 Boot теперь обнаруживает проблемы с настройкой сети или приложения и уведомляет пользователей о них непосредственно во время входа.

переключатель Windows 365

Windows 365 улучшенное отключение переключения (предварительная версия)

Теперь пользователи могут легко отключиться от облачного компьютера, не выходя из локального рабочего стола. Дополнительные сведения см. в разделе Windows 365 Switch.

Windows 365 переключение идентификаторов рабочего стола (предварительная версия)

При переключении между рабочими столами с помощью представления задач каждый рабочий стол определяется как облачный или локальный компьютер.

Windows 365 состояние переключения подключения (предварительная версия)

При использовании Windows 365 Switch с Windows 365 Frontline облачными компьютерами пользователи теперь видят состояние подключения и сведения о времени ожидания на экране подключения. В случае ошибки пользователи могут скопировать идентификатор корреляции, чтобы устранить проблему.

Неделя с 10 декабря 2023 г.

Безопасность устройств

Windows 365 поддержка ключа клиента Microsoft Purview (предварительная версия)

Windows 365 теперь поддерживает шифрование облачных компьютеров путем настройки ключа клиента Microsoft Purview. Дополнительные сведения см. в разделе Шифрование служб с помощью ключа клиента Microsoft Purview.

Неделя с 4 декабря 2023 г. (выпуск службы 2311)

Управление устройствами

Windows 365 загрузка теперь доступна для Windows 365 государственных организаций

Windows 365 Загрузка теперь доступна для клиентов сообщества государственных организаций США (GCC), использующих Windows 365 правительственных организаций. Дополнительные сведения см. в статье Что такое Windows 365 boot?.

Работа конечных пользователей

Изменение пользовательского интерфейса в веб-клиенте

Меню значка шестеренки обновлено.

Новое приложение Microsoft Teams теперь доступно для Windows 365

Новое приложение Microsoft Teams перешло из предварительной версии и стало общедоступным. Она оптимизирована для повышения производительности и более эффективного использования ресурсов на облачных компьютерах. Дополнительные сведения см. в разделе Обновление до новой инфраструктуры виртуализированных рабочих столов Teams.

Новое приложение Microsoft Teams пока недоступно в образах Windows 365 коллекции.

Управление и устранение неполадок

Новый отчет: состояние действия (предварительная версия)

Теперь доступен новый отчет, который позволяет узнать, какие действия успешно выполнены на облачных компьютерах. Для неудачных действий также будут указаны возможные причины. Дополнительные сведения см. в статье Отчет о действиях облачного компьютера.

Новый параметр фильтра для отчета подключенных облачных компьютеров frontline

Новый фильтр доступен в отчете Подключенные облачные компьютеры frontline. Этот новый фильтр отображает почасовые данные для различных периодов данных. Дополнительные сведения см. в разделе Отчет о подключенных облачных компьютерах Frontline (предварительная версия).

Неделя с 13 ноября 2023 г.

Безопасность устройств

Защита от захвата экрана в каталоге параметров Windows 365

Теперь вы можете реализовать защиту от захвата экрана для облачных компьютеров с помощью каталога параметров. Наряду с использованием водяных знаков, захват экрана является сдерживающим фактором для утечки данных и потери данных. Дополнительные сведения см . в разделах Включение защиты от захвата экрана в Виртуальном рабочем столе Azure и Настройка административного шаблона.

Эта функция не поддерживается в Android, iOS или веб-клиентах. Включение этой функции блокирует доступ пользователей к облачным компьютерам при использовании этих клиентов.

Поддержка водяных знаков в каталоге параметров Windows 365

Теперь вы можете реализовать водяные знаки для облачных компьютеров с помощью каталога параметров. Наряду с захватом экрана, подложка является сдерживающим фактором для утечки данных и потери данных. Дополнительные сведения см. в разделах Подложка в Виртуальном рабочем столе Azure и Настройка административного шаблона.

Поддержка защищенного хранилища (предварительная версия)

Windows 365 Корпоративная и Frontline теперь поддерживают microsoft Purview Customer Lockbox.

Дополнительные сведения см. в разделе Microsoft Purview Customer Lockbox.

Подготовка

Единый вход теперь общедоступен

Следующие обновления единого входа вышли из предварительной версии и теперь являются общедоступными:

- Единый вход для Microsoft Entra присоединенных и Microsoft Entra гибридных облачных компьютеров.

- Вы можете включить единый вход отдельно для каждой политики подготовки, чтобы применить его к новым облачным компьютерам.
- Единый вход можно применить к существующим облачным компьютерам.
- Новый проверка сетевого подключения Azure для Microsoft Entra политик подготовки с гибридным присоединением, чтобы убедиться, что домен правильно настроен для единого входа.

Эти обновления также доступны для Windows 365 Frontline.

Новые предложения GPU для облачных компьютеров (предварительная версия)

Теперь для облачных компьютеров Windows 365 Enterprise доступны три новых предложения GPU. Дополнительные сведения см. в разделе Облачные компьютеры GPU.

Работа конечных пользователей

Windows App теперь доступна в общедоступной предварительной версии

Windows App позволяет пользователям безопасно подключаться к устройствам и приложениям Windows. Поддерживаемые удаленные устройства:

- Виртуальный рабочий стол Azure
- Облачный компьютер Windows 365
- Microsoft Dev Box
- Службы удаленных рабочих столов
- Удаленный компьютер

Windows App доступно для Windows, macOS, iOS и iPadOS, а также веб-браузеров.

Дополнительные сведения см. в статье Что такое Windows App?

Неделя с 30 октября 2023 г. (выпуск службы 2310)

Управление устройствами

Обновление разрешений для проверки облачного компьютера

Теперь вам потребуется дополнительная роль Участник данных BLOB-объектов хранилища, чтобы разместить облачный компьютер под проверкой. Дополнительные сведения см. в разделе Размещение Windows 365 Корпоративная облачного компьютера под проверкой.

Подготовка устройств

Два новых размера для облачных компьютеров

Теперь для облачных компьютеров Windows 365 доступны два новых размера:

- 16 виртуальных ЦП,64 ГБ ОЗУ/512 ГБ памяти
- 16 в ЦП/ 64 ГБ ОЗУ/1 ТБ хранилища

Эти 16 лицензий виртуальных ЦП можно приобрести и назначить так же, как вы покупаете и назначаете другие лицензии Windows 365.

Новые образы коллекции

Теперь для Windows 365 облачных компьютеров доступны два новых образа коллекции:

- предварительная версия Windows 11 + Приложения Microsoft 365 23H2
- предварительная версия Windows 11 и оптимизация ОС 23H2

Новые образы коллекции можно выбрать при создании политики подготовки.

Разное

Новые API Graph для Windows 365 Frontline

Теперь для Windows 365 Frontline доступен новый API graph.

Управление и устранение неполадок

Журналы аудита, поддерживаемые в Azure Log Analytics

Теперь вы можете отправлять Windows 365 данные журнала аудита непосредственно в Azure Log Analytics, Концентратор событий или в некоторые сторонние решения. Дополнительные сведения см. в статье Отправка журналов аудита Windows 365 в параметры диагностики в Azure Monitor.

Неделя с 25 сентября 2023 г. (выпуск службы 2309)

Управление устройствами

Действие изменения размера теперь общедоступно

Действие изменения размера перемещено из предварительной версии и переходит в общедоступную версию. Эта функция также доступна для клиентов Windows 365 для государственных организаций и Windows 365 государственных организаций, использующих Windows 365 Корпоративная. Действие изменения размера в настоящее время недоступно для Windows 365 Frontline. Дополнительные сведения см. в разделе Изменение размера Облачного компьютера.

Windows 365 загрузка теперь общедоступна

Windows 365 загрузка была переведена из предварительной версии и стала общедоступной. Дополнительные сведения см. в статье Что такое загрузка Windows 365? В настоящее время эта функция недоступна для Windows 365 государственных организаций.

Управление и устранение неполадок

Новые параметры фильтра в отчете об использовании облачных компьютеров

Теперь для отчета **об использовании облачных компьютеров** доступны два новых параметра фильтра:

- **Параметр фильтра "Дата последнего подключения"** : **нет подключения в течение последних 60 дней**
- **Параметр фильтра по времени подключения** : **нет (0 часов)**

Дополнительные сведения см. в статье Отчет об использовании облачных компьютеров.

Новый отчет: облачные компьютеры, которые не могут подключиться

Теперь доступен новый отчет, который содержит метрики, помогающие администраторам оценивать состояние подключения устройства на уровне клиента и надежность. Например, можно наблюдать:

- устройства с неработоспособными узлами.
- подключения пользователей, которые постоянно или часто завершаются сбоем.
- системные проблемы, например проблема с инфраструктурой Azure, которая влияет на способность пользователя подключаться.

Дополнительные сведения см. в статье Облачные компьютеры, которые недоступны в отчете.

Улучшения в отчете о качестве подключения к облачному компьютеру

Улучшения в отчете о качестве подключения к облачному компьютеру включают:

- Более полное представление общей производительности облачных компьютеров.
- Более подробное представление устройств, когда они находятся в состоянии низкой производительности из-за большого времени кругового пути.
- Видимость на уровне клиента до последних или текущих для:
  - Время кругового пути.
  - Пропускная способность.
  - Время подключения.
  - Использование UDP.
- Сведения о подключении по IP-адресу клиента и связанному шлюзу CPC.
- Фильтры для всех столбцов.

Подготовка

Обновления единого входа

Теперь доступны следующие обновления, относящиеся к единому входу:

- Функции общедоступной предварительной версии.
  - Единый вход для облачных компьютеров Microsoft Entra гибридного присоединения.
  - Единый вход можно включить отдельно для каждой политики подготовки.
  - Новое проверка сетевого подключения Azure, чтобы убедиться, что сеть правильно настроена для единого входа.

- Применение единого входа к существующим Microsoft Entra присоединенным и Microsoft Entra гибридным облачным компьютерам.

Дополнительные сведения см. в разделах Создание политики подготовки и Изменение политики подготовки.

Работа конечных пользователей

Windows 365 Switch теперь общедоступен

Windows 365 Switch вышел из предварительной версии и стал общедоступным. Дополнительные сведения см. в разделе Windows 365 Switch. В настоящее время эта функция недоступна для Windows 365 государственных организаций.

Неделя с 18 сентября 2023 г.

Документация

Windows 365 справочная документация обновлена для Microsoft Entra ID

Windows 365 справочная документация обновлена для ребрендинга Azure Active Directory на Microsoft Entra ID. Дополнительные сведения см. в статье Новое имя для Azure Active Directory. Некоторые области пользовательского интерфейса Microsoft Intune еще не обновлены до Microsoft Entra ID, поэтому вы можете увидеть различия до тех пор, пока не будут сделаны эти обновления.

Неделя с 28 августа 2023 г. (выпуск службы 2308)

Управление и устранение неполадок

Системные оповещения и Уведомления по электронной почте стали общедоступными

Системные оповещения и Уведомления по электронной почте вышли из предварительной версии и стали общедоступными. Дополнительные сведения см. в разделе Оповещения.

Новый отчет: подключенные облачные компьютеры frontline

Теперь доступен отчет подключенных облачных компьютеров frontline. Дополнительные сведения см. в разделе Отчет подключенных облачных компьютеров Frontline.

Отчет о производительности ресурсов Endpoint Analytics теперь доступен для клиентов GCCH

Отчет о производительности ресурсов Аналитики конечных точек теперь доступен для клиентов с высоким уровнем облака сообщества для государственных организаций (GCCH). Дополнительные сведения см. в разделе Отчет о производительности ресурсов.

Страница отчета "Обзор нового облачного компьютера"

Доступ ко всем отчетам облачных компьютеров теперь можно получить в разделе **Обзор облачных компьютеров** в разделе **Управление устройствами**.

Неделя с 21 августа 2023 г.

Партнеры

Использование клиентов VMWare Horizon и протокола Blast с Windows 365 Корпоративная (общедоступная предварительная версия)

Клиенты VMWare Horizon и протокол Blast можно использовать с Windows 365 Корпоративная облачных компьютеров. Это общедоступная предварительная версия. Дополнительные сведения см. в статье Настройка VMware Horizon для Windows 365 Корпоративная.

Неделя с 7 августа 2023 г.

Работа конечных пользователей

поддержка представления задач Windows 11 для облачных компьютеров (предварительная версия)

Windows 365 переключение позволяет пользователям подключаться к облачному компьютеру с помощью представления задачи Windows 11. Они также могут использовать представление задач для переключения между облачным компьютером и локальным устройством. Дополнительные сведения см. в статье Windows 365 Switch и в статье справки пользователя Windows 365 переключение.

Поддержка LG webOS 23 на windows365.microsoft.com

Веб-сайт Windows 365, windows365.microsoft.com, теперь поддерживает LG webOS 23.

Безопасность

Поддержка защиты от незаконного изменения для Windows 365

Windows 365 теперь поддерживает использование политики антивирусной программы безопасности конечных точек для управления защитой от незаконного изменения для Windows 365 облачных компьютеров. Для поддержки защиты от незаконного применения требуется подключение устройств к Microsoft Defender для конечной точки, прежде чем будет применена политика, которая включает защиту от незаконного изменения.

Неделя с 31 июля 2023 г. (выпуск службы 2307)

Управление устройствами

Перемещение облачного компьютера теперь общедоступно

Перенос облачного компьютера вышел из предварительной версии и стал общедоступным. Дополнительные сведения см. в разделе Перемещение облачного компьютера.

Новый параметр, позволяющий пользователям повторно создавать собственные облачные компьютеры

Теперь вы можете предоставить пользователям разрешение на сброс (повторную подготовку) собственного облачного компьютера. Дополнительные сведения см. в статье Создание пользователя локальным администратором.

Безопасность устройств

Обновление минимальных привилегий сетевого подключения Azure (ANC)

Теперь доступны новые, более безопасные минимальные привилегии. Необходимо вручную удалить старую сетевую участник роль из ресурсов, где был создан ANC. Дополнительные сведения см. в разделе Управление доступом на основе ролей.

Разное

Кнопка "Предоставить отзыв" для администраторов теперь общедоступна

Кнопка "**Предоставить отзыв** " переместилась из предварительной версии и стала общедоступной.

Неделя с 17 июля 2023 г.

Работа конечных пользователей

поддержка камеры веб-клиента Windows 365 (предварительная версия)

Теперь пользователи могут предоставить облачному компьютеру доступ к камере локального устройства.

Неделя с 3 июля 2023 г. (выпуск службы 2306)

Управление устройствами

Windows 365 Frontline теперь общедоступна

Windows 365 Frontline вышел из предварительной версии и стал общедоступным. Дополнительные сведения см. в статье Что такое Windows 365 Frontline?

Поддержка групповых лицензий для изменения размера облачного компьютера

Как одно, так и массовое изменение размера теперь поддерживают облачные компьютеры, которые были подготовлены с лицензиями на основе групп.

Работа конечных пользователей

Windows365.microsoft.com кнопка "Открыть в браузере" включает приложение Windows 365 и приложение "Открыть в удаленном рабочем столе"

Теперь у пользователей есть два варианта при нажатии раскрывающейся кнопки **Открыть в браузере** , чтобы открыть сеанс пользователя облачного компьютера на странице windows365.microsoft.com:

- **Открыть в приложение Windows 365**
- **Открыть в приложении "Удаленный рабочий стол"**

приложение Windows 365 уведомления об обновлениях для пользователей

приложение Windows 365 пользователи получат уведомление о доступности обновления. Если пользователи решили выполнить обновление, приложение закрывается, и по завершении обновления они получат уведомление Windows.

Управление и устранение неполадок

Отчет о производительности ресурсов в Endpoint Analytics теперь доступен для Windows 365 государственных организаций

Отчет о производительности ресурсов в Endpoint Analytics теперь доступен для Windows 365 государственных организаций. Дополнительные сведения см. в разделе Отчет о производительности ресурсов.

Идентификаторы корреляции для уведомлений о сетевом подключении Azure

Состояние работоспособности сетевого подключения Azure проверка в Microsoft Intune теперь содержит идентификатор корреляции. Этот идентификатор помогает группе

поддержки устранять проблемы с клиентами. Обязательно укажите идентификатор при обращении в службу поддержки Майкрософт.

правительство Windows 365

приложение Windows 365 поддержка сред Windows 365 для государственных организаций

Теперь приложение Windows 365 поддерживает Windows 365 среды для государственных организаций.

приложение Windows 365 закрепление облачного компьютера на панели задач теперь поддерживает Windows 365 для государственных организаций

пользователи Windows 365 для государственных организаций теперь могут закрепить свой облачный компьютер на панели задач в приложение Windows 365 для Windows 11 платформ.

Неделя с 12 июня 2023 г.

Приложения

поддержка Windows 365 государственных организаций для рабочих нагрузок на основе виртуализации

Рабочие нагрузки на основе виртуализации теперь поддерживаются в средах Windows 365 для государственных организаций. Дополнительные сведения см. в разделе Настройка рабочих нагрузок на основе виртуализации на облачном компьютере.

Документация

Новая статья документации: Схема архитектуры высокого уровня

Мы опубликовали новую статью справочной документации. Дополнительные сведения см. в статье Схема архитектуры высокого уровня.

Неделя с 5 июня 2023 г.

Разное

Центр администрирования Microsoft 365: руководство по расширенному развертыванию Windows 365 облачных компьютеров

На странице Руководства по расширенному развертыванию в Центр администрирования Microsoft 365 есть новое руководство, которое поможет администраторам планировать, развертывать и масштабировать Windows 365 Корпоративная в своей организации. В этом руководстве содержится контрольный список задач по настройке облачного компьютера и рекомендации, а также рекомендации, основанные на конфигурации клиента.

Windows 365 Корпоративная теперь могут быть приобретены государственными клиентами

Windows 365 Корпоративная теперь могут приобретаться клиентами с существующим клиентом Облака сообщества для государственных организаций (GCC). Такие клиенты могут использовать свою коммерческую подписку Azure, если они хотят использовать пользовательские образы и сетевые подключения Azure. (Ранее клиенты с клиентом GCC могли покупать только Windows 365 государственных организаций. Для пользовательских образов и сетевых подключений Azure требовалась Azure для государственных организаций подписка.) Windows 365 Корпоративная — это коммерческий продукт с условиями коммерческого лицензирования.

Windows 365 Корпоративная соответствует FedRAMP. За исключением FedRAMP, Windows 365 Корпоративная не обеспечивает такое же соответствие требованиям, как Windows 365 правительства. CJIS и IRS 1075 не поддерживаются в Windows 365 Корпоративная.

правительство Windows 365

средство настройки Windows 365 государственных организаций

Теперь доступен новый инструмент настройки Windows 365 для государственных организаций. Он заменяет скрипты PowerShell, которые использовались для настройки сопоставления клиентов и разрешений. Дополнительные сведения см. в статье Настройка клиентов для Windows 365 государственных организаций.

Неделя с 29 мая 2023 г. (выпуск службы 2305)

Управление устройствами

Общедоступные точки восстановления облачного компьютера по запросу и копирование в учетную запись хранения Azure

Точки восстановления облачного компьютера по запросу и копирование в учетную запись хранения Azure вышли из предварительной версии и стали общедоступными. Дополнительные сведения см. в статье Создание точек восстановления по запросу вручную для облачных компьютеров и совместное использование точек восстановления облачных компьютеров в учетной записи хранения Azure.

Shortpath для управляемых и частных сетей

Управляемая сеть RDP Shortpath доступна для Windows 365. Дополнительные сведения о RDP Shortpath в Windows 365 см. в статье Использование RDP Shortpath для частных сетей с Windows 365 .

Перемещение облачного компьютера

Новый параметр политики подготовки позволяет определить новый регион или ANC для политики подготовки. При инициации перемещения:

1. Все облачные компьютеры в политике подготовки, которые больше не соответствуют обновленному региону или ANC, будут завершены.
2. Все такие облачные компьютеры будут перемещены в новый регион или ANC.

Для завершения перемещений может потребоваться несколько часов.

Новые облачные компьютеры, созданные политикой подготовки, будут созданы в новом регионе или ANC.

Дополнительные сведения см. в разделе Перемещение облачного компьютера.

Разное

Кнопка "Предоставить отзыв" для администраторов (предварительная версия)

Кнопка "**Предоставить отзыв**" теперь доступна на нескольких страницах Windows 365 администрирования в Центре администрирования Intune.

Управление и устранение неполадок

Администратор оповещение о переходе облачного компьютера в льготный период

Теперь администраторы получают оповещения, когда облачный компьютер вступает в льготный период. Дополнительные сведения о льготных периодах см. в статье Общие сведения об управлении устройствами для облачных компьютеров. Сведения о просмотре и настройке оповещений см. в разделе Оповещения в Windows 365.

приложение Windows 365

приложение Windows 365 поддерживает темный режим

Теперь приложение Windows 365 поддерживает темный режим. Конечные пользователи могут настроить приложение Windows 365 на светлый или темный режим или в соответствии с параметрами системы.

поддержка приложение Windows 365 параметров для нескольких мониторов

Теперь пользователи могут изменять несколько параметров монитора в приложение Windows 365.

правительство Windows 365

улучшение настройки сетевого подключения Azure Windows 365 государственных организаций

Во время создания или редактирования сетевого подключения Azure (ANC) вместо копирования и вставки сведений (например, идентификатор подписки и имя виртуальной сети) для ANC теперь можно выбрать параметры в раскрывающемся меню. Дополнительные сведения см. в статье Настройка клиентов для Windows 365 государственных организаций.

Неделя с 22 мая 2023 г.

Управление устройствами

Windows 365 загрузка: пользователи могут входить непосредственно на облачный компьютер с физического устройства (предварительная версия)

Windows 365 загрузка позволяет администраторам настраивать Windows 11 физических устройств, чтобы пользователи могли:

- Избегайте входа на физическое устройство.
- Войдите непосредственно в Облачный компьютер Windows 365 на физическом устройстве.

Дополнительные сведения см. в статье Что такое загрузка Windows 365?

Документация

Новая статья документации: Установка приложение Windows 365 на физических устройствах с помощью Intune

Мы опубликовали новую статью справочной документации. Дополнительные сведения см. в статье Использование Intune, установка приложение Windows 365 на физических устройствах.

Неделя с 24 апреля 2023 г. (выпуск службы 2304)

Работа конечных пользователей

перенаправление сочетаний клавиш веб-клиента Windows 365

Windows 365 пользователи веб-клиента теперь могут использовать сочетания клавиш (например, ALT+TAB) на своем облачном компьютере. Эти сочетания клавиш обычно перехватываются операционной системой узла и не отправляются на облачный компьютер. Дополнительные сведения об этих сочетаниях клавиш см. в статье Доступ к облачному компьютеру.

приложение Windows 365: закрепление облачного компьютера на панели задач

Теперь пользователи могут закрепить свой облачный компьютер на панели задач в приложение Windows 365. Это позволяет им запускать облачный компьютер со значка панели задач, не заходя в центр подключений.

Windows365.microsoft.com темном режиме

Теперь у вас есть возможность использовать темный режим на windows365.microsoft.com. Дополнительные сведения см. в разделе Доступ к облачному компьютеру.

Подготовка

Windows 365 теперь поддерживает Северную Африку и Центральную Швецию

Облачный компьютер Windows 365 теперь поддерживает Северную Африку и Центральную Швецию. Дополнительные сведения см. в статье Поддерживаемые регионы Azure для подготовки облачных компьютеров.

правительство Windows 365

Windows 365 для государственных организаций с пользовательскими образами или сетевыми подключениями Azure

Для клиентов Windows 365 для государственных организаций **страницы Пользовательские образы** и **сетевое подключение Azure** были обновлены, чтобы было ясно, что:

- Прежде чем использовать пользовательские образы с Windows 365 для государственных организаций, необходимо связать коммерческий клиент Azure с клиентом Azure для государственных организаций.
- Прежде чем использовать сетевые подключения Azure с Windows 365 для государственных организаций, необходимо связать свой коммерческий клиент Azure с клиентом Azure для государственных организаций.

Неделя с 10 апреля 2023 г.

Работа конечных пользователей

Перенаправление расположения

Теперь пользователи могут включить перенаправление расположения, чтобы облачные компьютеры использовали правильное географическое расположение. Дополнительные сведения см. в разделе Перенаправление расположения.

Неделя с 3 апреля 2023 г.

Управление устройствами

Windows 365 Frontline

Windows 365 Frontline — это новая версия Windows 365, которая помогает организациям сократить расходы, предоставляя одну лицензию для подготовки трех виртуальных машин облачных компьютеров. Для каждой приобретаемой лицензии Windows 365 Frontline можно подготовить три разных облачных компьютера, которые нельзя использовать одновременно. Вместо этого каждый пользователь получает уникальный облачный компьютер, который он может использовать, если два других пользователя с той же лицензией не вошли в свои облачные компьютеры. Дополнительные сведения см. в статье Что такое Windows 365 Frontline?

Преобразование лицензий Windows 365 в лицензии более высокого уровня

Клиенты с активным прямым соглашением Enterprise теперь могут преобразовывать лицензии на Windows 365 более низкого уровня в лицензии более высокого уровня. Чтобы узнать больше, обратитесь к специалисту в области.

Документация

Новая статья документации: Относительная производительность для различных размеров облачных компьютеров

Мы опубликовали новую статью справочной документации. Дополнительные сведения см. в статье Относительная производительность для разных размеров облачных компьютеров.

Неделя с 28 марта 2023 г. (выпуск службы 2303)

Подготовка устройств

Шаблон настраиваемого имени облачного компьютера

Теперь можно создать шаблон для автоматического создания уникальных имен для новых облачных компьютеров. Дополнительные сведения см. в статье Создание политик подготовки.

Безопасность устройств

Теги FQDN

Теги FQDN помогают клиентам упростить создание и обслуживание необходимых правил для исходящего сетевого трафика через брандмауэры Azure. Дополнительные сведения см. в разделе Использование Брандмауэр Azure для управления средами Windows 365 и защиты.

Разное

Windows 365 и FedRAMP

Windows 365 Корпоративная была оценена уполномоченным аудитором FedRAMP для удовлетворения требований FedRAMP в центрах обработки данных в континентальной части США.

правительство Windows 365

Windows 365 поддержка Gov для передачи файлов с облачного компьютера с помощью веб-клиента windows365.microsoft.com

Вы можете использовать веб-клиент windows365.microsoft.com для передачи файлов на Windows 365 Gov Cloud PC и с нее. Дополнительные сведения см. в разделе Перенос файлов на облачный компьютер и с него.

Более высокое разрешение экрана облачного компьютера для Windows 365 Gov

пользователи Windows 365 Gov Cloud PC теперь могут выбирать более высокое разрешение экрана при подключении к облачному компьютеру из

https://windows365.microsoft.com .

Неделя с 6 марта 2023 г.

Управление устройствами

Создание точек восстановления облачных компьютеров по запросу и их копирование в учетную запись хранения Azure

Теперь вы можете создавать точки восстановления облачных компьютеров по запросу и копировать их в учетную запись хранения Azure. Дополнительные сведения см. в статье Создание точек восстановления по запросу вручную для облачных компьютеров и совместное использование точек восстановления облачных компьютеров в учетной записи хранения Azure.

Управление доступом на основе ролей

Изменения разрешений для операций сетевого подключения Azure

Разрешения, необходимые для редактирования, создания и удаления сетевых подключений Azure (ANC) и работоспособности проверка повторных попыток, изменились. Теперь у вас должны быть разрешения администратора Intune или администратора Windows 365. Дополнительные сведения см. в статье Сетевые подключения Azure.

Неделя с 27 февраля 2023 г. (выпуск службы 2302)

Приложения

приложение Windows 365 теперь общедоступна

Приложение Windows 365 вышел из предварительной версии и стал общедоступным.

Улучшенное воспроизведение видео с помощью перенаправления мультимедиа теперь общедоступно

Улучшенная производительность воспроизведения видео на облачных компьютерах с помощью перенаправления мультимедиа (MMR) переместилась из предварительной версии и стала общедоступной. Дополнительные сведения см. в разделе Улучшение воспроизведения видео.

Веб-клиент cloud PC: улучшенный интерфейс обратной связи для конечных пользователей

Веб-клиент cloud PC (доступный из windows365.microsoft.com) имеет улучшенный интерфейс обратной связи для конечных пользователей, чтобы предоставлять отзывы.

Управление устройствами

Аппаратное ускорение веб-клиента windows365.microsoft.com

В веб-клиенте windows365.microsoft.com теперь можно воспользоваться преимуществами аппаратного ускорения. Этот параметр включен по умолчанию и повышает производительность перемещения для таких действий, как прокрутка, перемещение окон или воспроизведение видео.

Настройка установленного языка и региона для подготовки облачных компьютеров в средах GCC/H

При создании политики подготовки администраторы теперь могут настроить установленный язык и регион для новых облачных компьютеров в средах Сообщества для государственных организаций США (GCC) и GCC High. Дополнительные сведения см. в статье Предоставление пользователям локализованного интерфейса Windows.

Подготовка устройств

Добавление дополнительных Connections сети Azure в политику подготовки

Новый параметр сетевого подключения Azure (ANC) позволяет добавлять дополнительные ACS в политику подготовки и определять порядок приоритета для их использования. Подготовив несколько АНК в разных регионах Azure, администраторы могут сделать подготовку более надежной в редких случаях ограничения емкости в регионе.

Поддержка GCC/H для параметра geography в политике подготовки Windows 365

Параметр **География** в политиках подготовки теперь поддерживается для облака сообщества для государственных организаций США (GCC) и сред GCC High. Дополнительные сведения см. в статье Создание политик подготовки.

Документация

Новая статья документации: жизненный цикл учетных данных домена сетевого подключения Azure

Мы опубликовали новую статью справочной документации. Дополнительные сведения см. в статье Жизненный цикл учетных данных домена сетевого подключения Azure.

Неделя с 20 февраля 2023 г.

Партнеры

Поддержка Citrix HDX Plus теперь общедоступна

Windows 365 поддержка Citrix HDX Plus вышла из предварительной версии и стала общедоступной. Дополнительные сведения см. в статье Настройка Citrix HDX Plus для Windows 365 Корпоративная.

Неделя с 6 февраля 2023 г.

Приложения

Вложенная виртуализация теперь поддерживает облачные компьютеры с 4vCPU

Windows 365 вложенная виртуализация теперь поддерживает облачные компьютеры с 4 виртуальными ЦП. Дополнительные сведения см. в статье Настройка поддержки рабочих нагрузок на основе виртуализации.

Неделя с 30 января 2023 г. (выпуск службы 2301)

Приложения

приложение Windows 365 теперь поддерживает Windows 10

Теперь приложение Windows 365 поддерживает Windows 10.

Microsoft Teams: общий доступ к окнам приложений из Облачный компьютер Windows 365

В Microsoft Teams теперь можно предоставлять общий доступ к определенным окнам с рабочего стола облачного компьютера. Ранее вы могли предоставить общий доступ только к полному рабочему столу Облачного компьютера.

Работа конечных пользователей

Открытие облачных компьютеров в приложении удаленного рабочего стола из windows365.microsoft.com

С windows365.microsoft.com теперь можно открыть облачный компьютер в приложении удаленного рабочего стола. Дополнительные сведения см. в разделе Доступ к облачному компьютеру.

Улучшенный интерфейс обратной связи для конечных пользователей

windows365.microsoft.com усовершенствовал интерфейс для конечных пользователей для предоставления отзывов.

Получение сведений о подключении к облачному компьютеру из windows365.microsoft.com

На windows365.microsoft.com теперь вы можете получить сведения о подключении к облачному компьютеру, такие как транспортный протокол, время кругового пути, частота кадров и многое другое.

Неделя с 16 января 2023 г.

Управление и устранение неполадок

Windows 365 государственная поддержка судебного аудита облачных компьютеров

Судебно-медицинский аудит теперь доступен для Windows 365 правительства. Дополнительные сведения см. в статьях Цифровая экспертиза и облачные компьютеры Windows 365 Корпоративной и Помещение облачного компьютера на проверку.

Неделя с 2 января 2023 г.

Управление доступом на основе ролей

Поддержка пользовательских Windows 365 ролей RBAC теперь общедоступна

Поддержка пользовательских Windows 365 ролей управления доступом на основе ролей (RBAC) была перенесена из предварительной версии и стала общедоступной. Эти настраиваемые роли теперь также поддерживаются для Windows 365 для государственных организаций (облако сообщества для государственных организаций и облако высокого уровня сообщества для государственных организаций). Дополнительные сведения см. в статье Настраиваемые роли.

Неделя с 12 декабря 2022 г.

Подготовка

Подготовка облачных компьютеров, присоединенных к Azure Active Directory, с помощью единого входа (общедоступная предварительная версия)

Windows 365 теперь поддерживает создание облачных компьютеров, присоединенных к Azure Active Directory, которые используют единый вход для входа в Cloud PC. На существующих облачных компьютерах не будет настроен единый вход. Дополнительные сведения см. в разделах Создание политики подготовки и Изменение политики подготовки.

Подготовка

Настройка установленного языка и региона для подготовки общедоступных облачных компьютеров

Предварительная настройка языка для облачных компьютеров вышла из предварительной версии и стала общедоступной. Администраторы могут выбрать **пакет Язык & регион** в разделе **Конфигурация** в политике подготовки, чтобы предварительно настроить язык для устройств конечных точек. Дополнительные сведения см. в статье Использование политики подготовки для настройки языка интерфейса по умолчанию на облачных компьютерах.

Управление устройствами

Новый столбец стороннего соединителя на странице "Все устройства"

На **странице Все устройства** есть новый столбец: **Сторонний соединитель**. Дополнительные сведения см. в статье Общие сведения об управлении устройствами для облачных компьютеров.

Повторная установка агента Citrix

Теперь можно использовать параметр **Retry Agent Citrix** вместо повторной попытки полной подготовки. Дополнительные сведения см. в статье Повторная установка агента Citrix.

Документация

Новая статья документации: Windows 365 варианты развертывания

Мы опубликовали новую статью справочной документации. Дополнительные сведения см. в разделе варианты развертывания Windows 365.

Неделя с 5 декабря 2022 г.

Управление устройствами

Поддержка RDP Shortpath для общедоступных сетей теперь общедоступна

Поддержка RDP Shortpath для общедоступных сетей вышла из предварительной версии и стала общедоступной. Дополнительные сведения о RDP Shortpath см. в статье Использование RDP Shortpath для общедоступных сетей с Windows 365.

Неделя с 28 ноября 2022 г.

Подготовка

Новый параметр Geography в политике подготовки Windows 365

Новый параметр **Geography** предоставляет администраторам два способа выбора регионов Azure во время подготовки.

- Вы можете выбрать конкретный регион, чтобы убедиться, что облачные компьютеры подготовлены только в этом регионе.
- Вы можете выбрать **автоматически,** чтобы служба Windows 365 автоматически выбирала регион (в географическом регионе) во время подготовки.

Существующие политики подготовки будут автоматически заполнять параметры **География** и **Регион** на основе существующих параметров. Никаких действий администратора не требуется.

Дополнительные сведения см. в статье Создание политик подготовки.

приложение Windows 365

Обновлена установка приложение Windows 365 для установки зависимых приложений

Процесс установки приложение Windows 365 обновлен для автоматической установки зависимых приложений.

Политика Azure Active Directory обновлена для приложение Windows 365

Политика Azure Active Directory (Azure AD) обновлена, поэтому для использования приложение Windows 365 не требуется вносить дополнительные изменения в политику условного доступа.

Неделя с 14 ноября 2022 г.

Документация

Новая статья документации: Использование страницы состояния регистрации с облачными компьютерами

Мы опубликовали новую статью справочной документации. Дополнительные сведения см. в статье Использование страницы состояния регистрации на облачных компьютерах.

Неделя с 7 ноября 2022 г.

правительство Windows 365

Windows 365 для государственных организаций теперь поддерживает Windows 11 и безопасную загрузку

Windows 365 правительство теперь поддерживает следующие функции:

- Создание облачных компьютеров, использующих безопасную загрузку.
- Windows 11 параметры в списке образов коллекции.
- Создание пользовательских образов под управлением Windows 11 (должны быть виртуальными машинами 2-го поколения).

Неделя с 24 октября 2022 г.

Управление устройствами

Восстановление на определенный момент времени теперь общедоступно

Восстановление на момент времени перешло из предварительной версии и стало общедоступным. Дополнительные сведения см. в статье Восстановление до состояния на определенный момент времени для Windows 365 Корпоративная.

Подготовка

Новый поддерживаемый регион Azure: Север ОАЭ

Теперь для подготовки Облачный компьютер Windows 365 поддерживается новый регион Azure: Север ОАЭ.

Дополнительные сведения о поддерживаемых регионах Azure см. в статье Поддерживаемые регионы Azure для подготовки облачных компьютеров.

Неделя с 17 октября 2022 г.

Управление и устранение неполадок

Новый проверка работоспособности сетевого подключения Azure

Добавлен новый проверка проверки работоспособности сетевого подключения Azure: **доступный сервер подключения UDP**. Дополнительные сведения см. в статье Проверки работоспособности сетевых подключений Azure.

Судебно-медицинский аудит облачных компьютеров теперь общедоступен

Судебно-медицинский аудит вышел из предварительной версии и стал общедоступным. Дополнительные сведения см. в статьях Цифровая экспертиза и облачные компьютеры Windows 365 Корпоративной и Помещение облачного компьютера на проверку.

Неделя с 10 октября 2022 г.

Приложения

приложение Windows 365 в общедоступной предварительной версии

Новое приложение для входа в Windows 365 облачных компьютеров и управления ими теперь доступно в общедоступной предварительной версии. Приложение предоставляет функции, аналогичные windows365.microsoft.com веб-сайту, для доступа к облачным компьютерам и управления ими.

Подготовка устройств

Поддержка сред для государственных организаций США

Государственные организации теперь могут использовать службы Windows 365 сначала в высокооблачной среде сообщества государственных организаций США (GCC), а затем в средах GCC. Все службы Windows 365 зависимостей также должны использоваться организацией в соответствующей среде для государственных организаций. Дополнительные сведения см. в статье Что такое Windows 365 государственных организаций?

Партнеры

Использование Citrix HDX Plus с Windows 365 Корпоративная

Теперь вы можете использовать Citrix HDX Plus с Windows 365 Корпоративная облачными компьютерами. Дополнительные сведения см. в статье Настройка Citrix HDX Plus для Windows 365 Корпоративная.

Управление и устранение неполадок

Отчет об использовании облачных компьютеров

Теперь доступен новый отчет для облачных компьютеров. Отчет **об использовании облачных компьютеров** показывает, сколько часов пользователи были подключены к своим облачным компьютерам. Также отображаются сведения об отдельных облачных компьютерах и агрегированных данных. Дополнительные сведения см. в статье Отчет об использовании облачных компьютеров.

Отчет о проблемах с качеством подключения облачного компьютера

Теперь доступен новый отчет для облачных компьютеров. В отчете о **проблемах с качеством подключения облачных компьютеров** содержатся сведения о времени кругового пути, доступной пропускной способности и времени входа в удаленное взаимодействие. Также отображаются сведения об отдельных облачных компьютерах и агрегированных данных. Дополнительные сведения см. в разделе Отчет о качестве подключения к облачному компьютеру.

Неделя с 26 сентября 2022 г. (выпуск службы 2209)

Управление и устранение неполадок

Системные оповещения и Уведомления по электронной почте (предварительная версия)

Теперь вы можете настроить системные оповещения и автоматические сообщения электронной почты, чтобы получать уведомления при возникновении определенных событий, предупреждений или ошибок в службе Windows 365. Подмножество критически важных проблем с облачными компьютерами будет автоматически отправлено администраторам. Кроме того, можно определить правила генерации оповещений, например целевую аудиторию (устройства, группы пользователей, клиенты), пороговые значения, частоту и каналы уведомлений. Дополнительные сведения см. в разделе Оповещения.

Разное

Изменение URL-адреса списка разрешений для Windows 365

Мы добавили новую конечную точку, которая должна быть доступна для службы Windows 365: *.infra.windows365.microsoft.com". Это часть текущей работы по консолидации конечных точек, чтобы сократить количество полных доменных имен, необходимых для доступа к службе.

Неделя с 19 сентября 2022 г.

Управление устройствами

Уменьшение размера облачных компьютеров (предварительная версия)

Теперь можно уменьшить объем оперативной памяти и спецификаций облачного компьютера (за исключением размера диска). Дополнительные сведения см. в разделе Изменение размера Облачного компьютера.

Подготовка устройств

Облачный компьютер Windows 365 поддержка Windows 11 Корпоративная версии 22H2

Теперь доступны новые образы коллекции с поддержкой Windows 11 версии 22H2. Следующие образы коллекции можно использовать для недавно подготовленных облачных компьютеров:

- Приложения Win11 22H2 + M365
- Win11 22H2 + Оптимизация

Неделя с 29 августа 2022 г. (выпуск службы 2208)

Управление и устранение неполадок

Новая проверка работоспособности: готовность языкового пакета локализации

На вкладке **Сетевое подключение Azure** есть новый проверка **работоспособности: готовность языкового пакета локализации**. Этот проверка работоспособности проверяет возможность установки операционной системы и языковых пакетов Microsoft 365. Он также гарантирует, что ссылка на скачивание пакета локализации доступна. Дополнительные сведения см. в статье Проверки работоспособности сетевого подключения Azure.

Обзор проверок работоспособности и ошибок подключения к облачному компьютеру в Центре администрирования Microsoft Intune

Теперь вы можете просмотреть проверки работоспособности подключения и ошибки в Центре администрирования Microsoft Intune, чтобы понять, возникают ли проблемы с подключением у пользователей. Вы также получите средство устранения неполадок, помогающее устранить проблемы с подключением. Чтобы просмотреть проверки, выберите **Устройства**>**Windows 365**>**Сети**> Azure выберите подключение в списке >**Обзор**. Эта функция будет выпущена для всех клиентов в течение следующих нескольких недель.

Подготовка

Новые поддерживаемые регионы Azure: Восточная Азия, Центральная Корея, Восточная Норвегия, Северная Швейцария

Новые регионы Azure теперь поддерживаются для подготовки Облачный компьютер Windows 365: Восточная Азия, Центральная Корея, Восточная Норвегия и Северная Швейцария.

Дополнительные сведения о поддерживаемых регионах Azure см. в статье Поддерживаемые регионы Azure для подготовки облачных компьютеров.

Неделя с 22 августа 2022 г.

Документация

Новая статья документации: Ограничение Office 365 служб облачными компьютерами

Мы опубликовали новую статью справочной документации. Дополнительные сведения см. в статье Ограничение Office 365 служб облачными компьютерами.

Неделя с 15 августа 2022 г.

Управление приложениями

Конфигурация языка и региона теперь также применяется к Приложения Microsoft 365

Политики подготовки, настроенные для языка, теперь также применяются к Приложения Microsoft 365. Когда пользователь впервые входит в систему, его Приложения Microsoft 365 будет использовать настроенный язык. Дополнительные сведения см. в разделе Локализация интерфейса Windows.

Управление и устранение неполадок

Отчет о подключении удаленного взаимодействия в Аналитике конечных точек теперь общедоступен

Отчет о подключении удаленного взаимодействия в Endpoint Analytics вышел из предварительной версии и стал общедоступным. Дополнительные сведения см. в статье Отчет о подключениях для удаленного взаимодействия.

Отчет о производительности ресурсов в Endpoint Analytics теперь общедоступен

Отчет о производительности ресурсов в Endpoint Analytics вышел из предварительной версии и стал общедоступным. Дополнительные сведения см. в разделе Отчет о производительности ресурсов.

Неделя с 8 августа 2022 г.

Документация

Новая статья в документации: безопасность Windows 365

Мы опубликовали новую статью справочной документации. Дополнительные сведения см. в статье Безопасность Windows365.

Неделя с 25 июля 2022 г.

Поддержка действий по изменению размера для дополнительных облачных компьютеров

Действие по изменению размера теперь поддерживает облачные компьютеры, присоединенные к Azure Active Directory.

Неделя с 18 июля 2022 г.

Приложения

Параметр синхронизации почты Outlook на облачном компьютере

На новых и повторно подготовленных облачных компьютерах теперь можно установить 6 или 12 месяцев для параметра синхронизации почты Outlook.

Подготовка устройств

Подготовка облачных компьютеров с безопасной загрузкой

Поддержка создания облачных компьютеров, использующих функцию Безопасная загрузка, теперь доступна в Европе, APAC и регионах Северной Америки. На существующих облачных компьютерах безопасная загрузка не будет включена автоматически.

Неделя с 4 июля 2022 г. (выпуск службы 2206)

Приложения

Поддержка рабочих нагрузок на основе виртуализации теперь общедоступна

Поддержка рабочих нагрузок на основе виртуализации перешла из предварительной версии в общедоступную. Дополнительные сведения см. в разделе Настройка рабочих нагрузок на основе виртуализации на облачном компьютере.

Работа конечных пользователей

Перенос файлов с облачного компьютера с помощью веб-клиента windows365.microsoft.com

Вы можете использовать веб-клиент windows365.microsoft.com для передачи файлов на свой облачный компьютер и с него. Дополнительные сведения см. в разделе Перенос файлов на облачный компьютер и с него.

Управление и устранение неполадок

Новая проверка работоспособности: убедитесь, что ограничения регистрации Intune разрешают регистрацию Windows.

На вкладке **сетевого подключения Azure** появилась новая проверка работоспособности: **ограничения регистрации Intune** разрешают регистрацию Windows. Эта проверка работоспособности подтверждает, что ограничения регистрации Intune настроены для разрешения регистрации Windows. Windows 365 Enterprise требует регистрации в Intune во время подготовки.

Неделя с 6 июня 2022 г. (выпуск службы 2205)

Управление и устранение неполадок

Экспертный аудит облачных компьютеров

Теперь вы можете поместить облачный компьютер на проверку. Это действие запускает процесс создания надежного моментального снимка облачного компьютера. Затем можно проанализировать моментальный снимок с помощью решений для обнаружения электронных данных. Дополнительные сведения см. в статьях Цифровая экспертиза и облачные компьютеры Windows 365 Корпоративной и Помещение облачного компьютера на проверку.

Неделя с 16 мая 2022 г.

Управление устройствами

Поддержка RDP Shortpath для общедоступных сетей

Облачные компьютеры с Windows 365 Корпоративная теперь поддерживают RDP Shortpath для общедоступных сетей. Дополнительные сведения об RDP Shortpath см. в статье Использование RDP Shortpath для общедоступных сетей (предварительная версия) с Windows 365.

Окончание поддержки Windows 10 версии 1909 (19H2) в Windows 365

Windows 365 больше не поддерживает Windows 10 версии 1909 (19H2).

Взаимодействие с пользователем

Поддержка Облачного компьютера Windows 365 для фоновых эффектов Teams

Облачные компьютеры с Windows 365 теперь поддерживают фоновые эффекты в Teams. Дополнительные сведения см. в блоге Фоновые эффекты Microsoft Teams, обычно доступные в Windows 365.

Облачный компьютер Windows 365 поддержки нескольких окон Teams и позвоните мне

Облачные компьютеры с Windows 365 теперь поддерживают многооконный режим и функцию "Позвонить мне" в Teams. Дополнительные сведения см. в блоге Поддержка нескольких окон Teams и функции "Позвонить мне" обычно доступны в Windows 365.

Неделя с 9 мая 2022 г. (выпуск службы 2204)

Управление устройствами

Поддержка облачных компьютеров, присоединенных к Azure AD, теперь общедоступна

Поддержка облачных компьютеров, присоединенных к Azure AD, перешла из предварительной версии в общедоступную.

Подготовка

Подготовка облачных компьютеров с безопасной загрузкой

Поддержка облачных компьютеров для функции безопасной загрузки теперь развертывается в регионах Азиатско-Тихоокеанского региона (APAC) и Европе. Эта функция станет доступной для всех клиентов в течение следующих нескольких месяцев.

Неделя со 2 мая 2022 г.

Документация

Новая статья документации: управление облачными компьютерами Windows 365 с помощью диспетчера конфигураций

Мы опубликовали новую статью справочной документации. Дополнительные сведения см. в статье Управление облачными компьютерами Windows 365 с помощью диспетчера конфигураций.

Неделя с 18 апреля 2022 г.

Локальное сетевое подключение переименовано в сетевое подключение Azure

Термин **локальное сетевое подключение** заменен на **сетевое подключение Azure** во всех пользовательских интерфейсах, документации и коммуникации.

Изменение часового пояса облачного компьютера

Пользователи без прав администратора теперь могут изменять часовой пояс своего облачного компьютера.

Неделя с 11 апреля 2022 г.

Сценарии

Репозиторий GitHub Windows365-PSScripts теперь открыт для вкладов

Репозиторий GitHub Windows365-PSScripts теперь открыт. Он содержит сценарии, связанные с Windows 365, которые помогают администраторам управлять облачными компьютерами. Вы также можете добавить собственные сценарии, чтобы помочь другим пользователям применять Windows 365.

Дополнительные сведения см. в файле сведений репозитория GitHub Windows365-PSScripts.

Неделя с 4 апреля 2022 г. (выпуск службы 2203)

Приложения

Субтитры в режиме реального времени для Microsoft Teams на Windows 365 облачных компьютерах

Для Windows 365 Корпоративная и облачных компьютеров для бизнеса Microsoft Teams теперь может обнаруживать, что говорится на собрании, и отображать субтитры в режиме реального времени. Субтитры можно включить и отключить.

Чтобы использовать динамические субтитры в собрании, перейдите к элементам управления собранием и выберите **Дополнительные параметры** и Включить субтитры в

режиме реального времени.

Дополнительные сведения см. в разделах Динамические субтитры Microsoft Teams, общедоступные на Windows 365 и Использование динамических субтитров в собрании Teams.

Встроенная виртуализация (предварительная версия)

Для большинства поддерживаемых в настоящее время регионов лицензии Windows 365 8 виртуальных ЦП/32 ГБ теперь поддерживают встроенные виртуализации для разных сценариев разработчика, чтобы использовать такие системы, как WSL/Hyper-V. Юго-Восточная Азия и западная часть США 2 в настоящее время не поддерживают эту функцию. Дополнительные сведения см. в разделе Настройка встроенной виртуализации на облачном компьютере.

Улучшенное воспроизведение видео с помощью перенаправления мультимедиа

Вы можете повысить производительность воспроизведения видео на облачных компьютерах с помощью перенаправления мультимедиа (MMR). Дополнительные сведения см. в разделе Улучшение воспроизведения видео.

Управление устройствами

Веб-клиент windows365.microsoft.com теперь общедоступен

Веб-клиент windows365.microsoft.com перешел из предварительной версии в общедоступную.

Подготовка устройств

Отправка пользовательского образа без сетевого подключения Azure

Клиенты, использующие присоединение к Azure Active Directory (Azure AD) без использования виртуальной сети Azure, теперь могут отправлять пользовательские образы непосредственно на вкладке образов в Microsoft Intune. Ранее для отправки образа клиентам необходимо было создать ANC для целевой подписки Azure, которая предоставляет образ.

Имя облачного компьютера добавляется к имени сетевого интерфейса

Имя облачного компьютера теперь добавляется к имени сетевого интерфейса на портале Azure. Это упрощает поиск IP-адреса облачного компьютера при выборе сетевого подключения Azure.

Характер работы пользователей

Отзывы конечных пользователей

Конечные пользователи теперь могут отправлять отзывы корпорации Майкрософт из веб-клиента Windows 365 и непосредственно на windows365.microsoft.com.

Сбор журналов ошибок конечных пользователей

Теперь пользователи могут собирать журналы ошибок.

Неделя с 24 марта 2022 г.

Управление устройствами

Новое удаленное действие: Удаленная помощь

Удаленное действие Удаленная помощь (в Центре администрирования Microsoft Intune) позволяет администраторам запускать удаленный сеанс на облачном компьютере пользователя.

Неделя с 28 февраля 2022 г. (выпуск службы 2202)

Управление устройствами

Восстановление до точки во времени (предварительная версия)

Администраторы и пользователи теперь могут восстанавливать облачный компьютер до состояния на определенный момент времени в прошлом. Доступно несколько краткосрочных и долгосрочных точек восстановления. Дополнительные сведения см. в

статье Восстановление до состояния на определенный момент времени для Windows 365 Корпоративная.

Более высокое разрешение экрана облачных компьютеров (предварительная версия)

Теперь пользователи облачных компьютеров могут выбрать более высокое разрешения экрана при подключении к облачному компьютеру из https://windows365.microsoft.com.

Документация

Новая статья в документации: утвержденные партнеры Windows 365

Мы опубликовали новую статью справочной документации. Дополнительные сведения см. в статье Утвержденные партнеры Windows 365.

Неделя с 14 февраля 2022 г.

Документация

Новая статья документации: удостоверение и проверка подлинности в Windows 365

Мы опубликовали новую статью справочной документации. Дополнительные сведения см. в статье Удостоверение и проверка подлинности в Windows 365.

Управление устройствами

Поддержка облачных компьютеров с присоединением к Azure AD

Windows 365 Корпоративная теперь поддерживает облачные компьютеры, которые присоединены к Azure AD. Эти устройства могут работать в любой из следующих сетей.

- Сеть, размещенная на сервере Майкрософт:
  - Вам не нужно добавлять инфраструктуру Azure
  - Вам не нужно создавать сетевое подключение Azure
- Ваша собственная сеть (с использованием сетевого подключения Azure)

Настройка установленного языка и региона для подготовки облачных компьютеров

При создании политики подготовки администраторы теперь могут настроить установленный язык и регион для новых облачных компьютеров. Ранее облачные компьютеры создавались только с использованием английского языка (США). Дополнительные сведения см. в статье Предоставление пользователям локализованного интерфейса Windows.

Управление и устранение неполадок

Использование сбора диагностики для сбора дополнительных сведений с устройств Windows 365 с помощью удаленных действий Intune

Удаленное действие Intune по сбору диагностики теперь собирает дополнительные сведения с облачных компьютеров Windows 365.

Новые сведения для облачных компьютеров Windows 365 включают следующие данные реестра.

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\AddIns\WebRTC Redirector
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Teams\

Дополнительные данные об удаленном действии **Сбор диагностики** см. в статье Сбор диагностики с устройства Windows.

Подготовка

Новые поддерживаемые регионы Azure: Центральная часть США и Центрально-Западная Германия

В настоящее время для облачных компьютеров Windows 365 подготавливаются два новых региона Azure: Центральная часть США и Центрально-Западная Германия.

Дополнительные сведения о поддерживаемых регионах Azure см. в статье Поддерживаемые регионы Azure для подготовки облачных компьютеров.

Неделя с 17 января 2022 г.

Новая статья документации: оптимизация Cisco Webex для Облачного компьютера Windows 365

Мы опубликовали новую статью справочной документации. Дополнительные сведения см. в статье Оптимизация Cisco Webex для Облачного компьютера Windows 365.

Неделя с 10 января 2022 г.

Новая документация: шифрование данных в Windows 365

Мы добавили в справочную документацию сведения по шифрованию для облачных компьютеров Windows 365. Дополнительные сведения см. в статье Шифрование данных в Windows 365.

Неделя с 3 января 2022 г.

Новая документация: цикл обновления образа коллекции

Мы добавили в справочную документацию сведения по циклу обновлений для образов коллекции облачных компьютеров Windows 365. Дополнительные сведения см. в статье Цикл обновления образа коллекции.

Неделя с 13 декабря 2021 г.

Управление устройствами

Облачные компьютеры в льготном периоде засчитываются в активное использование лицензии на облачные компьютеры

Облачные компьютеры со льготным периодом теперь засчитываются в активное использование лицензии на облачные компьютеры. Эта политика гарантирует, что активное выделение облачных компьютеров вашей организации соответствует общему количеству доступных лицензий в вашем клиенте.

Дополнительные сведения о льготном периоде см. в статьях Общие сведения об управлении устройствами и Окончание льготного периода.

Неделя 29 ноября 2021 г. (выпуск службы 2111)

Управление устройствами

Состояние окончания поддержки операционной системы для Облачных компьютеров

На странице **Политики подготовки** появился новый столбец: **Состояние образа**. В нем указано, используется ли в образе устройства для каждой политики подготовки операционная система (ОС), которая поддерживается обновлениями безопасности Microsoft Windows и прочими обновлениями. Дополнительные сведения см. в разделе Политики жизненного цикла и окончание поддержки операционных систем Облачных компьютеров.

Новая статья документации: оптимизация Zoom для Облачных компьютеров Windows 365

Мы опубликовали новую статью справочной документации. Дополнительные сведения см. в статье Оптимизация Zoom для Облачных компьютеров Windows 365.

Безопасность устройств

Две новых базовых конфигурации безопасности для Облачных компьютеров Windows 11

Теперь Windows 365 Корпоративная поддерживает следующие базовые конфигурации безопасности Windows 11:

- **Защита от незаконных изменений**: помогает защитить Облачные компьютеры от злоумышленников, которые минуют такие функции безопасности, как антивирусная защита.
- **Сканирование сценариев**: помогает определить возможные угрозы, перехватывая сценарии и сканируя их перед запуском.

Дополнительные сведения об обновлениях базовых конфигураций безопасности Windows 11 см. в разделе Базовая конфигурация безопасности Windows 11. Дополнительные сведения о настройке базовых конфигураций безопасности для Облачных компьютеров см. в разделе Развертывание базовых конфигураций безопасности.

Неделя с 1 ноября 2021 г. (выпуск службы 2110)

Управление устройствами

Улучшенный пользовательский интерфейс для сетевого доступа к облачным компьютерам

Улучшения пользовательского интерфейса на странице windows365.microsoft.com:

- Ускорение загрузки.
- Повышение надежности работы.
- Параметры локальных ресурсов (принтер, микрофон, буфер обмена).
- Альтернативные параметры клавиатуры.
- Изменение параметров во время сеанса.
- Поддержка специальных возможностей.

Подготовка

Изменено максимальное время ожидания подготовки на новое значение пять часов

Чтобы повысить надежность, изменено максимальное время ожидания подготовки на новое значение пять часов.

Управление доступом на основе ролей

Настраиваемые роли RBAC Windows 365 в общедоступной предварительной версии

Пользовательские Windows 365 роли управления доступом на основе ролей (RBAC) теперь доступны в Центре администрирования Microsoft Intune. Вы можете выбирать разрешения Windows 365 для создания настраиваемых ролей под потребности организации. Вы также можете создать настраиваемые роли Windows 365 и Intune, а также предоставить администраторам обеих служб детальные разрешения администратора. Дополнительные сведения см. в статье Настраиваемые роли.

Неделя с 11 октября 2021 г. (выпуск службы 2109)

Управление устройствами

Поддержка Изменения размера для лицензий на предварительные и пробные версии

Если у вас есть сочетание платных и бесплатных пробных лицензий, удаленные действия Изменения размера сначала будут использовать платные лицензии. Когда эти лицензии закончатся, будут использоваться ваши пробные лицензии. Дополнительные сведения см. в разделе Изменение размера Облачного компьютера.

Подготовка устройств

Улучшение проверки работоспособности

Проверка работоспособности **DNS может разрешить домен Active Directory** улучшена. Добавлен новый шаг для поиска следующей записи Azure Active Directory DNS. Если его не удается найти, проверка завершается сбоем.

_ldap._tcp.yourDomain.com -type SRV

Управление доступом на основе ролей

Роль администратора Windows 365

Роль администратора Windows 365 теперь доступна для администраторов с помощью назначения ролей в Центре администрирования Microsoft Intune и Azure Active Directory (Azure AD) для Windows. С помощью этой роли администраторы могут широко управлять Облачными компьютерами, пользователями, устройствами и группами с Windows 365 Enterprise. Эта новая роль дополняет другие существующие роли, которые в настоящее время поддерживаются Windows 365: Azure AD глобальный Администратор, Intune Администратор и облачный компьютер в Microsoft Intune. Дополнительные сведения см. в разделе Управление доступом на основе ролей.

Неделя с 4 октября 2021 г.

Управление устройствами

Поддержка Windows 11

Windows 365 Enterprise поддерживает Windows 11 в качестве операционной системы Облачного компьютера.

Для Облачных компьютеров с Windows 11 требуются виртуальные машины 2-го поколения. Сведения о преобразовании существующих пользовательских образов устройств 1-го поколения в устройства 2-го поколения см. в разделе Преобразование существующего пользовательского образа устройства в виртуальную машину 2-го поколения.

Неделя с 13 сентября 2021 г.

Управление устройствами

Новый скрипт PowerShell для установки языков на пользовательские образы устройств

Скрипт PowerShell Windows365LanguagesInstaller может установить 38 дополнительных языков на пользовательские образы устройств. Дополнительные сведения см. в разделе Локализация интерфейса Windows.

Неделя с 6 сентября 2021 г. (версия службы 2108)

Управление устройствами

Возможность завершить льготный период

При определенных условиях Облачный компьютер переводится на семидневный льготный период. В конце этого периода Облачный компьютер будет отозван, а пользователь потеряет доступ.

Теперь вы сможете немедленно завершить льготный период для отдельных Облачных компьютеров. Если вы завершите льготный период вручную, вам не придется ждать все семь дней, чтобы отменить доступ пользователя к Облачному компьютеру.

Дополнительные сведения о льготных периодах см. в разделе Завершение льготного периода.

Неделя с 30 августа 2021 г.

Управление и устранение неполадок

Отчет о производительности ресурсов в службе "Аналитика конечных точек"

В Аналитике конечных точек появился новый отчет под названием **Производительность ресурсов**. **Отчет о производительности ресурсов** содержит метрики производительности ЦП и ОЗУ на Облачных компьютерах. Дополнительные сведения см. в разделе Отчет о производительности ресурсов.

Отчет о соединениях удаленного взаимодействия в Аналитике конечных точек

В Аналитике конечных точек появился новый отчет под названием **Отчет о соединениях удаленного взаимодействия**. Отчет состоит из следующих метрик:

- **Время входа для Облачного компьютера (с)** — общее время, необходимое пользователям для подключения к Облачному компьютеру.
- **Время кругового пути (мс)** — подробные сведения о скорости и надежности сетевых подключений из расположения пользователя.

Дополнительные сведения см. в статье Отчет о подключениях для удаленного взаимодействия.

Неделя со 2 августа 2021 г.

Выпущена общедоступная версия Windows 365

Windows 365 — это новая служба корпорации Майкрософт, которая автоматически создает облачные компьютеры для пользователей. Облачные компьютеры — это новая категория гибридных персональных компьютеров, использующая ресурсы облака и устройство доступа для предоставления полнофункциональной и персонализированной виртуальной машины Windows. Администраторы могут использовать Microsoft Intune для определения конфигураций и приложений, подготовленных для облачного компьютера каждого пользователя. Пользователи могут получить доступ к своим облачным компьютерам с любого устройства и в любом месте. Windows 365 хранит облачный компьютер пользователя и данные в облаке, а не на устройстве, обеспечивая безопасную работу.

Дополнительные сведения о Windows 365 приведены здесь.

Дальнейшие действия

Информацию о лицензировании Windows 365 см. на странице о ценах на Windows 365.

В разработке для Windows 365 Корпоративная

Статья • 01.05.2025

Чтобы помочь в подготовке и планировании, на этой странице перечислены Windows 365 обновления и функции, которые находятся в разработке, но еще не выпущены. Помимо сведений на этой странице:

- Если предполагается, что вам нужно принять меры перед изменением, мы публикуем дополнительную запись в Центре сообщений Office.
- Когда компонент входит в рабочую среду, описание функции перемещается с этой страницы на новые.
- Эта страница и страница "Новые возможности" периодически обновляются. Проверьте наличие дополнительных обновлений.
- Аналогичные функции могут быть объявлены в разное время для Windows 365 для бизнеса.

> **Примечание**
>
> Эта страница отражает наши текущие ожидания относительно Windows 365 возможностей в предстоящем выпуске. Даты и отдельные функции могут измениться. На этой странице описаны не все функции разработки.

Эта статья была обновлена в последний раз в дату, указанную в заголовке выше.

Управление устройствами

Windows 365 варианты аварийного восстановления

В будущем обновлении администраторы будут иметь два варианта аварийного восстановления: существующее аварийное восстановление между регионами и новое аварийное восстановление плюс. Последний выделяет второй облачный компьютер во время настройки, что повышает целевое время восстановления (RTO). Так как облачный компьютер для восстановления уже существует, на момент сбоя не существует риска емкости.

Безопасность устройств

поддержка Windows 365 для государственных организаций для ключа клиента Microsoft Purview

Windows 365 правительство будет поддерживать шифрование облачных компьютеров путем настройки ключа клиента Microsoft Purview. Дополнительные сведения см. в разделе Шифрование служб с помощью ключа клиента Microsoft Purview.

Разное

Дополнительные регионы, добавляя к глобальной поддержке ретранслятора TURN

Поддержка ретранслятора TURN будет улучшена за счет расширения с 14 до более чем 40 регионов по всему миру. Это расширение позволит сократить задержку и повысить надежность подключения за счет обслуживания пользователей из более разных расположений. Выделенный диапазон IP-адресов для Windows 365 трафика, отделенный от ретранслятора TURN ACS, оптимизирует и изолирует трафик для AVD и Windows 365. Это позволит клиентам обойти определенные сетевые ограничения и повысить качество и скорость Windows 365 трафика.

Управление и устранение неполадок

Проверка подключения пользователей вручную

Конечные пользователи смогут вручную выполнять проверки подключения на своих облачных компьютерах с windows365.microsoft.com.

Загрузка Windows 365

Возврат к локальному рабочему столу

В режиме загрузки Windows 365 (только Windows 11) пользователи смогут вернуться к физическому рабочему столу устройства с любого из следующих вариантов:

- Экран CTRL-ALT-DEL
- Экраны ошибок облачного компьютера Администраторы смогут настроить эту функцию в интерактивном сценарии загрузки.

Windows 365 Frontline

Изменение размера Windows 365 Frontline облачных компьютеров в выделенном режиме

Администраторы смогут изменять размер Windows 365 Frontline облачных пк в выделенном режиме.

Дальнейшие действия

Дополнительные сведения о последних событиях см. в статье Новые возможности Windows 365.

Облачный компьютер с поддержкой ИИ (frontier preview)

Введение

Облачные компьютеры с поддержкой ИИ предлагают улучшенные функции поиска Windows и click to Do, доступные в настоящее время только на компьютерах Copilot+. В этой статье рассматриваются требования к настройке, взаимодействие с пользователями и ИТ-администраторами, сведения о конфиденциальности и безопасности, а также руководство по устранению неполадок для упрощения развертывания и управления.

> **Внимание**
>
> Будущая доступность этих функций зависит от результатов этой общедоступной предварительной версии Frontier и может быть изменена.

Требования

Чтобы использовать облачные компьютеры с поддержкой ИИ во время Frontier Preview, необходимо соответствовать спецификациям пользователей и облачных компьютеров, назначить включение ИИ облачным компьютерам в Microsoft Intune и зарегистрироваться в бета-версии программы предварительной оценки Windows.

Спецификации пользовательских и облачных компьютеров

Спецификации пользователей

Так как Frontier Preview предлагается в рамках программы предварительной оценки Windows, организации (и участвующие пользователи) должны быть предварительно зарегистрированы в программе предварительной оценки Windows перед подготовкой облачных компьютеров. Дополнительные сведения см. в разделе О программе предварительной оценки Windows.

Спецификации облачных компьютеров

Чтобы использовать функции с поддержкой ИИ, облачный компьютер должен соответствовать следующим требованиям:

- Иметь номер SKU Windows 365 Корпоративная, который имеет по крайней мере 8 виртуальных ЦП, 32 ГБ ОЗУ и 256 ГБ общего дискового хранилища.

- Развертывается в одном из следующих поддерживаемых регионов:
  - Западная часть США 2
  - Западная часть США 3
  - Восточная часть США
  - Восточная часть США 2
  - Центральная Индия
  - Центральная часть США
  - Юго-Восточная Азия
  - Восток Австралии
  - Южная часть Соединенного Королевства
  - Западная Европа
  - Северная Европа

- Версия сборки ОС Windows **24H2 (>= 26100.6584)** или **25H2 (>= 26200.6584)**.

- Включите политику выполнения **RemoteSigned** на облачном компьютере.
  - Открытие **PowerShell** на облачном компьютере с правами администратора (запуск от имени администратора)
  - Выполните следующую команду: Set-ExecutionPolicy -ExecutionPolicy RemoteSigned -Scope CurrentUser

- Включение политики **Включить функции, представленные через обслуживание, которые отключены по умолчанию**
  - Откройте приложение **Локальныйредактор групповая политика**. (В результатах поиска на панели задач она может отображаться как **Изменение групповой политики** .)
  - Перейдите в **раздел Компоненты Windows/клиентский компонент Центра обновления Windows/Управление взаимодействием с конечным пользователем/Включите функции, представленные через обслуживание, которые отключены по умолчанию**. (Если этот путь не отображается, начните с проверки в разделе **Конфигурация компьютера/Административные шаблоны**.)
  - Щелкните правой кнопкой мыши политику, выберите **Изменить** , а затем во всплывающем окне выберите **Включить** , а затем — **Применить**.
  - Откройте приложение **Параметры**, перейдите к **клиентский компонент Центра обновления Windows**, выберите **Проверить наличие обновлений**, установите все ожидающие обновления, а затем перезагрузите облачный компьютер.

- Если ваш облачный компьютер уже включен в программу предварительной оценки Windows, убедитесь, что на нем есть **сборка ОС 26120.6682 или более поздней версии, прежде чем приступать к остальным инструкциям**. (Если у вас более низкая сборка ОС, воспользуйтесь последней Обновления Windows. Если вы не можете достичь минимального номера сборки ОС, попросите ИТ-администратора включить получение Обновления качества.)

- Если облачный компьютер **еще не** зарегистрирован в программе предварительной оценки Windows, убедитесь, что на нем есть **сборка ОС 26100.6584 или более поздней версии, прежде чем приступать к остальным инструкциям**. (Если у вас более низкая сборка ОС, воспользуйтесь последней Обновления Windows. Если вы не можете достичь минимального номера сборки ОС, попросите ИТ-администратора включить получение Обновления качества.)

Назначение поддержки ИИ облачным компьютерам в Intune

После регистрации пользователей в программе предварительной оценки Windows вы можете назначить включение ИИ облачным компьютерам в Intune, чтобы получить связанные функции, а затем скачать и установить обновления бета-канала программы предварительной оценки Windows. Дополнительные сведения см. в статье Управление функциями с поддержкой ИИ (Frontier Preview).

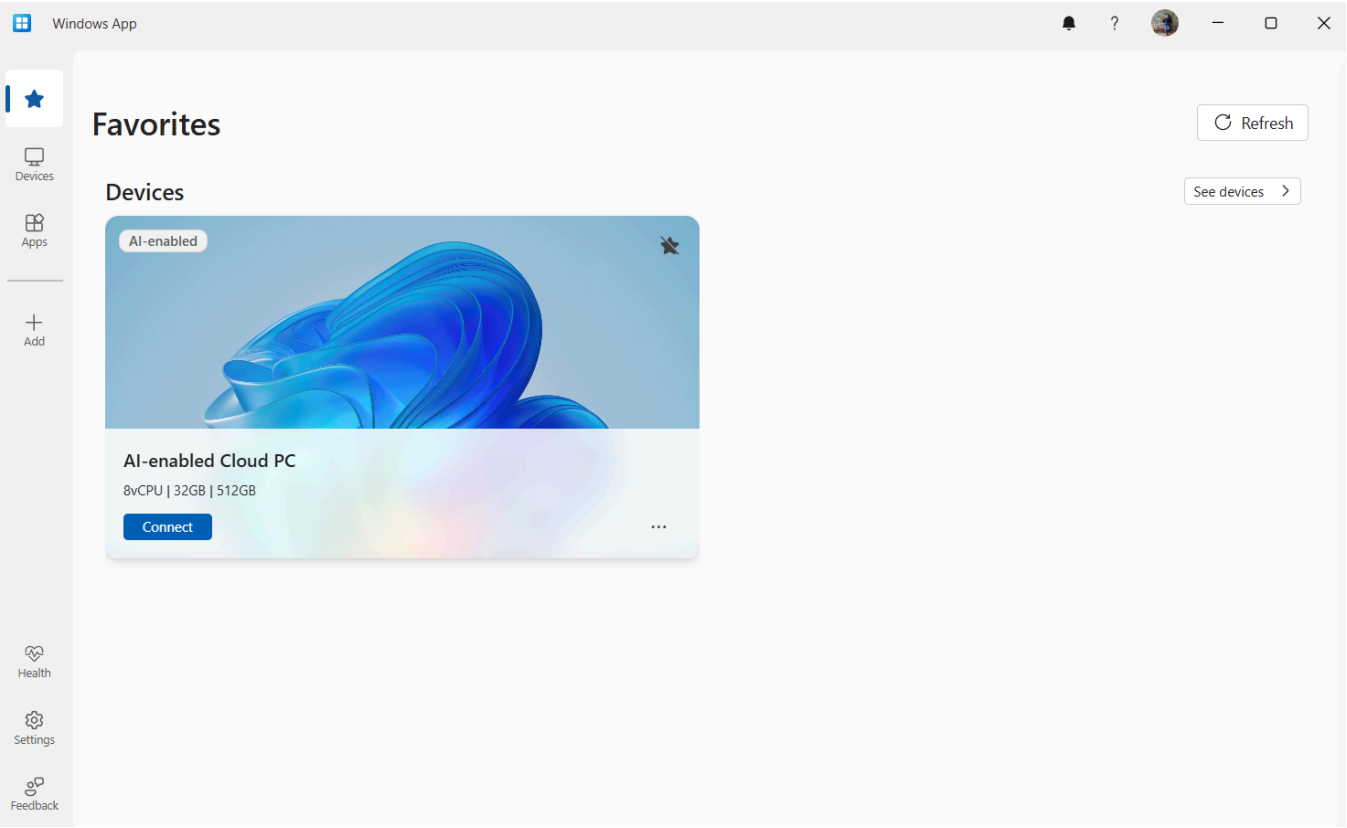
Проверка состояния облачного компьютера с поддержкой ИИ

После предоставления облачным компьютерам прав с поддержкой ИИ и регистрации в канале предварительной оценки Windows для бета-версии может потребоваться до **48 часов** , чтобы связанные функции стали пригодными для использования, так как фоновые процессы должны завершить настройку, прежде чем они будут доступны. По истечении этого периода ожидания **проверка для дополнительных Обновления Windows иперезагрузите облачный компьютер (и повторяйте это действие, пока не будет ожидающих обновлений).** Скорее всего, потребуется повторить проверку и применить обновления 3–5 раз. После этого состояние с поддержкой ИИ можно проверить в нескольких местах:

- Windows App
- Панель задач Windows
- Отчеты Intune

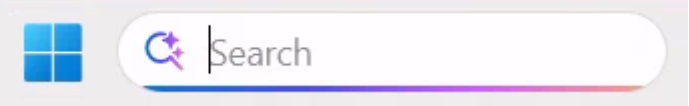
Windows App

Облачные компьютеры с поддержкой ИИ имеют тег "С поддержкой ИИ" на устройстве, карта в Windows App. Это помогает пользователям отличать устройства с поддержкой ИИ от других доступных облачных компьютеров.



Панель задач Windows (из облачного компьютера)

Облачные компьютеры с поддержкой ИИ имеют увеличительное стекло со значком сверкания в поле поиска на панели задач.



> **Примечание.**
>
> После клиентский компонент Центра обновления Windows, сверки могут исчезнуть из значка лупы. Если при щелчке в поле поиска Windows не восстанавливается значок лупы со сверкающими сверканиями, см. статью Известные проблемы с облачным компьютером с поддержкой ИИ — Windows 365 для изучения его отсутствия.

Отчеты Intune

Дополнительные сведения см. в разделе Управление функциями с поддержкой ИИ (Frontier Preview) о том, как ИТ-администраторы могут использовать Intune для проверки, что облачные компьютеры поддерживают ИИ.

Поддерживаемые функции

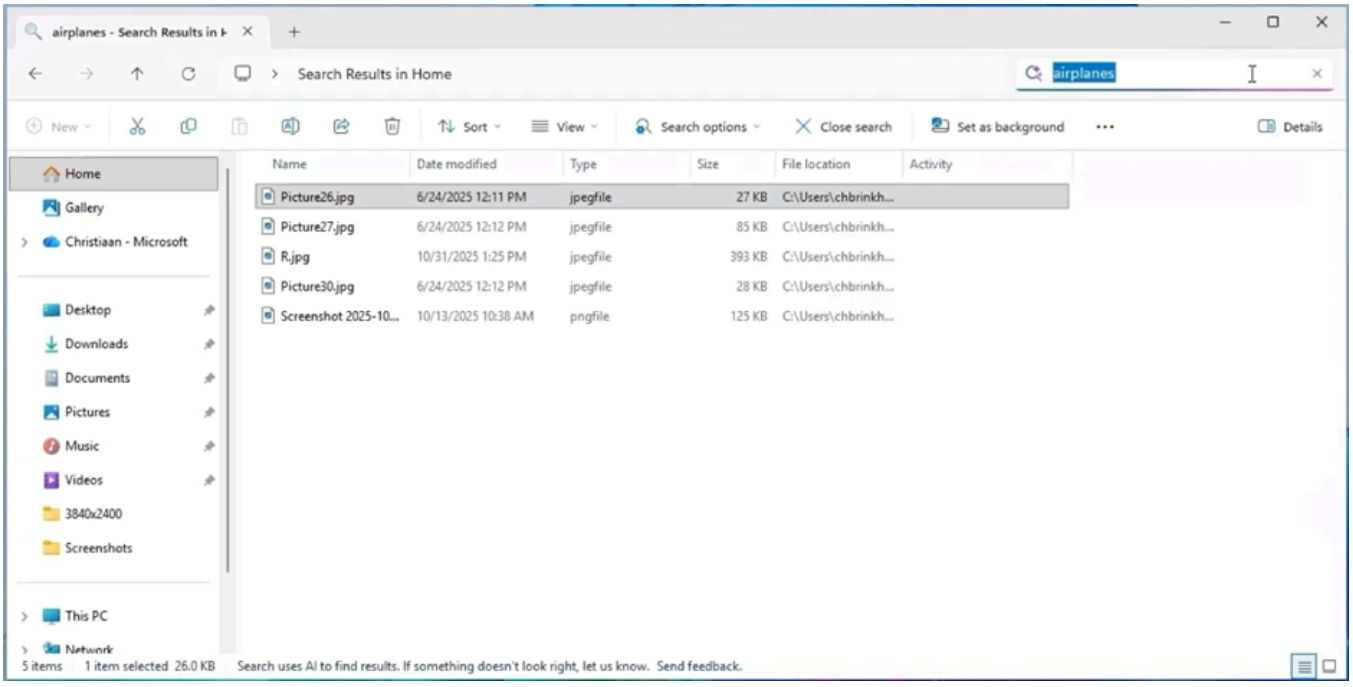
Облачные компьютеры с поддержкой ИИ предоставляют следующие функции, доступные на компьютерах Copilot+:

- Улучшенный поиск Windows
- Щелкните, чтобы сделать

Улучшенный поиск Windows

Улучшенный поиск Windows позволяет пользователям находить файлы с помощью описательных запросов, используя ИИ для интерпретации намерений и предоставления релевантных результатов в поле "Поиск Windows" на панели задач и в проводник. Например, если у вас есть изображение самолета с именем "Picture26.jpg" и выполняется поиск "Самолет", должен появиться правильный файл.

Отказ от ответственности: работает только с определенными форматами текста, изображений и документов; оптимизировано для выбранных языков (английский, китайский (упрощенное письмо), французский, немецкий, японский и испанский).



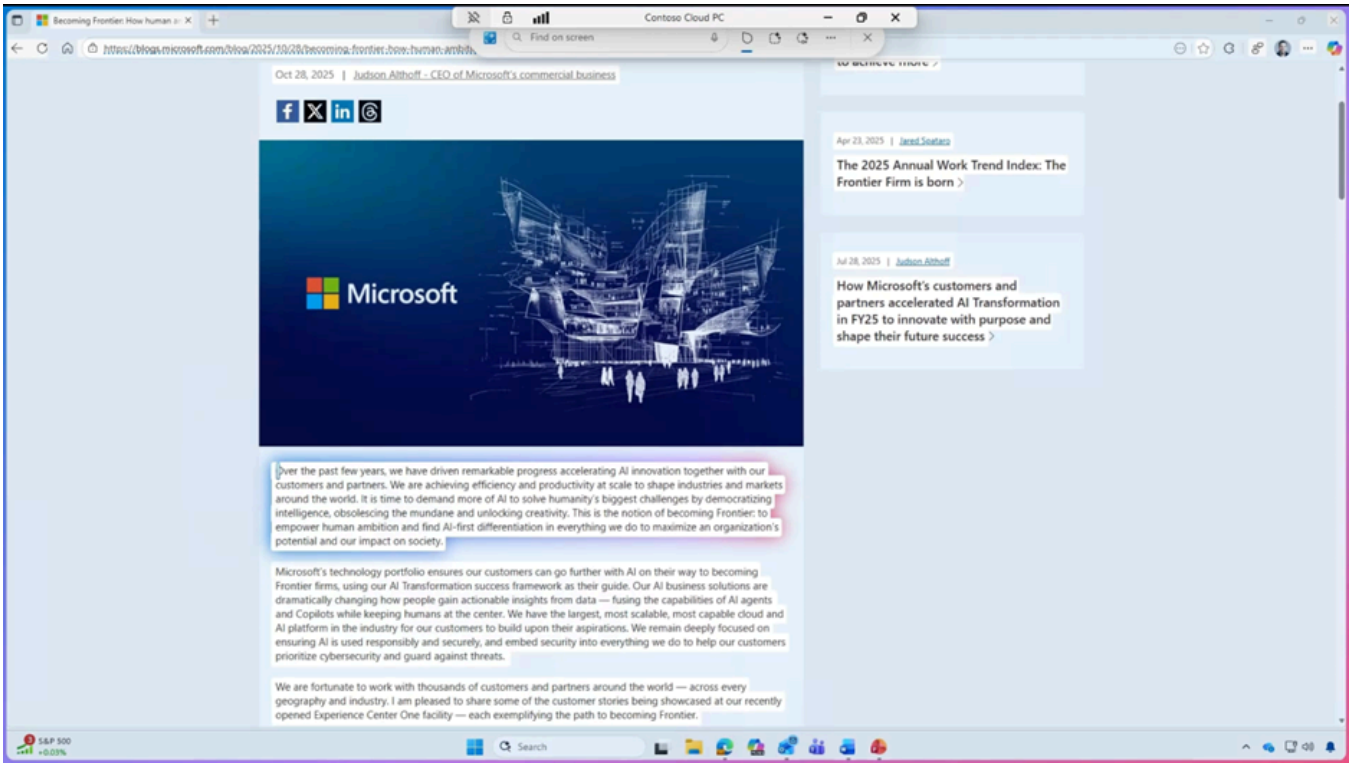
Улучшенный поиск Windows также позволяет пользователям выполнять поиск в нескольких источниках, включая локальные файлы и облачное хранилище, через

OneDrive. Пользователи могут выполнять поиск на основе содержимого файлов, а не только метаданных, таких как название. Этот унифицированный интерфейс работает в поле поиска Windows на панели задач и в проводник.

Дополнительные сведения об улучшенном поиске Windows см. в разделах Быстрый поиск файлов с помощью улучшенного поиска Windows и семантическое индексирование для Microsoft 365 Copilot.

Щелкните, чтобы сделать

Щелкните Сделать, чтобы упростить действия, необходимые для выполнения стандартных действий с выделенным текстом или изображениями на экране. Чтобы активировать эту функцию, нажмите клавишу Windows + Q или удерживайте клавишу Windows, щелкнув элемент на экране левой кнопкой мыши.



> ⓘ **Примечание.**
>
> Необходимо запустить приложение **Click to Do** , прежде чем использовать эту функцию в первый раз после включения ИИ и после **каждого** перезапуска облачного компьютера. После этого можно использовать сочетания клавиш для активации click to Do.

> ⓘ **Примечание.**

В настоящее время некоторые интеллектуальные текстовые действия пока не поддерживаются на облачном компьютере. Текстовые действия с приложениями Майкрософт, такими как Word и Блокнот, работают, но запрос Microsoft 365 Copilot пока не работает.

> **Примечание.**
>
> Действия с изображением теперь доступны на разных устройствах; другие действия зависят от устройства, региона, языка и наборов символов. Для некоторых действий требуется подписка.

Дополнительные сведения о щелчке для выполнения см. в разделе Click to Do: do more with your screen — служба поддержки Майкрософт.

Сведения о конфиденциальности и безопасности

Облачные компьютеры с поддержкой ИИ соответствуют документации по конфиденциальности для Windows 365 здесь: Конфиденциальность и данные в Windows 365:

1. **Обработка данных**. Функции с поддержкой ИИ на Windows 365 облачных компьютерах обрабатывают данные временно с помощью безопасной облачной службы Windows 365. Личные или пользовательские данные не хранятся в облачной службе в любое время и не используются для обучения каких-либо моделей ИИ.
2. **Хранилище данных**. Все данные и индексы хранятся на облачном компьютере. Это поведение не изменилось по сравнению с существующими функциями ИИ Windows.
3. **Элементы управления клиентами**. ИТ-администратор клиента может включить связанные функции ИИ для конкретных пользователей и облачных компьютеров. Эти функции отключены по умолчанию, поэтому ИТ-администратор должен сначала включить их.

Дополнительные сведения о конфиденциальности, данных клиента и содержимом клиентов см. в Windows 365 статье Конфиденциальность и данные в Windows 365.

Устранение неполадок

Сведения об известных проблемах с облачными компьютерами с поддержкой ИИ см. в статье Известные проблемы с облачными компьютерами с поддержкой ИИ — Windows

365.

Last updated on 19.11.2025

Архитектура Windows 365

Статья • 31.01.2025

Windows 365 предоставляет модель лицензирования на одного пользователя в месяц путем размещения облачных компьютеров от имени клиентов в Microsoft Azure. При использовании такой модели отпадает необходимость рассматривать хранение, архитектуру инфраструктуры вычислений или затраты. Архитектура Windows 365 также позволяет использовать имеющиеся инвестиции в сеть и безопасность Azure. Каждый облачный компьютер подготавливается в соответствии с конфигурацией, определяемой в разделе Windows 365 Центра администрирования Microsoft Intune.

Возможность подключения к виртуальной сети

На каждом облачном компьютере в Microsoft Azure имеется сетевая карта виртуальной машины (NIC). Доступно два варианта управления NIC:

- Если вы используете Microsoft Entra присоединение и размещенную сеть Майкрософт, вам не нужно использовать подписку Azure или управлять сетевым адаптером.
- Если вы используете собственную сеть и сетевое подключение Azure (ANC), NIC создаются с помощью Windows 365 в вашей подписке Azure.

NIC подключаются к виртуальной сети Azure на основе конфигурации сетевого подключения Azure (ANC).

Windows 365 поддерживается во многих регионах Azure. Вы можете управлять используемым регионом Azure двумя способами.

- Выбрав сеть, размещенную в Майкрософт, и регион Azure.
- Выбрав виртуальную сеть Azure в подписке Azure при создании ANC.

Регион виртуальной сети Azure определяет место создания и размещения Облачного компьютера.

При использовании собственной виртуальной сети вы можете расширить доступ между вашими текущими регионами Azure и другими регионами Azure, поддерживаемыми Windows 365. Чтобы расширить доступ на другие регионы можно использовать пиринг между виртуальными сетями Azure или Виртуальную глобальную сеть.

С помощью собственной виртуальной сети Azure Windows 365 позволяет использовать функции безопасности и маршрутизации виртуальной сети, в том числе следующие:

- Группы безопасности сети Azure
- Определяемая пользователем маршрутизация
- Брандмауэр Azure
- Сетевые виртуальные устройства (NVAs)

> **Совет**
>
> Для фильтрации веб-содержимого и защиты сети для Облачных компьютеров рекомендуется использовать функции **Защита сети** и **Веб-защита** Microsoft Defender для конечной точки. Эти функции можно развернуть в физических и виртуальных конечных точках с помощью центра администрирования Microsoft Intune.

интеграция Microsoft Intune

Microsoft Intune используется для управления всеми облачными компьютерами. Microsoft Intune и связанные компоненты Windows имеют различные конечные точки сети, которые должны быть разрешены через виртуальная сеть. Конечные точки Apple и Android можно безопасно игнорировать, если вы не используете Microsoft Intune для управления этими типами устройств.

> **Совет**
>
> Обязательно разрешите доступ к **службам уведомлений Windows (WNS)**. Вы можете не сразу заметить последствия, если доступ заблокирован. Однако WNS позволяет Microsoft Intune немедленно активировать действия в конечных точках Windows, а не ждать обычных интервалов опроса политики на этих устройствах или опроса политик при запуске или входе в систему. WNS **рекомендует** устанавливать прямое подключение клиента Windows к WNS.

Вам нужно предоставить доступ только к подмножеству конечных точек в зависимости от расположения клиента Microsoft Intune. Чтобы найти расположение клиента (или единицу масштабирования Azure (ASU),войдите в Центр администрирования Microsoft Intune, выберите **Администрирование**>**клиента Сведения о клиенте**. В разделе **Расположение клиента** будет, например, отображаться "Северная Америка 0501" или "Европа

0202". Строки в документации по Microsoft Intune различаются по географическому региону. Регионы обозначены первыми двумя буквами в имени (na = Северная Америка, eu = Европа, ap = Азиатско-Тихоокеанский регион). Так как клиенты могут перемещаться в пределах региона, рекомендуется разрешить доступ ко всему региону, а не к определенной конечной точке в этом регионе.

Дополнительные сведения о Microsoft Intune регионах служб и сведения о расположении данных см. в разделе Хранение и обработка данных в Intune.

Службы удостоверений

Windows 365 использует как Microsoft Entra ID, так и локальная служба Active Directory Доменные службы (AD DS). Microsoft Entra ID предоставляет:

- Проверку подлинности пользователей для Windows 365 (как и для любой другой службы Microsoft 365).
- Службы удостоверений устройств для Microsoft Intune Microsoft Entra гибридного присоединения или Microsoft Entra присоединения.

При настройке облачных компьютеров для использования Microsoft Entra гибридного присоединения AD DS предоставляет следующие возможности:

- Локальное присоединение к домену для облачных компьютеров.
- Проверка подлинности пользователей для подключений по протоколу удаленного рабочего стола (RDP).

При настройке облачных компьютеров для использования Microsoft Entra присоединения Microsoft Entra ID предоставляет следующие возможности:

- Механизм присоединения к домену для облачных компьютеров.
- Проверку подлинности пользователей для подключений RDP.

Дополнительные сведения о том, как службы удостоверений влияют на развертывание и использование облачных компьютеров, а также управление ими, см. в разделе Удостоверение и проверка подлинности.

Microsoft Entra ID

Microsoft Entra ID обеспечивает проверку подлинности и авторизацию пользователей как для веб-портала Windows 365, так и для клиентских приложений удаленного рабочего стола. Оба поддерживают современную проверку подлинности, что означает, что Microsoft Entra условный доступ можно интегрировать для предоставления:

- многофакторная проверка подлинности
- ограничений на основе расположения;
- управления рисками при входе;
- ограничений сеанса, в том числе следующего:
  - частоты входа для клиентов удаленного рабочего стола и веб-портала Windows 365;
  - сохраняемости файлов cookie для веб-портала Windows 365;
- элементов управления соответствием устройств.

Дополнительные сведения об использовании условного доступа Microsoft Entra с Windows 365 см. в разделе Настройка политик условного доступа.

Доменные службы Active Directory

Windows 365 облачные компьютеры могут быть Microsoft Entra присоединены к гибридной среде или Microsoft Entra. При использовании Microsoft Entra гибридного присоединения облачные компьютеры должны присоединиться к домену AD DS. Этот домен должен быть синхронизирован с Microsoft Entra ID. Контроллеры домена могут размещаться в Azure или локально. При размещении в локальной среде необходимо установить подключение из Azure к локальной среде. Подключение может иметь форму маршрута Azure Express или VPN типа "сеть — сеть". Дополнительные сведения об установке гибридных сетевых подключений см. в статье Реализация безопасной гибридной сети. Подключение должно разрешать обмен данными между облачными компьютерами и контроллерами домена, которых требует Active Directory. Дополнительные сведения см. в статье Настройка брандмауэра для работы с доменом AD и отношениями доверия.

Подключение пользователей

Возможность подключения к Облачному компьютеру обеспечивается Виртуальным рабочим столом Azure. Входящие подключения напрямую через Интернет с облачным компьютером не устанавливаются. Вместо этого подключения выполняются с помощью:

- Облачного компьютера к конечным точкам виртуального рабочего стола Azure.
- Клиентов удаленного рабочего стола к конечным точкам виртуального рабочего стола Azure.

Дополнительные сведения об этих портах см. в разделе список обязательных URL-адресов для Виртуального рабочего стола Azure. Чтобы упростить настройку

средств управления безопасностью сети, используйте теги службы для Виртуального рабочего стола Azure, чтобы идентифицировать эти конечные точки. Дополнительные сведения о тегах служб Azure см. в статьеОбзор тегов служб Azure.

Для установки этих подключений не требуется настраивать облачные компьютеры. Windows 365 легко интегрирует компоненты подключения к Виртуальному рабочему столу Azure в образы из коллекции или пользовательские образы.

Дополнительные сведения о сетевой архитектуре Виртуального рабочего стола Azure см. в статье Общие сведения о сетевом подключении к Виртуальному рабочему столу Azure.

Облачные компьютеры с Windows 365 не поддерживают сторонние посредники подключений.

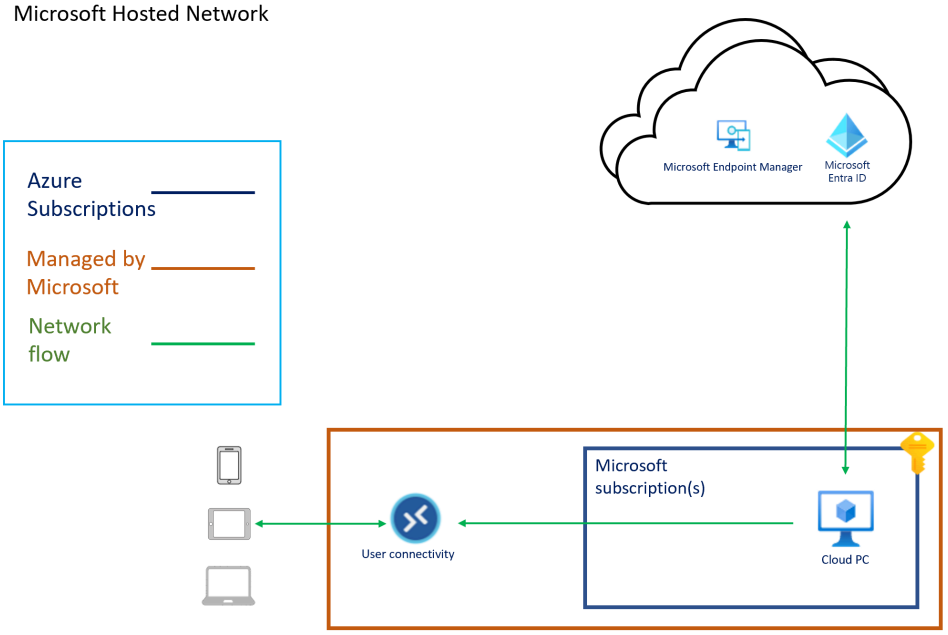
Архитектура размещения от имени

Архитектура размещения от имени позволяет службам Майкрософт после делегирования владельцем подписки соответствующих разрешений с надлежащей областью действия виртуальной сети подключать размещенные службы Azure к клиентской подписке. Такая модель подключения позволяет службе Майкрософт предоставлять программное обеспечение как услугу и службы с пользовательским лицензированием в противоположность стандартным службам на основе потребления.

На следующих схемах показана логическая архитектура конфигурации Microsoft Entra соединения с использованием размещенной сети Майкрософт, конфигурация Microsoft Entra соединения с использованием сетевого подключения клиента ("принеси свою собственную сеть") и конфигурация гибридного соединения Microsoft Entra с использованием ANC соответственно.

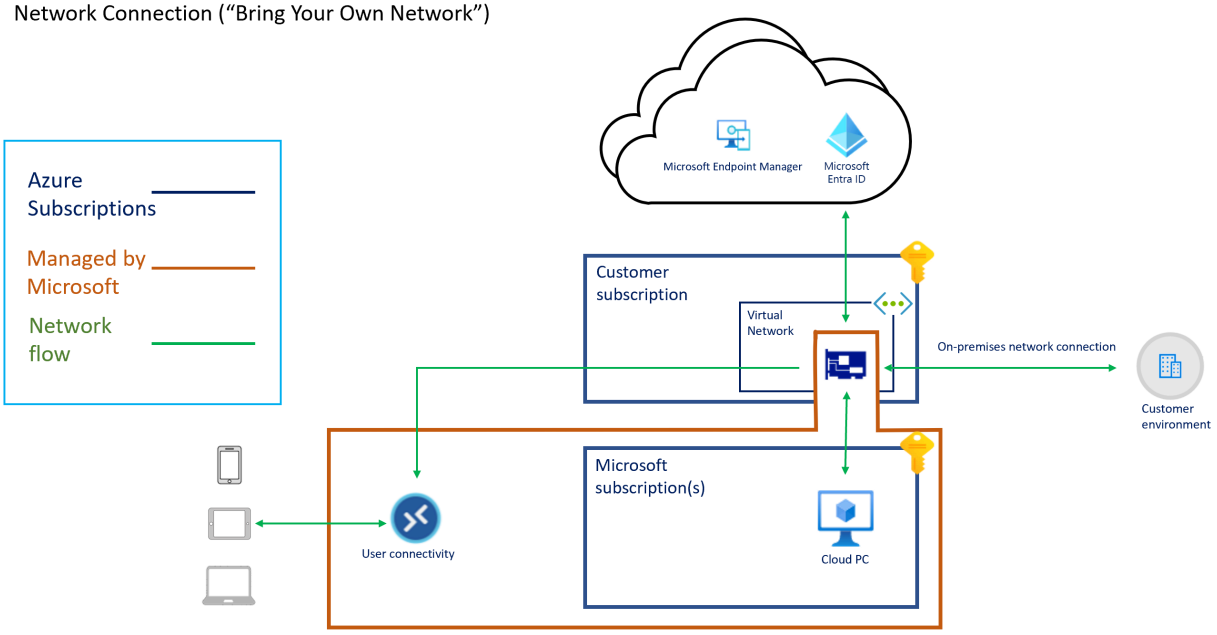
Microsoft Entra join

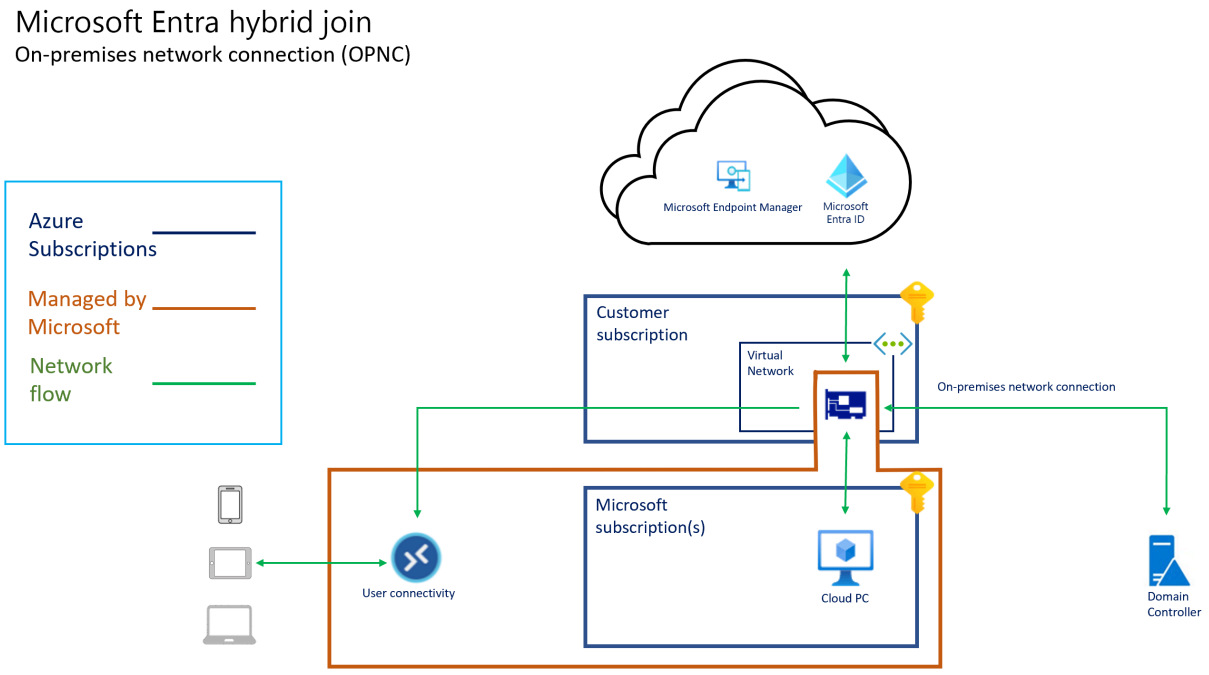
Microsoft Hosted Network



Microsoft Entra join

Network Connection ("Bring Your Own Network")





Все возможности подключения к облачному компьютеру обеспечивает сетевая карта виртуальной машины. Архитектура "размещение от имени" означает, что облачные ПК существуют в подписке, которая принадлежит Корпорации Майкрософт. В связи с этим корпорация Майкрософт берет на себя расходы на выполнение этой инфраструктуры и управление ею.

Windows 365 управляет емкостью и доступностью в регионе в подписках Windows 365. Windows 365 определяет размер и тип виртуальной машины в зависимости от лицензии, назначенной пользователю. Windows 365 определяет регион Azure для размещения ваших облачных компьютеров в зависимости от виртуальной сети, которую вы выбрали при создании локального сетевого подключения.

Windows 365 соответствует политикам защиты данных Microsoft 365. Защита данных клиентов в корпоративных облачных службах Майкрософт обеспечивается с применением различных технологий и процессов:

- различные формы шифрования;
- изоляция логики от других клиентов;
- доступ для ограниченного, контролируемого и защищенного набора пользователей из конкретных клиентов;
- защита от доступа с помощью управления доступом на основе ролей;
- репликация на несколько серверов, в несколько конечных точек хранилища и центров обработки данных для обеспечения избыточности;
- отслеживание несанкционированного доступа, чрезмерного потребления ресурсов и доступности.

Дополнительные сведения о шифровании облачных компьютеров Windows 365 см. в статье Шифрование данных в Windows 365.

Дальнейшие действия

Узнайте об удостоверениях и проверки подлинности Windows 365.

Обратная связь

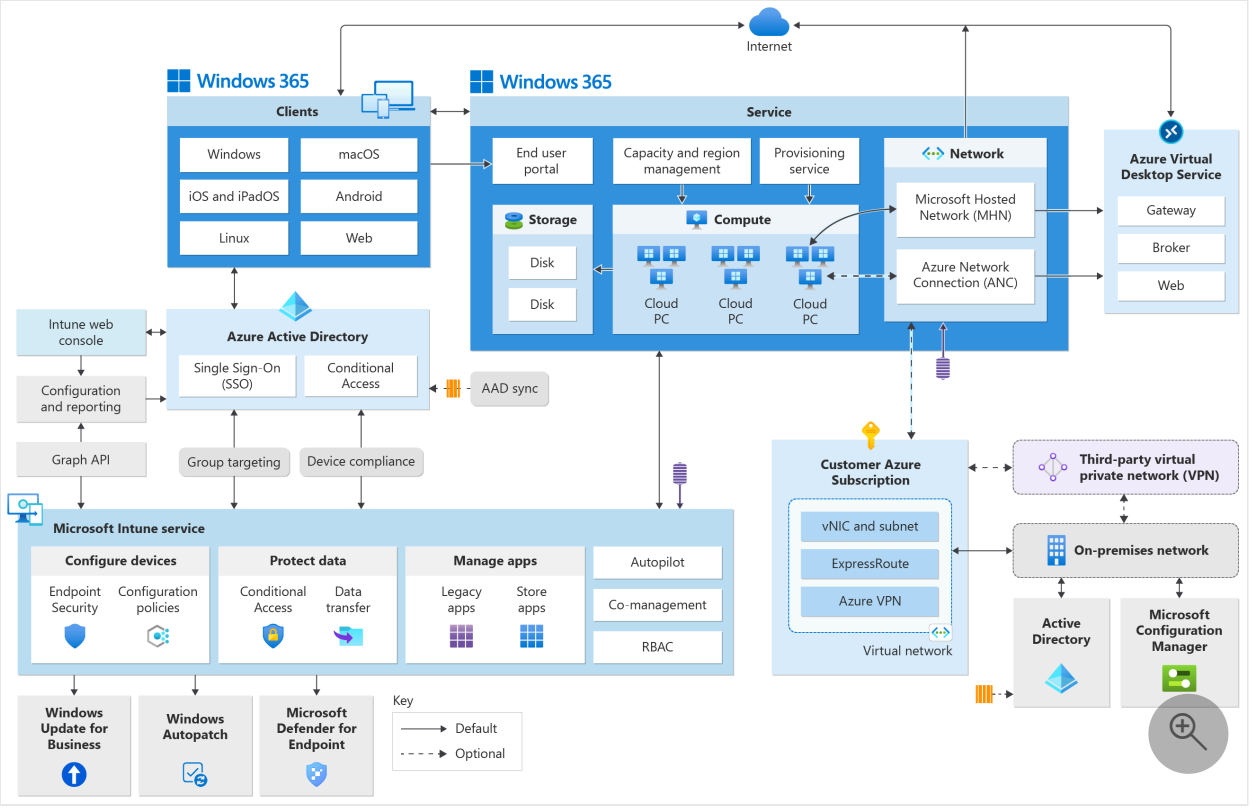
Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Высокоуровневая архитектура для Windows 365

Статья • 31.01.2025

В этом справочнике показана высокоуровневая архитектура для Windows 365.



Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

устойчивость службы Windows 365

Статья • 31.01.2025

Windows 365 предназначена для обеспечения отказоустойчивой и надежной службы для организаций и конечных пользователей, подключающихся к облачным компьютерам и использующих их.

Windows 365 использует службу Виртуального рабочего стола Azure для подключения и брокера подключений конечных пользователей к облачному компьютеру в любом из поддерживаемых регионов Azure из любого места и на любом устройстве. Чтобы свести к минимуму сбои и обеспечить поддержку запросов конечных пользователей и администраторов, устойчивость создается в этих службах. Кроме того, Windows 365 использует другой набор инфраструктуры платформы, которая предоставляет множество функций администратора и конечных пользователей, которые управляют общим интерфейсом Windows 365. Корпорация Майкрософт полностью управляет этой инфраструктурой.

Windows 365 — это служба "программное обеспечение как услуга" (SaaS), в которой клиентам службы не требуется создавать, развертывать и управлять сложной инфраструктурой. Как служба SaaS корпорация Майкрософт управляет базовой инфраструктурой для всех отдельных служб Windows 365. Это управление поддерживает глобальную, полностью доступную и отказоустойчивую службу, на которую клиенты могут полагаться при ежедневном использовании облачных компьютеров. Корпорация Майкрософт постоянно работает над улучшением архитектуры службы, чтобы повысить устойчивость и время восстановления в случае сбоя в любой из связанных служб Azure. Однако, как служба SaaS, Windows 365 требует общей ответственности за предоставление услуг конечным пользователям. Windows 365 соответствует рекомендациям и рекомендациям Microsoft 365 по обеспечению непрерывности бизнес-процессов и обязанностям облачных партнеров.

Помимо уровня подключения к Виртуальному рабочему столу Azure, Windows 365 управляет множеством выделенных служб, спроектированных как микрослужбы для поддержки гибких операций и независимости. Каждая из этих служб выполняет определенные задачи, связанные с запросами администратора или конечного пользователя. Вот некоторые примеры:

- Служба подготовки Windows 365 обрабатывает запросы на развертывание для подготовки облачных компьютеров в соответствии со спецификациями и расположениями, определенными администратором, выполняющим запрос.

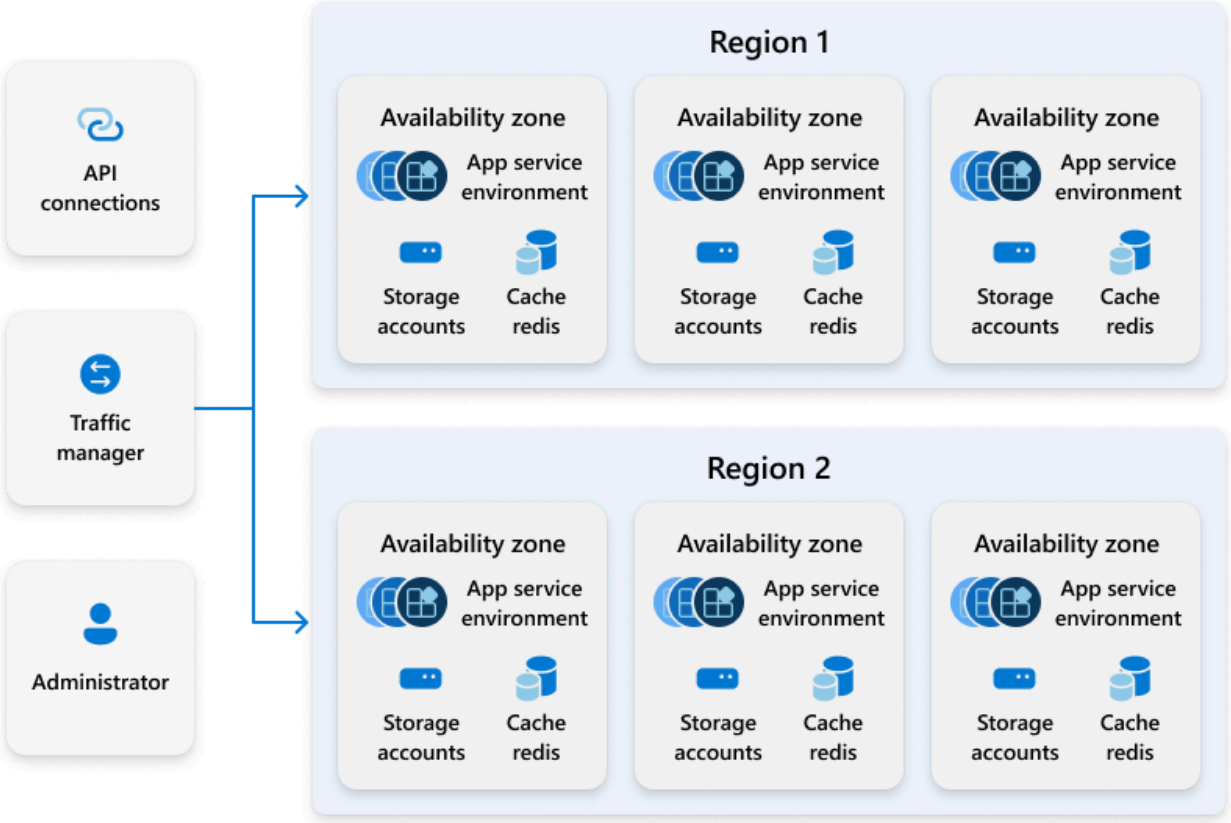
- Служба уведомлений Entra ID отслеживает изменения администраторов Microsoft Entra ID групп, подписок и лицензий, которые активируют новые развертывания.
- Другие службы управляют:
  - Портал администрирования.
  - Портал конечного пользователя.
  - Аварийное восстановление.
  - Диагностика.
  - Устранение неполадок.
  - Мониторинг служб.
  - И все остальные функции Windows 365.

Каждая из этих служб:

- Это собственная веб-служба, использующая стандартные службы инфраструктуры Azure. Каждая служба имеет определенный набор дополнительных требований к инфраструктуре Azure, таких как CosmosDB, хранилище Azure и центры событий.
- Разработан для обеспечения устойчивости. Например, для требований к хранилищу служб используется учетная запись хранения Azure с глобально избыточным хранилищем (GRS). Для служб баз данных, таких как CosmosDB, хранилище данных реплицируется между регионами.
- Разработано для использования служб устойчивости Azure, таких как зоны доступности Azure и отработка отказа между регионами.

На следующей схеме показана архитектура примера службы. Windows 365 распределяет свою инфраструктуру между несколькими зонами доступности в пределах одного региона и между несколькими регионами Azure. Служба работает в активном режиме. Это обеспечивает устойчивость в регионах и между регионами. Если в регионе происходит сбой, служба продолжает работать. Если регион завершается сбоем, служба передается в инфраструктуру дополнительного региона, и обычные операции продолжаются.

Пример архитектуры службы Windows 365, которая позволяет администраторам или конечным пользователям выполнять операции:



Устойчивость виртуальной машины

Каждая Облачный компьютер Windows 365 является одним экземпляром виртуальной машины Azure. Устойчивость обеспечивается на уровне узла Azure для устранения любых проблем с непрерывностью вычислений. Дополнительные сведения см. в статье Общие сведения о непрерывности бизнес-процессов и аварийном восстановлении.

Устойчивость клиента

Windows App — это клиент Windows 365, используемый для подключения к облачному компьютеру. Windows App также можно использовать для подключения к любой windows в облачной службе, например Виртуальному рабочему столу Azure, Microsoft DevBox и службам удаленных рабочих столов, а также для подключений RemotePC или прямых подключений по протоколу RDP. Windows App регулярно обновляется для предоставления пользователям новых функциональных возможностей.

Существует два механизма развертывания для тестирования клиента после того, как он прошел обширное внутреннее тестирование:

- Круг участников программы предварительной оценки, где клиент тестируется набором пользователей, которые выбрали этот круг. Затем предоставляется

обратная связь, и ошибки можно исправить перед развертыванием в общедоступном круге.

- Windows App размещается в Магазине Windows, что обеспечивает надежную глобальную службу распространения программного обеспечения. В Windows App используется постепенное развертывание пакета Microsoft Store, которое позволяет майкрософт обновлять группы компьютеров в течение указанного периода времени. Отслеживая отзывы и аналитику использования этих начальных групп, мы можем убедиться, что обновление готово, прежде чем развертывать его в более широком сообществе. Дополнительные сведения см. в разделе Постепенное развертывание пакета.

Рекомендации для клиентов

Поскольку Windows 365 несет общую ответственность за общую доставку услуг, существуют некоторые рекомендации, которые клиенты должны следовать для повышения устойчивости общей службы.

Размещенная сеть Майкрософт. При создании политики подготовки используйте размещенную сеть Майкрософт. Размещенная сеть Майкрософт — это вариант сети, управляемый корпорацией Майкрософт, где для сетевого подключения к облачному компьютеру не требуется виртуальная сеть Azure или подписка. Этот параметр позволяет корпорации Майкрософт принимать решения о размещении виртуальных машин облачных компьютеров и снижает вероятность проблем с подготовкой. Дополнительные сведения см. в разделе Размещенная сеть Майкрософт.

Сетевое подключение Azure. Если вам требуется детальный контроль корпоративного сетевого трафика (правила брандмауэра, пользовательские маршруты или локальный сетевой доступ), функция сетевого подключения Azure (ANC) позволяет использовать собственную виртуальную сеть Azure или подписку в Windows 365. Для клиентов, использующих ANC, создайте несколько подключений и определите приоритеты этих подключений в порядке использования отработки отказа. Эта приоритизация обеспечивает отработку отказа сетевого подключения в случае сбоя сети. Дополнительные сведения см. в статье Сетевое подключение Azure.

Восстановление на определенный момент времени. Эта служба позволяет полностью восстановить облачный компьютер до предыдущего состояния. Вы можете настроить службу для автоматического создания точек восстановления в коротких и длительных периодах времени. Дополнительные сведения см . в разделе Восстановление на определенный момент времени.

Аварийное восстановление между регионами. Эта Windows 365 надстройка создает моментальные снимки облачных компьютеров. Эти моментальные снимки размещаются в географически удаленных расположениях, определяемых клиентом. Моментальные снимки можно восстановить на облачных компьютерах, работающих в выбранном расположении во время события аварийного восстановления. Дополнительные сведения см. в разделе Аварийное восстановление между регионами.

Дальнейшие действия

Архитектура Windows 365

Схема архитектуры высокого уровня для Windows 365

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Удостоверение и проверка подлинности Windows 365

02.10.2025

Удостоверение пользователя облачного компьютера определяет, какие службы управления доступом управляют этим пользователем и облачным компьютером. Это удостоверение определяет:

- Типы облачных компьютеров, к которым у пользователя есть доступ.
- Типы необлачных ресурсов компьютеров, к которым у пользователя есть доступ.

Устройство также может иметь удостоверение, определенное по типу соединения с идентификатором Microsoft Entra. Для устройства тип соединения определяет:

- Наличие препятствий между устройством и контроллером домена.
- Управление устройством.
- Проверка подлинности пользователей на устройстве.

Типы удостоверений

Существует четыре типа удостоверений:

- **Гибридное удостоверение**. Пользователи или устройства, созданные в локальная служба Active Directory Доменные службы, а затем синхронизированы с идентификатором Microsoft Entra.
- **Облачная идентификация**. Пользователи или устройства, созданные и существующие только в Microsoft Entra идентификаторе.
- **Федеративное удостоверение**. Пользователи, созданные в стороннем поставщике удостоверений, другие пользователи, Microsoft Entra идентификатор или доменные службы Active Directory, а затем федеративные с идентификатором Microsoft Entra.
- **Внешнее удостоверение**. Пользователи, созданные и управляемые за пределами клиента Microsoft Entra, но приглашенные в клиент Microsoft Entra для доступа к ресурсам вашей организации.

> **Примечание**
>
> - Windows 365 поддерживает федеративные удостоверения, если включен **единый вход**.
> - Windows 365 поддерживает внешние удостоверения (предварительная версия). Все требования и ограничения см. во **внешнем удостоверении**

(предварительная версия).

Внешнее удостоверение (предварительная версия)

Поддержка внешних удостоверений (предварительная версия) позволяет приглашать пользователей в клиент Entra ID и предоставлять им облачные компьютеры. Существует несколько требований и ограничений при предоставлении облачных компьютеров для внешних удостоверений:

- Требования
  - **Операционная система облачного компьютера**. Облачный компьютер должен работать под управлением Windows 11 Корпоративная версии 24H2 или более поздней с накопительным Обновления 2025-09 для Windows 11 (KB5065789) или более поздней версии.
  - **Тип присоединения к облачному компьютеру**. Облачный компьютер должен быть присоединен к Entra.
  - **Единый вход**. Для облачного компьютера необходимо настроить единый вход .
  - **Windows App клиент**. Внешнее удостоверение должно подключаться из Windows App в Windows или в веб-браузере.
  - **Лицензирование**. Убедитесь, что внешние удостоверения имеют соответствующие права для программного обеспечения и служб на облачном компьютере. Дополнительные сведения см. в Windows 365 руководстве по лицензированию.
- Ограничения
  - **Политики конфигурации устройств Intune**. Политики конфигурации устройств, назначенные внешнему удостоверению, не будут применяться к облачному компьютеру пользователя. Вместо этого назначьте устройствам политики конфигурации устройств.
  - **доступность Windows 365 для государственных организаций**: поддерживаются только Windows 365 коммерческие выпуски (Enterprise, Business и Frontline). Windows 365 правительство не поддерживается.
  - **Межоблачные приглашения: пользователи из нескольких** облаков не поддерживаются. Облачные компьютеры можно предоставлять только пользователям, которые вы приглашаете от поставщиков удостоверений социальных сетей, Microsoft Entra пользователей из коммерческого облака Microsoft Azure или других поставщиков удостоверений, зарегистрированных в вашем клиенте рабочей силы. Вы не можете подготовить облачные компьютеры для пользователей, которых вы приглашаете из Microsoft Azure для государственных организаций или Microsoft Azure под управлением 21Vianet.

- **Защита маркеров**: Microsoft Entra имеет определенные ограничения для защиты маркеров для внешних удостоверений. Узнайте больше о поддержке Windows App защиты маркеров на платформе.
- **Проверка подлинности Kerberos**. Внешние удостоверения не могут проходить проверку подлинности в локальных ресурсах с помощью протоколов Kerberos или NTLM.

Рекомендации по настройке среды для внешних удостоверений и рекомендации по лицензированию Windows 365 см. в Microsoft Entra рекомендациях по B2B.

Типы соединения с устройствами

Существует два типа соединения, которые можно выбрать при подготовке облачного компьютера:

- **Microsoft Entra гибридное присоединение**. Если вы выберете этот тип соединения, Windows 365 присоединяет ваш облачный компьютер к указанному домену Windows Server Active Directory. Затем, если ваша организация правильно настроена для Microsoft Entra гибридного присоединения, устройство синхронизируется с идентификатором Microsoft Entra.
- **Microsoft Entra присоединение**. Если вы выбрали этот тип соединения, Windows 365 присоединяет ваш облачный компьютер непосредственно к идентификатору Microsoft Entra.

В следующей таблице показаны основные возможности или требования, основанные на выбранном типе соединения.

Развернуть таблицу

Возможности или требования	Microsoft Entra гибридное соединение	Microsoft Entra присоединение
Подписка Azure	Обязательна	Необязательный
Отсутствие препятствий между виртуальной сетью Azure и контроллером домена	Обязательна	Необязательный
Тип удостоверения пользователя, поддерживаемый для входа	Только гибридные пользователи	Гибридные пользователи, пользователи только в облаке или внешние удостоверения (предварительная версия)

Возможности или требования	Microsoft Entra гибридное соединение	Microsoft Entra присоединение
Управление политиками	Объекты групповой политики (GPO) или управление мобильными устройствами Intune	Только управление мобильными устройствами Intune
Поддерживается вход в Windows Hello для бизнеса	Да, и между подключающимся устройством и контроллером домена не должно быть препятствий через прямую сеть или VPN	Да

Проверка подлинности

Когда пользователь обращается к облачному компьютеру, существует три отдельных этапа проверки подлинности:

- **Проверка подлинности облачной службы**. Проверка подлинности в службе Windows 365, которая включает подписку на ресурсы и проверку подлинности шлюза, выполняется с помощью идентификатора Microsoft Entra.
- **Проверка подлинности удаленного сеанса**: проверка подлинности на облачном компьютере. Существует несколько способов проверки подлинности в удаленном сеансе, включая рекомендуемый единый вход .
- **Проверка подлинности в сеансе**. Проверка подлинности приложений и веб-сайтов на облачном компьютере.

Чтобы получить список учетных данных, доступных на разных клиентах для каждого этапа проверки подлинности, сравните клиенты на разных платформах.

> ⓘ **Важно!**
>
> Для правильной работы проверки подлинности локальный компьютер пользователя также должен иметь доступ к URL-адресам в разделе **Клиенты удаленных рабочих столовсписка обязательных URL-адресов Виртуального рабочего стола Azure**.

Windows 365 предлагает единый вход (определяется как единый запрос на проверку подлинности, который может удовлетворить как проверку подлинности службы Windows 365, так и проверку подлинности облачного компьютера) в рамках службы. Дополнительные сведения см. в статье Единый вход.

В следующих разделах содержатся дополнительные сведения об этих этапах проверки подлинности.

Проверка подлинности облачной службы

Пользователи должны проходить проверку подлинности с помощью службы Windows 365 в следующих случаях:

- Они получают доступ к windows.cloud.microsoft.
- Они переходят по URL-адресу, который напрямую связан с их облачным компьютером.
- Они используют поддерживаемый клиент для перечисления своих облачных компьютеров.

Чтобы получить доступ к службе Windows 365, пользователи должны сначала пройти проверку подлинности в службе, выполнив вход с помощью учетной записи Microsoft Entra идентификатора.

Многофакторная проверка подлинности

Следуйте инструкциям в разделе Настройка политик условного доступа, чтобы узнать, как применить Microsoft Entra многофакторной проверки подлинности для облачных компьютеров. В этой статье также показано, как настроить частоту запроса пользователей на ввод учетных данных.

Проверка подлинности без пароля

Для проверки подлинности в службе пользователи могут использовать любой тип проверки подлинности, поддерживаемый идентификатором Microsoft Entra, например Windows Hello для бизнеса и другие параметры проверки подлинности без пароля (например, ключи FIDO).

Проверка подлинности интеллектуальной карта

Чтобы использовать смарт-карта для проверки подлинности для Microsoft Entra идентификатора, необходимо сначала настроить проверку подлинности на основе сертификата Microsoft Entra или настроить AD FS для проверки подлинности на основе сертификата пользователя.

Сторонние поставщики удостоверений

Вы можете использовать сторонних поставщиков удостоверений, если они объединяются с Microsoft Entra идентификатором.

Проверка подлинности удаленного сеанса

Если единый вход еще не включен и пользователи не сохранили учетные данные локально, им также необходимо пройти проверку подлинности на облачном компьютере при запуске подключения.

Единый вход (SSO)

Единый вход (SSO) позволяет подключению пропускать запрос учетных данных Cloud PC и автоматически входить в Windows с помощью Microsoft Entra проверки подлинности. Microsoft Entra проверка подлинности предоставляет другие преимущества, включая проверку подлинности без пароля и поддержку сторонних поставщиков удостоверений. Чтобы приступить к работе, ознакомьтесь с инструкциями по настройке единого входа.

> ⓘ **Важно!**
>
> Для входа на облачный компьютер необходимо настроить единый вход для внешних удостоверений. Если единый вход не настроен, пользователь зависнет в запросе на проверку подлинности удаленного сеанса.

Без единого входа клиент запрашивает у пользователей учетные данные облачного компьютера для каждого подключения. Единственный способ избежать запроса — сохранить учетные данные в клиенте. Рекомендуется сохранять учетные данные только на защищенных устройствах, чтобы запретить другим пользователям доступ к вашим ресурсам.

Проверка подлинности в сеансе

После подключения к облачному компьютеру может появиться запрос на проверку подлинности внутри сеанса. В этом разделе объясняется, как использовать в этом сценарии учетные данные, отличные от имени пользователя и пароля.

Проверка подлинности без пароля в сеансе

Windows 365 поддерживает проверку подлинности без пароля в сеансе с помощью Windows Hello для бизнеса или устройств безопасности, таких как ключи FIDO, при использовании классического клиента Windows. Проверка подлинности без пароля включается автоматически, если облачный компьютер и локальный компьютер используют следующие операционные системы:

- Windows 11 Корпоративная с установленным накопительным Обновления 2022-10 для Windows 11 (KB5018418) или более поздней версии.
- Windows 10 Корпоративная версии 20H2 или более поздней с установленным накопительным пакетом Обновления 2022-10 для Windows 10 (KB5018410) или более поздней версии.

Если этот параметр включен, все запросы WebAuthn в сеансе перенаправляются на локальный компьютер. Для завершения процесса проверки подлинности можно использовать Windows Hello для бизнеса или локально подключенные устройства безопасности.

Чтобы получить доступ к ресурсам Microsoft Entra с помощью Windows Hello для бизнеса или устройств безопасности, необходимо включить ключ безопасности FIDO2 в качестве метода проверки подлинности для пользователей. Чтобы включить этот метод, выполните действия, описанные в разделе Включение метода ключа безопасности FIDO2.

Проверка подлинности интеллектуальной карта в сеансе

Чтобы использовать интеллектуальный карта в сеансе, установите драйверы смарт-карта на облачном компьютере и разрешите перенаправление интеллектуальной карта в рамках управления перенаправлениями устройств RDP для облачных компьютеров. Просмотрите таблицу сравнения клиентов, чтобы убедиться, что клиент поддерживает перенаправление интеллектуального карта.

Дальнейшие действия

Узнайте о жизненном цикле облачного компьютера.

Выбор правильного решения учетных данных без пароля для развертывания Windows 365

08.10.2025

Обзор

Пароли являются общей целью кибератак. Использование только имен пользователей и паролей не является безопасным для любой организации. Хотя многофакторная проверка подлинности (MFA) может блокировать более 99,2 % атак, MFA не застрахована от фишинга или других сложных угроз. Переход на проверку подлинности без пароля повышает уровень безопасности и улучшает взаимодействие с пользователем, что упрощает и делает безопасную проверку подлинности более привлекательной.

Преимущества проверки подлинности без пароля

Проверка подлинности без пароля обеспечивает ряд преимуществ по сравнению с традиционными системами на основе паролей:

- **Уменьшена область атаки:** Устраняет риски кражи паролей, повторного использования, фишинга и атак методом подбора.
- **Улучшенный пользовательский интерфейс:** Пользователям не нужно запоминать сложные пароли или управлять частыми сбросами. Проверка подлинности выполняется быстрее и менее подвержена ошибкам.
- **Более надежная система безопасности:** Современные методы без пароля используют криптографические ключи, биометрические данные и учетные данные, привязанные к устройству, которые более безопасны, чем пароли.
- **Упрощенный доступ:** Пользователи могут безопасно получать доступ к корпоративным ресурсам с различных устройств, поддерживая политики безопасности организации.

Основные сведения о пользовательских сценариях

Чтобы выбрать правильное решение без пароля, необходимо понимать, как пользователи получают доступ к корпоративным ресурсам, где они работают и как хранятся учетные данные. Рекомендуется предлагать несколько надежных вариантов проверки подлинности для удовлетворения различных потребностей. В этом руководстве используются три репрезентативных лица:

Персона 1: Мобильный торговый представитель

- Часто путешествует и посещает клиентов.
- Использует рабочий Windows 11 ноутбук в качестве основного устройства.
- Иногда использует личный iPad и устройство Windows 365 Link на общих рабочих столах.

Persona 2: Call Center Associate

- Работает из одного офиса с помощью выделенной рабочей станции.
- Обращается к корпоративным ресурсам через Windows 365 загрузки в облако.
- Организация предпочитает не выпускать дополнительное оборудование и не применяет MFA на личных устройствах.

Persona 3: Factory Floor Operator

- Использует ИТ-системы редко, главным образом для задач отдела кадров.
- Обращается к ресурсам из киоска в офисе или удаленно из дома.

Параметры проверки подлинности без пароля

Существует несколько вариантов без пароля, каждый из которых имеет уникальные преимущества и компромиссы в переносимости, удобства использования и безопасности.

параметры Device-Linked без пароля

Для пользователей с выделенными устройствами эти решения связывают учетные данные с определенными системами Windows или macOS.

Windows Hello для бизнеса

Windows Hello для бизнеса — это выделенное решение майкрософт для устройств без пароля.

- Обеспечивает надежную и устойчивую к фишингу проверку подлинности для Windows 10 и 11.
- Учетные данные защищены с помощью доверенного платформенного модуля (TPM) устройства.
- Пользователи проходят проверку подлинности с помощью биометрических данных (распознавание лиц, отпечатков пальцев) или ПИН-кода, который никогда не покидает устройство.
- **Ограничение:** Учетные данные зависят от устройства. Настройка требуется на каждом устройстве, и для регистрации могут потребоваться переносимые учетные данные (например, MFA для мобильных устройств, токен FIDO2 или временный пропуск доступа).

Учетные данные платформы для macOS

Учетные данные платформы для macOS предоставляют аналогичный пользовательский интерфейс для пользователей Mac, как Windows Hello на пк с Windows.

- Предлагает аналогичный интерфейс для пользователей Windows Hello для бизнеса для Mac.
- Использует аппаратный криптографический ключ для единого входа (SSO) в приложениях, использующих идентификатор Microsoft Entra.
- Требуется регистрация устройства с помощью поставщика управления мобильными устройствами (MDM) и регистрация с помощью Entra ID.
- **Ограничение:** Учетные данные также зависят от устройства.

Параметры без пароля для мобильных устройств

Мобильные решения устраняют ограничение учетных данных, привязанных к устройству, включив проверку подлинности на нескольких или общих устройствах.

Sign-In телефона (Microsoft Authenticator)

- Разрешает вход без пароля с помощью уведомлений от Entra ID.
- Удобный и простой в развертывании, но не считается устойчивым к фишингу.
- **Заметка:** Нет прямого подключения между мобильным устройством и устройством, для которого выполняется проверка подлинности.

Ключи доступа и ключи FIDO2

Ключи доступа — это современные устойчивые к фишингу учетные данные, основанные на стандартах FIDO. Они могут быть аппаратными (ключи безопасности FIDO2) или

программными (хранятся на телефоне или компьютере).

- **Ключи безопасности FIDO2:** Физические устройства, обеспечивающие надежную и устойчивую к фишингу проверку подлинности. Они поддерживают подключения USB, NFC и Bluetooth.
- **Ключи доступа программного обеспечения:** Хранится на устройстве и связан с устройством проверки подлинности, часто через Bluetooth.
- **Ключи доступа Microsoft Authenticator:** Entra ID ключи доступа можно хранить на устройствах iOS и Android, что обеспечивает устойчивый к фишингу интерфейс без пароля.

Методы подключения:

- **USB A/ USB C:** Прямое подключение, переносимое, но может быть потеряно.
- **NFC:** Сенсорный интерфейс, часто интегрированный с эмблемами сотрудников.
- **Bluetooth:** Включает проверку подлинности на расстоянии, но требует зарядки.

Второй фактор: Для разблокировки ключей FIDO требуется ПИН-код или биометрические данные.

Рекомендации persona

Персона 1: Мобильный торговый представитель

- **Основной:** Windows Hello для бизнеса на выделенном Windows 11 компьютере для быстрого и безопасного доступа.
- **Вторичный:** Мобильные учетные данные (например, Microsoft Authenticator) для гибкости.
- **Общие и личные устройства:** Ключ безопасности FIDO2 для удобного доступа на Windows 365 Link устройствах и личных устройствах iPad.

Persona 2: Call Center Associate

- **Основной:** Windows Hello для бизнеса на выделенном офисном компьютере.
- **Вторичный:** Ключ безопасности FIDO2 с поддержкой NFC, интегрированный с эмблемой доступа сотрудника для использования на других устройствах.

Persona 3: Factory Floor Operator

- **Первичный:** Ключ доступа через Microsoft Authenticator для безопасного доступа между устройствами.

- **Альтернатива:** Биометрический ключ FIDO2 для сред, где мобильные устройства не разрешены.

Заключение

Для успешного развертывания без пароля требуется понимание уникальных потребностей каждого пользователя. Объединяя Windows Hello для бизнеса, ключи безопасности FIDO2 и ключи доступа через Microsoft Authenticator, организации могут обеспечить надежную безопасность и удобство взаимодействия с пользователем. Предложение нескольких вариантов проверки подлинности обеспечивает максимальную гибкость и производительность при сохранении высоких стандартов безопасности.

Чтобы обеспечить отличный пользовательский интерфейс, необходимо учитывать различные потребности и рабочие среды каждого пользователя. Развертывая сочетание Windows Hello для бизнеса, ключей FIDO2 различных типов и ключей доступа с помощью Microsoft Authenticator, мы обеспечиваем надежную безопасность и удобство взаимодействия с пользователем. Этот многоуровневый подход не только повышает уровень безопасности, но и повышает гибкость и удобство, включив в себя сценарии, начиная от офисной работы и заканчивая высокозащищенными или мобильными средами. В конечном счете, предоставление нескольких вариантов проверки подлинности позволяет пользователям оставаться продуктивными, сохраняя при этом высокие стандарты безопасности, независимо от их роли или расположения.

Единый вход — поток подробной проверки подлинности в Облаке Windows

31.10.2025

Введение

В этом документе подробно описан поток проверки подлинности единого входа (SSO) в Windows Cloud в сценариях гибридного удостоверения. В нем рассматривается интеграция объектов Kerberos и RdsAadAuth, выделены шаги, связанные с процессом проверки подлинности. В основном разделе , Поток проверки подлинности единого входа Windows Cloud, объясняется, как RDS Azure Проверки подлинности Active Directory (AAD) применяется в качестве протокола и обеспечивает безопасный доступ к облачным и локальным ресурсам.

Целевая аудитория

- **Специалисты по безопасности:** Основное внимание уделяется обеспечению безопасности механизмов проверки подлинности и защите конфиденциальных данных.
- **Системные архитекторы:** Участвует в разработке и интеграции решений единого входа в общую ИТ-архитектуру.
- **Менеджеры по продуктам:** Контроль над разработкой и реализацией функций единого входа и обеспечение их соответствия бизнес-требованиям.
- **Разработчики:** Работа над техническими аспектами интеграции единого входа с различными приложениями и службами.
- **Сотрудники по соответствию требованиям.** Обеспечение того, чтобы реализация единого входа соблюдала соответствующие правила и стандарты.

Единый вход с помощью Windows 365 и виртуального рабочего стола Azure — проверка подлинности потока маркеров & (протокол проверки подлинности AAD RDS)

Развернуть таблицу

Протокол единого входа Cloud-Native	Гибридное доверие Kerberos
RDS AAD Auth — это новый протокол проверки подлинности удаленного рабочего стола, интегрированный с идентификатором Microsoft Entra. Он заменяет устаревшие методы (например, PKU2U/RDSTLS) с помощью маркеров Entra ID для входа в Windows. Этот метод обеспечивает простой **единый вход** без других запросов и поддерживает современные учетные данные (включая методы без пароля) для входа в cloud PC.	В сценариях гибридного присоединения к идентификатору Microsoft Entra Entra ID работает с объектом Kerberos Server для расширения проверки подлинности в локальной среде AD. Entra ID может выдать частичный билет Kerberos (TGT) для домена AD пользователя, который облачный компьютер обменивает с локальным контроллером домена для полного TGT. С помощью основного маркера обновления Entra ID и AD TGT облачный компьютер может легко получить доступ к облачным и локальным ресурсам в одном сеансе единого входа.

Обзор Windows 365 единого входа с RDS AAD Auth

Windows 365 Облачные компьютеры поддерживают собственный единый вход с помощью протокола проверки подлинности Microsoft Entra идентификаторов удаленных рабочих столов (RDS AAD Auth). Если для Windows 365 включен единый вход, RDS AAD Auth становится методом проверки подлинности по умолчанию. Этот метод проверки подлинности используется, если для клиентской ОС, Windows App клиента и ОС виртуальной машины (ВМ) разрешено использовать протокол. Протокол включен по умолчанию, преднамеренные действия по отключению.

[MS-RDPBCGR]: последовательность подключения RDS AAD Auth | Microsoft Learn

Этот протокол считается как функцией безопасности, так и облачным методом проверки подлинности, так как он применяется Microsoft Entra учетных данных на основе идентификаторов и маркеров вместо паролей. По сути, это расширенный режим безопасности протокола удаленного рабочего стола (RDP), работающий по протоколу TLS, в котором Microsoft Entra ID выдает маркер доступа, привязанный к конкретному целевому устройству, с протоколом, реализованным для сокращения повторного использования маркера.

[MS-RDPBCGR]: получение маркера доступа RDP | Microsoft Learn

Основные преимущества

Проверка подлинности AAD RDS обеспечивает реальный единый вход для пользователей облачных компьютеров. После первоначального входа с идентификатором Microsoft Entra при запуске удаленного сеанса пользователям больше не будет предложено. идентификатор Microsoft Entra выступает в качестве поставщика удостоверений как для

службы Windows 365 (включая инфраструктуру подключения), так и для входа в Windows облачного компьютера.

Этот механизм обеспечивает первоклассную интеграцию с политиками условного доступа и MFA: администраторы могут применять политики (включая требование MFA или соответствующие требованиям устройства) при входе на облачный компьютер, нацелив облачное приложение Windows Cloud Login в условном доступе. Протокол также поддерживает современные факторы проверки подлинности (Windows Hello, ключи FIDO2 и т. д.), обеспечивая потоки входа без пароля на облачный компьютер.

Использование маркеров идентификаторов Microsoft Entra и сертификатов устройств делает подключение устойчивым к фишингу и атакам типа "злоумышленник в середине": маркер RDP недолговечен и криптографически привязан к удостоверению целевого устройства, а канал TLS обеспечивает проверку и шифрование удостоверений сервера.

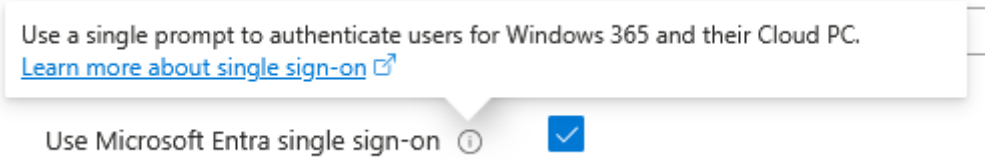
Поддерживаемые среды

RDS AAD Auth работает как для облачных компьютеров, присоединенных к Entra (AADJ), так и для облачных компьютеров с гибридным присоединением к Entra. (Он не поддерживается для виртуальных машин, присоединенных к Microsoft Entra идентификатором Доменные службы, так как они не являются истинными AADJ/HAADJ.) На стороне клиента любой поддерживаемый клиент удаленного рабочего стола (Windows MSTSC, Windows App, веб-клиент и т. д.), обновленный для использования нового протокола, может инициировать подключение на основе Microsoft Entra идентификатора.

Примечательно, что в отличие от более старой проверки подлинности PKU2U локальный клиентский компьютер не требует присоединения к домену или AAD для работы проверки подлинности AAD RDS. Доверие устанавливается с помощью идентификатора Microsoft Entra и удостоверения устройства облачного компьютера. Клиентом может быть любое устройство, на котором пользователь может пройти проверку подлинности для Microsoft Entra идентификатора. На стороне облачного компьютера (узла сеансов) требуется Windows 10/11 или Windows Server 2022 (и полностью исправленный сервер 2019 для Entra). Кроме того, для гибридных сценариев необходимо создать серверный объект Kerberos в локальной доменные службы Active Directory (AD DS), чтобы включить доверие Kerberos с идентификатором Microsoft Entra (описано далее).

Сводка

Включение единого входа в Windows 365 означает, что RDS AAD Auth обрабатывает все имя входа: пользователь проходит проверку подлинности с помощью Entra ID и легко войдет в свой облачный компьютер.



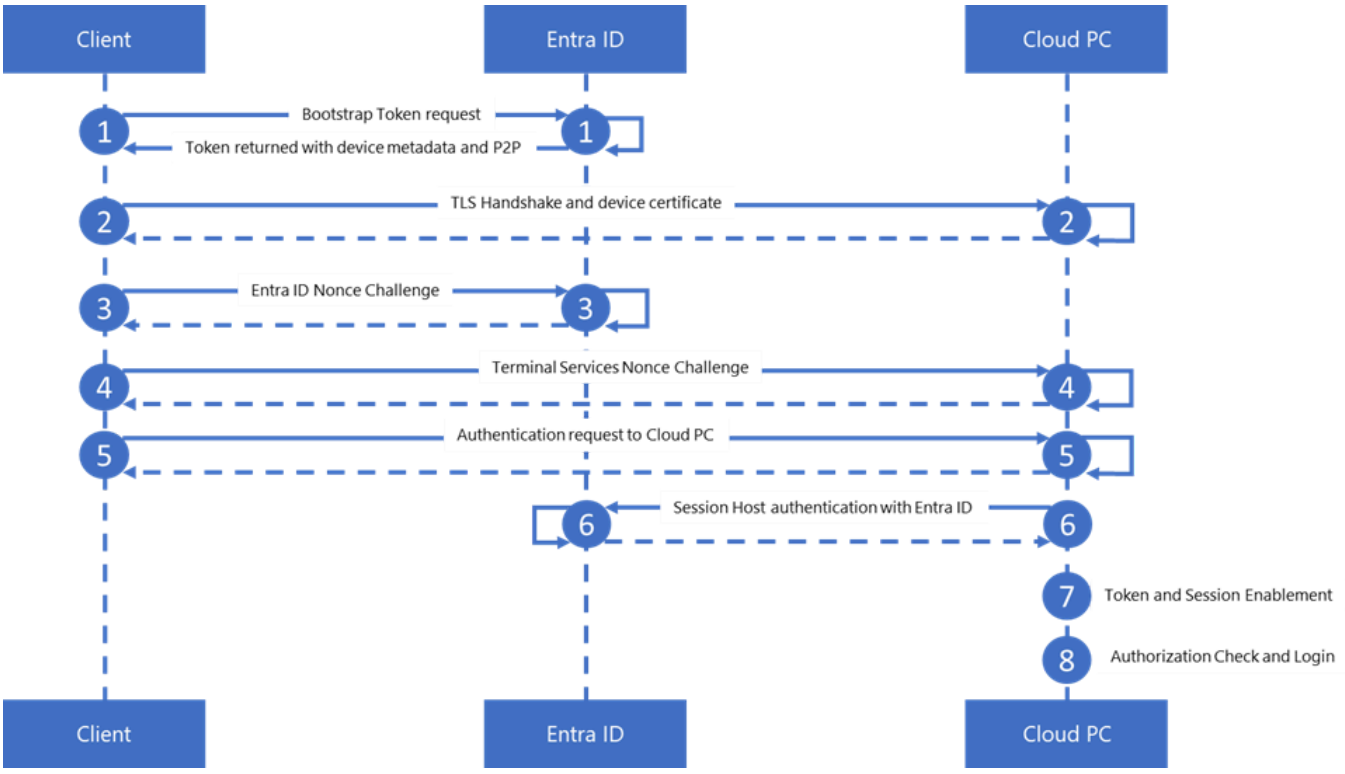
Windows 365 удостоверение и проверка подлинности | Microsoft Learn

В сценарии гибридного присоединения проверка подлинности пользователя выполняется прозрачно по идентификатору Microsoft Entra и локальному AD, если облачный компьютер является гибридным присоединением к Entra. Microsoft Entra идентификатор не может напрямую заносить пользователя в AD, поэтому для завершения локальной проверки подлинности (через доверие к Cloud Kerberos) используется специальный билет Kerberos идентификатора Microsoft Entra идентификатора.

Эта уникальная возможность позволяет пользователю получить доступ к облачным ресурсам (с помощью основного маркера обновления идентификатора Microsoft Entra) и локальным ресурсам (через TGT Kerberos) без дополнительных запросов на вход. В следующих разделах подробно описывается поток маркеров и последовательность взаимодействия клиента и сервера.

Последовательность потока маркеров — шаги проверки подлинности Microsoft Entra идентификатора

Процесс проверки подлинности AAD RDS включает многофакторный обмен данными между клиентом удаленного рабочего стола (Windows App или MSTSC), идентификатором Microsoft Entra и облачным компьютером (узлом сеансов). Ниже приведена высокоуровневая последовательность потока маркеров:



Развернуть таблицу

Шаг	Взаимодействие	Описание
1	Клиент —> Entra ID	**Получение маркера начальной загрузки:** Клиент удаленного рабочего стола сначала получает маркер начальной загрузки для целевого облачного компьютера. Он использует пакет SDK для Microsoft Entra для запроса этого маркера у Entra ID, предоставляя идентификатор облачного компьютера (его Microsoft Entra ID, полное доменное имя (FQDN) или идентификатор). Перед выполнением этого запроса клиент создает эфемерную пару асимметричных ключей. Открытый ключ включается в запрос маркера начальной загрузки, чтобы Entra ID могли привязать выданный маркер к этому ключу. Это устанавливает отношение подтверждения владения (PoP): маркер RDP, выданный позже Entra ID может использоваться только владельцем соответствующего закрытого ключа. После проверки удостоверения клиента и применения применимых политик условного доступа Microsoft Entra id находит целевой облачный компьютер и возвращает маркер начальной загрузки вместе с метаданными устройства, включая корневой сертификат P2P клиента, идентификатор устройства Entra и идентификатор клиента. Этот маркер начальной загрузки представляет собой делегирование Microsoft Entra, которое облачный компьютер использует для получения маркера входа пользователя во время создания сеанса RDP. Так как маркер привязан к PoP, кражи только маркера RDP недостаточно. злоумышленнику также потребуется временный закрытый ключ. Вот почему один и тот же временный ключ необходимо повторно использовать на шаге 5.
2	Клиент <—> облачный	**Подтверждение TLS и сертификат устройства:** Клиент инициирует подтверждение TLS/SSL с облачным компьютером (по протоколу RDP).

Шаг	Взаимодействие	Описание
	компьютер	Для Azure Виртуального рабочего стола (AVD) и Windows 365 клиент устанавливает подтверждение TLS с узлом сеанса с помощью самозаверяющего сертификата, созданного узлом. Этот сертификат является доверенным, так как брокер AVD или Windows 365 проверяет его во время оркестрации, включая этап проверки подлинности компьютера с клиентом в облако. Проверка подлинности с брокером зависит от этого процесса проверки брокера и не использует сертификат MS-Organization-P2P-Access, выданный Microsoft Entra. Сертификат MS-Organization-P2P-Access в основном используется для сценариев PKU2U (одноранговой kerberos), таких как одноранговая проверка подлинности и некоторые службы удаленных рабочих столов (RDS) Azure AD случаев проверки подлинности. Обычно он не участвует в подтверждениях TLS при посредничестве посредника для AVD или Windows 365. Это подтверждает, что клиент действительно подключается к предполагаемому устройству, Microsoft Entra присоединению (устранение проблем с человеком в середине). После установки канала TLS и проверки узла все дальнейшие обмены происходят по этому безопасному каналу.
3	Клиент —> Entra ID	**Microsoft Entra id Nonce Challenge.** Параллельно или далее клиент связывается с Microsoft Entra идентификатором для получения **номера Nonce** (одноразового номера). Этот параметр nonce является проблемой со стороны Microsoft Entra, чтобы обеспечить актуальность запроса проверки подлинности. Microsoft Entra идентификатор возвращает клиенту значение nonce, которое клиент включает в окончательное подтверждение маркера, чтобы предотвратить атаки на воспроизведение.
4	Клиент —> облачный компьютер	**Службы терминалов Nonce (TS Nonce):** Затем клиент получает nonce служб терминалов (TS) с облачного компьютера. Локальный центр безопасности (LSA) на облачном компьютере создает этот параметр nonce, чтобы убедиться, что он исходит из доверенного компонента и является уникальным для сеанса. После согласования X.224 облачный компьютер инициирует подтверждение проверки подлинности AAD RDS, отправляя созданное сервером TS nonce клиенту по установленному каналу TLS. Этот параметр nonce позже используется для привязки запроса проверки подлинности к этому конкретному сеансу.
5	Клиент —> облачный компьютер	**Отправка запроса проверки подлинности на облачный компьютер:** Теперь клиент содержит три элемента: маркер начальной загрузки (шаг 1), идентификатор Microsoft Entra nonce (шаг 2) и TS nonce (шаг 3). Он объединяет их в утверждение RDP, подписывает утверждение локальным временным ключом для обеспечения целостности и подлинности и отправляет его на облачный компьютер в рамках запроса на вход. По сути, клиент доказывает облачному компьютеру, что "у меня есть маркер идентификатора Microsoft Entra для этого устройства, и вот свежие нокесы как от Entra, так и от вас".

Шаг	Взаимодействие	Описание
6	Облачный компьютер (LSA CloudAP) —> Entra ID	**Проверка подлинности узла с Entra ID.** Подключаемый модуль Cloud PC/Entra ID получает утверждение и проверяет его. Облачный компьютер проверяет утверждение RDP, связавшись с идентификатором Microsoft Entra. Это гарантирует, что маркер начальной загрузки, Microsoft Entra идентификатор nonce и TS nonce проверяются до установки сеанса пользователя. идентификатор Microsoft Entra проверяет, что маркер начальной загрузки имеет отступ для правильного устройства (совпадающего идентификатора устройства и клиента) и что Microsoft Entra nonce из шага 3 соответствуют ожиданиям. TS nonce из шага 4 проверяется локально LSA облачного компьютера во время обработки утверждения. После проверки идентификатор Microsoft Entra выдает **основной маркер обновления (PRT)** для пользователя, который, по сути, является маркером сеанса с длительным сроком существования для этого пользователя на этом облачном компьютере. Наряду с PRT идентификатор Microsoft Entra может включать маркер приложения RDP (маркер доступа OAuth для службы RDP) и в гибридных сценариях частичный билет kerberos Ticket-Granting (TGT), чтобы включить Microsoft Entra доверие Kerberos для доступа к локальным ресурсам.
7	Облачный ПК	**Включение маркеров и сеансов:** Выданный Microsoft Entra **PRT** возвращается в компонент CloudAP облачного компьютера. Облачный компьютер теперь имеет действительный маркер сеанса Microsoft Entra идентификатора для пользователя. PRT шифруется и сохраняется в кэше маркеров безопасности облачного компьютера для повторного использования. CloudAP также извлекает **маркер доступа NT** (маркер входа в Windows) из маркера приложения RDP, включенного в PRT. Токен NT представляет удостоверение пользователя на локальном компьютере. Служба терминалов использует этот маркер для обработки входа в Windows.
8	Облачный ПК	**Проверки авторизации и вход:** Авторизация применяется через проверка доступа к дескриптору безопасности прослушивателя RDP, что гарантирует, что у пользователя есть необходимые разрешения для входа в удаленный сеанс. Если доступ проверка выполнен успешно, Winlogon завершает процесс входа, разблокируя существующий сеанс или создавая новый сеанс рабочего стола для пользователя. На этом этапе пользователь полностью вошел в облачный компьютер. Если эти проверки пройдены, облачный компьютер завершает вход через Winlogon, разблокируя существующий сеанс или создает новый сеанс рабочего стола для пользователя. На этом этапе пользователь полностью вошел в облачный компьютер.

Результат

Теперь пользователь проходит проверку подлинности на облачном компьютере с помощью учетных данных идентификатора Microsoft Entra и имеет основной маркер обновления (PRT). Чтобы это работало, облачный компьютер должен быть присоединен Microsoft Entra идентификатором (или гибридным присоединением AAD), так как проверка подлинности устройства требуется для Entra ID, чтобы выдать PRT. При наличии PRT пользователь может легко войти в Windows и получить доступ к защищенным Entra ID ресурсам (например, приложениям Microsoft 365) без повторного ввода учетных данных. Однако политики условного доступа могут по-прежнему требовать дополнительных факторов. Например, если сеанс RDP был установлен с использованием только пароля, но Office 365 требует многофакторной проверки подлинности, пользователю может потребоваться дополнительный фактор. Во многих случаях приложения, интегрированные с WAM, или компоненты Windows могут обновлять PRT с помощью MFA, уменьшая количество повторяющихся запросов.

Поток гибридной проверки подлинности — доверие к облаку Kerberos для локальной среды

Для облачных компьютеров с **гибридным присоединением к Entra** указанный выше поток маркеров дополняется **Microsoft Entra доверия Kerberos**, чтобы разрешить доступ к локальным ресурсам. Так как облачный компьютер, присоединенный к гибридной среде, должен проходить проверку подлинности в локальной службе Active Directory (для файловых ресурсов или устаревших приложений), Microsoft Entra идентификатор не может напрямую предоставить учетные данные домена AD. Здесь вступает в игру **серверный объект Kerberos** .

При попытке единого входа в гибридное присоединенное устройство Microsoft Entra идентификатор (Entra ID) использует объект сервера Kerberos для **выдачи частичного TGT Kerberos** для локального домена AD пользователя.

В приведенном выше потоке маркеров на шаге 6, когда CloudAP связывается Microsoft Entra идентификатор, Microsoft Entra id не только выдает PRT, но и создает TGT Kerberos (билет предоставления билета), который включает идентификатор безопасности Active Directory пользователя (SID) и шифруется для этого домена. Это часто называется *частичным TGT* , так как он не содержит данных авторизации (отсутствие членства в группах и т. д.), а только идентификацию пользователя.

Облачный компьютер получает этот частичный TGT от идентификатора Microsoft Entra вместе с PRT. **По сети** облачный компьютер (через LSA) затем связывается с **локальным контроллером домена** для домена AD пользователя и представляет частичный TGT. Контроллер домена, признавая, что он был выдан доверием Kerberos Microsoft Entra ID, обменивает его на **полное TGT Kerberos** для пользователя (процесс, аналогичный

обычному доверию Kerberos между областями). Теперь облачный компьютер получил стандартный ad TGT, как если бы пользователь вошел в систему с учетными данными AD. На этом этапе облачный компьютер содержит **два ключевых маркера**: Microsoft Entra ID PRT (для облачной проверки подлинности) и AD Kerberos TGT (для локальной проверки подлинности).

При наличии обоих маркеров **пользователь может легко получить доступ к облачным и локальным ресурсам** с облачного компьютера. Например, пользователь может использовать свой облачный компьютер для открытия SharePoint Online (который использует PRT для единого входа), а также сопоставить сетевой диск с файловый сервер (который использует AD TGT для единого входа) без дополнительных запросов на вход.

Это чудо гибридного единого входа возможно только в том случае, если ваша среда настроена для microsoft cloud Kerberos: для этого требуется настроить объект сервера Kerberos в AD и синхронизировать его с Entra ID с помощью Microsoft Entra ID Connect. (Этот объект не является реальным сервером— это представление в AD, которое Microsoft Entra идентификатор использует для создания действительных билетов Kerberos.)

По сути, **объект сервера Kerberos** позволяет Microsoft Entra id действовать как центр распространения ключей домена (центр распространения ключей) для первоначального входа, преодолевая разрыв, чтобы облачный компьютер подумал, что "AD частично вошел в систему этого пользователя", и локальный контроллер домена может завершить задание.

Вопросы безопасности

Частичный TGT, выданный идентификатором Microsoft Entra, содержит минимальную информацию (только идентификатор пользователя). Это гарантирует, что Microsoft Entra id не принимает никаких решений об авторизации. Они остаются в локальном контроллере домена, когда он выдает полный TGT (включая членство в группах и т. д.).

Весь обмен защищен: частичный TGT шифруется таким образом, что только локальные контроллеры домена (через ключи объекта сервера Kerberos) могут расшифровать его. Таким образом, только допустимый контроллер домена может превратить его в доступный TGT. Связь облачного компьютера с контроллером домена для торговли билетом использует стандартный протокол Kerberos по сети (что может потребовать наличия прямой видимости облачного компьютера или VPN-подключения к контроллеру домена).

После получения полного TGT пользовательский интерфейс будет таким же, как если бы он вошел в систему с помощью пароля домена, за исключением того, что все это

произошло с использованием учетных данных Microsoft Entra идентификатора под капотом.

Заключение

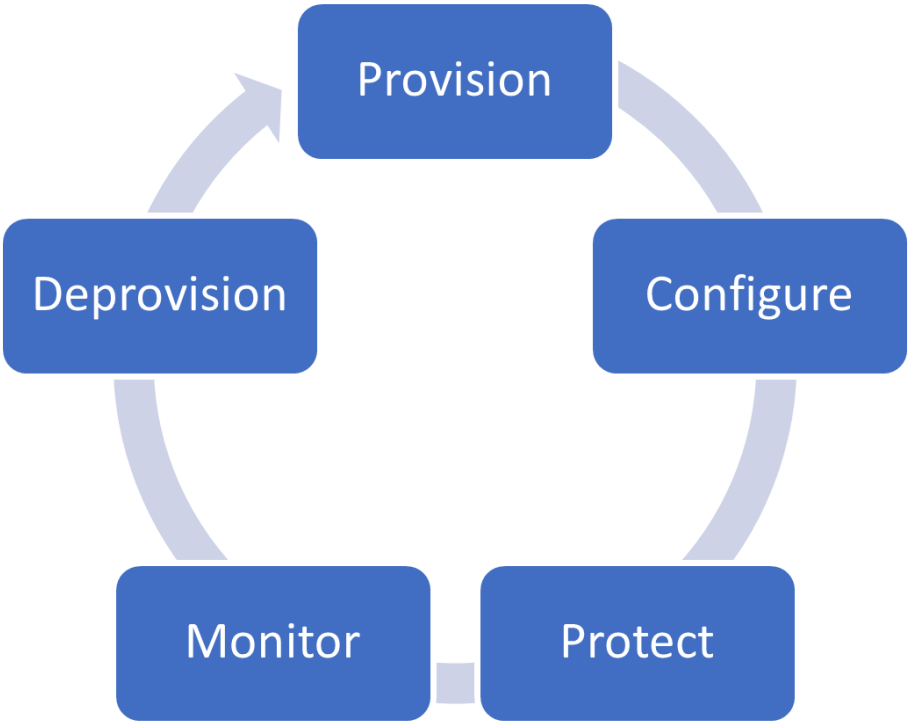
Подробный поток единого входа с использованием объектов Kerberos и RdsAadAuth подчеркивает синергию между традиционными протоколами проверки подлинности и современными облачными системами идентификации. Объединенный подход обеспечивает безопасный, масштабируемый и удобный доступ к локальным и облачным ресурсам. Это делает его идеальным решением для организаций, стремятся реализовать комплексные и эффективные механизмы проверки подлинности.

Жизненный цикл облачного компьютера

Статья • 31.01.2025

Windows 365 координирует жизненные циклы всех облачных компьютеров и управляет ими. Так как облачные компьютеры существуют только в облаке, управление жизненными циклами облачных компьютеров проще, чем управление жизненными циклами физических устройств Windows. Облачные компьютеры поддерживают преимущества управляемости и безопасности, присущие облаку.

Жизненный цикл облачного компьютера состоит из пяти этапов.



Подготовка

Windows 365 предоставляет оптимизированный интерфейс для развертывания облачных компьютеров. Интерфейс администратора для настройки развертывания интегрирован в Центр администрирования Microsoft Intune. Облачные компьютеры подготавливаются в службе Windows 365, подключаются к Azure, присоединяются к Microsoft Entra ID и регистрируются в Microsoft Intune.

Назначая пользователю лицензию Windows 365 и добавляя его в группу, к которой применяется политика подготовки, вы активируете автоматическую подготовку облачного компьютера пользователя.

Каждый облачный компьютер создается с помощью образаоперационной системы. Windows 365 содержит коллекцию образов по умолчанию, обеспечивающих возможность удаленного подключения, оптимизированную как для Windows, так и для Microsoft 365. Вы также можете отправить собственные пользовательские образы, и Windows 365 оптимизирует их.

В Windows 365 также существует инфраструктура мониторинга и искусственные тесты подготовки, встроенные в сетевые подключения Azure. Эти тесты регулярно выполняются для проверки сети и других необходимых компонентов. Эти тесты помогают свести к минимуму сбои при подготовке из-за проблем среды и помогают быстрее их устранить.

Configure (Настроить)

Облачные компьютеры необходимо настроить и защитить так же, как и любые другие конечные точки в существующей среде. Чтобы сделать эту конфигурацию простой, в рамках предоставления каждый облачный компьютер с Windows 365:

- Microsoft Entra присоединено или
- Microsoft Entra гибридное присоединение.

После присоединения облачные компьютеры регистрируются в Microsoft Intune. Такая регистрация означает, что каждый облачный компьютер мгновенно готов к Microsoft Entra условного доступа и управления с помощью Microsoft Intune, включая совместное управление при необходимости.

Microsoft Intune помогает проверить соответствие облачных компьютеров с помощью политик соответствия требованиям. Windows 365 также предоставляет оптимизированные базовые показатели безопасности для облачных компьютеров. Они помогают обеспечить безопасную настройку облачных компьютеров с минимальными издержками. Эти базовые показатели оптимизированы, чтобы исключить влияние на удаленное подключение.

Защита

Windows 365 интегрируется с остальными решениями Microsoft 365 для обеспечения защиты облачных компьютеров. Вы можете использовать интеграцию Microsoft Intune с Microsoft Defender для конечной точки для защиты облачных компьютеров с момента их подготовки. Эта защита включает использование возможностей обнаружения и нейтрализации атак на конечные точки в Microsoft Defender для конечной точки, чтобы определить риск для устройства.

Windows 365 также можно защитить с помощью Microsoft Entra условного доступа. Эта защита включает возможность исключения самой Windows 365 из политик соответствия устройств требованиям, чтобы пользователи могли получать доступ к своим облачным ПК с любого устройства. Для безопасной проверки подлинности пользователей можно по-прежнему использовать многофакторную проверку подлинности, политику рисков при входе и другие механизмы управления.

Windows 365 использует возможность автоматического сканирования Центра обновления Windows для установки последних улучшений. Чтобы обеспечить быструю установку обновлений, конечный пользователь должен как можно скорее войти в облачный компьютер, подготовленный к работе.

Можно также отключить буфер обмена и перенаправление дисков для обеспечения защиты от потери данных. Отключение не позволяет пользователям выполнять следующие действия.

- Копировать и вставлять информацию с облачных компьютеров в другие неуправляемые расположения.
- Сохранять файлы на личных устройствах с облачных компьютеров.

Отслеживать

Ключевым требованием облачных компьютеров является наличие виртуального оборудования, соответствующего потребностям конечного пользователя. Windows 365 интегрируется с аналитикой конечных точек в Оценке производительности Майкрософт. Аналитика конечных точек позволяет измерять загрузку вычислительных ресурсов и памяти на облачных компьютерах. Затем с помощью Windows 365 можно изменить размер этих компьютеров, чтобы они соответствовали требованиям пользователей и их приложений. Это действие изменения размера возникает в Microsoft Intune вместе с другими действиями устройства, чтобы обеспечить беспроблемное взаимодействие между облачными компьютерами и другими конечными точками.

Вы также можете использовать исправление в аналитике конечных точек, чтобы улучшить мониторинг и исправление облачных компьютеров. Исправление позволяет расширить встроенные оптимизации Microsoft 365, которые Windows 365 предоставляет, включая оптимизацию для разнородной ИТ-среды.

Отзыв

Существует несколько способов безопасного удаления доступа пользователя к облачному компьютеру. Если вы удалите лицензию пользователя или политику целевого предоставления, его облачный компьютер будет переведен на семидневный льготный период. В течение этого льготного периода можно исправлять ошибки и восстанавливать функционал без ущерба для пользователя. Чтобы немедленно заблокировать доступ, отключите учетную запись пользователя в локальная служба Active Directory и отмените маркеры обновления пользователя в Microsoft Entra ID.

По окончании срока действия льготного периода Windows 365 полностью отменит подготовку облачного компьютера и его хранилища. Облачные компьютеры шифруют с помощью серверного шифрования в хранилище дисков Azure (ключи, управляемые платформой), чтобы безопасно отзывать устройства.

Дальнейшие действия

Обзор процесса подготовки

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Обзор подготовки к работе

Статья • 14.04.2025

Подготовка к работе в Windows 365 — это автоматизированный процесс, который:

1. создает виртуальную машину для облачного компьютера;
2. настраивает ее для пользователя;
3. выполняет другие задачи для ее подготовки к использованию;
4. Создает и предоставляет учетные данные для входа, которые администраторы могут передавать конечным пользователям.

Для настройки процесса подготовки администраторам необходимо только предоставить некоторые сведения о конфигурации. Затем для пользователей, имеющих лицензию на Windows 365 и соответствующие сведениям о конфигурации, автоматически подготавливается облачный компьютер. Подготовка к работе выполняется один раз для каждого пользователя и каждой лицензии. Любая заданная пара пользователя и лицензии может обладать только одним подготовленным для нее облачным компьютером.

Сколько облачных компьютеров можно подготовить для каждого пользователя?

Каждый пользователь может иметь до одного облачного компьютера из каждого номера SKU Windows 365 Корпоративная и нескольких Windows 365 Frontline облачных компьютеров.

Высокоуровневый процесс

В общих чертах процесс подготовки к работе выглядит следующим образом.

1. Вы создаете политику подготовки для управления доступом к облачным компьютерам. Политики подготовки — это подсистемы, которые собирают и настраивают облачные компьютеры, а также предоставляют пользователям доступ к ним. В политике вы предоставляете сведения о сети, образе, используемом для создания каждого облачного компьютера, и Microsoft Entra группе пользователей.
2. Когда пользователю в группе пользователей Microsoft Entra назначается лицензия на Windows 365, Windows 365 автоматически подготавливает облачный компьютер для пользователя. Эта автоматизация состоит из трех этапов, скрытых от администратора. Дополнительные сведения об этом автоматизированном процессе см. в статье Сведения о процессе автоматической подготовки.

3. После подготовки пользователь может войти на облачный компьютер Windows из любого места.

Объекты политики подготовки

Политика подготовки Windows 365 — это объект в центре администрирования Microsoft Intune, который управляет созданием облачного компьютера.

Администратор при создании политики подготовки должен указать следующие сведения.

- **Сеть**. Размещенная в Майкрософт сеть или сетевое подключение Azure (ANC) определяет, как устройство присоединяется к Microsoft Entra ID и как управляется сетью. В зависимости от типа соединения, ANC может содержать подробные сведения описывающие:
  - Подписка Azure, связанная с облачным компьютером.
  - домен и подразделение, которые необходимо присоединить;
  - учетные данные Active Directory, которые необходимо использовать.
- **Образ**. Образ Windows используется в качестве эталонного для всех облачных компьютеров, подготовленных с помощью этой политики. Можно выбрать образ из коллекции или предоставить собственный пользовательский образ.
- **Конфигурация**. Вы можете управлять дополнительными параметрами, настроенными при подготовке облачного компьютера.
- **Назначение**. Назначение определяет одну или несколько Microsoft Entra групп пользователей. Windows 365 автоматически подготавливает облачный компьютер для каждого лицензированного пользователя в группах пользователей Microsoft Entra политики. Если пользователь будет добавлен в группы пользователей, он также получает облачный компьютер.

Без этой информации Windows 365 не сможет подготовить к работе облачные компьютеры.

После создания политики подготовки Windows 365 обрабатывает весь процесс подготовки для автоматического получения лицензированных пользователей собственных облачных компьютеров. После подготовки облачных компьютеров вы можете сообщить конечным пользователям о том, что их облачные компьютеры готовы к входу.

Изменение этих конфигураций не влияет на ранее подготовленные облачные компьютеры. Однако все недавно подготовленные (или повторно подготовленные) облачные компьютеры отражают обновленные параметры.

Изменения в политиках подготовки

После завершения подготовки облачного компьютера она не повторится, если вы не выполните повторную подготовку вручную.

Изменения, внесенные в любую часть политики подготовки, не вызывают повторную подготовку. Такие изменения не применяются к ранее подготовленным облачным компьютерам. Изменения политики подготовки будут применяться только к облачным компьютерам, которые подготавливаются или повторно подготавливаются после изменений.

Если имя политики подготовки изменено, она не обновляет имя облачного компьютера в разделе Все облачные компьютеры и не обновляет имя enrollmentProfileName в Microsoft Entra ID.

Некоторые параметры политики подготовки нельзя изменить после первоначального создания. Эти параметры включают тип лицензии (Enterprise и Frontline) и тип frontline (выделенный или общий). Для устройств с интерфейсной линией в режиме общего доступа нельзя изменить параметры Entra ID тип присоединения, сеть, география или регион. Если вам нужно изменить эти свойства для устройств с интерфейсом в общем режиме, можно создать новую политику и удалить старую.

Удаление политики подготовки

Политику подготовки можно удалить только в том случае, если она не назначена каким-либо Microsoft Entra группам.

Удаление целевой политики подготовки, которая использовалась для успешной подготовки облачных компьютеров, переводит облачные компьютеры в льготный период. По истечении льготного периода облачные компьютеры удаляются автоматически.

Разрешение конфликтов политики подготовки

Так как политики подготовки назначаются группам пользователей, существует вероятность перекрытия групп или пользователей.

Если пользователю назначено несколько политик подготовки, подготовка учитывает первую назначенную политику подготовки и игнорирует все остальные. Для обеспечения согласованности подготовки рекомендуется избегать перекрытия целевых объектов политик.

Назначения политик подготовки

Назначение политики включает использование групп для назначения политик подготовки пользователям. Каждому пользователю может быть назначена только одна политика подготовки. Первая политика, которому они назначены, используется для подготовки любых облачных компьютеров, на которые они имеют лицензию (все последующие назначения другим политикам игнорируются).

Существует два способа назначения политик подготовки:

- **Дискретный** (предпочтительный): выделенная группа создается специально для назначения политики подготовки. Этот метод удобен в сценариях, когда определенным пользователям или отделам требуются уникальные конфигурации для облачных компьютеров или привилегии доступа.
- **Гибридная** среда. Политика подготовки назначается непосредственно группе лицензий на основе группы. Этот метод может быть полезен для небольших развертываний при управлении несколькими командами с одинаковыми требованиями, при этом ожидается мало изменений.

Повторная попытка подготовки

Если подготовка облачного компьютера завершается неудачей, выполняются две повторные попытки. После трех неудачных попыток выполнить подготовку:

1. процесс подготовки останавливается;
2. облачный компьютер помечается как *неисправный*;
3. Отображается сообщение об ошибке.

После устранения первопричины ошибки можно вручную запустить повторную попытку процесса подготовки, нажав кнопку **Повторить** в диалоговом окне ошибки.

Повторная подготовка

Удаленное действие **повторной подготовки** позволяет администраторам выполнять повторную подготовку облачных компьютеров к работе. Это действие полезно в следующих случаях.

- Тестирование различных конфигураций облачных компьютеров.
- Подготовленный облачный компьютер не работает надлежащим образом.
- Пользователь просто хочет начать работу с новым облачным компьютером.

Действие **повторной подготовки** можно также использовать, когда облачный компьютер находится в состоянии **Не удалось выполнить подготовку** в узле подготовки Windows

365. Повторную подготовку можно рассматривать как процесс, аналогичный сбросу физического устройства.

При повторной подготовке облачного компьютера облачный компьютер удаляется и повторно создается как новый облачный компьютер. Удаляются все пользовательские данные, приложения, настройки и тому подобное.

Облачный компьютер повторно подготавливается к текущим настроенным параметрам в политике подготовки, ориентированной на группу Microsoft Entra пользователя. Если изображение, на который ссылается политика, изменилось или политика изменилась каким-либо другим способом, повторно подготовленный облачный компьютер использует новые параметры.

Для облачных компьютеров frontline в общем режиме можно выполнить массовую повторную подготовку всех облачных компьютеров в политике подготовки. Администраторы также могут выбрать процент облачных компьютеров, доступных для подключения пользователей, без влияния процесса повторной подготовки.

Дополнительные сведения см. в статье Повторная подготовка облачного компьютера.

Пользователи с несколькими лицензиями Windows 365

У пользователя может быть несколько лицензий Windows 365, позволяющих использовать несколько облачных компьютеров. Если у пользователя несколько лицензий, для каждой лицензии подготавливается облачный компьютер с соответствующими спецификациями.

Невозможно активировать различные политики подготовки для разных пользовательских лицензий. Пользователи с несколькими лицензиями подготавливают несколько облачных компьютеров с помощью одной политики подготовки.

Очистка

Когда происходит сбой подготовки облачного компьютера или заканчивается период отсрочки удаленного компьютера, Windows 365 очищает все объекты, созданные во время подготовки. Очистка выполняется приблизительно через три часа после сбоя.

Очищаются следующие объекты:

- объекты Intune;
- Microsoft Entra объектов устройств

- виртуальные сетевые адаптеры Azure.

Группы безопасности сети, созданные для облачных компьютеров, не очищаются, так как на них могут быть и другие объекты.

Все локальные Microsoft Entra учетные записи компьютеров, присоединенные к домену во время подготовки, не удаляются. Windows 365 не имеет достаточных разрешений для удаления локальных объектов-компьютеров, поэтому избыточные объекты-компьютеры отключаются. Мы рекомендуем вашей организации очистить эти отключенные компьютерные объекты во время регулярного процесса обслуживания.

Дальнейшие действия

Узнайте о сетевых подключениях Azure.

Обзор сетевого подключения Azure

Статья • 31.01.2025

Сетевое подключение Azure (ANC) — это объект в центре администрирования Microsoft Intune, который предоставляет профилям подготовки облачных компьютеров необходимые сведения для подключения к сетевым ресурсам. Используются АНК:

- При начальной подготовке Облачного компьютера.
- Когда Windows 365 периодически проверяет подключение к локальной инфраструктуре, чтобы обеспечить лучшее взаимодействие с конечными пользователями.

Типы сетевых подключений

В зависимости от их типа соединения выделяется два типа ANC. Оба позволяют управлять трафиком и доступом облачного компьютера к сетевым ресурсам, но у них разные требования к соединению.

- **Microsoft Entra присоединения**: не требует подключения к домену Windows Server Active Directory (AD).
- **Гибридное Microsoft Entra присоединение**. Требуется подключение к домену Windows Server AD. При создании ANC необходимо предоставить сведения о домене AD.

Подготовка

При подготовке облачного компьютера политика подготовки использует сведения в ANC для подготовки облачного компьютера в подсети Azure. Сведения, необходимые в ANC, включают:

- **Сведения о сети**: подписка Azure, группа ресурсов, виртуальная сеть и подсеть для связывания с облачным компьютером. При запуске политики подготовки создается Облачный компьютер в подписке Azure, размещенной в Майкрософт. Для подключения к локальной сети клиента виртуальная сетевая карта (vNic) внедряется в предоставленную клиентом виртуальную сеть Azure (vNet). Чтобы создать vNic, Windows 365 требуется достаточный уровень доступа к подписке Azure.
- **Домен Active Directory**: домен Active Directory для присоединения, целевое подразделение для объекта компьютера и учетные данные пользователей

Active Directory с достаточными разрешениями для присоединения к домену. При запуске политики подготовки Облачный компьютер присоединяется к этому домену Active Directory. Учетные данные безопасно хранятся в службе Windows 365.

Во время подготовки облачный компьютер подключается к подсети Azure и присоединяется к домену (Windows Server Active Directory или Microsoft Entra ID). В результате облачный компьютер:

- В вашей сети.
- Зарегистрировано в Microsoft Entra ID.
- Зарегистрировано в Microsoft Intune.
- Готов принимать запросы на вход пользователя.

Параметры ANC применяются к облачному компьютеру только во время подготовки.

Альтернативные АНК

Чтобы сделать подготовку облачных компьютеров более надежной в редких случаях ограничений емкости в регионе, можно назначить альтернативные ACS политике подготовки. Вы можете определить порядок приоритета anCs, которые использует политика. Если первый ANC недоступен, политика автоматически использует второй ANC в списке приоритетов. Если второй вариант недоступен, он переходит к следующему и т. д. Этот процесс позволяет администраторам подготовить несколько ANC в разных регионах Azure, что делает подготовку более надежной. Вам не нужно использовать несколько АНК. Дополнительные сведения об использовании альтернативных anCs при создании политик подготовки см. в разделе Создание политик подготовки.

Первая проверка работоспособности

Информация, включенная в ANC, используется для предоставления облачного компьютера. Для успешной подготовки ресурсы, упоминаемые в ANC, должны быть работоспособными и доступными. После создания объекта ANC Windows 365 проверяет следующее:

- Объекты, на которые ссылается ANC, работоспособны.
- К этим объектам можно подключиться.

Эти проверки работоспособности используют информацию ANC, предоставленную для подготовки облачного компьютера. Полный список проверок см. в статье

Проверки работоспособности сетевых подключений Azure.

Во время первой проверки работоспособности ANC нельзя назначить политике подготовки. После завершения проверки работоспособности ANC можно назначить одной или нескольким политикам подготовки.

Периодические проверки работоспособности

После подготовки информация в ANC также используется для мониторинга:

- работоспособности соединения между вашими сетевыми ресурсами;
- облачного компьютера, размещенного в подписке Майкрософт.

Windows 365 сообщает о проблемах конфигурации, которые могут привести к сбоям подготовки или плохому взаимодействию с конечными пользователями. Этот мониторинг снижает затраты на управление. Дополнительные сведения об этих периодических проверках см. в статье Проверки работоспособности сетевых подключений Azure.

Периодичность проверок работоспособности

Проверки ANC выполняются каждые 1–6 часов.

Комплексная полная проверка работоспособности может занять до 30 минут. Проверки работоспособности выполняются на временной виртуальной машине Azure, которая автоматически создается специально для этой цели. Эта виртуальная машина создается автоматически и удаляется после завершения проверок работоспособности. Виртуальная машина подключена к указанной виртуальной сети. Выполняются проверки, чтобы обеспечить успешную подготовку.

После завершения проверка результаты публикуются на панели сетевого подключения Azure Центра администрирования Microsoft Intune. Сведения о результатах проверки см. в статье Проверки работоспособности сетевых подключений Azure.

Повторная проверка работоспособности

Чтобы вручную активировать полную проверка работоспособности, войдите в Центр администрирования Microsoft Intune, выберите **Устройства**>**Windows 365 (в разделе Подготовка)**>**Сетевое подключение**> Azure выберите сетевое подключение > Azure **Повторите попытку**.

Разрешения, необходимые для сетевых подключений Azure

Мастеру ANC требуется доступ к Azure и, при необходимости, к локальным ресурсам домена. Для ANC требуются следующие разрешения:

- Intune роль администратора или Windows 365 администратора.
- Учетная запись пользователя Active Directory с достаточными разрешениями для присоединения домена AD к этому подразделению (Microsoft Entra только ACS гибридного присоединения).

Чтобы создать или изменить ANC, необходимо иметь по крайней мере роль читателя подписки в подписке Azure, где была размещена виртуальная сеть, связанная с ANC.

Полный список требований см. в статье Требования Windows 365.

Изменение сетевого подключения Azure

Изменение параметров в ANC не повлияет на Облачные компьютеры, ранее подготовленные с помощью этого ANC. Только облачные компьютеры, подготовленные после внесения изменений в ANC, отражают такие последующие изменения.

Если вы хотите изменить параметры, связанные с ANC, на ранее подготовленном Облачном компьютере, необходимо повторно подготовить его. Повторная подготовка — это деструктивное действие, поэтому убедитесь, что это то, что вы действительно хотите предпринять. Дополнительные сведения см. в разделе Повторная подготовка.

Удаление сетевого подключения Azure

Вы не можете удалить anc, который используется. Перед удалением объекта необходимо выполнить одно из следующих действий для каждой политики подготовки, которая использует этот ANC:

- Измените политику для использования другого ANC.
- Удалите политику. Для получения дополнительных сведений см. раздел Удаление сетевого подключения Azure.

После выполнения любой из этих операций можно удалить ANC.

Максимальное число сетевых подключений Azure

Каждый клиент имеет ограничение в 50 сетевых подключений Azure. Если вашей организации требуется более 50 сетевых подключений Azure, обратитесь в службу поддержки.

Неактивные АНК

AnCs, которые не используются в течение определенного периода времени, становятся неактивными. Неактивные ACS приостанавливают выполнение проверок работоспособности и не могут быть назначены политике подготовки до тех пор, пока anc повторно не активируется и проверки работоспособности успешно не будут завершены.

Вход пользователей

При попытке пользователя войти в свой облачный компьютер происходит проверка подлинности пользователя.

Для Microsoft Entra АНК гибридного присоединения ANC используется для маршрутизации запроса на проверку подлинности на контроллеры домена. Если ANC или сетевое подключение к вашему домену неисправны, вход пользователя невозможен. Кэшированные учетные данные Windows не могут использоваться по каналу удаленного рабочего стола, поэтому доступность контроллера домена очень важна. Убедитесь, что сеть работает стабильно, или разместите сервер контроллера домена в той же подсети, где находятся ваши Облачные компьютеры.

Для Microsoft Entra присоединения к ANC anc используется для маршрутизации запроса проверки подлинности в Microsoft Entra ID. Кэшированные учетные данные Windows нельзя использовать через канал удаленного рабочего стола, поэтому подключение к Microsoft Entra ID имеет решающее значение.

Дальнейшие действия

Дополнительные сведения об образах устройств

Создание сетевого подключения Azure

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Общие сведения об образах устройств

Статья • 31.01.2025

Windows 365 использует образы операционной системы по умолчанию, а также пользовательские образы для автоматического создания виртуальных Облачных компьютеров, предоставляемых конечным пользователям. Образы по умолчанию доступны из коллекции в Microsoft Intune при создании политики подготовки. Вы также можете отправлять пользовательские образы, созданные вами.

Требования к образу

Образы из marketplace и пользовательские образы должны соответствовать следующим требованиям:

- Поддерживаемые версии Windows 10 или Windows 11 Корпоративная.
- Изображения поколения 2.

  > **Примечание**
  >
  > Недавно мы изменили образы виртуальных машин **поколения 2** (Gen2). Новые пользовательские образы должны быть поколения 2 (Gen2). Существующие пользовательские образы, загруженные на основе поколения 1, останутся активными.

- Образ никогда не должен быть Active Directory, Microsoft Entra ID присоединен, Intune зарегистрирован или зарегистрирован для совместного управления. Дополнительные сведения см. в статье Sysprep не работает правильно на устройстве, зарегистрированном в MDM.
- Обобщенный образ виртуальной машины.
- Образы виртуальных машин с одним сеансом (несколько сеансов не поддерживается).
- Раздел восстановления отсутствует. Сведения об удалении раздела восстановления см. в статье Команда Windows Server: Удаление раздела.
- Размер диска ОС: 64 ГБ по умолчанию. Размер диска ОС автоматически изменяется в соответствии с размером, указанным в описании SKU Windows 365 лицензии.

Пользовательский образ также должен соответствовать следующим дополнительным требованиям:

- Существует в подписке Azure.
- Хранится в Azure в виде управляемого образа .

> **Примечание**
>
> Некоторые выпуски операционной системы Windows, такие как выпуски N или LTSC, не поддерживаются. Чтобы получить наилучшие результаты при создании пользовательского образа, используйте один из образов из коллекции облачных компьютеров в качестве начального шаблона.

Хранение управляемого образа в Azure приводит к расходам. Однако клиенты могут удалить управляемый образ из Azure после успешной отправки его в качестве пользовательского образа в Microsoft Intune.

Образы коллекции

Windows 365 предоставляет встроенную коллекцию образов Windows Enterprise, доступную через поток создания политики подготовки. Каждый образ помогает администраторам с уже включенными предустановленными политиками аудита, такими как политики учетных записей, вход и выход из системы, доступ к объектам и изменение политики.

Они реплицируются во все регионы Azure, чтобы обеспечить быстрый процесс подготовки. Эти образы обновляются ежемесячно:

- Оптимизация для улучшения взаимодействия с пользователем.
- Последние обновления для системы безопасности, чтобы конечные пользователи имели безопасный и удобный интерфейс.

На выбор предоставляется два набора образов в разных версиях Windows Корпоративная:

- **Образы с предварительно установленными приложениями Microsoft 365**: приложения Microsoft 365 и оптимизация для Teams уже установлены. Предварительно применяются следующие параметры:
  - Раздел реестра IsWVDEnvironment (Teams).
  - Среда выполнения C++ (Teams).
  - Средство перенаправления WebRTC (Teams).
  - Microsoft Teams (Teams).
  - Параметры Microsoft Edge, такие как спящая вкладка, принудительный вход в браузер, ускорение запуска и оптимизация первого времени на основе

Microsoft Entra ID и синхронизации. Дополнительные сведения см. в статье Настройка параметров политики Microsoft Edge с помощью Microsoft Intune.
    - Параметры первой конфигурации Microsoft Outlook (автоматический вход на основе Microsoft Entra профиля, поддержка других профилей).
- **Изображения без предустановленных приложений**. Простое изображение без предустановленных приложений (найдите изображения без **приложений M365** в имени).

Оба типа изображений согласованы в объектах групповой политики. Все различия связаны с предустановленными приложениями.

Цикл обновления образа коллекции

Все поддерживаемые образы коллекции Windows 365 обновляются ежемесячно после запланированного выпуска исправлений для систем обслуживания и доставки Windows. Это обновление происходит примерно в середине каждого месяца. Обновленные Windows 365 образы становятся доступными в Intune для подготовки в конце третьей недели месяца.

Каждое обновленное образа включает следующее.

- Ежемесячные обновления образа Windows 10/11
- Обновления безопасности и функций приложений Microsoft 365
    - Windows 365 образы коллекции включают последний выпуск Monthly Enterprise Channel с последними обновлениями для системы безопасности.
- Обновления Microsoft Teams
- Обновления службы перенаправителя WebRTC

Предустановленные приложения являются последней версией, доступной в начале второго вторника этого месяца. Все обновления приложений, опубликованные в этот день, включаются в обновление образа за последующий месяц.

Новые облачные компьютеры автоматически создаются с помощью последних образов. Для существующих облачных компьютеров обновления можно получать путем повторной подготовки.

Пользовательские образы

Если ни один из образов коллекции по умолчанию не соответствует вашим требованиям, вы можете отправить до 20 пользовательских образов устройств.

Дополнительные сведения о создании такого пользовательского образа см. в статье Создание управляемого образа универсальной виртуальной машины в Azure.

Пользовательский образ можно создать, используя любой из образов, упомянутых ранее в качестве отправной точки. Например, можно начать с одного из этих образов, а затем установить дополнительные приложения и внести дополнительные изменения в конфигурацию.

> **Примечание**
>
> Для пользовательских образов в приложении Teams следуйте инструкциям, описанным в разделе **Создание пользовательского образа облачного компьютера, поддерживающего Microsoft Teams** , чтобы настроить необходимые оптимизации. Образы с наборами шифрования дисков не поддерживаются.

Дополнительные сведения о добавлении образа устройства в Windows 365 см. в разделе Добавление и удаление пользовательских образов устройств.

При отправке пользовательского образа устройства Windows 365:

1. Копирует образ во временную подписку.
2. Выполняет следующие проверки для образа:
   a. Проверяет, выполнены ли все требования к образу Windows 365.
   b. Развертывает виртуальную машину и гарантирует, что образы можно загрузить и подготовить как Облачный компьютер.
3. Если у вас есть Microsoft Entra гибридное подключение, Windows 365 реплицирует образ во всех регионах Azure, где у вас есть сетевое подключение Azure.
4. Если у вас есть подключение Microsoft Entra присоединения, Windows 365 реплицирует образ в подготовленный регион во время подготовки.

Дальнейшие действия

Дополнительные сведения о конфигурации устройств.

Сведения об использовании приложений, например Microsoft Teams, с помощью облачных компьютеров..

Сведения о восстановлении облачного компьютера до предыдущего состояния

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Политики жизненного цикла и окончание поддержки операционных систем Облачных компьютеров

Статья • 31.01.2025

Политики жизненного цикла регулируют обслуживание и поддержку (включая окончание поддержки) операционных систем (ОС). Жизненный цикл — это период времени, в течение которого корпорация Майкрософт поддерживает ОС и выпускает для нее ежемесячные обновления безопасности. Дополнительные сведения о жизненных циклах см. в разделах Часто задаваемые вопросы о жизненном цикле — общее и Часто задаваемые вопросы о жизненном цикле — Windows.

Облачный компьютер Windows 365 работает на ОС Windows и следует политике жизненного цикла Майкрософт. После того как ОС на Облачном компьютере достигнет окончания поддержки, она прекратит получать:

- Обновления для системы безопасности
- Обновления, не связанные с безопасностью
- Вспомогательные службы поддержки

Состояние образа

Windows 365 отслеживает сведения об окончании поддержки в Microsoft Intune на странице **Политики подготовки** в разделе **Состояние изображения**. В этом столбце можно узнать, поддерживается ли ОС в образе, используемом каждой политикой подготовки.

Развернуть таблицу

Состояние образа	Образ коллекции	Пользовательский образ
Поддерживается	Облачные компьютеры, созданные с помощью этой политики, имеют ОС Windows, поддерживаемую корпорацией Майкрософт, и могут получать обновления.	То же самое, что и образ коллекции.
Предупреждение	Срок службы поддержки ОС истек менее шести месяцев назад. Облачные	Облачные компьютеры, созданные с помощью этой

Состояние образа	Образ коллекции	Пользовательский образ
	компьютеры, созданные с помощью этой политики, имеют ОС, которая не поддерживается. Такие Облачные компьютеры уязвимы и не получают обновлений безопасности.	политики, имеют ОС, которая не поддерживается. Такие Облачные компьютеры уязвимы и не получают обновлений безопасности.
Не поддерживается	Облачные компьютеры, созданные с помощью этой политики, имеют ОС Windows, которая не поддерживается более полугода. Эту политику больше нельзя назначить пользователям. Чтобы устранить эту проблему, замените образ ОС в политике подготовки на образ с поддерживаемой ОС. Существующие Облачные компьютеры, ранее созданные с помощью этой политики: - Уязвимы и не получают обновлений безопасности. - Не могут пройти подготовку или повторную подготовку. Попытки подготовки Облачного компьютера из этой политики дадут сбой с сообщением **Образ Windows не поддерживается**.	Неприменимо

Эти значения состояния для пользовательских образов также отображаются в столбце **Состояние поддержки ОС** на странице **Образы устройства**.

Политики подготовки

Начиная с даты окончания поддержки, образы коллекции с истекшим сроком действия ОС нельзя будет выбрать для вновь созданных политик подготовки. Также образы будут недоступны для использования при редактировании существующих политик подготовки.

Ограничения действий устройства для неподдерживаемых образов

Облачные компьютеры, связанные с политиками подготовки с использованием образов в неподдерживаемом состоянии, не могут быть повторно подготовлены или сброшены. Любые действия устройства, требующие подготовки, например

повторная подготовка, не могут выполняться на таких облачных компьютерах. На изменение размера устройства не влияет неподдерживаемое состояние.

Удаленные изображения

Образы из коллекции редко могут удаляться до даты окончания поддержки. Такие удаленные образы проходят те же состояния **Предупреждения** и **Неподдерживаемые** , что и операционная система.

Находясь в состоянии Предупреждение, вы можете использовать существующие политики подготовки для развертывания устройств с помощью образа, но вы не можете создать новые политики подготовки с помощью образа.

Для **образов в неподдерживаемом** состоянии подготовка невозможна.

Запланированному удалению всегда предшествует упреждающая связь центра сообщений.

Дальнейшие действия

Чтобы изменить образ устройства для политики подготовки, см. статью Изменить политики подготовки.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Разрешения пользователей

Статья • 31.01.2025

Для некоторых операций Windows 365 требуются разрешения для других служб. Далее приведены примеры таких операций.

- Создание сетевого подключения Azure (ANC)
- Добавление пользовательского образа

Windows 365 использует разрешения управления доступом на основе ролей Azure (RBAC), необходимые для соответствующих операций.

Создание сетевых подключений Azure

Вы создаете ANC, чтобы определять подключения между вашей сетью и системой Windows 365, для успешной подготовки облачных компьютеров. При создании ANC субъекту-службе Windows 365 требуются следующие разрешения:

- **Разрешение на чтение в подписке Azure**: это разрешение используется для упрощения процесса добавления пользовательского образа.
- **Роль участника сетевого интерфейса Windows365 в указанной группе ресурсов**. Это разрешение используется для создания сетевых карточек в выбранной группе ресурсов.
- **Роль пользователя сети Windows365 в виртуальной сети**. Это разрешение используется для подключения созданных сетевых карточек к выбранной виртуальной сети.

При создании ANC вы должны войти в систему с учетной записью владельца подписки.

> **Совет**
>
> При использовании параметра размещенной сети Майкрософт с образом коллекции вам не нужно предоставлять Windows 365 субъекту-службе эти разрешения.

Подробнее см.: Создание сетевого подключения Azure.

Добавление пользовательского образа

Если вы уже создали ANC для связанной с образом подписки Azure, новые разрешения не требуются.

При использовании Windows 365 с размещенной сетью Майкрософт и пользовательским образом субъекту-службе Windows 365 требуется следующее разрешение на отправку пользовательского образа:

- Читатель подписки

Когда вы загружаете пользовательское изображение, вы должны войти в систему с учетной записью владельца или администратора подписки.

Дополнительные сведения см. в разделе "Добавление или удаление пользовательских образов устройств".

Дальнейшие действия

Что такое управление доступом на основе ролей Azure (Azure RBAC)?

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Конфигурация устройства для облачных компьютеров

Статья • 31.01.2025

После подготовки облачного компьютера вы можете управлять им, как и любым другим устройством Windows в Microsoft Intune. Вы можете создать профили конфигурации устройств , чтобы включить и отключить различные параметры в Windows.

Дальнейшие действия

Дополнительные сведения см. в разделе Применение функций и параметров на устройствах с помощью профилей устройств в документации по Microsoft Intune.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Что такое Windows 365 правительство?

23.09.2025

Windows 365 для государственных организаций — это облачная служба, которая автоматически создает виртуальные машины (облачные компьютеры) для пользователей государственных организаций США. Эта служба распространяется на регулируемое облако сообщества для государственных организаций США (GCC) и общедоступное облако. Он соответствует требованиям федерального, государственного и местного правительства США для безопасной потоковой передачи приложений, данных, содержимого и параметров Windows на облачных компьютерах из регулируемых облаков на любое устройство в любое время.

Windows 365 государственными клиентами являются государственные учреждения или государственные учреждения, которые имеют право использовать услуги, размещенные в GCC и GCC High. Службы в облаках GCC и GCC High должны соответствовать определенным требованиям и проходить тщательные проверки аудита, прежде чем клиентам будет разрешено их использовать.

Для сред GCC пользователи, которые получают доступ к Windows 365 облачным компьютерам для государственных организаций, имеют удостоверение в общедоступном облаке, а базовые ресурсы и содержимое защищены в регулируемом облаке для государственных организаций США. Клиенты GCC, которым не требуется защита базовых ресурсов и содержимого в регулируемом облаке для государственных организаций США, могут приобрести Windows 365 Корпоративная использования.

Windows 365 для государственных организаций поддерживает этот сценарий безопасным, масштабируемым и прозрачным способом. Она предоставляет администраторам гибкие возможности для управления пользователями в общедоступном облаке, ресурсами в облаке для государственных организаций и динамической связью между ними.

Windows 365 правительство доступно для клиентов GCC и GCC High в США, а также подрядчиков (в американских организациях), владеющих или обрабатывающих данные от имени государственных учреждений США.

Дополнительные сведения об облачных компьютерах и Windows 365 см. в статье Что такое Windows 365? Дополнительные сведения о покупке см. в разделе Как приобрести Windows 365 для государственных организаций.

Функции, еще не поддерживаемые Windows 365 государственных организаций

Следующие функции пока не поддерживаются для Windows 365 GCC или GCC High.

- Унифицированная панель мониторинга
- Базовые показатели безопасности Windows 365
- Windows 365 системных оповещений в Microsoft Intune для облачных компьютеров
- Отзыв, инициированный пользователем на портале конечного пользователя и веб-клиенте Windows 365
- Citrix HDX Plus для Windows 365
- Перенаправление мультимедиа для улучшенного воспроизведения видео
- Microsoft Dev Box
- Системные оповещения и Уведомления по электронной почте
- отзывы Администратор
- Облачные компьютеры GPU
- Поддержка журналов аудита в Azure Log Analytics
- Новый клиент Microsoft Teams
- Windows 365 загрузки (доступно для GCC, недоступно для GCC High)
- Судебно-медицинские доказательства Microsoft Purview
- переключатель Windows 365
- Windows 365 Frontline облачный компьютер в общем режиме недоступен для GCC и GCC High
- Аварийное восстановление между регионами
- Поддержка клиентов Omnissa Horizon и протокола Blast
- Ключ клиента Microsoft Purview
- HP Anyware для Windows 365
- RDP Shortpath для общедоступных сетей через TURN
- Windows 365 Link
- Настройка перенаправления клиентских устройств для Windows App в iOS,iPadOS/Android с помощью Intune
- Copilot в Intune для Windows 365
- Внешние удостоверения

Дальнейшие действия

Дополнительные сведения о Windows 365 см. в статье Что такое Windows 365?

Что такое Windows 365 Frontline?

04.07.2025

Windows 365 Frontline — это версия Windows 365, которая помогает организациям сократить затраты, позволяя им подготавливать облачный компьютер, который может использоваться несколькими пользователями с одной лицензией.

Windows 365 Frontline сейчас доступна только для Глобального облака Azure.

Доступ к облачным компьютерам передней линии нельзя получить непосредственно из приложения удаленного рабочего стола. Вместо этого необходимо использовать Windows App, если вы хотите получить доступ к компьютеру Frontline Cloud. Вы можете найти Windows App в Microsoft Store или получить доступ к windows.cloud.microsoft с помощью браузера.

Windows 365 Frontline имеет два разных режима: выделенный и общий режим.

Windows 365 Frontline в выделенном режиме

Одна лицензия:

- Позволяет подготовить до трех облачных компьютеров, которые можно использовать неконкурентно, каждый из которых назначается одному пользователю.
- Предоставляет один одновременный сеанс.

Windows 365 Frontline выделенный режим предназначен специально для работников, которым требуется выделенный облачный компьютер, но им не нужен доступ 24/7. Эта система лучше поддерживает более эластичные и распределенные организации, работающие на разных устройствах. Облачные компьютеры frontline в выделенном режиме могут быть полезны для пользователей, которые:

- По расписанию смены.
- Работа в часовых поясах и регионах.
- Неполный рабочий момент.
- Персонал контингента.

Максимальное количество активных сеансов Windows 365 Frontline облачных компьютеров в организации равно количеству приобретенных Windows 365 Frontline лицензий. Например, если вы приобрели 10 лицензий, в выделенном режиме можно подготовить до 30 облачных компьютеров. Десять из этих облачных компьютеров могут быть активными в данный момент времени. Активные сеансы управляются

автоматически. Когда пользователь выходит со своего облачного компьютера, сеанс освобождается для другого пользователя, чтобы начать использовать свой облачный компьютер. Существует буфер параллелизма, превышающий максимальное количество раз в день. Дополнительные сведения см. в разделе Буфер параллелизма.

> **Примечание**
>
> Windows 365 Frontline облачные компьютеры в выделенном режиме автоматически отключается после того, как пользователь выходит из облачного компьютера, и включается при попытке подключения пользователя. Подключение к облачному компьютеру может занять больше времени. Это время подключения не включает выполнение скриптов входа, заданных организациями. После входа пользователя облачный компьютер остается в состоянии питания в течение двух часов. Если пользователь пытается повторно подключиться во время включения облачного компьютера, время подключения совпадает с Windows 365 Корпоративная облачных компьютеров.

Интеллектуальный предварительный запуск для Windows 365 Frontline в выделенном режиме (предварительная версия)

Windows 365 Frontline облачные компьютеры в выделенном режиме могут прогнозировать, когда пользователь подключается и предварительно запускает свой облачный компьютер, прежде чем выполнять вход каждый день. Этот прогноз позволяет увеличить время запуска облачных компьютеров таких пользователей. Например, если пользователь подключается к облачному компьютеру каждый день в 9:00, система распознает это через несколько дней. Когда это произойдет, система запускает облачный компьютер этого пользователя примерно за 30 минут до 9:00 каждый день и будет поддерживать его питание в течение двух часов до подключения пользователя. Таким образом, когда пользователь подключается в 9:00, его облачный компьютер уже запущен и он может быстро подключиться. Если пользователь подключается за пределами обычного времени запуска, он должен дождаться запуска облачного компьютера.

Чтобы прогноз работал должным образом, пользователи должны подключаться к своим облачным компьютерам по крайней мере в течение трех дней за последние 30 дней. Если у пользователя нет шаблона подключения, прогноз может быть не точным, и предварительный запуск не будет работать должным образом.

Предварительно запущенные облачные компьютеры не потребляют лицензию на подключение к сеансу, пока подключение пользователя не будет завершено. Если

пользователь не подключится в течение двух часов, облачный компьютер автоматически завершает работу.

Интеллектуальная предварительная версия доступна в общедоступной предварительной версии. В течение этого времени он применяется ко всему клиенту и включен по умолчанию (и не может быть отключен администраторами).

Windows 365 Frontline в режиме общего доступа

Одна лицензия:

- Позволяет подготовить один облачный компьютер, который можно совместно использовать для группы пользователей.
- Предоставляет один одновременный сеанс.

Windows 365 Frontline в режиме общего доступа предназначен специально для работников, которые

- Требовать доступ к облачному компьютеру для выполнения специализированных задач в течение короткого времени в течение рабочего дня.
- Не требуется сохраняемость данных.

Облачные компьютеры frontline в режиме общего доступа могут быть полезны для пользователей, которые:

- Сотрудники, которые работают с клиентами.
- Внешние подрядчики.

Максимальное количество активных сеансов Windows 365 Frontline облачных компьютеров в организации равно количеству Windows 365 Frontline лицензий, настроенных для определенной группы. Например, если назначить 10 Windows 365 Frontline общих лицензий, для группы можно подготовить 10 облачных компьютеров. Только один пользователь может подключиться к общему облачному компьютеру в данный момент времени. Когда пользователь выходит из облачного компьютера, все данные пользователя удаляются, а облачный компьютер освобождается для начала использования другим пользователем. Буфер параллелизма не существует для переднего облачного компьютера в общем режиме.

Мониторинг буфера параллелизма

Вы можете отслеживать использование буфера параллелизма с помощью почасового отчета о подключении передней линии. Вы можете использовать оповещение о параллелизме frontline для получения оповещений при каждом активации буфера

параллелизма. Буфер параллелизма не применяется к облачным компьютерам с поддержкой GPU и облачным компьютерам Frontline в общем режиме.

Функции, еще не поддерживаемые Windows 365 Frontline

Следующие функции пока не поддерживаются для Windows 365 Frontline.

- Изменение размера удаленного действия облачного компьютера
- Аварийное восстановление между регионами
- Ключ клиента Microsoft Purview

Windows 365 Frontline в режиме общего доступа можно подготовить только в следующих регионах Azure:

- Восток Австралии
- Центральная Канада
- Северная Европа
- Центральная Индия
- Восточная Япония
- Западная Япония
- Северная часть Южной Африки
- Южная часть Соединенного Королевства
- Центральная часть США
- Восточная часть США
- Восточная часть США 2
- Западная часть США 3
- Центрально-южная часть США
- Восточная Азия
- Юго-Восточная Азия

Дальнейшие действия

Дополнительные сведения о Windows 365 Frontline см. в разделе:

- Массовая повторная подготовка Windows 365 Frontline облачных компьютеров в общем режиме
- Отчет подключенных облачных компьютеров frontline
- лицензирование Windows 365 Frontline

лицензирование Windows 365 Frontline

17.06.2025

Windows 365 Frontline лицензии можно приобрести через Центр администрирования Microsoft 365. Вы можете подтвердить количество лицензий в разделе **Выставление счетов — Ваши продукты**.

Windows 365 Frontline лицензии — это лицензии в пуле, применяемые на уровне клиента, а не назначаются пользователям напрямую. В Центр администрирования Microsoft 365 отображаются лицензии Windows 365 Frontline, назначенные нолю пользователей. Чтобы узнать, сколько лицензий используется, используйте отчет об использовании Windows 365.

Windows 365 Frontline является отдельным продуктом и не регулируется условиями лицензии Microsoft 365 F1/F3.

Требования лицензирования

Чтобы использовать Windows 365 Frontline, каждый пользователь должен иметь следующие лицензии:

- Windows 11 Корпоративная или Windows 10 Корпоративная
- Microsoft Intune
- Microsoft Entra ID P1.

Помимо независимой доступности, лицензии Windows Enterprise, Intune и Microsoft Entra ID включены в:

- Microsoft 365 E3
- Microsoft 365 E5
- Microsoft 365 F3
- Microsoft 365 A3
- Microsoft 365 A5
- Microsoft 365 бизнес премиум
- Microsoft 365 для образования подписки на преимущество использования учащимися

Дальнейшие действия

Дополнительные сведения о Windows 365 Frontline см. в разделе:

- Что такое Windows 365 Frontline?

- Управление Windows Frontline Cloud

Управление облачными компьютерами Windows 365 Frontline

17.06.2025

Windows 365 Frontline облачными компьютерами можно управлять с помощью Microsoft Intune, а также других облачных компьютеров и устройств в клиенте. Windows 365 Frontline поддерживает:

- Подготовка облачных компьютеров после приобретения лицензий .
- Управление облачными компьютерами.
- Настройка и применение политик.
- Развертывание приложений.
- Выполнение удаленных действий на облачных компьютерах.
- Создание отчетов.

Облачные компьютеры можно просмотреть на двух страницах:

- **Все устройства**. Включите столбец **Модель** , чтобы отличить облачные компьютеры Frontline от других.
- **Все облачные компьютеры**. Этот список можно отфильтровать, чтобы отобразить только облачные компьютеры frontline с помощью фильтра **типа компьютера** .

В неактивном состоянии Windows 365 Frontline облачные компьютеры в выделенном режиме находятся в отключенном состоянии. Состояние питания облачного компьютера можно подтвердить на странице "**Обзор** " для устройства.

Для оптимального взаимодействия с пользователем убедитесь, что:

- Настройте профили кругов клиентский компонент Центра обновления Windows.
- Установите ограничение времени для сеансов бездействия удаленного рабочего стола.

Дальнейшие действия

Дополнительные сведения о Windows 365 Frontline см. в разделе:

- Что такое Windows 365 Frontline?
- Обзор управления устройствами для Облачных компьютеров

Синхронизация взаимодействия с пользователем для Windows 365 frontline в общем режиме

Обзор

Синхронизация взаимодействия с пользователем — это функция для Windows 365 облачных компьютеров Frontline в общем режиме и Windows 365 облачных приложений. Это облачное решение обеспечивает простой и согласованный интерфейс для пользователей в сеансах Cloud PC и Cloud App. Корпорация Майкрософт управляет инфраструктурой и платформой, уменьшая сложность и затраты по сравнению с традиционными решениями. Эта функция сохраняет персонализацию Windows, пользовательские параметры (включая специальные возможности), параметры приложения и данные приложения. Это гарантирует, что пользователи будут иметь согласованный и продуктивный интерфейс при каждом входе в cloud PC или Cloud App.

> **Совет**
>
> Синхронизация взаимодействия с пользователем — это функция оптимизации взаимодействия для общих облачных компьютеров и облачных приложений. Он не предназначен для резервного копирования или аварийного восстановления данных пользователей.

Рис. 1. Что такое синхронизация взаимодействия с пользователем

Эта функция предоставляет хранилище пользователей в пуле для каждой политики. Если этот параметр включен, каждый пользователь получает собственное выделенное хранилище, размещенное в Microsoft Cloud.

Предварительные условия

- лицензия Windows 365 Frontline
- Доступ к необходимым конечным точкам Windows 365 и Microsoft 365
- разрешения на управление Intune

Как работает синхронизация взаимодействия с пользователем

Синхронизация взаимодействия с пользователем создает и подключает отдельное хранилище пользователей к общим облачным компьютерам. Когда пользователь входит в систему, его отдельное хранилище присоединяется, предоставляя доступ к его параметрам, файлам и данным приложения. При выходе из системы хранилище пользователя отсоединяется и сохраняется в Microsoft Cloud для использования при следующем входе.

Система автоматически обрабатывает загрузку профилей и управление хранилищем, не требуя традиционных решений для управления профилями.

Включение синхронизации взаимодействия с пользователем

При создании и назначении политики подготовки выберите **Включить синхронизацию взаимодействия с пользователем** в разделе конфигурации. Здесь можно выбрать размер хранилища пользователя из пяти доступных вариантов: 4 ГБ, 8 ГБ, 16 ГБ, 32 ГБ и 64 ГБ.

Создание новых политик с помощью синхронизации взаимодействия с пользователем

Следуйте стандартному процессу создания политики подготовки и установите флажок **Включить синхронизацию взаимодействия с пользователем** во время настройки.

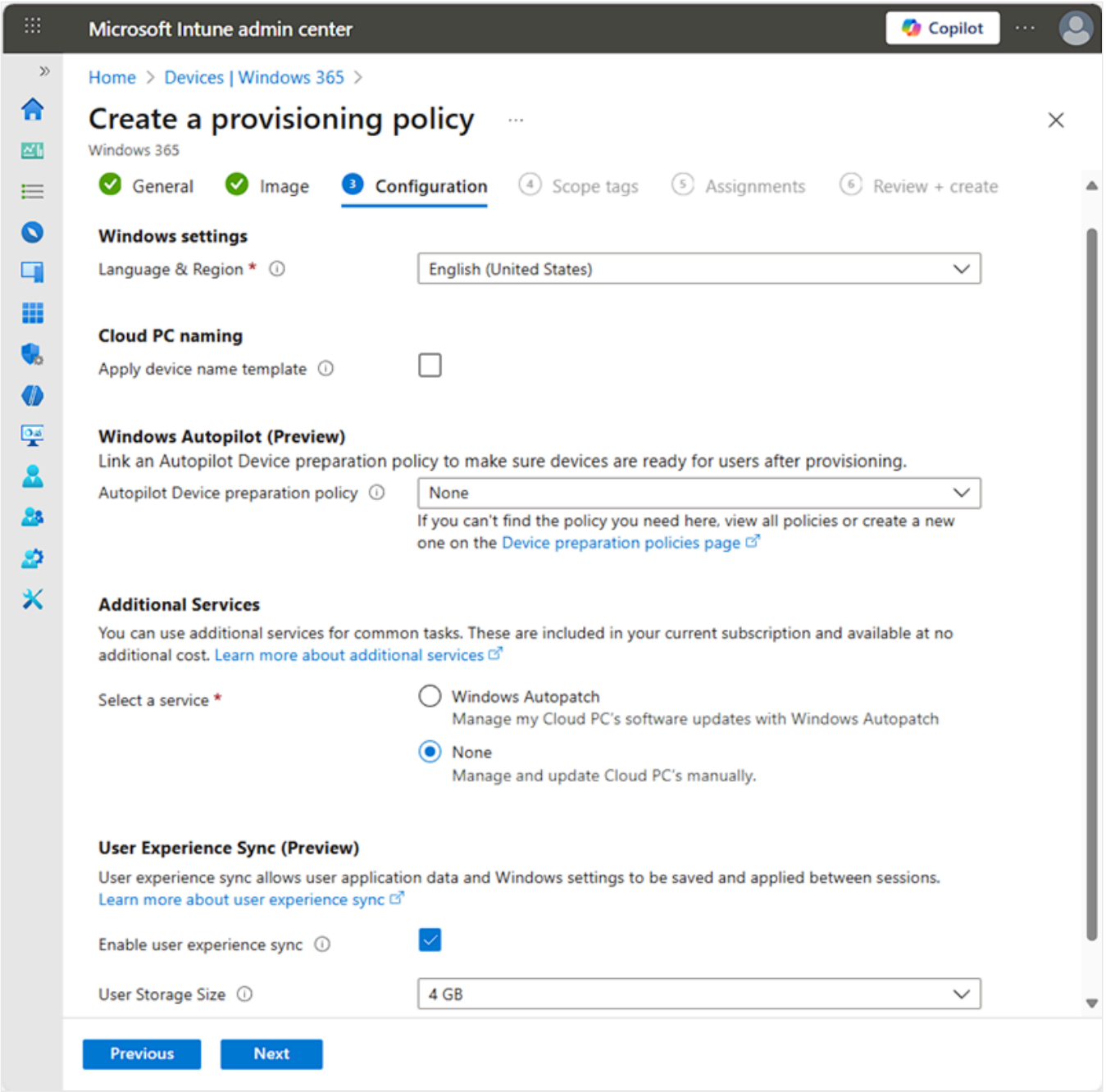


Рис. 2. Включение синхронизации взаимодействия с пользователем во время создания политики

Включение и отключение существующих политик

Чтобы включить или отключить функцию в существующей политике подготовки, выполните следующие действия.

> ⓘ **Внимание**
>
> Включение или отключение синхронизации взаимодействия с пользователем требует удаления и повторного добавления назначения. Это приведет к отзыву всех облачных компьютеров и подготовке новых облачных компьютеров.

1. **Удаление** текущего назначения группы с вкладки **"Свойства"**
2. **Изменение** раздела конфигурации и переключатель **Включить синхронизацию взаимодействия с пользователем**
3. **[Необязательно]** Выбор размера пользовательского хранилища (*только включение*)
4. **Обновление** политики
5. **Повторное добавление** назначения группы

Хранилище пользователей

Синхронизация взаимодействия с пользователем предоставляет ограниченный объем хранилища пользователей в пуле, который входит в вашу лицензию Frontline. Ограничение хранилища вычисляется на основе размера диска ОС из конфигурации облачного компьютера и умножается на количество облачных компьютеров в назначении.

Ограничения хранилища

- Размер облачного компьютера включает виртуальный ЦП, память и хранилище ОС (например, 4vCPU/16 ГБ/128 ГБ).
- Размер хранилища ОС × число облачных компьютеров = общий объем хранилища в пуле (128 x 10 = 1,28 ТБ)

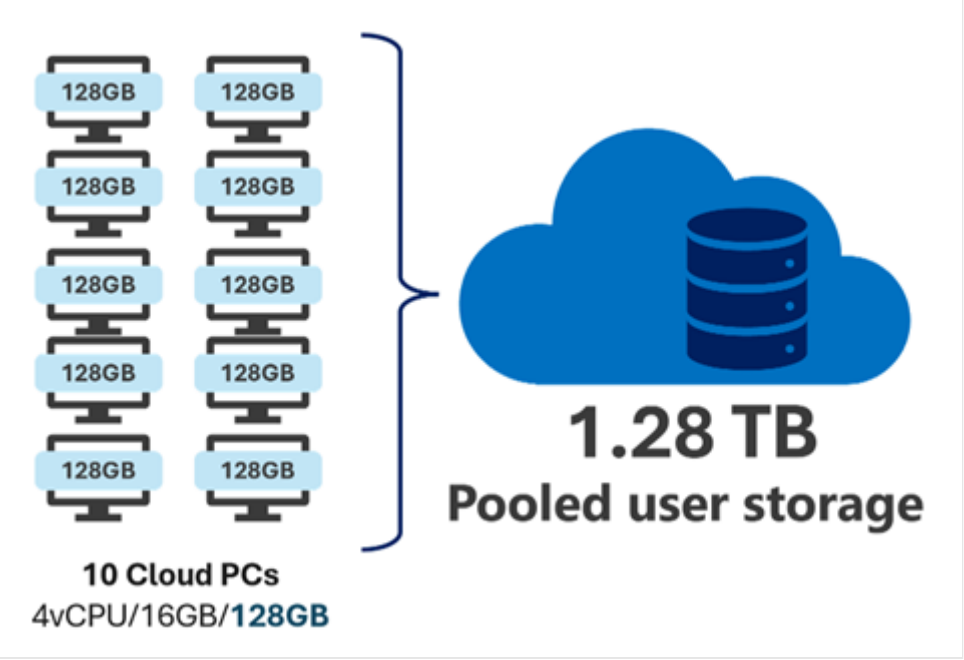


Рис. 3. Вычисление хранилища пользователей в пуле на основе размера и количества облачных компьютеров

ⓘ **Внимание**

Хранилище в пуле уникально для каждой политики и назначения. Удаление назначения приведет к окончательному удалению всего пользовательского хранилища.

Ограничения хранилища и квоты

- **Максимальный объем хранилища на пользователя**: определяется выбранным размером (от 4 ДО 64 ГБ)
- **Ограничения хранилища на уровне политики**: на основе количества облачных компьютеров и размера хранилища ОС

ⓘ **Примечание.**

- **Превышены ограничения**. Новые пользователи могут входить в систему с помощью временного профиля, но не могут создавать пользовательское хранилище при превышении объема хранилища в пуле. Пользователи с существующим хранилищем пользователей могут входить в систему с помощью персонализированного интерфейса.
- **Превышен период допуска**. При превышении ограничения хранилища в пуле период допуска составляет 7 дней. По истечении периода допустимости служба автоматически удаляет отдельное хранилище пользователей с самой старой меткой времени последнего присоединения. После того как хранилище в пуле превысит ограничение, период допуска сбрасывается до следующего события превышения предела.

Управление хранилищем пользователей

Синхронизация взаимодействия с пользователем предоставляет комплексные возможности управления для мониторинга и администрирования хранилища пользователей в развертывании.

Доступ к управлению хранилищем пользователей

Чтобы просмотреть хранилище пользователей и управлять ими, выполните приведенные ниже действия.

1. Перейдите в **центр администрирования Microsoft Intune**.
2. Перейдите в **раздел Устройства**>**Windows 365**>**Политики подготовки**.

3. Выберите политику синхронизации взаимодействия с пользователем.
4. Перейдите на вкладку **User Storage (Хранилище пользователей**).

Общие сведения о пользовательском хранилище

На вкладке Пользовательское хранилище представлено полное представление о выделении хранилища.

- **Сведения о хранилище**: размер облачного компьютера, количество и настроенный размер пользовательского хранилища
- **Общий объем хранилища пользователей в пуле**: максимальное доступное хранилище для политики
- **Доступное хранилище пользователей в пуле**: оставшаяся емкость хранилища
- **Используемое хранилище пользователей в пуле**: используемое в настоящее время хранилище
- **Сведения о хранилище отдельных пользователей**: размер, состояние и метка времени последнего присоединения для каждого пользователя

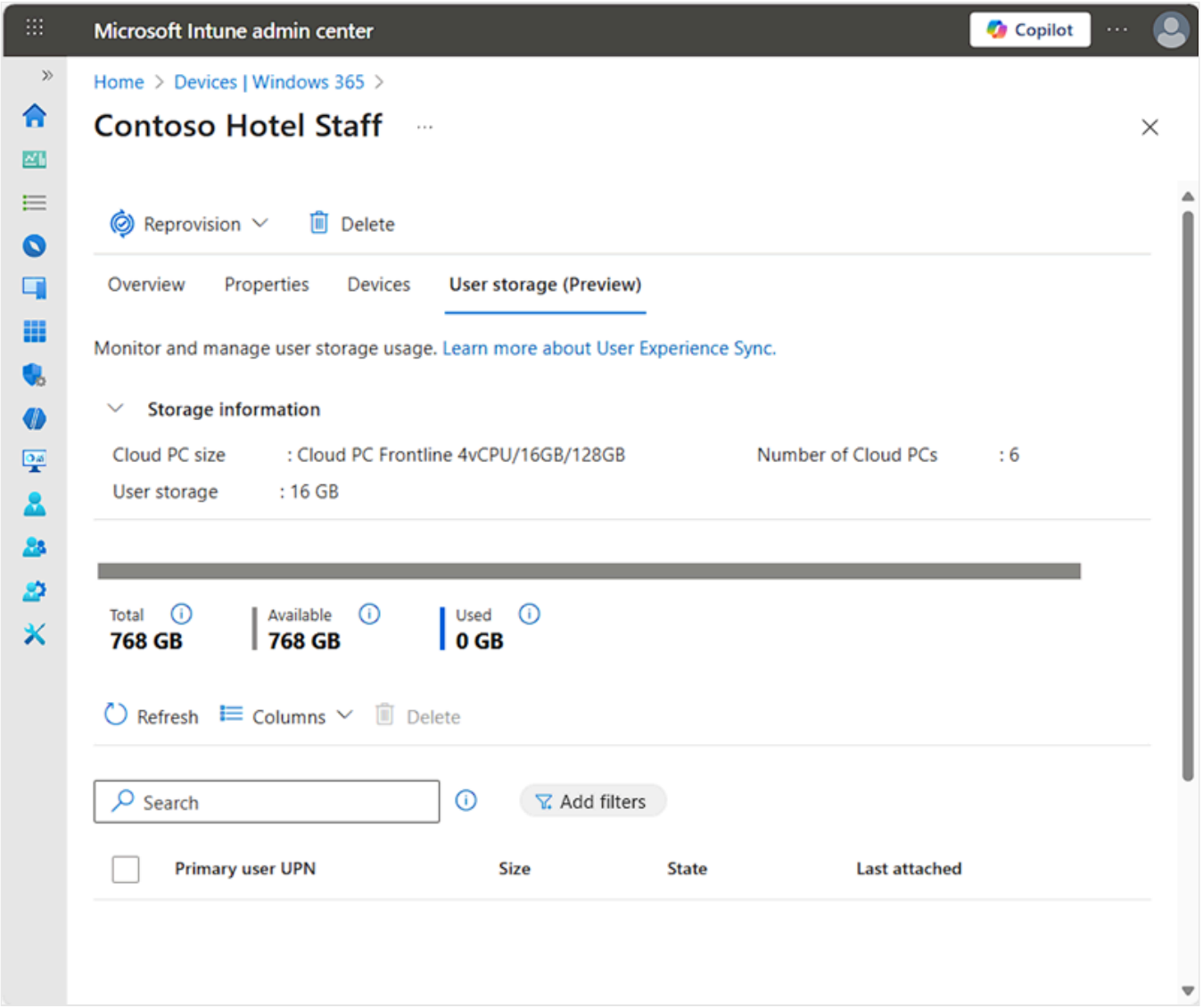


Рис. 4. Мониторинг и управление хранилищем пользователей

Мониторинг использования хранилища

Настройка упреждающего мониторинга

Включение оповещений хранилища:

- Перейдите в раздел**Оповещенияадминистрирования**> клиента.
- Включите правило генерации оповещений Об **ограничениях хранилища в режиме взаимодействия с пользователем с интерфейсом frontline Cloud PC** .
- Настройте параметры уведомлений для команды администрирования.

Регулярное расписание мониторинга:

- Еженедельно проверяйте использование хранилища.
- Отслеживайте шаблоны роста хранилища пользователей.
- Определите неактивное пользовательское хранилище для потенциальной очистки.

Политики оптимизации хранилища

Настройка функций Windows для оптимизации использования хранилища:

Перенаправление OneDrive:

- Применение параметров групповая политика OneDrive
- Управление файлами по запросу, перемещение известных папок и ограничение пространства.

Управление данными браузера.

- Настройка политик Microsoft Edge
- Управление кэшем и временным хранением данных

Конфигурация storage Sense:

- Развертывание политик контроля хранилища
- Автоматизация очистки временных файлов, загрузки и файлов с облачной поддержкой (OneDrive)

Управление хранилищем отдельных пользователей

Удаление пользовательского хранилища

Чтобы удалить хранилище отдельных пользователей, выполните приведенные далее действия.

Удаление одного пользователя:

1. На вкладке **User Storage (Хранилище пользователей**) найдите целевого пользователя.
2. Установите флажок рядом с хранилищем пользователя.
3. Щелкните **Удалить** на панели действий.
4. Подтвердите удаление в диалоговом окне.

Массовое удаление пользователей:

1. Установите флажки для выбора нескольких пользователей.
2. Щелкните **Удалить** на панели действий.
3. Просмотрите выбранных пользователей в диалоговом окне подтверждения.
4. Подтвердите массовое удаление.

> ⚠ **Предупреждение**
>
> При удалении хранилища пользователей удаляются все пользовательские параметры, файлы и данные приложения. Это действие невозможно отменить.

Когда следует удалять пользовательское хранилище

Рассмотрите возможность удаления пользовательского хранилища в следующих сценариях:

- **Неактивные пользователи**: пользователи, которые не обращались к облачным компьютерам в течение длительного периода времени
- **Управление емкостью хранилища**. При приближении к ограничениям хранилища в пуле
- **Устранение неполадок**: устранение постоянных проблем с профилем пользователей

Хранимые данные

Пользовательское хранилище содержит все данные из `C:\Users\%username%`, включая:

- Параметры пользователей и данные приложения
- Файлы реестра (`NTUSER.dat` и `USRCLASS.dat`)
- Личные файлы и папки

Исключенные сведения

Некоторые типы данных автоматически исключаются, так как они не могут использоваться на разных устройствах:

Некорамируемые данные приложения

- `AppData\Local\Packages\*\AC`
- `AppData\Local\Packages\*\SystemAppData`
- `AppData\Local\Packages\*\LocalCache`
- `AppData\Local\Packages\*\TempState`
- `AppData\Local\Packages\*\AppData`

Некорамируемые данные удостоверений

- `AppData\Local\Packages\Microsoft.AAD.BrokerPlugin_cw5n1h2txyewy`
- `AppData\Local\Packages\Microsoft.Windows.CloudExperienceHost_cw5n1h2txyewy`
- `AppData\Local\Microsoft\TokenBroker`
- `AppData\Local\Microsoft\OneAuth`
- `AppData\Local\Microsoft\IdentityCache`

Ссылки:Класс ApplicationData (Windows.Storage) | Удостоверение устройства и виртуализация рабочего стола

> ⓘ **Примечание.**
>
> Невозможно настроить данные, которые исключаются из хранилища. Например, oneDrive, Edge и Storage Sense имеют параметры политики, которые можно применять к устройствам в Windows 365 которые влияют на хранение или очистку данных.

Взаимодействие с пользователем

Настройка первого пользователя

Когда пользователь впервые входит в cloud PC или Cloud App с включенной синхронизацией взаимодействия с пользователем, система автоматически создает и присоединяет его личное хранилище и начинает сбор данных.

Процесс входа

1. Пользователь проходит проверку подлинности на облачном компьютере или в облачном приложении

    - *Начальный вход*:
        - Создано новое пользовательское хранилище
        - Параметры пользователя и данные приложения перенаправляются в хранилище пользователей.
    - *Последующие входы:*
        - Подключено существующее пользовательское хранилище
        - Параметры пользователя и данные приложения загружаются из предыдущего сеанса

2. Сеанс пользователя начинается с персонализированной среды

3. Взаимодействие с пользователем автоматически сохраняется в отдельном хранилище пользователей.

Сохраняемость данных приложения

Для администраторов или Intune установленных приложений параметры будут сохраняться в сеансах, обеспечивая согласованную среду пользователя независимо от того, к какому облачному компьютеру подключается пользователь.

> ⓘ **Примечание.**
>
> Синхронизация взаимодействия с пользователем не перемещает и не сохраняет установленные пользователем приложения. Сохраняются только данные приложения (параметры и настройки).

Вопросы и ответы

Вопрос. Можно ли перенести существующие профили FSLogix в службу синхронизации взаимодействия с пользователем?

О. Прямая миграция не поддерживается. Пользователям потребуется воссоздать свою персонализацию при первом использовании синхронизации взаимодействия с пользователем.

Вопрос. Что произойдет, если пользователь превысит выделение хранилища?

О. Взаимодействие с пользователем будет ухудшаться с периодическим и потенциально неизвестным поведением. Хранилище пользователя может быть удалено или политика может быть изменена на больший размер хранилища пользователя (*влияет на всех пользователей*).

Вопрос. Можно ли изменить размер хранилища после включения синхронизации взаимодействия с пользователем?

Ответ. Да, размер хранилища устанавливается при включении функции и может быть изменен позже.

Вопрос. Доступна ли синхронизация взаимодействия с пользователем для выделенных облачных компьютеров?

О. Нет, он доступен только для Windows 365 Frontline в общем режиме и облачных приложениях.

Вопрос. Как синхронизация взаимодействия с пользователем сравнивается с традиционными решениями профилей?

О. Синхронизация взаимодействия с пользователем предназначена для оптимизации взаимодействия с конечными пользователями на общих облачных компьютерах и является облачным решением.

Связанная документация

- Общие сведения о Windows 365 frontline
- Документация по облачным приложениям
- Создание политик подготовки
- Лицензирование frontline
- Рекомендации о размере облачного компьютера

Дальнейшие действия

- Руководство по устранению неполадок
- Известные проблемы с Windows 365 Frontline

Last updated on 19.11.2025

Буфер параллелизма для Windows 365 Frontline облачных компьютеров в выделенном режиме

17.06.2025

Windows 365 Frontline в выделенном режиме включает буфер параллелизма, который позволяет клиенту временно превысить максимальное ограничение параллелизма для Windows 365 Frontline облачных компьютеров.

Например, когда рабочие роли перекрываются во время смены, предыдущей рабочей роли может потребоваться завершить что-то перед выходом. Кроме того, входящий рабочий элемент может потребоваться начать на несколько минут раньше. Буфер параллелизма предназначен для того, чтобы обеспечить такое редкое и краткое использование, чтобы убедиться, что на рабочие роли не влияют непредвиденные блокировки.

Буфер параллелизма можно использовать до четырех раз в день с максимальным количеством часов в каждом экземпляре. Этот час начинается с момента, когда клиент превысил максимальное ограничение параллелизма.

Временные блоки

Чрезмерное использование буфера параллелизма временно блокирует его дальнейшее использование в течение следующих 48 часов. Временный блок накладывается, когда:

- В четырех или более случаях в течение 24-часового периода буфер параллелизма используется более одного часа.

Хотя они временно заблокированы, вы по-прежнему можете использовать Windows 365 Frontline облачные компьютеры в выделенном режиме до максимального предела параллелизма.

Постоянные блоки

Если клиент временно блокируется более двух раз в течение семи дней, он постоянно блокируется использовать буфер параллелизма.

Несмотря на постоянную блокировку, вы по-прежнему можете использовать облачные компьютеры Frontline до максимального предела параллелизма.

Чтобы разблокировать клиент, откройте запрос в службу поддержки на портале Intune.

Мониторинг буфера параллелизма

Вы можете отслеживать использование буфера параллелизма с помощью почасового отчета о подключении передней линии. Вы можете использовать оповещение о параллелизме frontline для получения оповещений при каждом активации буфера параллелизма. Буфер параллелизма не применяется к облачным компьютерам с поддержкой GPU и облачным компьютерам Frontline в общем режиме.

Дальнейшие действия

Дополнительные сведения о Windows 365 Frontline см. в разделе:

- Что такое Windows 365 Frontline?
- лицензирование Windows 365 Frontline

Что такое Резерв Windows 365?

Резерв Windows 365 — это версия Windows 365, предназначенная для пользователей, работающих в основном на физических компьютерах. Она предоставляет организациям гибкий краткосрочный доступ к облачным компьютерам, чтобы обеспечить производительность сотрудников во время непредвиденных сбоев. Это предложение поддерживает непрерывность бизнес-процессов, обеспечивая быстрый и безопасный доступ к облачным компьютерам, когда физические устройства недоступны.

Обзор

Резерв Windows 365 позволяет организациям назначать сотрудникам лицензии с ежегодным сроком, который предоставляет доступ **к облачному компьютеру до 10 дней для каждого пользователя в год**. Резервные облачные компьютеры подготавливаются при необходимости, что снижает затраты и операционную сложность по сравнению с предоставлением физических устройств для кредитования или лицензий на облачные компьютеры с полным использованием.

Общие сценарии

- Потеря, кража или повреждение устройства
- Задержки при поставках оборудования
- Сбои или кибер-инциденты
- Краткосрочные потребности в персонале
- Пробные или тестовые среды

Лицензирование

- Каждому пользователю требуется лицензия на Резерв Windows 365.
- Каждая лицензия предоставляет до 10 дней доступа к облачному компьютеру в год для одного пользователя.

Предварительные требования и дополнительные сведения о лицензировании см. в разделе лицензирование Резерв Windows 365.

Принципы действия

Для ИТ-администраторов

управление Резерв Windows 365 интегрировано с Microsoft Intune.

- **Настройка**:
  - Заранее создавайте политики подготовки, назначения пользователей и параметры, чтобы убедиться, что Резерв Windows 365 готовы к быстрому развертыванию облачных компьютеров при необходимости.
  - Создайте или используйте существующие политики Microsoft Intune, чтобы Резерв Windows 365 автоматически загружать облачные компьютеры с приложениями, параметрами и политиками безопасности вашей организации.

- **Развертывание**. Если пользователям требуется Резерв Windows 365 облачных компьютеров, подготовьте их из Intune.

- **Мониторинг и управление**. Отслеживание лицензирования и использования в Intune. Отзыв облачных компьютеров, которые больше не требуются для сохранения оставшихся дней доступа на более поздний срок действия лицензии.

Для пользователей

доступ к Резерв Windows 365 можно получить с любого устройства и предназначен для простого взаимодействия.

- **Подключение**. После подготовки пользователи входят с рабочими учетными данными на Windows App или веб-портал на любом устройстве (Windows, Mac, iOS, Android) и щелкают, чтобы подключиться.
- **Мониторинг и управление**. Пользователи могут просматривать описание своего Резерв Windows 365 облачного компьютера, просматривать доступное время доступа и выполнять ограниченные действия, такие как перезапуск, сброс или возврат (отзыв) облачного компьютера на карта устройства в Windows App или веб-портале.

Основные преимущества

Быстрое восстановление производительности конечных пользователей

Если основное устройство пользователя недоступно, его производительность может зависнуть в течение нескольких дней, пока устройство будет отремонтировано или заменено. Резерв Windows 365 позволяет организациям быстро восстанавливать производительность, предоставляя безопасный и краткосрочный доступ к облачному

компьютеру, чтобы пользователи могли продолжать работать в ожидании доступности основного устройства.

С помощью Резерв Windows 365 администраторы могут:

- Подготовка облачных компьютеров при необходимости из Microsoft Intune, чтобы свести к минимуму время простоя
- Подготовка облачных компьютеров с помощью предварительно настроенных приложений и политик с помощью Microsoft Intune
- Обеспечение согласованного взаимодействия с любым устройством через Windows App на основе надежной производительности Windows Cloud

Централизованное управление ИТ

ИТ-администраторы могут совместно управлять физическими и облачными компьютерами в Microsoft Intune, что упрощает контроль и снижает сложность.

Резерв Windows 365 предложения:

- Простая настройка; не требуется специализированный опыт в области облака или виртуализации
- Снижение операционных издержек за счет управления на основе политик

Защита по проектированию

Безопасность является главным приоритетом для организаций. Резерв Windows 365 обеспечивает безопасный краткосрочный доступ к корпоративным данным и приложениям с любого устройства. Конфиденциальные данные остаются в облаке, что снижает риск, даже если пользователи подключаются из-за пределов корпоративной сети.

Управление облачными компьютерами с помощью Microsoft Intune помогает администраторам:

- Последовательное применение корпоративных политик безопасности к физическим устройствам и облачным компьютерам
- Включение безопасных подключений с неуправляемых устройств с помощью параметров безопасности, таких как политики условного доступа

Дальнейшие действия

Дополнительные сведения о развертывании Резерв Windows 365 в организации см. в разделе:

- Управление Резерв Windows 365
- лицензирование Резерв Windows 365
- часто задаваемые вопросы Резерв Windows 365

Last updated on 19.11.2025

Управление Резерв Windows 365

Это руководство предназначено для ИТ-администраторов, которым необходимо развертывать Резерв Windows 365 и управлять ими.

Содержимое организовано по двум основным областям:

- **Настройка**: начальные задачи, которые необходимо выполнить перед развертыванием.
- **Управление**: текущие действия для операций.

Настройка Резерв Windows 365

Предварительные условия

Лицензирование пользователей

- Каждому пользователю требуется **лицензия на Резерв Windows 365**.
- Лицензии обеспечивают **доступ к облачному компьютеру в течение 10 дней в год для одного пользователя**.
- Пользователи также должны иметь:
  - Windows 11 Корпоративная или Windows 10 Корпоративная
  - Microsoft Intune
  - Microsoft Entra ID P1

Дополнительные сведения см. в разделе лицензирование Резерв Windows 365.

> ⓘ **Примечание.**
>
> Резерв Windows 365 не требуется Azure AD ds или локальных доменов. Резерв Windows 365 облачные компьютеры всегда Microsoft Entra присоединены к размещенной сети Майкрософт.

Управление доступом на основе ролей

Чтобы управлять Резерв Windows 365, назначьте следующие роли администраторам в Microsoft Entra ID и Intune:

- Обязательный: администратор Windows 365
- Рекомендованный:

- администратор Intune (для управления отчетами и другими функциями Intune)
- Администратор пользователей (для управления группами безопасности Microsoft Entra)

Дополнительные сведения см. в разделе Управление доступом на основе ролей.

Настройка среды

- **Microsoft Intune**. Применение политик и приложений, предназначенных для пользователей, для согласованного взаимодействия. Дополнительные сведения см. в статье Применение функций и параметров на устройствах с помощью профилей устройств в Microsoft Intune
- **Сеть**. Убедитесь, что корпоративные брандмауэры не блокируют службу Windows 365. Дополнительные сведения см. в разделе требования к сети Windows 365.
- **Microsoft Entra присоединение**. Подтвердите готовность конечных точек присоединения к Microsoft Entra. Планирование реализации Microsoft Entra присоединения
- **группа Microsoft Entra**. Создайте или используйте существующую группу для подготовки назначения политики. Управление группами Microsoft Entra и членством в группах)

Создание политики резервной подготовки

Политики подготовки определяют параметры облачного компьютера, такие как география, язык и тип образа.

> ⓘ **Внимание**
>
> Чтобы выделить Резерв Windows 365 лицензии, назначьте группу Microsoft Entra политике подготовки резервирования. Вы можете подготовить облачные компьютеры пользователя, начиная с семи дней после назначения ему лицензии. Планируйте заранее, создавая и назначая политики задолго до того, как вам потребуется подготовить облачные компьютеры.

Действия

1. В Intune перейдите в раздел **Устройства** > **Windows 365** > **политики подготовки** и выберите **Создать политику**.
2. В разделе **Основные сведения** введите имя и описание.

3. [Только для Windows 365 Корпоративная и клиентов с интерфейсом] В разделе **Взаимодействие** выберите **Доступ к полному облачному компьютеру**. В разделе **Тип лицензии** выберите **Резервировать**.
4. Выберите **География** для резервирования облачных компьютеров.
5. [Необязательно] Измените образ коллекции.
6. [Необязательно] Настройте язык, регион и параметры именования.
7. [Необязательно] Добавление тегов область.
8. В разделе **Назначения** добавьте группы пользователей.
9. Просмотрите параметры и выберите **Создать**.

Управление Резерв Windows 365

Управление политиками подготовки

Перейдите в раздел **Устройства** > **Windows 365** > **политики подготовки** в Intune. Используйте фильтры или поиск, чтобы найти ссылку политики подготовки Резерв Windows 365.

Подготовка резервного облачного компьютера.

Резервные облачные компьютеры подготавливаются вручную.

> ⓘ **Внимание**
>
> **10-дневный период доступа начинается с подготовки облачного компьютера**. При необходимости подготавливайте по запросу, чтобы избежать ненужного использования лицензий.

Действия

1. В Intune откройте политику подготовки и выберите **Пользователи облачных компьютеров**.
2. Выберите одного или нескольких пользователей и щелкните **Подготовить**.
3. Подтвердите в диалоговом окне.
4. Отслеживайте изменения состояния с "**Не подготовлено**" на "**Подготовлено**".

Отзыв резервного облачного компьютера

> ⓘ **Внимание**
>
> **Отмена подготовки приостанавливает 10-дневный период доступа и удаляет облачный компьютер и все данные без резервного копирования.** Администраторы могут отзываться с Intune, а пользователи могут отзывать (возвращать) облачный компьютер в Windows App. Оба действия требуют подтверждения через второй запрос на согласие и действия администратора для повторной подготовки облачного компьютера. Нет моментальных снимков или льготных периодов, когда администраторы или пользователи отменяют подготовку; Поэтому перед отзывом убедитесь, что пользователи будут создавать резервные копии важных данных.

Отмена подготовки, как только устройство больше не требуется для сохранения оставшихся дней доступа на более поздний срок действия лицензии.

Действия

1. Перейдите в раздел **Устройства** или **Пользователи облачных компьютеров** в соответствии с политикой.
2. Выберите один или несколько облачных компьютеров и нажмите **кнопку Отменить подготовку.**
3. Подтвердите в диалоговом окне.
4. Отслеживайте изменения состояния с "**Подготовлено**" на "**Не подготовлено**".

Мониторинг резервных облачных компьютеров и управление ими

- **Политики подготовки: фильтрация** по типу лицензии = резервная.
- **Отчеты**:
  - лицензирование Резерв Windows 365
  - **Все облачные компьютеры**: тип лицензии фильтра = резервировать.

Конечные пользователи: подключение к Резерв Windows 365 облачному компьютеру

1. Откройте Windows App или веб-клиент на любом поддерживаемом устройстве.
2. Войдите с учетными данными организации.
3. Выполните фильтрацию по **Windows 365**, чтобы найти резервный облачный компьютер после его подготовки.

4. На устройстве карта запустите облачный компьютер и выполните такие действия, как перезапуск или сброс.
5. Проверьте тег **Reserve** , чтобы увидеть дату истечения срока доступа.

См. также

- Что такое Резерв Windows 365?
- лицензирование Резерв Windows 365
- часто задаваемые вопросы Резерв Windows 365

Last updated on 19.11.2025

Лицензирование Резерв Windows 365

Резерв Windows 365 лицензии предоставляют краткосрочный доступ к облачному компьютеру для обеспечения непрерывности бизнес-процессов и других краткосрочных потребностей. Каждая лицензия включает **до 10 дней доступа к облачному компьютеру на пользователя в год**.

Приобретение и назначение лицензий Резерв Windows 365

- **Приобретение**. Чтобы приобрести лицензии, обратитесь в Microsoft Sales. Подтвердите количество в Центре Администратор Майкрософт в разделе **Выставление счетов > ваших продуктов**.
- **Приложение на уровне клиента**. В Центре администрирования лицензии отображаются, назначенные нулю пользователей, так как Резерв Windows 365 лицензии применяются на уровне клиента.
- **Назначение лицензий**. Назначение лицензий Microsoft Entra группам пользователей при создании политики подготовки в Intune.
- **Мониторинг использования**. Просмотр назначений и использования в отчете **о лицензировании Резерв Windows 365**.

> ⓘ **Примечание.**
>
> Резерв Windows 365 является отдельным продуктом и не соответствует правилам Microsoft 365 F1/F3 лицензии.

Предварительные условия

Чтобы использовать Резерв Windows 365, каждый пользователь должен иметь следующие лицензии:

- Windows 11 Корпоративная или Windows 10 Корпоративная
- Microsoft Intune
- Microsoft Entra ID P1

Эти лицензии включены в:

- Microsoft 365 E3, E5
- Microsoft 365 F3
- Microsoft 365 A3, A5

- Microsoft 365 бизнес премиум
- Microsoft 365 для образования подписки на преимущество использования учащимися

Модель лицензирования

Резерв Windows 365 — это годовая лицензия, управляемая через Microsoft Intune. Лицензии не назначаются в Центр администрирования Microsoft 365. Они применяются при создании политик подготовки в Intune и назначении их группам Entra.

> **Совет**
>
> Чтобы упростить управление и обеспечить быстрое реагирование во время перебоев, запланируйте одну Резерв Windows 365 лицензию для каждого пользователя, которого вы хотите охватить. Правила лицензирования запрещают совместное использование или пул резервных лицензий между пользователями.

Правила и ограничения

Применение

- Каждая резервная лицензия включает до 10 дней доступа к облачному компьютеру для одного пользователя в течение срока действия лицензии.
- 10-дневный доступ не может быть предоставлен пользователям.
- 10-дневный доступ начинается при подготовке облачного компьютера и приостанавливается при отзыве облачного компьютера.
- День измеряется с 24-часовыми шагами с момента подготовки облачного компьютера и согласован по часовым поясам; любое время, затраченное на подготовку в день, учитывается в этот день.
- 10-дневный доступ можно использовать последовательно или распределять по всему сроку лицензии, управляя подготовкой и отзывом.

Задание

- Администраторы создают политику подготовки в Microsoft Intune для назначения лицензий Microsoft Entra группам.

- Каждый пользователь в группе получает лицензию, если в клиенте достаточно доступных лицензий.
- Каждый пользователь может иметь одну лицензию на Резерв Windows 365 одновременно. После подготовки облачного компьютера его лицензия не может быть удалена или переназначена до истечения срока действия лицензии.

Задержка активации

- Облачный компьютер пользователя Резерв Windows 365 получает право на подготовку через семь дней после назначения лицензии.
- Семидневная задержка применяется только при первом назначении лицензии пользователю или после истечения срока действия лицензии.
- Администраторы могут отслеживать семидневную задержку после назначения в соответствии с политиками подготовки пользователей в Microsoft Intune.

> ⓘ **Внимание**
>
> Настройте и назначьте политики резервной подготовки на ранней стадии, чтобы избежать задержек подготовки, когда пользователям требуется доступ.

Переназначения

Явные действия администратора для переназначений лицензий отсутствуют. Администраторы могут управлять назначениями лицензий, изменяя членство в группах Entra или назначения групп Entra, чтобы Резерв Windows 365 политики подготовки.

- Неиспользуемые лицензии (где облачный компьютер никогда не был подготовлен). Когда пользователь удаляется из назначения политики подготовки, его лицензия возвращается в пул доступных лицензий в клиенте и может быть распространена среди новых пользователей.
- Использованные лицензии (где был подготовлен облачный компьютер). Когда пользователь удаляется из назначения политики подготовки, его лицензия остается назначенной ему на оставшуюся часть срока лицензии и не может вернуться в пул доступных лицензий для распространения среди новых пользователей.

Срок действия

По истечении срока действия лицензии истекают неиспользуемые дни.

Стек или расширения

Не поддерживается в общедоступной версии.

Дальнейшие действия

Дополнительные сведения о развертывании Резерв Windows 365 в организации см. в разделе:

- Что такое Резерв Windows 365?
- Управление Резерв Windows 365
- часто задаваемые вопросы Резерв Windows 365

Last updated on 19.11.2025

часто задаваемые вопросы Резерв Windows 365

В этой статье содержатся ответы на распространенные вопросы о Резерв Windows 365, включая поддержку функций, ограничения, лицензирование и управление.

Поддержка функций

Ниже перечислены подробные Резерв Windows 365 поддерживаемые функции и неподдерживаемые функции при общедоступной доступности. Со временем будут поддерживаться дополнительные функции.

✅ Поддерживается Резерв Windows 365

- Клиенты: Web, Windows, macOS, iOS, Android
- Загрузка Windows 365
- Windows 365 Link
- Сеть, размещенная в Майкрософт
- География выбора: Африка, Азия, Австралия, Канада, Европа, Индия, Ближний Восток, Центрально-Восточная и Западная часть США
- Единый вход
- Последние три Windows 11 изображений из коллекции (с приложениями Microsoft 365 и без нее)
- Языковые пакеты
- Шаблоны именования облачных компьютеров
- Теги области
- Подключение к бизнес-приложениям поддерживается при использовании VPN или аналогичного решения
- Действия с устройством: подготовка или настройка облачного компьютера, отзыв и возврат, перезагрузка, сброс, размещение облачного компьютера под проверкой, удаление из проверки
- Отчеты и оповещения:
  - лицензирование Резерв Windows 365
  - Оповещения ИТ-администраторов в Intune о сбоях подготовки и отзыва

❌ Не поддерживается Резерв Windows 365

- Спецификация размера облачного компьютера и хранилища
- Среды FedRAMP или GCC

- Клиенты: Удаленный рабочий стол (Майкрософт), LG WebOS
- Microsoft Entra гибридное соединение
- Microsoft Entra B2B
- Azure сетевых подключений или пользовательских виртуальных сетей
- Пользовательские образы или Windows 10 и более ранние образы коллекции
- Спецификация страны или региона облачного компьютера
- Политика подготовки устройств Windows Autopilot
- Ключи, управляемые клиентом (CMK)
- Несколько активных резервных облачных компьютеров на пользователя
- Моментальные снимки или восстановление на определенный момент времени
- Действия устройства: сбор диагностика, переименование, изменение размера, восстановление, моментальные снимки на определенный момент времени, синхронизация, полная проверка, быстрая проверка, включение и включение питания, устранение неполадок, обновление Защитника Windows
- Льготный период для облачных компьютеров
- Облачные приложения
- переключатель Windows 365
- Соединители партнеров (Citrix, Omnissa, HP Anyware)
- Рекомендации на основе ИИ
- Надстройки аварийного восстановления
- Облачные компьютеры с поддержкой GPU
- Отчеты: качество подключения, использование, работоспособность агента, рекомендации

> ⓘ **Примечание.**
>
> Эти списки функций не являются исчерпывающими, некоторые поддерживаемые и неподдерживаемые функции могут быть не перечислены. Если функция не указана в списке, предположим, что она не поддерживается, пока не будет сообщено об обратном.

Вопросы и ответы

Общие

Что такое Резерв Windows 365? Резерв Windows 365 — это версия Windows 365, предназначенная для пользователей, работающих в основном на физических компьютерах. Она предоставляет организациям гибкий краткосрочный доступ к облачным компьютерам, чтобы обеспечить производительность сотрудников во время

непредвиденных сбоев. Это предложение поддерживает непрерывность бизнес-процессов, обеспечивая быстрый и безопасный доступ к облачным компьютерам, когда физические устройства недоступны.

Облачные компьютеры предварительно настроены с корпоративными приложениями, параметрами и политиками Microsoft 365, управляемыми централизованно через Microsoft Intune. Пользователи могут безопасно подключаться из Windows App (Windows или iOS) или веб-портала на любом устройстве (Windows, Mac, iOS, Android).

Как это сравняется с физическим заемным компьютером? Физические заемные компьютеры предлагают автономный доступ и полный контроль над ОС, но включают в себя логистику подготовки и доставки, риски безопасности и более высокие затраты. Поддержка ограничена количеством доступных устройств. Windows 365 Резерв Windows 365 обеспечивает быстрый и безопасный доступ к рабочим ресурсам с любого устройства, централизованное управление и отсутствие накладных расходов на оборудование.

Чем она отличается от Windows 365 Корпоративная и frontline? Каждый из них предоставляет облачные компьютеры, но возможности функций различаются в зависимости от версии Windows 365 вы приобретаете. Резерв Windows 365 предназначена для краткосрочных сценариев, таких как потеря устройства, задержки доставки, простои или временное укомплектование персоналом. Резерв Windows 365 ограничивает доступ до **10 дней для каждого пользователя в год**, и каждый пользователь может иметь только одну лицензию на Резерв Windows 365 и облачный компьютер одновременно, даже если лицензии доступны и пользователю назначено несколько политик подготовки.

Чем она отличается от Windows 365 аварийного восстановления между регионами? Резерв Windows 365 — это автономное предложение, которое предоставляет до 10 дней доступа к облачному компьютеру на каждого пользователя в год с любого устройства, если его физическое устройство недоступно.

Windows 365 аварийное восстановление между регионами — это надстройка для Windows 365 Корпоративная и Windows 365 облачных компьютеров передней линии. Он реплицирует весь образ облачного компьютера в другой регион на основе последней точки восстановления, обеспечивая непрерывность бизнес-процессов во время региональных сбоев. Работа должна сохраняться в облачных службах Майкрософт, таких как OneDrive или SharePoint. После активации временные облачные компьютеры должны быть деактивированы в течение семи дней после окончания объявленного простоя.

У W365 Reserve разные конфигурации? Нет. W365 Reserve не предлагает выбор конфигурации. По умолчанию он использует **4 виртуальных ЦП, 16 ГБ ОЗУ, 128 ГБ**

хранилища и резервные SKU могут использоваться при достижении ограничений емкости.

Поддерживают ли Резерв Windows 365 спецификации стран или регионов для подготовки? Нет. Чтобы снизить риски и повысить эффективность, политики подготовки Резерв Windows 365 позволяют выбрать географию, а не конкретную страну или регион. Такая гибкость позволяет Резерв Windows 365 использовать имеющиеся ресурсы в разных странах и регионах в пределах географического региона, повышая охват и сокращая операционные узкие места, вызванные ограничениями емкости.

Поддерживает ли Резерв Windows 365 пользовательские образы или подключение к бизнес-приложениям? Нет. По умолчанию Резерв Windows 365 облачные компьютеры подготавливаются с использованием последнего образа коллекции Windows, поддерживаемого в географическом регионе развертывания с включенными приложениями Microsoft 365. Администраторы могут изменить свою политику подготовки, чтобы указать один из последних трех образов коллекции Windows и выбрать одну из версий с Приложения Microsoft 365 включены или исключены. Для поддержки подключения к бизнес-приложениям необходимо использовать VPN-подключение или аналогичное решение.

Поддерживает ли Резерв Windows 365 загрузку Windows 365? Да, Windows 365 загрузка совместима с Резерв Windows 365. Любое локальное устройство, настроенное с Windows 365 Boot, может загружаться непосредственно на Резерв Windows 365 облачный компьютер, обеспечивая простой, локальный интерфейс для пользователя.

Поддерживает ли Резерв Windows 365 Windows 365 Link? Да, Windows 365 Link совместима с Резерв Windows 365.

Лицензирование и доступ

Должен ли я быть клиентом Windows 365? Нет. Резерв Windows 365 — это автономная лицензия с теми же предварительными условиями, что и Enterprise и Frontline.

Сколько лицензий следует приобрести? Запланируйте одну лицензию на пользователя, которую вы хотите охватить. Лицензии нельзя использовать в пуле или совместном доступе.

Можно ли дождаться назначения лицензий, пока они не понадобятся пользователям, и немедленно подготовить их? Нет. Настройте и назначьте политики подготовки Резерв Windows 365 на ранней стадии, чтобы избежать задержек подготовки, когда пользователям требуется доступ. Облачный компьютер пользователя имеет право на подготовку, начиная с семи дней после назначения лицензии, поэтому лицензии не могут быть назначены и немедленно подготовлены для пользователя.

Эта задержка применяется только при первом назначении лицензии каждому пользователю или после истечения срока действия лицензии. После истечения задержки вы можете подготовить облачный компьютер пользователя в любое время в течение срока действия лицензии.

После назначения вы можете отслеживать право и состояние подготовки пользователей в соответствии с их политикой подготовки в Intune.

Может ли 10-дневный лимит быть общим или продленным? Нет. Пользователи не могут совместно использовать эти 10 дней. Расширения и стек не поддерживаются в общедоступной версии.

Когда начинается и останавливается 10-дневный период? 10-дневный период доступа начинается с подготовки облачного компьютера и заканчивается отзывом.

Что происходит по истечении 10 дней? Служба принимает snapshot хранения, чтобы свести к минимуму риск потери данных, а затем отзывает облачный компьютер. Облачный компьютер не может быть подготовлен повторно, так как срок доступа истек.

Кто может отозвать облачный компьютер Резерв Windows 365 и что делает отзыв? Отмена подготовки приостанавливает 10-дневный период доступа и удаляет облачный компьютер и все данные без резервного копирования.

Администраторы могут отзываться с Intune, а пользователи могут отзывать (возвращать) облачный компьютер в Windows App. Оба действия требуют подтверждения через второй запрос на согласие и действия администратора для повторной подготовки облачного компьютера. Нет моментальных снимков или льготных периодов, когда администраторы или пользователи отменяют подготовку; Поэтому перед отзывом убедитесь, что пользователи будут создавать резервные копии важных данных.

Отмена подготовки, как только устройство больше не требуется для сохранения оставшихся дней доступа на более поздний срок действия лицензии.

Доступность службы

Гарантирует ли Резерв Windows 365 емкость заранее? Нет. Резерв Windows 365 не обеспечивает предварительное выделение и не гарантирует емкость облачного компьютера. Если предпочтительный географический регион в политике подготовки имеет ограниченные проблемы с доступностью или работоспособностью служб при выполнении запроса на подготовку, облачные компьютеры могут быть не подготовлены до тех пор, пока емкость не станет доступной.

Что происходит во время крупномасштабных событий? Во время крупных сбоев или сбоев на доступность Резерв Windows 365 могут влиять сетевые подключения, базовые зависимости служб или загрузка служб.

Скорость и масштаб подготовки зависят от вашего клиента и географического расположения. При выполнении нескольких действий по подготовке рекомендуется в первую очередь приоритизовать подготовку для наиболее важных пользователей.

Мы работаем над максимальной доступностью в крупных сбоях.

Требуется ли Интернет? Да. Windows 365 зависит от сетевого подключения.

Устройство

Включен ли физический компьютер? Нет. Пользователи подключаются с любого устройства, управляемого или неуправляемого (ПК, планшета, телефона), поддерживаемого политиками организации, с помощью Windows App или интернета.

Является ли облачный компьютер Резерв Windows 365 копией компьютера пользователя? Нет. Резерв Windows 365 предоставляет предварительно настроенный облачный компьютер с корпоративными приложениями и политиками из Intune. Локальные данные с компьютера пользователя не восстанавливаются на Резерв Windows 365 облачном компьютере.

Известные ограничения

Массовая подготовка имеет ограничение в 100 устройств в минуту. Если вы одновременно подготавливаете более 100 устройств в Intune или PowerShell, все они начинают подготовку, но некоторые из них могут завершиться ошибкой, и вам потребуется повторить попытку. Мы работаем над устранением этого ограничения.

Некоторые пользователи в назначенной группе не перечислены в политике > Резерв Windows 365 подготовки пользователей облачных компьютеров. Чтобы устранить неполадки, перейдите в **раздел Intune > Отчеты об > облачном компьютере Резерв Windows 365 > лицензирование**. В этом отчете перечислены все пользователи в клиенте, назначенном политике подготовки Резерв Windows 365, лицензии на Резерв Windows 365 или и тому, и тому. Используйте этот отчет, чтобы определить причину и дальнейшие действия. Причины и решения:

- Назначение политики подготовки. Пользователи отображаются только в первой назначенной им политике подготовки. Найдите пользователя в отчете, чтобы найти его основную ссылку на политику.

- Доступность лицензий: в разделе Пользователи облачных компьютеров отображаются только лицензированные пользователи. Если в клиенте недостаточно Резерв Windows 365 лицензий, не все пользователи в группе, назначенной политике подготовки, получают лицензию. Если в отчете **отображается значение 0 доступных лицензий в клиенте**, приобретите дополнительные лицензии или измените назначение политики Резерв Windows 365, чтобы освободить неиспользуемые лицензии.

Дальнейшие действия

- Что такое Резерв Windows 365?
- Управление Резерв Windows 365
- лицензирование Резерв Windows 365

Last updated on 19.11.2025

Безопасность Windows 365

Статья • 30.04.2025

Windows 365 обеспечивает сквозной поток подключения, который позволяет пользователям эффективно и безопасно выполнять свою работу. Windows 365 создается с учетом принципов "Никому не доверяй", обеспечивая основу для реализации элементов управления для лучшей защиты вашей среды в рамках 6 основных принципов "Никому не доверяй". Элементы управления "Никому не доверяй" можно реализовать для следующих категорий:

- Защита доступа к облачному компьютеру
  - Соответствует обеспечению безопасности **удостоверения**, где можно разместить дополнительные меры для того, кто может получить доступ к облачному компьютеру и при каких условиях.
- Защита самого устройства облачного компьютера
  - Соответствует защите **конечной точки**, где можно разместить дополнительные меры на устройствах облачных компьютеров, так как это устройство используется для доступа к данным организации.
- Защита данных облачного компьютера и других данных, доступных при использовании облачного компьютера
  - Соответствует защите **данных**, где можно разместить дополнительные меры для самих данных или того, как пользователь Облачного компьютера обращается к данным.

Ознакомьтесь со следующими разделами, чтобы лучше понять компоненты и функции, доступные для защиты среды облачного компьютера.

Безопасный доступ к облачному компьютеру

Первое соображение для защиты среды — защита доступа к облачному компьютеру.

Как описано в разделе Идентификация и проверка подлинности, для доступа к облачному компьютеру существует две проблемы проверки подлинности:

- службы Windows 365, а также
- облачного компьютера.

Основным элементом управления для защиты доступа является использование условного доступа Microsoft Entra для условного предоставления доступа к службе Windows 365. Сведения о том, как защитить доступ к облачному компьютеру, см. в статье Настройка политик условного доступа.

Защита устройств облачных компьютеров

Второе соображение для защиты среды — защита самого устройства облачного компьютера.

Функции безопасности, включенные по умолчанию

На всех новых облачных компьютерах по умолчанию включены следующие компоненты безопасности:

- **vTPM**. Сокращение от виртуального доверенного платформенного модуля, vTPM предоставляет облачным компьютерам собственный выделенный экземпляр доверенного платформенного модуля, который выступает в качестве безопасного хранилища для ключей и измерений. Дополнительные сведения см. в статье vTPM.
- **Безопасная загрузка**. Безопасная загрузка — это функция, которая предотвращает загрузку операционной системы Windows, если на компьютере установлены ненадежные rootkit или загрузочные комплекты. Дополнительные сведения см. в статье Безопасная загрузка.
- Целостность кода гипервизора (HVCI)*
- Microsoft Defender Credential Guard*

* По умолчанию включен только для облачных компьютеров, на которых запущен образ Windows 11 коллекции.

Функции безопасности, требующие определенных номеров SKU или конфигурации облачных компьютеров

Следующие компоненты безопасности включены по умолчанию в определенных SKU или конфигурациях облачных компьютеров:

- **Рабочие нагрузки на основе виртуализации**
  - **Описание**. Рабочие нагрузки на основе виртуализации обычно требуют, чтобы устройство Windows включило функцию Hyper-V и выполняло рабочие нагрузки в изолированном пространстве, чтобы защитить ОС Windows от любых угроз безопасности.
  - **Функции безопасности**:
    - Application Guard в Microsoft Defender
    - Песочница Windows
  - **Требуемая конфигурация**. Облачный компьютер должен иметь 4 виртуальных ЦП и 16 ГБ ОЗУ или более. Дополнительные сведения см. в статье Настройка поддержки рабочих нагрузок на основе виртуализации.

> **Примечание**
>
> Учитывая технологическую сложность, обещание безопасности Application Guard в Microsoft Defender (MDAG) может не выполняться на виртуальных машинах и в средах VDI. Таким образом, MDAG в настоящее время официально не поддерживается на виртуальных машинах и в средах VDI. Однако для тестирования и автоматизации на непроизводственных компьютерах можно включить MDAG на виртуальной машине, включив вложенную виртуализацию Hyper-V на узле.

Защищенное хранилище Microsoft Purview

Блокировка клиента Microsoft Purview может быть включена администратором. Это гарантирует, что корпорация Майкрософт не сможет получить доступ к содержимому клиента для выполнения операций обслуживания без вашего явного согласия. В Центр администрирования Microsoft 365 вы можете включить или отключить блокировку клиента. Дополнительные сведения см. в разделе Microsoft Purview Customer Lockbox.

Защита данных облачного компьютера

Третье соображение для защиты среды — защита данных облачного компьютера и других данных, которые предоставляются с помощью облачного компьютера.

Безопасность данных облачных компьютеров

Сами данные облачных компьютеров защищаются с помощью шифрования. Дополнительные сведения см. в разделе Шифрование данных в Windows 365.

Безопасность данных, доступных на облачном компьютере

Защита данных, доступных пользователям на облачных компьютерах, должна ничем не отличаться от защиты данных, доступных пользователям на компьютерах Windows, назначаемых работой. Доступ к облачному компьютеру должен осуществляться через протокол удаленного рабочего стола (RDP).

Сведения об управлении функциями RDP, доступными пользователю во время подключения к облачному компьютеру, см. в статье Управление перенаправлениями устройств RDP для облачных компьютеров.

Безопасность обновления клиента

Windows 365 облачные компьютеры можно получить с различных платформ операционной системы и клиентов, доступных на этих платформах.

- **Платформы ОС Windows**: доступ к Windows 365 можно получить с помощью клиента удаленного рабочего стола для Windows и Windows App. Оба этих приложения получают обновления с помощью службы клиентский компонент Центра обновления Windows. Дополнительные сведения см. в разделе безопасность клиентский компонент Центра обновления Windows.
- **Устройства Apple (macOS и iOS):** клиентские приложения удаленного рабочего стола и их обновления распространяются магазином приложений Apple. Дополнительные сведения о мерах безопасности MacOS и iOS см. в разделе Безопасность платформы Apple.
- **Платформы Android**: приложения платформы Android, скачанные из магазинов Google Play, соответствуют условиям магазина Google play. Дополнительные сведения см. в разделе Условия обслуживания Google Play.

Дальнейшие действия

Дополнительные сведения о безопасности клиентский компонент Центра обновления Windows см. в разделе безопасность клиентский компонент Центра обновления Windows.

Шифрование данных в Windows 365

Статья • 31.01.2025

Windows 365 шифрует неактивные и передаваемые данные, как описано в этой статье.

Шифрование статических данных

Для защиты данных организации диски Windows 365 Корпоративная и диски облачных компьютеров для бизнеса шифруются с помощью шифрования со стороны сервера хранения Azure (SSE).

Шифрование уровня хранилища обеспечивает следующие преимущества.

- Когда данные сохраняются в облаке, неактивные данные на диске облачного компьютера, размещенного корпорацией Майкрософт, автоматически шифруются.
- Диски облачного компьютера Windows 365 шифруются прозрачно с помощью 256-битного шифрования AES, современного блочного шифра. Шифрование соответствует требованиям FIPS 140-2. Шифрование на этом уровне не влияет на производительность облачных компьютеров.
- Шифрование применяется к каждому компьютеру в облаке в каждом регионе без дополнительных затрат.

Следующие объекты Windows 365 Корпоративная и Windows 365 для бизнеса автоматически шифруются во время хранения с помощью ключей, управляемых платформой:

- диски;
- снимки;
- изображения;

Windows 365 как услуга рассматривает все данные, хранимые на дисках Windows 365, как контент клиента. Дополнительные сведения см. в статье Конфиденциальность и персональные данные в Windows 365.

> **Примечание**
>
> BitLocker не поддерживается в качестве варианта шифрования для облачных компьютеров Windows 365. Дополнительные сведения см. в статье Использование виртуальных машин с Windows 10 в Intune.

Шифрование транзитных данных

Windows 365 использует протокол TLS для защиты данных при передаче. TLS обеспечивает следующее.

- Строгая проверка подлинности
- Конфиденциальность и целостность сообщений (позволяет обнаруживать взлом, перехват и подделку сообщений)
- Взаимодействие
- Гибкость алгоритма
- Простота развертывания и использования

TLS 1.2 используется для всех подключений из Windows 365 к компонентам инфраструктуры виртуального рабочего стола Azure. Эти компоненты используют те же шифры TLS 1.2, что и Azure Front Door. Дополнительные технические сведения о наборах шифров см. в техническом справочнике по Microsoft 365. Сведения о шифровании. Для транспорта с обратным подключением поддерживается ПРОТОКОЛ TLS 1.3. Дополнительные сведения см. в статье Общие сведения о подключении к Виртуальному рабочему столу Azure.

Дальнейшие действия

Дополнительные сведения о модулях шифрования, которые являются базовыми для управляемых дисков Azure, см. в статье API шифрования нового поколения.

Дополнительные сведения о возможностях сетевого подключения и шифровании удаленного подключения RDP см. в статье Общие сведения о возможностях сетевого подключения виртуального рабочего стола Azure.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Защищенное хранилище Microsoft Purview

Статья • 03.02.2025

В этой статье содержатся рекомендации по развертыванию и настройке для клиентского хранилища. Защищенное хранилище поддерживает запросы на доступ к данным в Exchange Online, SharePoint, OneDrive, Teams и Windows 365. Кроме того, все Microsoft 365 Copilot взаимодействия охватываются клиентской блокировкой через поддержку, доступную для Exchange Online. Чтобы порекомендовать поддержку для других служб, отправьте запрос на портале отзывов.

Чтобы ознакомиться с вариантами лицензирования пользователей, чтобы воспользоваться преимуществами предложений Microsoft Purview, ознакомьтесь с руководством по лицензированию Microsoft 365 по обеспечению безопасности & соответствия требованиям.

Защищенное хранилище гарантирует, что корпорация Майкрософт не сможет получить доступ к вашему содержимому для выполнения служебных операций без вашего явного одобрения. Защищенное хранилище приводит вас к процессу утверждения, который корпорация Майкрософт использует для обеспечения доступа к вашему содержимому только авторизованным запросам. Дополнительные сведения о процессе рабочего процесса Майкрософт см. в статье Управление привилегированным доступом.

Иногда инженеры Майкрософт помогают устранять неполадки, возникающие в службе. Как правило, инженеры устраняют проблемы с помощью обширных средств телеметрии и отладки, которые корпорация Майкрософт использует для своих служб. Однако в некоторых случаях требуется, чтобы инженер Корпорации Майкрософт мог получить доступ к вашему содержимому, чтобы определить первопричину и устранить проблему. Клиентская блокировка требует, чтобы инженер запросит у вас доступ в качестве заключительного шага в рабочем процессе утверждения. Это позволяет утвердить или отклонить запрос для вашей организации, а также обеспечить прямой доступ к содержимому.

Совет

Если вы не являетесь клиентом E5, используйте 90-дневную пробную версию решений Microsoft Purview, чтобы узнать, как дополнительные возможности Purview могут помочь вашей организации управлять безопасностью данных и

соответствием требованиям. Начните сейчас в центре пробных версий Microsoft Purview. Сведения о регистрации и условиях пробной версии.

> **Важно!**
>
> Microsoft рекомендует использовать роли с наименьшим количеством разрешений. Минимизация числа пользователей с ролью глобального администратора помогает повысить безопасность организации. Дополнительные сведения о ролях и разрешениях Microsoft Purview.

Обзор защищенного хранилища клиента

https://learn-video.azurefd.net/vod/player?id=016276d0-7e5d-43b5-8dee-8d4c6c542e23&locale=ru-ru&embedUrl=%2Fpurview%2Fcustomer-lockbox-requests

Рабочий процесс для защищенного хранилища

Ниже описан типичный рабочий процесс, когда инженер Майкрософт запускает запрос на блокировку клиента:

1. Сотрудник организации испытывает проблему с почтовым ящиком Microsoft 365.
2. Пользователь диагностирует проблему, но не может устранить ее, поэтому отправляет запрос в службу поддержки Майкрософт.
3. Инженер службы поддержки Майкрософт проверяет запрос на обслуживание и определяет необходимость доступа к клиенту организации для устранения проблемы.
4. Инженер службы поддержки Майкрософт входит в средство запроса "Защищенное хранилище" и выполняет запрос на доступ к данным, который включает имя клиента организации, номер запроса на обслуживание, ожидаемое время начала доступа (начинается сразу после утверждения, если не указано), предполагаемое время, в течение которых инженеру требуется доступ к данным, и служба, для которую выполняется запрос.
5. Когда менеджер службы поддержки Майкрософт утвердит запрос, защищенное хранилище по электронной почте отправляет сотруднику

организации, ответственному за утверждение, уведомление о запросе доступа от Майкрософт, ожидающем рассмотрения.

Microsoft 365

Action required

A Customer Lockbox request is pending your approval

Sign in to the Microsoft 365 admin center to approve or deny this request.

Request details

Product	Exchange
Service Request #	0001-dc35d1f3-82ce-4378-82e4-a5c673784443
Request ID	0001-dc35d1f3-82ce-4378-82e4-a5c673784443
Tenant	Contoso
Requestor	Microsoft Operator
Reason	Troubleshoot issues impacting the customer's service
Create Time	8/28/2020 12:14:18 PM
Duration	12
Requestor's Location	United States
Expires	8/29/2020 12:14:18 PM

If a Customer Lockbox request is denied or isn't approved within 12 hours, the request expires. If this happens, you might continue to experience a specific service issue that could be resolved by allowing an engineer to access the content.

Learn more about approving Customer Lockbox requests.

Review Microsoft 365 data access policies.

Privacy Statement

Microsoft Corporation, One Microsoft Way, Redmond, WA 98052

Microsoft

Любой пользователь, которому назначена роль администратора утверждающего доступ к защищенному хранилищу в Центр администрирования Microsoft 365, может утверждать запросы на блокировку клиента.

6. Утверждающий входит в Центр администрирования Microsoft 365 и утверждает запрос. При этом создается запись аудита, которую можно найти с помощью поиска по журналу аудита. Дополнительные сведения см. в разделе Аудит запросов на блокировку клиентов.

   Если клиент отклоняет запрос или не утверждает запрос в течение 12 часов, срок действия запроса истекает, и инженеру Майкрософт не предоставляется доступ.

   > **Важно!**
   >
   > Корпорация Майкрософт не включает ссылки в защищенное хранилище Уведомления по электронной почте требует входа в Office 365.

7. После утверждения запроса утверждающий из организации инженер Майкрософт получает сообщение об утверждении, входит в клиент и устраняет проблему клиента. Доступ предоставляется инженерам Майкрософт на указанное время, по истечении которого он автоматически аннулируется.

> **Примечание**
>
> Все действия, выполняемые инженером Майкрософт, регистрируются в журнале аудита. Вы можете найти и просмотреть эти записи аудита.

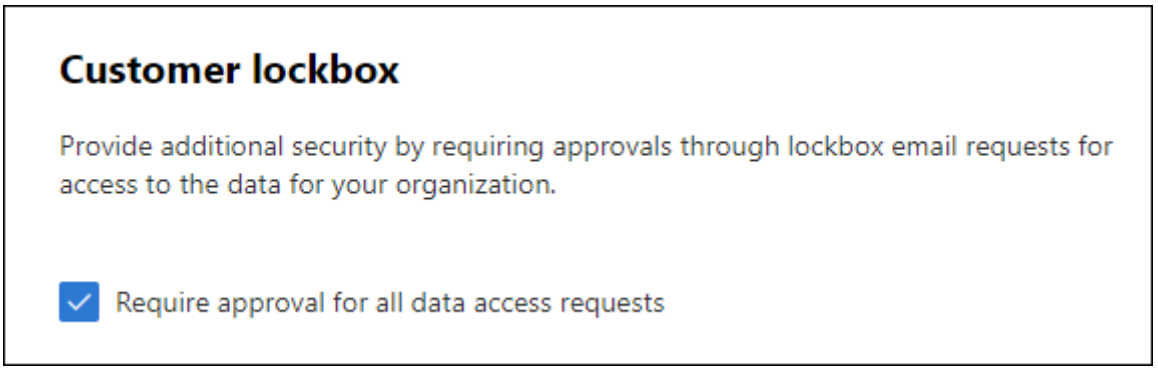
Включение или отключение запросов на блокировку клиента

Включить элементы управления "Защищенное хранилище" можно в Центре администрирования Microsoft 365. При включении клиентской блокировки корпорация Майкрософт должна получить одобрение вашей организации перед доступом к любому содержимому вашего клиента.

1. Используя рабочую или учебную учетную запись, у которого назначена роль **глобального администратора или утверждающего доступа к защищенному хранилищу,** перейдите на страницу https://admin.microsoft.com и выполните вход.

2. Выберите **Параметры**>**Организации Параметры**>**Безопасность & Конфиденциальность**.

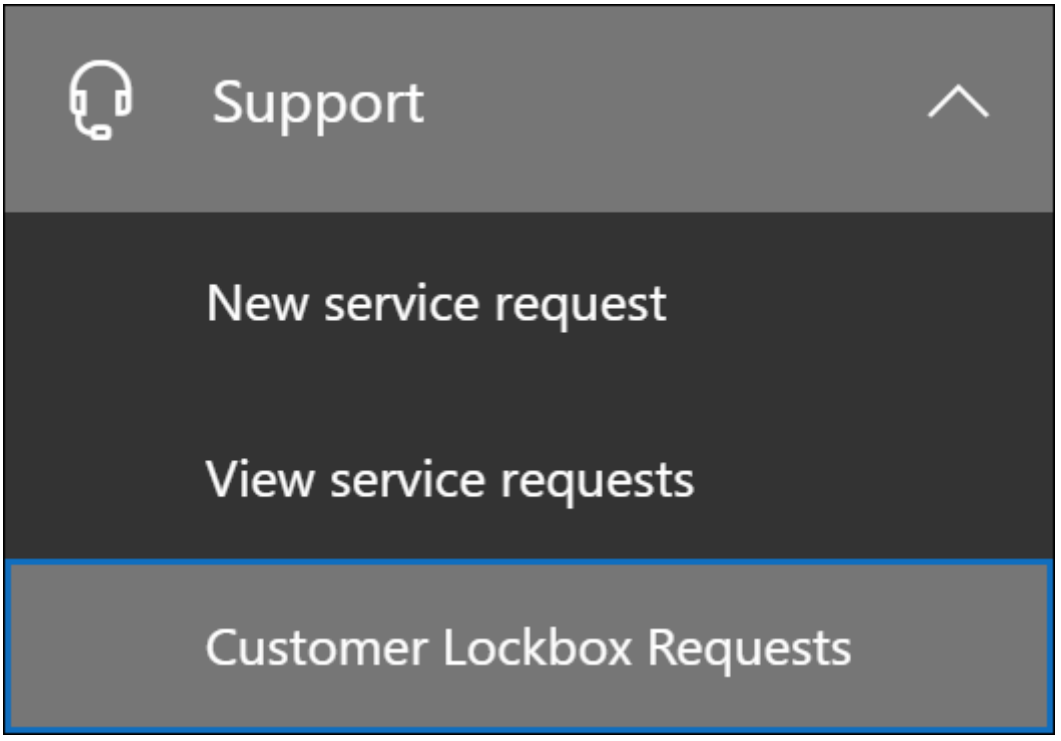
3. Выберите **Безопасность & конфиденциальность**, а затем в левом столбце выберите **Защищенное хранилище клиента** . Установите флажок **Требовать утверждения для всех запросов на доступ к данным** и сохраните изменения, чтобы включить эту функцию.



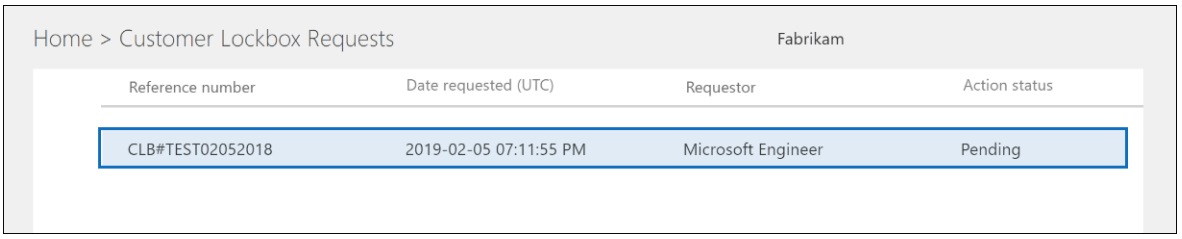
Одобрение и отклонение запроса на доступ к защищенному хранилищу

1. Используя рабочую или учебную учетную запись, у которого назначена роль **глобального администратора или утверждающего доступа к защищенному хранилищу,** перейдите на страницу https://admin.microsoft.com и выполните вход.

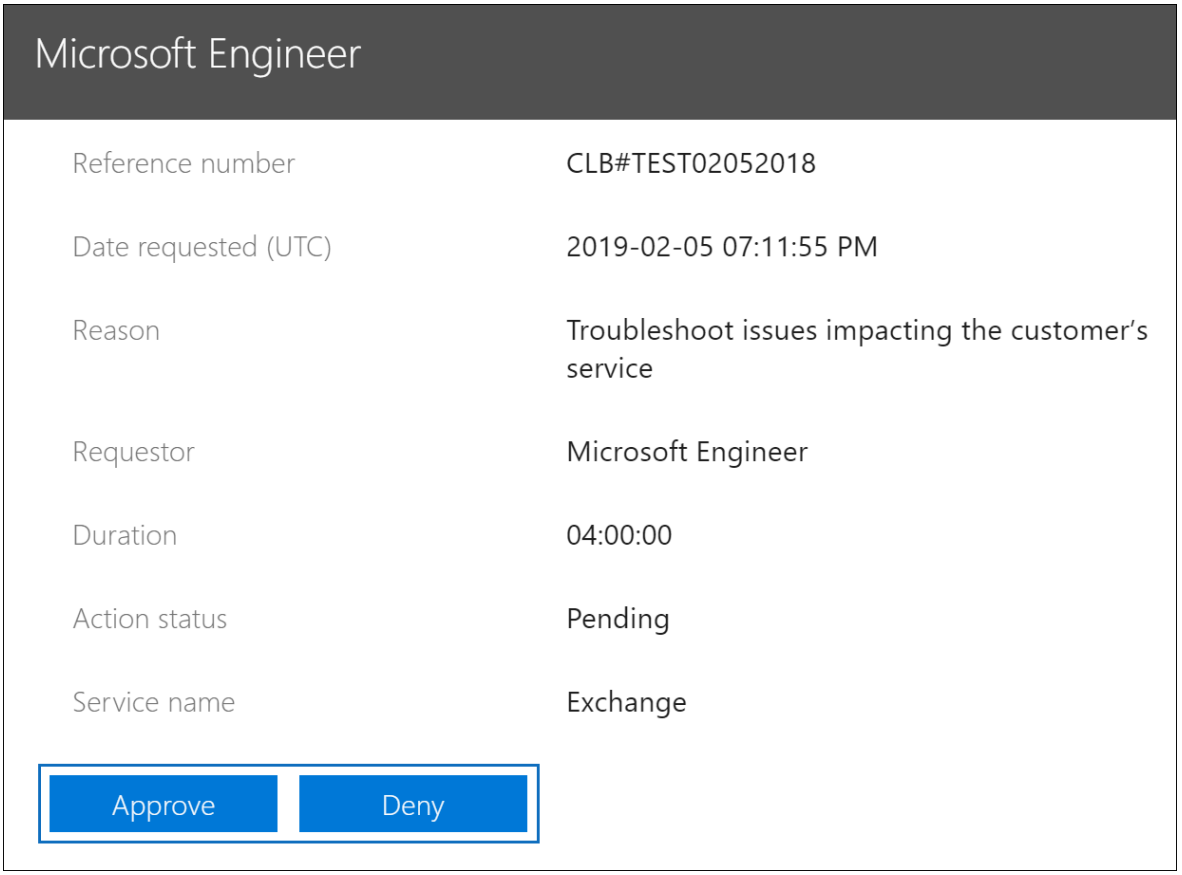
2. Выберите **Запросы на блокировку для клиентов в службе поддержки**>.



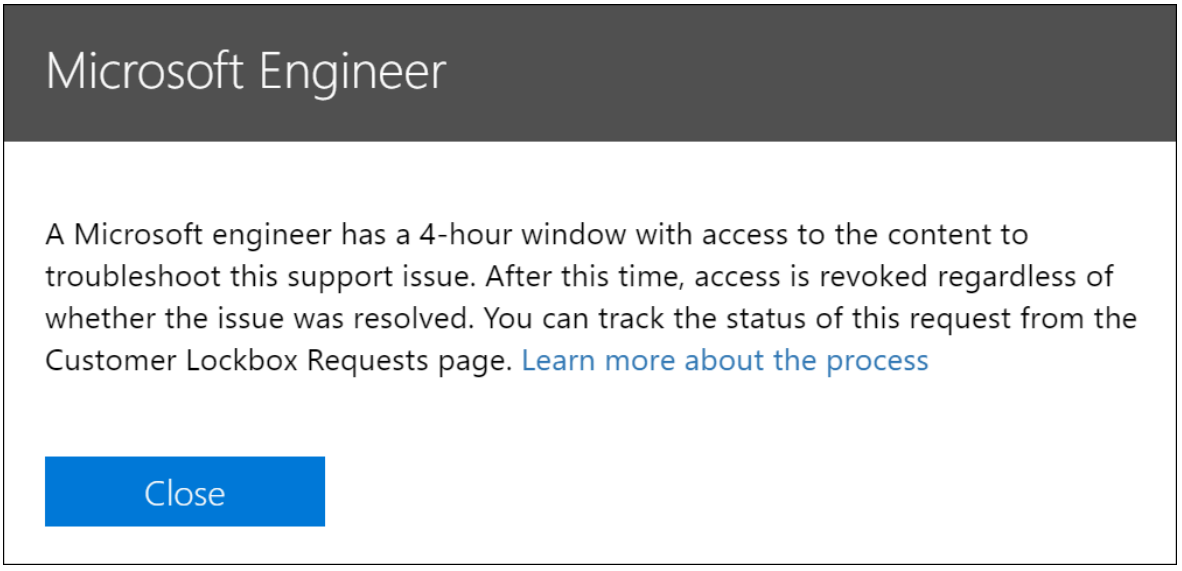
Отобразится список запросов к защищенному хранилищу.



3. Выберите запрос на блокировку клиента, а затем выберите **Утвердить** или **Отклонить**.



Появится сообщение с подтверждением об утверждении запроса на блокировку клиента.



> **Примечание**
>
> Используйте командлет Set-AccessToCustomerDataRequest для утверждения, отклонения или отмены запросов на блокировку клиентов Microsoft Purview, которые управляют доступом к вашим данным инженерами службы поддержки Майкрософт. Дополнительные сведения см. в разделе Set-AccessToCustomerDataRequest.

Аудит запросов на доступ к защищенному хранилищу

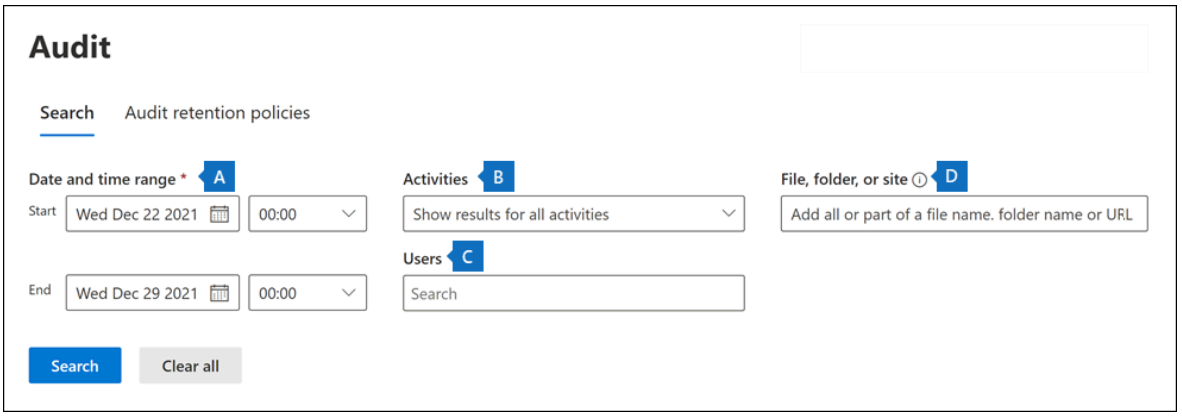
Записи аудита, соответствующие запросам защищенного хранилища клиентов, регистрируются в журнале аудита Microsoft 365. Доступ к этим журналам можно получить с помощью средства поиска по журналам аудита в Портал соответствия требованиям Microsoft Purview. Действия, связанные с принятием или отклонением запроса на блокировку клиента, и действия, выполняемые инженерами Майкрософт (при утверждении запросов на доступ), также регистрируются в журнале аудита. Вы можете найти и просмотреть эти записи аудита.

Поиск действий, связанных с запросами к защищенному хранилищу клиента, в журнале аудита

Прежде чем вы сможете использовать журнал аудита для отслеживания запросов к защищенному хранилищу клиента, необходимо выполнить некоторые действия, чтобы настроить ведение журнала аудита, включая назначение разрешений на поиск в журнале аудита. Дополнительные сведения см. в статье Начало работы с решениями аудита. Завершив настройку, выполните следующие действия, чтобы создать поисковый запрос журнала аудита для возврата записей аудита, связанных с хранилищем клиента:

1. Перейдите по адресу https://compliance.microsoft.com .
2. Войдите с помощью учетной записи, которая получила соответствующие разрешения для поиска в журнале аудита.
3. В левой области Центра соответствия требованиям выберите **Аудит**.

   Появится вкладка **Поиск** на странице **Аудит** .



4. Настройте указанные ниже условия.

   a. **Дата начала** и **дата окончания**. Выберите диапазон дат и времени, чтобы просмотреть события, которые произошли за этот период.

   b. **Действия**. Оставьте это поле пустым, чтобы поиск возвращал записи аудита для всех действий. Это необходимо для возврата всех записей аудита, связанных с запросами на блокировку клиента и соответствующими действиями, выполняемыми инженерами Майкрософт.

   c. **Пользователи**. Оставьте это поле пустым.

   d. **Файл, папка или сайт**. Оставьте это поле пустым.

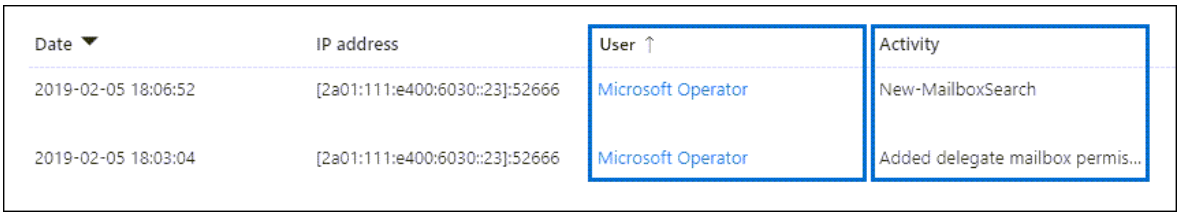
5. Чтобы выполнить поиск по указанным условиям, нажмите кнопку **Поиск**.

   Результаты поиска отображаются через несколько секунд. Дополнительные результаты поиска будут добавлены на страницу до завершения поиска.

6. Щелкните заголовок в столбце **Действие** , чтобы отсортировать результаты в алфавитном порядке по значениям в столбце **Действие** .

7. Прокрутите вниз и найдите записи аудита с действием **Set-AccessToCustomerDataRequest**. Записи с этим действием связаны с утверждением в вашей организации, утверждающим или отклоняющим запрос на блокировку клиента.

8. Кроме того, щелкните заголовок в столбце **Пользователь** , чтобы отсортировать результаты в алфавитном порядке, используя значения в столбце **Пользователь** . Найдите значение **Оператора Майкрософт**, которое указывает на действия, выполняемые инженером Майкрософт в ответ на утвержденный запрос на блокировку клиента. В столбце **Действие** отображается действие, выполненное инженером.



Date	IP address	User	Activity
2019-02-05 18:06:52	[2a01:111:e400:6030::23]:52666	Microsoft Operator	New-MailboxSearch
2019-02-05 18:03:04	[2a01:111:e400:6030::23]:52666	Microsoft Operator	Added delegate mailbox permis...

9. В списке результатов щелкните запись аудита, чтобы отобразить ее.

Экспорт результатов поиска в журнале аудита

Вы также можете экспортировать результаты поиска по журналу аудита в CSV-файл, а затем открыть файл в Excel, чтобы использовать возможности фильтрации и сортировки, чтобы упростить поиск и просмотр записей аудита, связанных с запросом на доступ к защищенному хранилищу.

Чтобы экспортировать записи аудита, выполните предыдущие действия для поиска в журнале аудита. После завершения поиска выберите **Экспорт** > **Скачать все результаты** в верхней части страницы результатов поиска. После завершения экспорта можно скачать CSV-файл на локальный компьютер. Более подробные инструкции см. в статье Экспорт, настройка и просмотр записей журнала аудита.

Скачав файл, вы можете открыть его в Excel, а затем отфильтровать в столбце **Операции** записи аудита для действий **Set-AccessToCustomerDataRequest** . Вы также можете отфильтровать столбец **UserIds** (используя значение **Оператор Майкрософт**), чтобы отобразить записи аудита для действий, выполняемых инженерами Майкрософт.

> ⓘ **Примечание**
>
> При просмотре записей аудита в CSV-файле дополнительные сведения содержатся в столбце **AuditData** . Сведения в этом столбце содержатся в объекте JSON, который содержит несколько свойств, настроенных как пары *property:value* , разделенные запятыми. Функцию преобразования JSON можно использовать в Редактор Power Query в Excel, чтобы разделить каждое свойство объекта JSON в столбце **AuditData** на несколько столбцов, чтобы каждое свойство было собственным. Это упрощает интерпретацию этой информации. Подробные инструкции см. в разделе Форматирование экспортированного журнала аудита с помощью Редактор Power Query.

Поиск и экспорт записей аудита с помощью PowerShell

Альтернативой использованию средства поиска аудита в Портал соответствия требованиям Microsoft Purview является выполнение командлета Search-UnifiedAuditLog в Exchange Online PowerShell. Одним из преимуществ использования PowerShell является то, что вы можете специально искать действия **Set-AccessToCustomerDataRequest** или действия, выполняемые инженерами Майкрософт, связанные с запросом на блокировку клиента.

После подключения к Exchange Online PowerShell выполните одну из следующих команд. Замените заполнители определенным диапазоном дат.

`Set-AccessToCustomerDataRequest` Поиск действий

PowerShell

```
Search-UnifiedAuditLog -StartDate xx/xx/xxxx -EndDate xx/xx/xxxx -Operations
Set-AccessToCustomerDataRequest
```

Поиск действий, выполняемых инженерами Майкрософт

PowerShell

```
Search-UnifiedAuditLog -StartDate xx/xx/xxxx -EndDate xx/xx/xxxx -UserIds
"Microsoft Operator"
```

Дополнительные сведения и примеры см. в статье Использование PowerShell для поиска и экспорта записей журнала аудита.

Мы также предоставили скрипт PowerShell, который можно использовать для поиска в журнале аудита и экспорта результатов в CSV-файл. Дополнительные сведения см. в статье Использование скрипта PowerShell для поиска в журнале аудита.

Запись аудита для запроса на блокировку клиента

Когда сотрудник вашей организации утверждает или отклоняет запрос на блокировку клиента, запись аудита регистрируется в журнале аудита, содержащую следующие сведения.

Развернуть таблицу

Свойство записи аудита	Описание
Date	Дата и время одобрения или отклонения запроса на доступ к защищенному хранилищу.
IP-адрес	IP-адрес компьютера, используемого утверждающий для одобрения или отклонения запроса.
Пользователь	Учетная запись службы BOXServiceAccount@[customerforest].prod.outlook.com.
Действие	Set-AccessToCustomerDataRequest; это действие аудита, которое регистрируется при одобрении или отклонении запроса на доступ к защищенному хранилищу.
Элемент	Guid запроса на блокировку клиента

На следующем снимку экрана показан пример записи аудита, которая соответствует утвержденному запросу на блокировку клиента. Если запрос на защищенное хранилище клиента был отклонен, значение параметра будет иметь значение `ApprovalDecision` `Deny`.

Date:	2019-02-05 16:46:06
IP address:	[2a01:111:f100:3002::8987:3552]:47621
User:	BOXServiceAccount@namprd17.prod.outlook.com
Activity:	Set-AccessToCustomerDataRequest
Item:	979f5fcc-8442-44f9-a363-c56ab355d452
Detail:	
ClientIP:	[2a01:111:f100:3002::8987:3552]:47621
CreationTime:	2019-02-06T00:46:06
ExternalAccess:	true
Id:	6096e057-d524-4f44-dc18-08d68bcc7abd
ObjectId:	979f5fcc-8442-44f9-a363-c56ab355d452
Operation:	Set-AccessToCustomerDataRequest
OrganizationId:	dac0e46e-6bf4-4227-b525-676a25342e91
OrganizationName:	pam0131.onmicrosoft.com
OriginatingServer:	BN6PR17MB2003 (15.20.1580.012)
Parameters:	


```
[
  {
    "Name": "Comment",
    "Value": "O365AdminPortal"
  },
  {
    "Name": "ApprovalDecision",
    "Value": "Approve"
  },
  {
    "Name": "RequestId",
    "Value": "979f5fcc-8442-44f9-a363-c56ab355d452"
  }
]
```


RecordType:	1
ResultStatus:	True
SessionId:	
UserId:	BOXServiceAccount@namprd17.prod.outlook.com
UserKey:	BOXServiceAccount@namprd17.prod.outlook.com
UserType:	3
Version:	1
Workload:	Exchange

Запись аудита для действия, выполненного инженером Майкрософт

Действия, выполняемые инженером Майкрософт после утверждения запроса на доступ к защищенному хранилищу (что может привести к доступу к содержимому

клиента), регистрируются в журнале аудита. Эти записи содержат следующие сведения.

Развернуть таблицу

Свойство записи аудита	Описание
Date	Дата выполнения действия. Время выполнения этого действия будет в течение 4 часов с момента утверждения запроса на блокировку клиента.
IP-адрес	IP-адрес компьютера, использованного инженером Майкрософт.
Пользователь	Оператор Майкрософт; это значение указывает, что запись связана с запросом на блокировку клиента.
Действие	Имя действия, выполненного инженером Майкрософт.
Элемент	<пустой>

Вопросы и ответы

К каким службам Microsoft 365 применяется блокировка клиента?

В настоящее время защищенное хранилище поддерживается в Exchange Online, SharePoint Online, OneDrive для бизнеса, Teams и Windows 365.

Доступно ли клиентское хранилище для всех клиентов?

Защищенное хранилище входит в состав подписок Microsoft 365 или Office 365 E5 и может быть добавлено в другие планы с помощью подписки на Information Protection и соответствие требованиям или надстройку расширенного соответствия требованиям. Для клиентов из государственных организаций блокировка клиента входит в подписку Microsoft 365 или Office 365 G5. Дополнительные сведения см. в разделе Планы и цены .

Что такое содержимое клиента?

Содержимое клиента — это данные, созданные пользователями служб и приложений Microsoft 365. Ниже приведены примеры контента клиента.

- Текст или вложения электронного письма
- Содержимое сайта SharePoint
- Сведения в тексте файла SharePoint
- Skype для бизнеса текст файла презентации
- Мгновенные сообщения или голосовые беседы
- Текст, введенный в чатах Teams и каналах Teams, например в чатах 1:1, групповых чатах, общих каналах, частных каналах и чате собраний
- Другие данные, вставляемые в потоки чата Teams, такие как фрагменты кода, изображения, аудио- и видеосообщения, а также ссылки
- Данные приложений и ботов в чатах Teams и каналах Teams
- Веб-канал действий Teams
- Записи и расшифровки собраний Teams
- Голосовая почта
- Файлы, размещенные в чатах и каналах Teams
- взаимодействие Microsoft 365 Copilot
- Созданные клиентом большие двоичные объекты или структурированные данные хранилищ (например, контейнеры SQL)
- Принадлежащая клиенту информация для обеспечения безопасности (например, сертификаты, ключи шифрования и пароли)
- Выводы и все последующие выводы, если содержимое клиента остается

Дополнительные сведения о содержимом клиента в Office 365 см. в центре управления безопасностью Office 365 .

Кто получает уведомление о запросе на доступ к моему содержимому?

Глобальные администраторы и все пользователи, которым назначена роль администратора утверждающего доступ к защищенному хранилищу клиента,

получают уведомления. Это также те же пользователи, которые могут утверждать запросы на блокировку клиента.

Кто может утвердить или отклонить эти запросы в моей организации?

Глобальные администраторы и любой пользователь, которому назначена роль администратора утверждающего доступ к защищенному хранилищу, могут утверждать запросы на блокировку клиента. Клиенты управляют этими назначениями ролей в своих организациях.

Разделы справки согласиться на доступ к защищенному хранилищу?

Глобальный администратор может включить и настроить защищенное хранилище клиента в Центр администрирования Microsoft 365.

Если я утвержу запрос на блокировку клиента, что может сделать инженер и как узнать, что сделал инженер Майкрософт?

После утверждения запроса на блокировку клиента инженер Майкрософт предоставил эти необходимые привилегии для доступа к содержимому клиента с помощью предварительно утвержденных командлетов. Действия, выполняемые инженерами Майкрософт в ответ на запросы к защищенному хранилищу, регистрируются и доступны в журнале аудита в Центре соответствия требованиям безопасности &.

Разделы справки знаете, что корпорация Майкрософт выполняет процесс утверждения?

Вы можете перекрестно ссылаться на уведомления об утверждении по электронной почте, отправленные администраторам и утверждателям в вашей организации, в журнале запросов к защищенному хранилищу в Центр администрирования Microsoft 365 .

Защищенное хранилище клиентов входит в последний отчет об аудите SOC 1 SSAE 16 . Дополнительные сведения см. в последних отчетах на портале Microsoft Service Trust Portal .

Может ли корпорация Майкрософт изменить список утверждающих лиц для моего клиента? Если нет, как это предотвратить?

Только глобальный администратор в вашей организации может указать, кто может утверждать запросы на блокировку клиента. Это означает, что только члены группы глобальный администратор в Microsoft Entra ID могут указать, кто может утверждать запрос. Членство в группе глобальный администратор в Microsoft Entra ID управляется только вашей организацией.

Что делать, если мне нужны дополнительные сведения о запросе на доступ к содержимому, чтобы утвердить его?

Каждый запрос на блокировку клиента содержит номер запроса на обслуживание Microsoft 365. Вы можете связаться с служба поддержки Майкрософт и сослаться на этот номер службы, чтобы получить дополнительные сведения о запросе.

Когда запрос на блокировку клиента утверждается, как долго действительны разрешения?

В настоящее время максимальный срок действия разрешений на доступ, предоставляемых инженерам Майкрософт, равен 4 часам. Кроме того, инженер Майкрософт может запросить более короткий период.

Как получить журнал всех запросов на блокировку клиента?

Все запросы на блокировку клиента отображаются в Центр администрирования Microsoft 365 .

Разделы справки сопоставлять запросы на доступ к содержимому с соответствующими журналами аудита?

Веб-канал действий Центра соответствия требованиям содержит действия журнала в защищенном хранилище клиента. Клиенты могут перекрестно ссылаться на действия в журнале защищенного хранилища клиентов из веб-канала действий на полученный запрос электронной почты.

Что происходит, если клиент не отвечает на запрос к защищенному хранилищу?

По умолчанию срок действия запросов на доступ к защищенному хранилищу равен 12 часам. Если вы не ответите на запрос в течение 12 часов, срок действия запроса истекает.

Что делает корпорация Майкрософт, когда клиент отклоняет запрос на доступ к защищенному хранилищу?

Если клиент отклоняет запрос на блокировку клиента, доступ к содержимому клиента не происходит. Если у пользователя в вашей организации по-прежнему возникает проблема со службой, требующая от Корпорации Майкрософт доступа к содержимому клиента для решения проблемы, проблема со службой может сохраниться, и корпорация Майкрософт сообщит об этом пользователю.

Разделы справки настроить оповещения при утверждении запроса?

Встроенная возможность оповещения администраторов отсутствует. Однако администраторы могут настраивать оповещения с помощью Microsoft Defender for Cloud Apps.

Защищает ли клиентская блокировка от запросов данных от правоохранительных органов или других третьих лиц?

Нет. Корпорация Майкрософт серьезно относится к сторонним запросам данных клиентов. Как поставщик облачных служб корпорация Майкрософт всегда выступает за конфиденциальность данных клиентов. В случае получения повестки корпорация Майкрософт всегда пытается перенаправить стороннюю сторону клиенту для получения информации. (Читайте блог Брэда Смита: Защита данных клиентов от государственного слежки). Мы периодически публикуем подробные сведения о запросах правоохранительных органов, получаемых корпорацией Майкрософт.

Дополнительные сведения см. в центре управления безопасностью Майкрософт, посвященном запросам данных сторонних разработчиков, и в разделе "Раскрытие данных клиента" в Условиях использования веб-служб.

Как корпорация Майкрософт гарантирует, что сотрудник не имеет постоянного доступа к содержимому клиентов в Office 365 приложениях?

Корпорация Майкрософт реализует обширные профилактические меры с помощью систем контроля доступа и детективных мер для выявления и устранения попыток обойти эти системы управления доступом. Microsoft 365 работает с принципами минимальных привилегий и JIT-доступа. Таким образом, сотрудники Корпорации Майкрософт не имеют разрешения на доступ к содержимому клиентов на постоянной основе. Если разрешение предоставлено, оно предоставляется на ограниченный срок.

Microsoft 365 использует систему управления доступом под названием *Lockbox* для обработки запросов на разрешения, которые предоставляют возможность выполнения операционных и административных функций в службе. Оператор должен запросить доступ к содержимому клиента с помощью защищенного ящика, который затем требует, чтобы второй пользователь принял меры по запросу (например, утвердить его) перед предоставлением доступа. Этот второй человек не может быть инициатором запроса и должен быть назначен для утверждения доступа к содержимому клиента. Только если запрос утвержден, оператор получает временный доступ к содержимому клиента. По истечении периода повышения прав блокировка отменяет доступ.

Дополнительные сведения об общих методах безопасности Майкрософт см. в условиях использования веб-служб .

При каких обстоятельствах инженерам Майкрософт требуется доступ к моему содержимому?

Наиболее распространенным сценарием, когда инженерам Майкрософт требуется доступ к содержимому клиента, является запрос на поддержку, требующий доступа для устранения неполадок. Основной принцип Microsoft 365 заключается в том, что служба работает без доступа майкрософт к содержимому клиентов. Почти все операции службы, выполняемые корпорацией Майкрософт, полностью автоматизированы, а участие людей строго контролируется и абстрагируется от содержимого клиента. Цель Microsoft 365 — доступ к содержимому клиента для поддержки службы не требуется, пока клиент не утвердит конкретный запрос на доступ Майкрософт.

Я уже думал, что мои данные защищены с помощью microsoft cloud, так зачем мне нужна блокировка клиента?

Защищенное хранилище обеспечивает дополнительный уровень управления, предлагая клиентам возможность явно авторизации доступа для операций службы. Демонстрируя наличие процедур для явной авторизации доступа к данным, заблокировка клиента также помогает клиентам выполнять определенные обязательства по соответствию, такие как HIPAA и FEDRAMP.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Жизненный цикл учетных данных домена сетевого подключения Azure

Статья • 23.04.2025

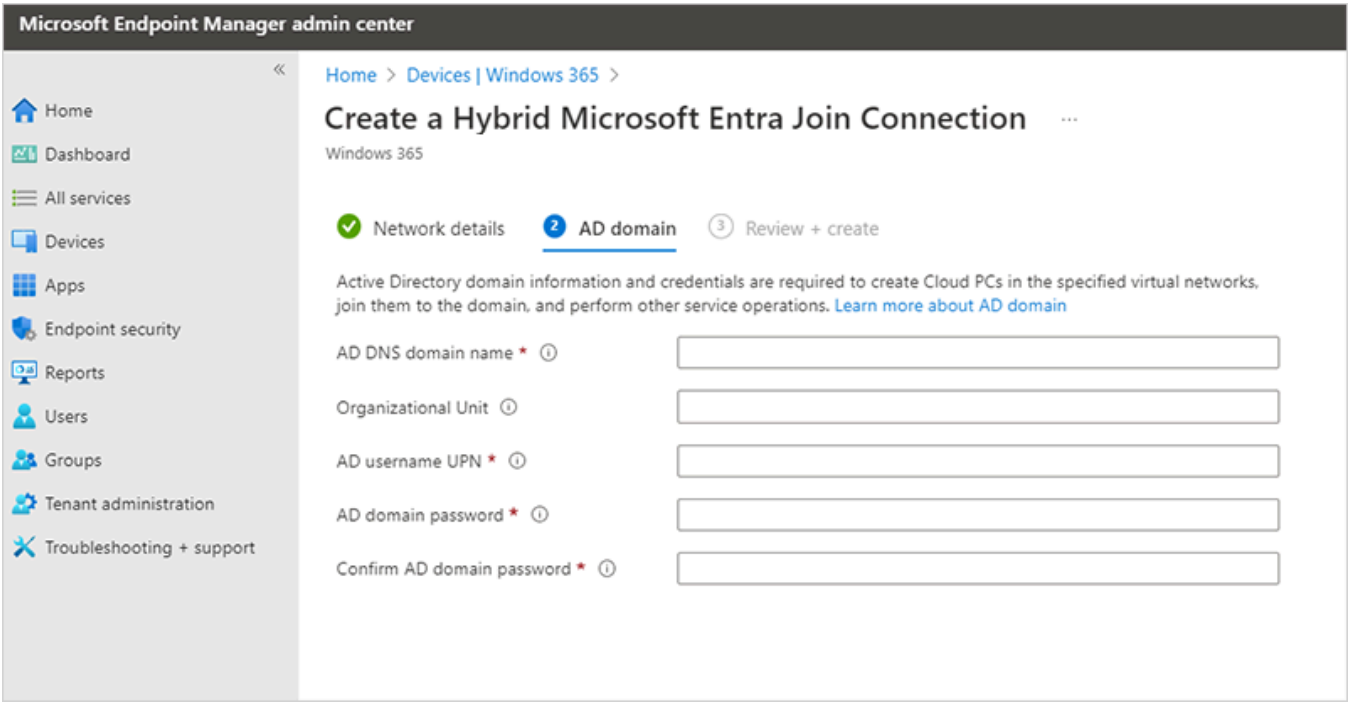
При создании сетевого подключения Azure (ANC) с помощью Microsoft Entra типа гибридного присоединения необходимо указать учетные данные локального домена. Это требование позволяет ANC взаимодействовать с локальными ресурсами.

В этой статье описывается, как Windows 365 защищает учетные данные локального домена и управляет ими в течение всего жизненного цикла Microsoft Entra гибридного присоединения ANC:

1. Предоставление учетных данных
2. Шифрование учетных данных
3. Обновление учетных данных
4. Удаление учетных данных

Предоставление учетных данных домена Microsoft Entra

При создании ANC необходимо указать учетные данные локальная служба Active Directory учетной записи пользователя, которая будет использоваться для присоединения к домену облачных компьютеров. Эти сведения, включая имя пользователя и пароль домена локальной учетной записи пользователя, укажите на странице домена AD:



Шифрование сведений о пароле домена

При создании ANC связанные с ним сведения сохраняются в службе Windows 365. Служба Windows 365 шифрует сведения о пароле домена с помощью хорошо защищенного ключа перед сохранением. Сведения о шифровании:

- Тип шифрования: сертификат azure Key Vault
- Тип ключа: RSA-HSM
- Алгоритм: RSAOAEP256

Действия по автоматическому шифрованию будут выполняться следующим образом.

1. Служба Windows 365 проверяет службу на наличие симметричного ключа для этого клиента.
2. Если ключ отсутствует или его срок действия истек, Windows 365 создает новый симметричный ключ для этого клиента с помощью генератора случайных чисел. Ключи создаются для каждого клиента.
3. Если ключ уже существует для этого клиента, он используется на следующих шагах.
4. После получения (нового или существующего) ключа клиента Windows 365 расшифровывает ключ с помощью выделенного сертификата корпоративного ЦС Windows 365.
5. Этот сертификат хранится в экземпляре azure Key Vault, управляемом корпорацией Майкрософт.
6. Windows 365 служба шифрует пароль с помощью расшифрованного ключа клиента.
7. Зашифрованный пароль сохраняется в службе Windows 365.

сертификаты Windows 365 Корпоративная

Windows 365 корпоративные сертификаты службы автоматически создаются и обновляются Key Vault Azure. Срок действия этого сертификата истекает через год. Служба Windows 365 регулярно проверяет состояние сертификата. За три месяца до истечения срока действия служба Windows 365 автоматически повторно создает новый сертификат. После создания нового сертификата он используется службой Windows 365 для повторного шифрования ключей клиента.

Алгоритм шифрования и расшифровки паролей

Windows 365 для шифрования учетных данных домена с ключом клиента используется метод шифрования, а затем MAC, как описано в rfc 7366. Один и тот же ключ используется для шифрования и расшифровки данных.

Сведения об алгоритме шифрования:

- Алгоритм шифрования: расширенное шифрование Standard симметричный ключ
- Режим шифра: цепочка блоков шифров
- Длина ключа: 256 бит
- Срок действия ключа: 12 месяцев
- Алгоритм проверки подлинности: HMACSHA256

Обновление учетных данных

Учетные данные часто меняются и нуждаются в обновлении. Windows 365 не обнаруживает изменения учетных данных учетной записи пользователя локальная служба Active Directory, связанной с ANC. Вместо этого Windows 365 зависит от клиентов, чтобы вручную обновить ANC с обновленными учетными данными.

При изменении учетных данных домена учетной записи пользователя, связанной с ANC, администратор Windows 365 должен вручную обновить новые учетные данные. Затем новые учетные данные автоматически повторно шифруются и обновляются в службе Windows 365.

> **Примечание**
>
> Если учетные данные домена изменены в среде локальная служба Active Directory, но вы не обновляете ANC вручную, Windows 365 по-прежнему будет использовать старые учетные данные для **проверок работоспособности** ANC. Таким образом, эти проверки работоспособности завершатся ошибкой, так как учетные данные в записи больше не действительны. Чтобы убедиться, что такие сбои не происходят, немедленно **обновите конфигурацию сетевого подключения Azure** новыми учетными данными.

Удаление учетных данных

После удаления ANC все данные, связанные с ANC, немедленно и безвозвратно удаляются из службы Windows 365.

Если учетная запись клиента деактивирована без удаления ANC, учетные данные хранятся в течение 29 дней. Если клиент повторно активируется в течение 29 дней, учетные данные ANC и домена восстанавливаются. Если клиент не активируется повторно в течение 29 дней, все АНК и связанные с ними сведения, включая учетные данные, окончательно удаляются.

Дальнейшие действия

Создайте сетевое подключение Azure.

Конфиденциальность, данные клиента и контент клиента в Windows 365

Статья • 31.01.2025

Windows 365 — это облачная служба, которая позволяет создавать и подготавливать к работе Облачные компьютеры для пользователей, а также управлять ими. Вы управляете облачными компьютерами с остальными устройствами с помощью Microsoft Intune (Windows 365 Корпоративная) или самообслуживания (Windows 365 для бизнеса). В этой документации содержатся сведения о платформе данных и соблюдении конфиденциальности для Windows 365. Если не указано иное, термин WIndows 365 в этом документе относится как к Windows 365 Корпоративная, так и к Windows 365 для бизнеса. Если приведенные ниже сведения различаются, каждый продукт будет называться отдельно.

Источники данных и назначение Windows 365

Windows 365 предоставляет свои услуги клиентам, собирая и используя данные из перечисленных ниже источников. Эти источники предоставляют исчерпывающее представление об устройствах, которыми управляет Windows 365.

- Microsoft Windows Enterprise — для управления процессом настройки устройства, управления подключениями к другим службам и оперативной поддержки для ИТ-специалистов.
- Microsoft Intune семейство продуктов — для управления устройствами и приложениями, защиты данных и конфигураций устройств.
- Аналитика конечных точек — часть семейства продуктов Microsoft Intune, специально для аналитических сведений об использовании устройств и приложений.
- Приложения Microsoft 365 для предприятий — для управления Приложениями Microsoft 365.

Для защиты и обслуживания зарегистрированных устройств служба Windows 365 обрабатывает и копирует данные из веб-служб и конвейеров данных, настроенных клиентом, в Windows 365. После интеграции данных из этих служб в Windows 365 к данным также применяются Условия продукта и Заявление о конфиденциальности корпорации Майкрософт, применимые к Windows 365.

Windows 365 обеспечивает надлежащие конфиденциальность, безопасность и устойчивость данных. Windows 365 использует дополнительные внутренние меры безопасности и конфиденциальности для обеспечения надлежащей обработки личных данных.

Хранилище данных Windows 365

В зависимости от региона и предпочтений клиента Windows 365 хранит контент клиента в регионах Azure в Северной Америке, Европе или Азиатско-Тихоокеанском регионе. Виртуальный диск облачного компьютера, содержимое клиента, данные и хранилище, связанные с облачным компьютером, находятся в регионе Azure, в который подготовлен облачный компьютер. Для Windows 365 Корпоративная регион определяется в параметрах размещенной сети Майкрософт или сетевого подключения Azure (ANC) в политике подготовки облачного компьютера. Windows 365 для бизнеса хранит данные клиента в регионе Azure самого Облачного компьютера.

Для управления облачным компьютером определенные данные, связанные с облачным компьютером (например, имя компьютера, диагностические данные и данные, созданные службой), хранятся в центрах обработки данных Azure в Северная Америка, Европе или Азиатско-Тихоокеанском регионе, как определено расположением клиента. Это хранилище сопоставляется на основе страны или региона клиента Microsoft Online с ближайшим регионом Azure.

Другие данные клиента, диагностические данные или данные, созданные службой, могут собираться Виртуальным рабочим столом Azure или Intune, так как Windows 365 зависит от этих служб.

Дополнительные сведения о расположении данных см. в:

- Microsoft Entra ID . Где находятся ваши данные?
- Расположения данных для Виртуального рабочего стола Azure
- Поддерживаемые регионы Windows 365
- Где хранятся данные клиентов Microsoft 365

Как долго хранятся данные клиента и контент клиента?

Windows 365 рассматривает диск Облачного компьютера и данные на самой ВМ как контент клиента.

При удалении пользователя из Windows 365 служба хранит персональные данные без оповещений в течение не более 90 дней. В пассивных сценариях данные хранятся не менее 90 дней и не более 180 дней. Чтобы получить доступ к данным клиента, сохраненным в пассивном сценарии, обратитесь в службу поддержки. В целях безопасности данные оповещений, собранные Microsoft Defender для конечной точки, хранятся в течение 180 дней, если клиент использует Microsoft Defender для конечной точки.

Дополнительные сведения о хранении данных см. в статье Хранение, удаление и уничтожение данных в Microsoft 365.

Windows 365 по умолчанию используется стандартная практика Microsoft Intune по аудиту, экспорту или удалению персональных данных.

Персональные данные обрабатываются в рамках ограничений в соответствии с требованиями для службы Intune согласно техническим мерам безопасности, гарантированным Условиями использования Веб-служб корпорации Майкрософт.

Дополнительные сведения об отдельных политиках хранения и хранения данных для всех зависимых служб см. в:

- Где хранятся данные клиентов Microsoft 365
- Сбор данных в Intune
- Хранение и обработка данных в Intune

Изоляция и управление доступом

Каждая подписка на внутренние данные клиента в Windows 365 Корпоративная содержит метаданные Виртуального рабочего стола Azure (AVD), Облачные компьютеры и хранилище из нескольких клиентов. Каждая виртуальная машина подключена к одной виртуальной сетевой интерфейсной карте (NIC). Во время подготовки Облачного компьютера к работе эта сетевая карта подключена к одной виртуальной сети в подписке Azure клиента. Виртуальная сеть определяется администратором клиента. Каждый Облачный компьютер назначается одному пользователю с помощью уровня посредника подключения AVD. Список управления доступом (ACL) для уровня AVD проверяется Microsoft Entra ID на уровне клиента и пользователя. Сетевой доступ в Windows 365 к Облачному компьютеру и с него находится под контролем и осуществляется по усмотрению каждого администратора клиента. Таким образом, пользователи клиента Б не смогут получить доступ к Облачным компьютерам в клиенте А, если только

администратор клиента A не выберет возможность подключения за пределами Windows 365 и AVD на сетевом уровне в собственной подписке.

Для Windows 365 для бизнеса в клиенте создаются одна или несколько выделенных виртуальных сетей. Служба автоматически создает дополнительные сети по мере необходимости и не гарантирует, что все компьютеры Windows 365 Business Cloud в одном клиенте будут иметь сетевое подключение друг к другу.

Вся описанная выше изоляция выполняется для каждого пользователя для каждого Облачного компьютера, поскольку Windows 365 не поддерживает многопользовательские сценарии.

Полное описание архитектуры Windows 365 см. в разделе Архитектура Windows 365. Дополнительные сведения об изоляции в Microsoft 365 см. в разделе Изоляция и управление доступом в Microsoft 365. Дополнительные данные об управлении доступом в Microsoft 365 можно найти в разделе Управление удостоверениями и доступом — контроль качества обслуживания в Майкрософт.

Соответствие требованиям и юридическая информация

Отчеты аудита для Windows 365 будут доступны для загрузки на портале Microsoft Service Trust Portal после их завершения. Портал Microsoft Service Trust Portal служит центральным репозиторием для корпоративных веб-служб Майкрософт.

Уведомление о конфиденциальности корпорации Майкрософт для пользователей продуктов, предоставляемых клиентами организации. В Заявлении о конфиденциальности корпорации Майкрософт пользователям сообщается, что при входе в продукты Майкрософт с использованием рабочей учетной записи а) их организация может контролировать и администрировать их учетную запись (в том числе управлять настройками конфиденциальности), а также получать доступ к данным пользователей и обрабатывать их, и б) корпорация Майкрософт может собирать и обрабатывать данные для предоставления услуг организации и пользователям.

Дальнейшие действия

Планирование развертывания Windows 365

Сведения о шифровании данных в Windows 365

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Руководство по планированию для Windows 365

Статья • 31.01.2025

Успешное развертывание Windows 365 начинается с тщательного планирования. В этом руководстве по планированию рассматривается общий порядок развертывания.

Определение целей

Организации используют Windows 365, чтобы предоставить пользователям среду рабочего стола Windows. Выясните, какова цель и чего необходимо достичь.

В этом разделе мы обсудим распространенные цели при использовании Windows 365. Рассмотрите цели для каждого из различных вариантов использования Windows 365.

Цель: доступ к корпоративным приложениям и данным

Определите элементы, доступ к которым необходим пользователям на Облачном компьютере. Если пользователи будут использовать Windows 365 в качестве замены рабочего стола, рассмотрите такие приложения, как Office 365, или средства совместной работы, такие как Teams. Если пользователи используют Windows 365 для доступа к специализированному программному обеспечению, следует рассмотреть возможность установки всех приложений для соответствующей сферы деятельности.

Задача: создать список приложений, которые необходимо использовать. Этот список необходимо адаптировать в соответствии с конкретным вариантом использования.

Цель: географические регионы

Определите, где физически находятся пользователи. Windows 365 может предоставить облачные компьютеры в нескольких расположениях Azure по всему миру. Предоставьте облачные компьютеры в расположении с наименьшей задержкой при передаче данных в физическое расположение ваших

пользователей. Дополнительные сведения см. в статье Поддерживаемые регионы Azure для подготовки облачных компьютеров.

> **Совет**
>
> Если в настоящее время используется регион Azure, которого нет в списке поддерживаемых регионов Azure для Windows 365, используйте пиринг между виртуальными сетями, чтобы подключить виртуальную сеть в поддерживаемом регионе Azure к сетям и ресурсам в регионах Azure, используемых в вашей подписке. Дополнительные сведения см. в статье **Звездообразная топология сети в Azure**. Вы также можете создать **звездообразную топологию сети с помощью Виртуальной глобальной сети Azure**.

Задача: составить карту расположения пользователей. Перечислите группы и регионы Azure, необходимые для всех вариантов использования.

Цель: управление облачными компьютерами

Вы будете управлять устройствами облачных компьютеров с помощью Центра администрирования Microsoft Intune. Регистрация облачных компьютеров автоматически выполняется во время подготовки. Решите, кто будет управлять облачными компьютерами и какие разрешения необходимо предоставить различным группам управления.

Задача: определить группы управления, которые будут выполнять настройку службы облачных компьютеров, управление облачным компьютером и распространение программного обеспечения на устройства. Определите, какие разрешения Microsoft Intune и Windows 365 будут назначены разным группам для управления устройствами.

Инвентаризация среды

Все пользователи подключаются к облачному компьютеру через клиент Windows App или поддерживаемый браузер. Это соединение позволяет пользователям получать доступ к облачному компьютеру с широкого спектра устройств.

Задача: для каждого варианта использования определить, как конечные пользователи будут подключаться к своим облачным компьютерам. Определите, какие платформы они будут использовать для подключения. Будут ли они использовать браузер или клиент Windows App для подключения?

Сведения о требованиях к подключению и поддерживаемых конфигурациях см. в разделе Требования.

Определение лицензирования

Спецификации каждого устройства облачного компьютера определяются конкретной лицензией.

Задача: рассмотреть все варианты использования и сопоставить рабочую нагрузку с конкретной необходимой лицензией. Следует протестировать все рабочие нагрузки для каждого варианта использования.

Рассмотрение управления конечными точками и инфраструктуры

У многих организаций уже имеется план управления устройствами. При наличии плана следует решить, добавлять ли в него облачные компьютеры или разрабатывать новый процесс.

Рассмотрите все политики и требования сети. У многих организаций имеются политики маршрутизации и отслеживания трафика. Дополнительные сведения о требованиях Windows 365 см. в разделе Требования.

Задача: определить, как будет осуществляться управлением всеми облачными компьютерами. Определите, как политики будут применяться (GPO или Intune), приложения — распространяться, а устройства — поддерживаться в актуальном состоянии. Проанализируйте топологию сети и определите, как сеть будет выполнять маршрутизацию на облачные компьютеры и в обратном направлении.

Создание плана развертывания

Следующий шаг — определение способа и времени получения пользователями облачных компьютеров.

- **Определите этапы развертывания**. Создайте несколько этапов развертывания на основе своей среды. Начните с пилотных и (или) тестовых групп. Ранние этапы должны включать пользователей, которые согласны с изменениями, хотят предоставлять обратную связь и знают, что являются первыми пользователями. Используйте эту обратную связь для улучшения процесса развертывания. Последующие этапы должны включать VIP и руководителей. Это позволяет совершенствовать развертывание по мере прохождения

этапов. Перед завершением этапа определите успешность его выполнения на основе целей. Изменяйте конфигурацию, документацию или уведомления, руководствуясь обратной связью.

- **Определите цели и метрики успеха**. Убедитесь, что поставленные цели согласуются с методологией SMART, то есть являются конкретными, измеримыми, достижимыми, реалистичными и своевременными. Запланируйте оценку показателей для целей на каждом этапе, чтобы отслеживать эффективность реализации проекта. Некоторые возможные метрики успеха: удовлетворенность пользователей по результатам опроса не ниже 80 %, использование на подготовленных устройствах составляет от 85 %.
- **Информирование о целях**. Включите цели во все информационные и учебные мероприятия, чтобы помочь пользователям понять, почему организация выбрала именно Windows 365.

Задача: создать план развертывания. Включите все варианты использования, поэтапные развертывания и измеримые критерии успеха.

Информирование об изменениях

Управление изменениями основано на четком и понятном информировании о предстоящих изменениях. Лучший способ обеспечить бесперебойное развертывание — следить за тем, чтобы пользователи были в курсе всех изменений и прерываний в работе.

Задача: план распространения должен включать важную информацию, способы уведомления пользователей и время информирования. План должен включать время и способы информирования, а также сведения, которые следует сообщать.

- Определите, какие сведения следует передавать. Передавать сведения следует несколько раз пользователям на различных этапах.
  - **Начальный этап**: общая рассылка, знакомящая пользователей с Windows 365. В рамках этой рассылки необходимо ответить на следующие ключевые вопросы.
    - Что такое облачный компьютер?
    - Почему организация использует облачный компьютер? Расскажите о преимуществах для пользователей и организации.
    - Предоставьте высокоуровневый план развертывания.
  - **Пилотный этап**: включите дополнительные сведения для пользователей пилотного этапа. Проследите за тем, чтобы они понимали, что принимают участие в пилотном этапе и должны предоставить обратную связь.

- **Этап подключения**: рассылка для конкретных пользователей и групп, которые должны приступить к использованию облачного компьютера. Это сообщение должно информировать конечных пользователей о том, что облачный компьютер готов к работе. Включите инструкции по подключению к облачному компьютеру с любой платформы, которую может использовать пользователь. На случай, если у пользователей возникнут проблемы, следует также предоставить контакты службы технической поддержки.
- Выберите способ передачи сведений об облачном компьютере целевым группам и пользователям. Вот некоторые примеры.
  - Общекорпоративные собрания, Microsoft Teams, корпоративная информационная рассылка и электронная почта.
  - Для информирования о подключении рассмотрите возможность отправки информации пользователям по электронной почте.

Служба технической поддержки и конечные пользователи

В планирование и реализацию мероприятий на ранних этапах развертывания Windows 365 следует включить ИТ-поддержку. Это позволит сотрудникам службы поддержки получить знания и опыт для более эффективного определения и устранения проблем. Это также подготовит их к поддержке развертываний в рабочей среде. Опытные специалисты службы технической поддержки и группы поддержки также помогают пользователям адаптироваться к новым изменениям.

Задача: обучение специалистов службы поддержки. Проверяйте принятие решений пользователями по метрикам успеха, установленным в плане развертывания.

- Определите, кто будет поддерживать пользователей. Во многих организациях предусмотрено несколько уровней поддержки. Определите, как на каждом уровне можно обеспечить поддержку подключения пользователей и использования ими Windows 365.
- Создайте рабочий процесс службы технической поддержки. Постоянно сообщайте о поддержке при устранении проблем и тенденциях, а также о других важных сведениях для всех уровней в группе поддержки.
- Обучите группы поддержки и специалистов службы технической поддержки. Рассмотрите возможность включения в обучение всех сценариев, в которых будет использоваться Windows 365. Рассмотрите также возможность обучения для всех поддерживаемых платформ Windows 365.

Обучение пользователей

Для обучения пользователей создайте следующие руководства:

- подключение к облачному компьютеру;
- использование облачного компьютера в конкретном сценарии;
- обращение за справкой и поддержкой в случае необходимости.

Дальнейшие действия

Сведения о требованиях для Windows 365

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Управление изменениями для Windows 365

03.10.2025

Обзор

Windows 365, например Microsoft 365, предоставляет современную облачную среду, которая позволяет пользователям получать доступ к виртуальным рабочим столам и приложениям для повышения производительности без затрат на локальную инфраструктуру. В традиционных развертываниях ИТ-администраторы управляют обновлениями, исправлениями для системы безопасности и внедрением функций. Благодаря Windows 365 как решение SaaS (программное обеспечение как услуга) корпорация Майкрософт автоматизирует обновления инфраструктуры, сокращая усилия вручную и переключая внимание на планирование и управление.

Однако быстрый и непрерывный характер обновлений SaaS может привести к новым проблемам, особенно для организаций со строгими нормативными требованиями или критически важных рабочих нагрузок. Это руководство поможет диспетчерам доставки ИТ-служб интегрировать Windows 365 в свои платформы управления изменениями, используя проверенные методики Microsoft 365 для простого перехода на облачные обновления.

1. Создание предварительной среды или пилотной группы пользователей

В регулируемых или сложных корпоративных средах оценка новых функций до широкого развертывания имеет важное значение. Хотя некоторые организации могут рассмотреть отдельный тестовый клиент для максимального контроля, такой подход может привести к сложности лицензирования и управления и не рекомендуется, если это не требуется для конкретных сценариев. Вместо этого большинство организаций назначают пилотную группу в своем рабочем клиенте для получения ранних выпусков. В эту группу обычно входят ИТ-сотрудники, технические специалисты или руководители отделов.

Ранний доступ к предварительным версиям функций позволяет вашей команде оценить влияние рабочих процессов и требования к соответствию. Сбор отзывов от различных заинтересованных лиц помогает выявить потенциальные проблемы до полного развертывания. При возникновении блокировщиков необходимо предоставить отзыв вашей команде по работе с учетными записями Майкрософт.

Структурированная предварительная среда сопоставляет модель непрерывного обновления Windows 365 с установленными подходами к управлению ИТ-службами, например библиотекой ИТ-инфраструктуры (ITIL), балансировкой гибкости и контролем.

> ⓘ **Примечание**
>
> Подход к предварительным версиям может развиваться. Ознакомьтесь с последними рекомендациями Майкрософт по управлению предварительными версиями на уровне клиента и на стороне клиента.

2. Использование записей "Планирование изменений"

Корпорация Майкрософт сообщает о предстоящих изменениях через Центр сообщений. Для Windows 365 целевые обновления отображаются в колонке Центр сообщений Центра администрирования Microsoft Intune. Администраторы, управляющие несколькими рабочими нагрузками, могут просматривать агрегированные сообщения на портале администрирования Microsoft 365, фильтруя по службам и категориям.

Назначьте соответствующие роли (глобальный администратор, читатель центра сообщений, администратор службы), чтобы участники команды, ответственные за управление изменениями, получали все соответствующие уведомления. Инструкции по настройке уведомлений см. в официальной документации майкрософт.

Интегрируйте уведомления "Планирование изменений" с такими инструментами, как Microsoft Планировщик или платформой управления ИТ-службами (например, ServiceNow), чтобы отслеживать задачи, назначать обязанности и планировать взаимодействие. Это гарантирует, что обновления не будут пропущены или спешить, поддерживая соответствие требованиям и эффективное взаимодействие с пользователями.

3. Регулярно проверяйте "Новые возможности" и "В разработке" для Windows 365

Администраторы должны регулярно проверка страницу "Новые возможности" и "В разработке" для Windows 365. Эти статьи обновляются ежемесячно и могут включать еженедельные изменения из-за зависимостей от других служб Microsoft 365. Частые проверки помогают командам подготовиться к новым функциям и избежать инцидентов в службе поддержки.

Перекрестные ссылки на публикации "План изменений" с записями "Новые возможности" для согласования обучения и взаимодействия с предстоящими выпусками.

Ведение журнала изменений для аудита и проверок системы управления. Такой упреждающий подход обеспечивает готовность и соответствие требованиям.

> **Совет**
>
> Рассмотрите возможность подписки на уведомления или использование автоматизации, чтобы оставаться в курсе, так как ручная проверка может быть обременительной.

4. Использование существующих знаний об управлении изменениями в Microsoft 365

Многие организации имеют надежные платформы управления изменениями для рабочих нагрузок Microsoft 365. Примените эти методики для Windows 365, выполнив следующие действия:

- Консультирование внутренних специалистов или команд, управляющих Microsoft 365, для получения аналитических сведений о пилотных группах, сборе отзывов и стратегиях коммуникации.
- Включение Windows 365 в обзоры Консультативного совета по изменениям (CAB) для прогнозирования влияния между службами, например проверки подлинности или сетевых изменений.
- Расширение политик соответствия требованиям и защиты данных с Microsoft 365 до Windows 365 с помощью таких средств, как Центр соответствия требованиям & безопасности.
- Взаимодействие с командами сети и Azure для учета изменений, влияющих на Windows 365, таких как настройка сети Azure или обновления брандмауэра.

Такой целостный подход обеспечивает комплексный контроль и сводит к минимуму риски.

Заключение

Windows 365 сочетает инновации SaaS с привычными корпоративными процессами. Для перехода от локального управления к гибкости облака требуется смена языка и региональных параметров и практики. Следуя этим рекомендациям (создавая предварительные версии сред, используя публикации "Планирование изменений", просматривая "Новые возможности" и применяя существующие знания, вы можете

интегрировать Windows 365 в платформы управления, обеспечивая структурированное, гибкое и непрерывное внедрение служб.

Основные выводы:

· Поддерживайте предварительную рабочую среду или пилотную группу для раннего тестирования компонентов.

· Используйте Центр сообщений для отслеживания и интеграции уведомлений об изменениях в рабочие процессы.

· Регулярно просматривайте новые возможности, чтобы следить за обновлениями.

· Сотрудничайте с коллегами, управляющими другими рабочими нагрузками Microsoft 365, чтобы расширить свой подход.

Эти методики позволяют вашей организации извлечь выгоду из скорости и инноваций Windows 365, сохраняя при этом необходимые нормативные и операционные средства контроля.

Windows 365 варианты развертывания в сети

Статья • 31.01.2025

У вас есть два варианта сетевого развертывания службы Windows 365:

- Использование сети, размещенной в Майкрософт
  - Рекомендуемый параметр.
  - Идеально подходит для Windows 365 функций SaaS (программное обеспечение как услуга) простоты, надежности и масштабируемости.
  - Поддерживает модель удостоверений Microsoft Entra присоединения.
  - Не требуется подписка Azure или опыт.
- Использование Connections сети Azure (ANC)
  - Поддерживает модели удостоверений Microsoft Entra присоединения и Microsoft Entra гибридных подключений.

Сеть, размещенная в Майкрософт

Это простой, надежный и масштабируемый вариант, предоставляющий возможность подключения к облачному компьютеру, где корпорация Майкрософт предоставляет службу в рамках настоящего подхода SaaS. При использовании этого параметра корпорация Майкрософт:

- Настраивает и полностью управляет инфраструктурой и связанными службами, необходимыми для предоставления пользователям функциональных облачных компьютеров.
- Управляет сетью, занимаемой облачными компьютерами.
- Предоставляет модель, согласованную с платформой "Никому не доверяй" среды конечных пользователей (EUC). Дополнительные сведения см. в статье Дополнительные сведения об облачных конечных точках.

Единственной ответственностью клиента является настройка облачных компьютеров и управление ими.

Корпорация Майкрософт рекомендует клиентам использовать этот параметр для развертывания Windows 365.

Вам не нужно создавать собственные подписки Azure, планировать, проектировать, развертывать инфраструктуру или управлять ею. Клиенты могут посвятить свою команду EUC сосредоточиться на управлении конфигурациями облачных

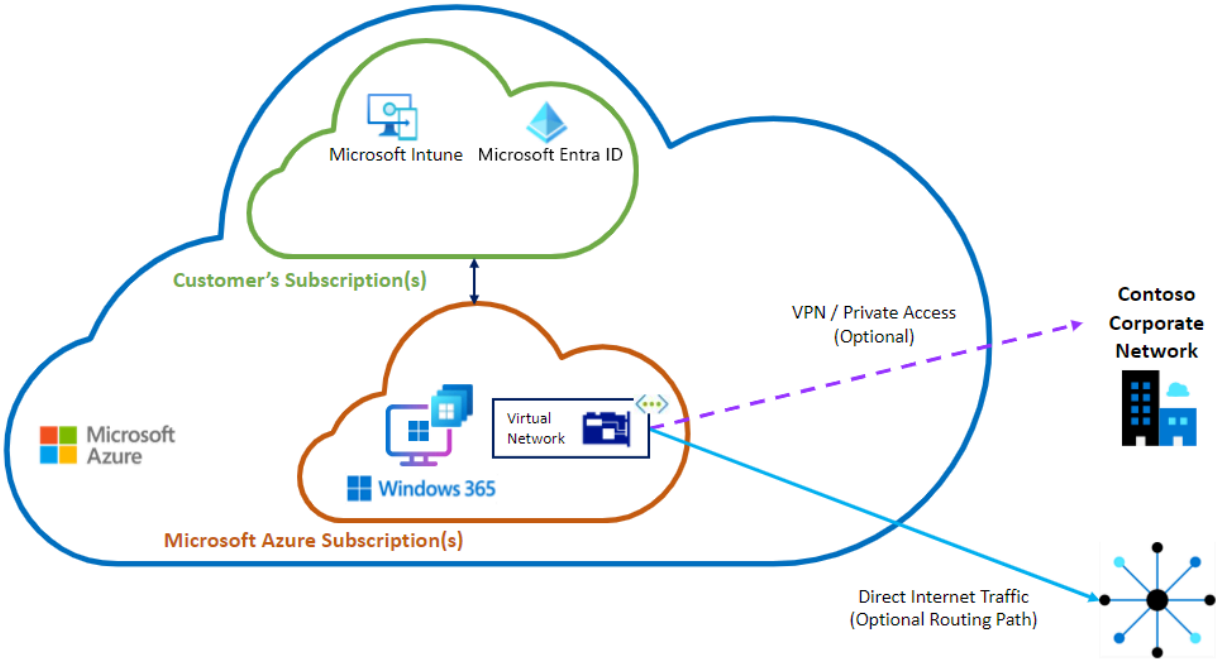
компьютеров и безопасностью из одного консоль управления, предоставляемого Intune.

Этот вариант аналогиен предоставлению сотруднику ноутбука для использования дома. Вы, как организация, не управляете сетью, в которую находится устройство. Вы полностью контролируете настройку, защиту и подключение устройства с Windows к локальной сети. Благодаря Windows 365 это управление возможно благодаря комплексным элементам управления безопасностью "Никому не доверяй", согласованным с адаптивными элементами управления безопасностью и конфигурациями.

Например, пользователи могут пройти проверку подлинности с помощью адаптивных элементов управления Microsoft Entra условного доступа. Корпоративное подключение можно обеспечить с помощью VPN. Для обеспечения безопасности в Интернете можно использовать облачный защищенный веб-шлюз (SWG). Преимущество заключается в том, что устройства можно развертывать в большом масштабе в течение короткого периода времени, когда это необходимо для отказоустойчивой сети с высокой пропускной способностью.

Схема: параметр сети, размещенный в Майкрософт, — только Microsoft Entra присоединение

На этой схеме показана сеть, размещенная корпорацией Майкрософт, с облачным компьютером и виртуальной сетью, карта в рамках подписки, управляемой корпорацией Майкрософт.



Преимущества параметра сети, размещенной в Майкрософт

- Подписка Azure не требуется. Корпорация Майкрософт предоставляет инфраструктуру, необходимую для работы облачного компьютера, и полностью управляет ею. Все, что вам нужно, — это необходимые лицензии.
- Нет дополнительных затрат на сетевую инфраструктуру. Затраты Azure на управление собственной виртуальной сетью (VNet) и виртуальными устройствами не применяются. Корпорация Майкрософт отвечает за сетевую инфраструктуру.
- Не требуется опыт работы или управление сетями Azure. Виртуальная сеть полностью управляется корпорацией Майкрософт.
- Низкая сложность и быстрое развертывание. Развертывание выполняется с низкой сложностью из-за минимальных зависимостей от элементов на стороне клиента.
- Выравнивание "Никому не доверяй". Модель "Никому не доверяй" для пользователя, конечной точки, рабочей нагрузки и сигналов данных используется для проверки, а не для применения доверия к сетевому расположению.
- Упрощение устранения неполадок и операций. Проще устранять и устранять проблемы с сетью, а также внедрять современное управление устройствами на основе политик Intune, элементов управления безопасностью и встроенных возможностей создания отчетов.

Рекомендации

Прежде чем использовать параметр сети, размещенной в Майкрософт, ознакомьтесь со следующими рекомендациями:

- Этот параметр несовместим с моделью гибридного соединения Microsoft Entra. Это развертывание только в облаке без подключения к локальная служба Active Directory Доменные службы инфраструктуре. Если у вас есть групповая политика политики управления на основе объектов, которые нельзя преобразовать в Intune, то этот вариант не подходит для вас.
- Нет контроля над виртуальной сетью. Виртуальный сетевой адаптер управляется корпорацией Майкрософт. Таким образом, все элементы управления сетью должны быть реализованы на самом облачном компьютере, аналогично физическим устройствам в сценарии работы из дома.
- Нет прямого доступа к локальным ресурсам. Для доступа к этим ресурсам требуется VPN-подключение или частное решение. При использовании VPN с

облачным компьютером используйте раздельное туннелирование , чтобы убедиться, что трафик RDP не направляется через VPN.
- Требуется собственная облачная модель управления, например Intune.
- Порт 25 заблокирован.
- Ping/ICMP заблокирован.
- Обмен данными между облачными компьютерами в локальной сети блокируется.
- Прямое входящее подключение к облачным компьютерам невозможно.
- Администраторы не могут управлять диапазонами IP-адресов и (или) адресным пространством, назначенным облачным компьютерам. Windows 365 автоматически обрабатывает IP-адреса.

Параметр "Сетевое подключение Azure"

При развертывании сетевого подключения Azure (ANC) вы полностью отвечаете за виртуальную сеть и ее конфигурацию. Если вы используете модель гибридного присоединения Microsoft Entra, необходимо использовать этот параметр развертывания. Этот параметр обеспечивает прямой доступ к локальным ресурсам Azure Directory и позволяет настроить цели сети и безопасности, например:

- Маршруты трафика.
- Порты и протоколы.
- Подключение active Directory DS и бизнес-приложений.
- Подключения шлюза с помощью VPN или ExpressRoute.
- Адресное пространство, используемое облачными компьютерами.
- Разрешения на обмен данными между облачными компьютерами.
- Прямые подключения по протоколу RDP к облачным компьютерам.

Вы выбираете виртуальную сеть из подписки Azure. Вы настроите политики подготовки, которые создают облачные компьютеры в виртуальной сети. Вы будете управлять подключением к облачному компьютеру, включая любые прямые исходящие данные из виртуальной сети и требуемый путь доступа к Интернету.

Сетевое подключение Azure поддерживает две модели развертывания удостоверений:

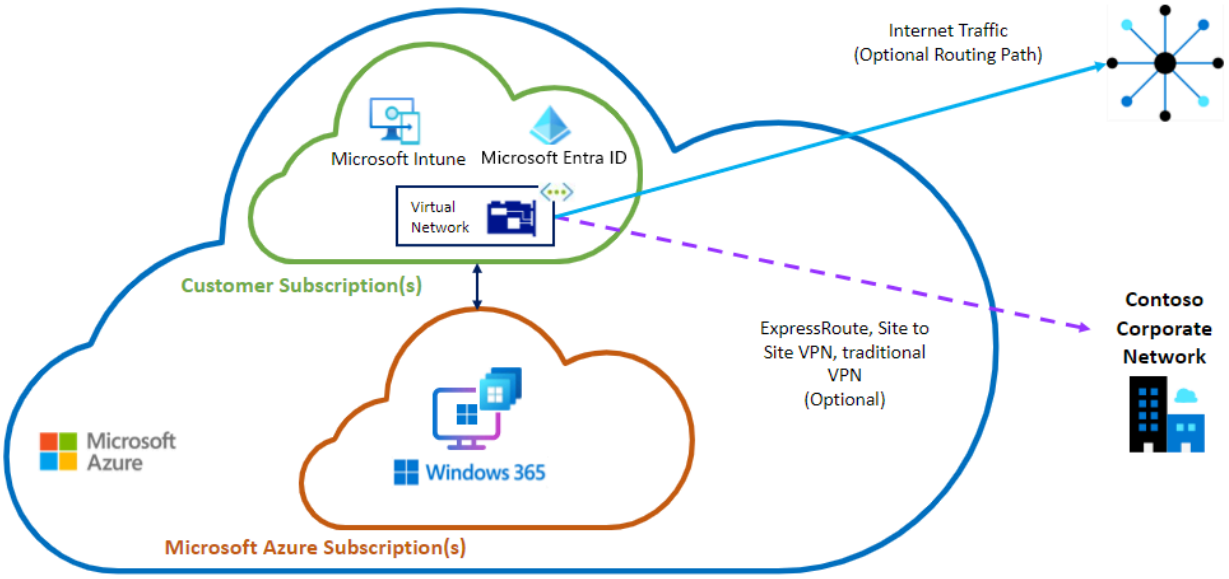
- Microsoft Entra присоединение
- Microsoft Entra гибридное соединение

Microsoft Entra присоединение

При использовании Microsoft Entra присоединения не требуется создавать подключение из виртуальной сети к локальной сети. Необходимо просто убедиться, что к требуемым конечным точкам имеется исходящее подключение к Интернету. Однако может потребоваться добавить локальное подключение для доступа к ресурсам, расположенным на локальных файловых серверах и приложениях. Вы можете создать подключение с помощью ExpressRoute или VPN типа "сеть — сеть", но эти параметры представляют дополнительные затраты и сложность.

Для простоты при использовании Microsoft Entra присоединения рекомендуется использовать ранее описанный параметр сети, размещенный в Майкрософт. В этом случае для доступа к корпоративным ресурсам можно использовать VPN-подключение или решение для частного доступа через Интернет.

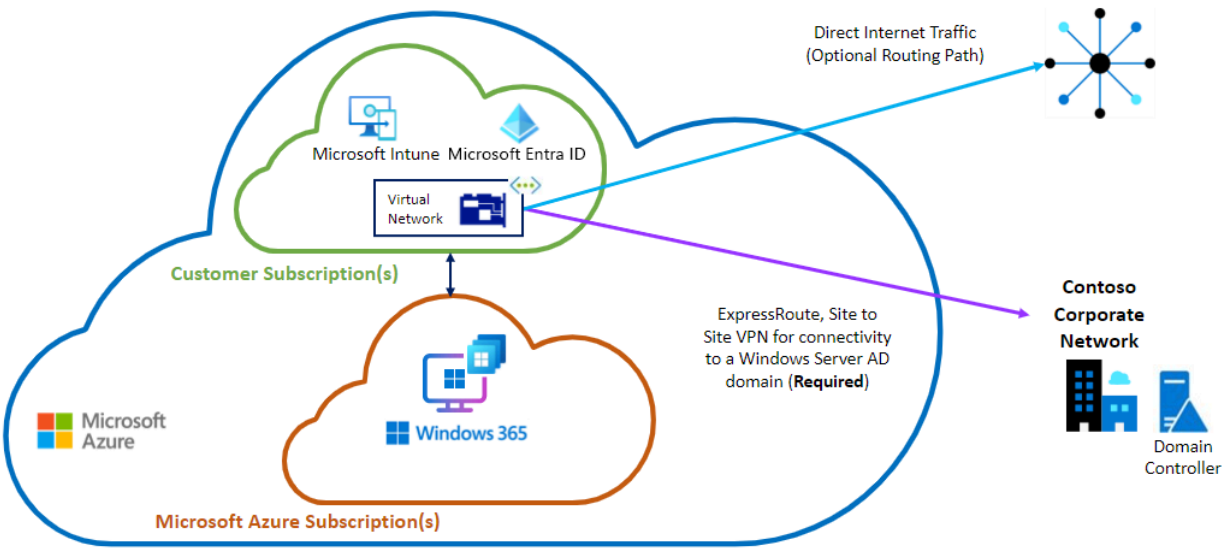
Схема: параметр ANC — Microsoft Entra соединение



Microsoft Entra гибридное соединение

При Microsoft Entra гибридного присоединения требуется подключение к локальной сети из виртуальной сети. Единственный способ связаться с инфраструктурой контроллера домена, расположенной в ней, — использовать параметр развертывания ANC. Это соединение является критически важным компонентом, поэтому следует проявлять осторожность для обеспечения надежности и избыточности.

Схема: параметр ANC — Microsoft Entra гибридное соединение



Преимущества параметра ANC

- Полный контроль над виртуальной сетью. Сетевой адаптер облачного компьютера находится в вашей собственной управляемой виртуальной сети.
- Прямая прямая видимость к локальной инфраструктуре. Виртуальную сеть можно настроить с vpn-подключением типа "сеть — сеть" или ExpressRoute обратно к локальной сети для прямого подключения к инфраструктуре каталога Azure или службам и приложениям, которые находятся в ней.
- Облачный компьютер работает так же, как в локальном расположении. Расширение корпоративной сети в виртуальную сеть означает, что облачный компьютер может работать так, как если бы он находится в пределах корпоративной сети.
- Простой пиринг с другими виртуальными сетями. Простое перекрестное подключение между виртуальной сетью облачного компьютера и другими виртуальными сетями в Azure. Это поддерживает прямое подключение к другим ресурсам, размещенным в Azure, которые используются организацией.

Рекомендации

Прежде чем использовать вариант развертывания ANC, ознакомьтесь со следующими рекомендациями.

- Требуется подписка Azure. Виртуальная сеть, используемая в этом сценарии, находится в вашей подписке Azure. Поэтому у вас должна быть подписка Azure и необходимые лицензии.
- Затраты на исходящий трафик. Так как виртуальная сеть связана с вашей учетной записью Azure, все затраты на исходящий трафик связаны с вашей

подпиской Azure.

- Дополнительные расходы на сетевую инфраструктуру. Затраты Azure на управление собственной виртуальной сетью применяются к подписке, связанной с этой виртуальной сетью.
- Требуется опыт работы с сетями Azure или управление. Необходимо предоставить опыт и управление для обслуживания виртуальной сети.
- Более высокая сложность. Необходимо управлять сетью и поддерживать ее, что является более сложной задачей, чем использование сети, размещенной в Майкрософт.
- Более длительное развертывание. Развертывание обычно дольше, чем при использовании параметра сети, размещенной в Майкрософт. Это дополнительное время вызвано большим количеством клиентских элементов, которые необходимо настроить в первую очередь.
- Более высокий риск. Развертывание ANC является более сложным, чем развертывание сети, размещенной в Майкрософт. Такая сложность повышает риск проблем с подключением.

Варианты одновременного использования

Параметры сети, размещенной в Майкрософт, и параметры ANC можно использовать одновременно. Например, можно использовать параметр ANC для подмножества развертываний с уникальными устаревшими требованиями. Для остальной части развертывания без этих требований можно использовать вариант сети, размещенной в Майкрософт.

Дальнейшие действия

Дополнительные сведения о процессе развертывания.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Оптимальная подготовка облачных компьютеров: рекомендации, основанные на расположении пользователей, расположении данных приложения и оптимизации сети

Важность расположения: данные пользователя, облачного компьютера и приложения

Расположение облачного компьютера может играть важную роль в производительности и взаимодействии с конечными пользователями облачных компьютеров. Когда облачный компьютер подготовлен вдали от физического расположения пользователя, это может привести к увеличению задержки, что может негативно повлиять на взаимодействие с облачным компьютером и производительность пользователей. Например, пользователи, удаленно обращающиеся к облачным компьютерам на разных континентах, могут испытывать более высокую задержку по сравнению с пользователями, расположенными ближе к региону, где подготовлен облачный компьютер.

Аналогичным образом важно понимать расположение данных приложения, особенно важное для приложений, чувствительных к задержкам, так как во время сеанса пользователи, скорее всего, получают к нему доступ. Данные приложения могут находиться в том же регионе, что и облачный компьютер, в другом регионе Azure или даже в локальной среде. В идеале пользователь, облачный компьютер и данные приложений находятся географически близко, например пользователь находится в Нью-йорке с облачным компьютером и данными Microsoft 365 в Azure восточной части США (Вирджиния), однако это не всегда так.

Если эти элементы не находятся совместно, администраторы должны тщательно выбрать регион подготовки облачных компьютеров, чтобы обеспечить бесперебойную работу. В Windows 365 Корпоративная регион облачного компьютера определяется в политике подготовки с помощью параметров размещенной сети Майкрософт (MHN) или Azure сетевого подключения (ANC). Если позже потребуются изменения, администраторы могут обновить политику подготовки, чтобы переместить облачные компьютеры в новый регион. Хотя это не активирует повторную подготовку, она удаляет точки восстановления из предыдущего региона, поэтому важное время и планирование.

Понимание того, как пользователи подключаются к Windows 365 облачным компьютерам, также является важной частью для оптимизации

производительности. Когда пользователь инициирует сеанс, трафик сначала направляется к ближайшему шлюзу Azure(определяется физическим расположением пользователя), а затем продолжается через магистральную Azure Майкрософт в регион, где подготовлен облачный компьютер.

Факторы, которые следует учитывать:

- **Близкое расположение пользователя к расположению облачного компьютера:** В general____ чем ближе пользователь к расположению облачного компьютера, тем быстрее время отклика ввода с клавиатуры и мыши и обновлений экрана.

- **Близкое расположение данных приложения к расположению облачного компьютера:** При определении расположения облачного компьютера учитывайте регион Azure или локальное расположение данных приложения. Для приложений, чувствительных к задержке, перемещение облачного компьютера ближе к данным приложения может повысить производительность.

- **Региональные правила и суверенитет данных:** Соблюдение региональных законов о независимости данных и конфиденциальности может ограничить возможности подготовки облачных компьютеров.

- **Пользовательский протокол datagram (UDP), предпочтительный по сравнению с протоколом TCP для оптимального взаимодействия с конечным пользователем:** RDP Shortpath использует транспорт на основе UDP через протокол URCP . URCP оптимизирует протокол UDP путем адаптации к условиям сети и реализации управления скоростью, что приводит к лучшей пропускной способности и большей задержке по сравнению с подключениями TCP/Websocket.

Хотя задержка между пользователями и Виртуальные машины (виртуальными машинами) ранее была ключевой проблемой, достижения в протоколах и использовании магистральной сети Майкрософт значительно снизили ее влияние. В результате размещение облачных компьютеров рядом с данными приложения теперь часто является приемлемым и даже предпочтительнее.

Надежное сетевое подключение для производительности облачного компьютера

Оптимальное сетевое подключение имеет важное значение для обеспечения беспроблемного взаимодействия с облачным компьютером. Стабильное и высокопроизводительное подключение к Интернету сводит к минимуму перебои,

вызванные сетевыми колебаниями, и обеспечивает беспроблемное взаимодействие с пользователем.

Так как пользователи могут получать доступ к своим облачным компьютерам с различных устройств и расположений, производительность подключения зависит от таких факторов, как сетевая маршрутизация и задержка. Чтобы повысить производительность, администраторы должны в идеале согласовать регион сети с регионом, в котором подготовлены Windows 365 облачные компьютеры. Кроме того, выбор протокола транспорта играет важную роль: Windows 365 использует протокол удаленного рабочего стола (RDP), который может работать как по протоколу TCP, так и по протоколу UDP. Хотя TCP обеспечивает надежную доставку, он обеспечивает более высокую задержку из-за строгих механизмов подтверждения и повторной передачи. UDP, с другой стороны, не связана с подключением и оптимизирована для трафика в режиме реального времени, что позволяет RDP обеспечить более плавный и быстрый интерфейс за счет уменьшения задержек в пути и лучшей обработки потери пакетов. По этой причине UDP предпочтительнее TCP для сеансов облачных компьютеров, особенно в тех случаях, когда низкая задержка и согласованная производительность имеют решающее значение.

Еще один важный аспект, который следует учитывать, заключается в том, что при использовании Azure сетевых Connections (ANCs) администраторы берут на себя дополнительные обязанности, включая разрешение системы доменных имен (DNS), планирование подсетей и IP-адресов, а также поддержание низкой задержки подключения к Azure регионам. Azure постоянно отслеживает задержку сети с помощью внутренних средств и публикует метрики производительности для поддержки оптимизации. Дополнительные сведения о Azure статистике задержки кругового пути сети см. в разделе Azure статистика задержки кругового пути сети | Microsoft Learn.

Ключевые сетевые факторы, которые следует учитывать:

- **Пропускная способность:** Обеспечение достаточной пропускной способности имеет важное значение для обработки передачи данных и поддержания высококачественных видеоконференций и производительности приложений.
- **Скрытое состояние:** Снижение задержки важно для облачных компьютеров, особенно в более сложных сценариях, таких как редактирование видео или разработка видеоигр.
- **Сетевая маршрутизация:** Избегайте ситуаций с сетевыми закреплениями, так как они могут значительно повлиять на задержку.

- **Протокол транспортного уровня:** UDP (вместе с URCP) обеспечивает более высокую пропускную способность, меньшую задержку передачи данных, уменьшая накладные расходы и оптимизируя производительность в режиме реального времени. Дополнительные преимущества UDP здесь RDP Shortpath | Microsoft Learn

- **Потеря пакетов:** Обратите внимание на снижение высокого уровня потери пакетов, так как это может нарушить производительность облачного компьютера и вызвать разочарование у пользователей.

- **Дрожание:** Изменчивость времени доставки пакетов может повлиять на согласованность взаимодействия с пользователем. Как и потеря пакетов, проверьте, чтобы уменьшить Jitter, где это возможно.

Администраторы могут использовать широкий спектр ресурсов при планировании подготовки облачных компьютеров для глобально распределенных команд, включая разнообразный набор регионов, поддерживаемых Azure, для принятия более обоснованных и стратегических решений.

Оптимизация подключения по протоколу удаленного рабочего стола (RDP) для Windows 365 позволяет значительно повысить надежность подключения, уменьшить задержку и увеличить доступную пропускную способность. Чтобы повысить производительность в сетях, управляемых клиентом (ANC), следует использовать **RDP Shortpath** , который включен по умолчанию. Эта функция устанавливает прямое подключение на основе UDP между поддерживаемым клиентом удаленного рабочего стола Windows и узлом сеансов. По умолчанию RDP сначала пытается установить UDP-подключение и возвращается к транспорту обратного подключения на основе TCP, который обеспечивает широкую совместимость и высокий уровень успешности.

RDP Shortpath поддерживает две конфигурации:

- **Управляемые сети**: прямой UDP или STUN

- **Общедоступные сети**: STUN или TURN

Примечание. Администраторы могут проверить подключение к конечным точкам STUN и TURN и убедиться, что базовые функции UDP работают, запустив исполняемый avdnettest.exe.

Кроме того, **RDP Multipath** повышает устойчивость сеанса за счет одновременной оценки нескольких путей UDP и динамического переключения между ними в режиме реального времени. Если один из путей завершается ошибкой, сеанс продолжается непрерывно по альтернативному маршруту, что позволяет минимизировать отставание и повысить стабильность. RDP Multipath в настоящее время доступен как для Azure Виртуального рабочего стола (AVD), так и для Windows 365.

Ценным ресурсом для администраторов, управляющих Windows 365 подключением, является **отчет о качестве подключений**, который обеспечивает видимость времени кругового пути (RTT) между клиентом и облачным компьютером, доступной пропускной способностью, протоколом и другими точками данных. Этот отчет помогает определить устройства, которые могут быть неэфтимы по сравнению с ожидаемыми показателями производительности.

Благодаря постоянным улучшениям Windows 365 подключения, таким как расширение регионов ретранслятора TURN и новый выделенный диапазон IP-адресов, повышена производительность протокола удаленного рабочего стола (RDP). Теперь RDP может поддерживать задержки до 200 мс, уменьшая важность географической близости между пользователем и его облачным компьютером. Вместо этого все более важно расположить облачные компьютеры ближе к данным приложения, к которые они получают доступ. Этот сдвиг помогает свести к минимуму задержку и оптимизировать производительность для конечных пользователей. Организациям рекомендуется тщательно оценивать региональные конфигурации размещения и сети, чтобы обеспечить бесперебойную и быструю работу облачных компьютеров. Мы настоятельно рекомендуем ознакомиться с этим документом для получения дополнительных сведений о принципах подключения Windows 365 | Microsoft Learn

Стратегии оптимальной подготовки облачных компьютеров

Региональная подготовка

Чтобы устранить проблемы с задержкой, связанные с расположением пользователя или расположением данных приложения, организациям следует рассмотреть возможность подготовки облачных компьютеров в центрах обработки данных, географически расположенных ближе к пользователям и (или) расположению данных приложения, в зависимости от того, что является более полезным.

Оптимизация сети

Администраторы должны убедиться, что сетевые конфигурации оптимизированы для использования облачных компьютеров. Это включает в себя приоритезирование сетей с низкой задержкой, использование преимуществ новых улучшений, увеличение распределения пропускной способности при необходимости и реализацию механизмов избыточности для минимизации времени простоя.

Мониторинг и аналитика

Непрерывный мониторинг производительности сети и активности пользователей имеет решающее значение для выявления узких мест и областей для улучшения. Отчеты и средства, которые анализируют задержку, использование пропускной способности и частоту ошибок, могут помочь в точной настройке параметров облачного компьютера, чтобы принимать обоснованные решения.

Гибридные модели

Для пользователей в регионах с ограниченной сетевой инфраструктурой гибридные модели, сочетающие локальные вычислительные ресурсы с доступом к облачному компьютеру, могут устранить проблемы с подключением. Такой подход помогает сбалансировать производительность и специальные возможности.

Профилирование пользователей

Понимание уникальных потребностей конечных пользователей, включая их расположение, сетевые возможности и требования к рабочей нагрузке, позволяет реализовать специализированные стратегии подготовки. Например, опытным пользователям, которым требуются интенсивные вычисления, могут потребоваться облачные компьютеры, подготовленные с более высокой пропускной способностью и меньшей задержкой, или определенные характеристики при обработке или памяти.

Преимущества оптимизированной подготовки облачных компьютеров

Оптимизированная подготовка облачных компьютеров с учетом расположения пользователей и параметров сети обеспечивает ряд преимуществ:

- **Улучшенный пользовательский интерфейс:** Более быстрое время отклика и сокращение проблем с подключением повышают производительность и удовлетворенность.
- **Экономичность:** Специализированная подготовка сводит к минимуму ненужное выделение ресурсов и оптимизирует расходы.
- **Масштабируемость:** Возможность быстро адаптировать конфигурации облачных компьютеров к изменяющимся расположениям пользователей и сетевым условиям поддерживает рост и гибкость.

- **Соответствие нормативным требованиям.** Подготовка облачных компьютеров в соответствующих регионах обеспечивает соблюдение местных законов и нормативных актов о защите данных.

Заключение

Оптимизированная подготовка облачных компьютеров требует тщательного изучения расположения пользователей и сетевого подключения для обеспечения оптимального взаимодействия. Устраняя эти факторы с помощью региональной подготовки, оптимизации сети и специализированных стратегий, организации могут обеспечить эффективность и удобство развертывания облачных компьютеров. По мере того как удаленная работа и цифровая совместная работа продолжают развиваться, приоритеты этих аспектов по-прежнему важны для успешной интеграции облачных компьютеров.

Last updated on 05.11.2025

Требования для установки Windows 365

Статья • 10.03.2025

Для использования облачных компьютеров необходимо выполнить следующие требования.

Требования Azure

Windows 365 Корпоративная и frontline

Нет, если планируется подготовка Microsoft Entra присоединенных облачных компьютеров в сети, размещенной корпорацией Майкрософт.

Если вы решите подготовить облачные компьютеры в собственной сети, потребуется активная подписка Azure со следующими конфигурациями.

- Достаточные разрешения для предоставления Windows 365:
  - Роль читателя в подписке Azure.
  - Сетевой интерфейс Windows365 участник роль в указанной группе ресурсов.
  - Роль пользователя сети Windows365 в виртуальной сети.

требования к Microsoft Entra ID и Intune

- Допустимый и работающий клиент Intune и Microsoft Entra.
- Intune ограничениях для регистрации типов устройств по умолчанию необходимо установить значение Разрешить платформу Windows (MDM) для корпоративной регистрации. Дополнительные сведения см. в разделе Ограничения регистрации устройств.
- Конфигурация инфраструктуры. Если планируется подготовка Microsoft Entra гибридных облачных компьютеров, необходимо настроить инфраструктуру для автоматического Microsoft Entra гибридного присоединения любых устройств, присоединенных к локальная служба Active Directory. Эта конфигурация позволяет идентифицировать их и управлять ими в облаке.
- Доменные службы Microsoft Entra не поддерживается, так как не поддерживает Microsoft Entra гибридное присоединение.

Требования к домену

Нет, если планируется подготовка Microsoft Entra присоединенных облачных компьютеров в сети, размещенной корпорацией Майкрософт.

Если вы решили подготовить Microsoft Entra гибридных облачных компьютеров, то в вашем домене потребуются следующие конфигурации:

- Если указано подразделение, убедитесь, что оно существует и является допустимым.
- Учетная запись пользователя Active Directory с достаточными разрешениями на присоединение компьютера к указанному подразделению в домене Active Directory. Если вы не укажете подразделение, учетная запись пользователя должна обладать достаточными разрешениями на присоединение компьютера к домену Active Directory.
- Учетные записи пользователей, назначенные облачным компьютерам, должны иметь синхронизированное удостоверение, доступное как в Active Directory, так и в Microsoft Entra ID.

> ⓘ **Примечание**
>
> Для учетной записи пользователя, используемой для присоединения облачных компьютеров к доменные службы Active Directory, настройте соответствующее делегирование, следуя инструкциям в разделе **Увеличение лимита учетной записи компьютера в подразделении**.

Требования к лицензированию

- Чтобы использовать Intune для управления устройствами, у вас должна быть лицензия на Intune.
- Windows 365 Корпоративная. Чтобы использовать облачный компьютер, пользователи должны иметь лицензии на Windows E3, Intune, Microsoft Entra ID P1 и Windows 365.
- Windows 365 Frontline: пользователи должны
  - У вас есть лицензии на Windows E3, Intune Microsoft Entra ID P1.
  - Добавьте в группу безопасности Microsoft Entra в политике подготовки, чтобы использовать облачный компьютер.

Требования к управлению

- Для управления облачными компьютерами необходимо использовать центр администрирования Microsoft Intune.
- Для управления конфигурациями облачных компьютеров требуется лицензия на Windows 365 Корпоративная или frontline.

Требования к ролям и удостоверениям

- Администратор роль. Для подготовки облачных компьютеров необходимо быть администратором Intune в Microsoft Entra ID или администратором Windows 365.
- Удостоверение пользователя: для настройки пользователей облачных компьютеров необходимо использовать гибридные удостоверения, чтобы они могли проходить проверку подлинности как в локальных, так и в облачных ресурсах.

Поддерживаемые регионы Azure для подготовки Облачных компьютеров

Windows 365 Корпоративная и frontline

Windows 365 управляет емкостью и доступностью базовых ресурсов Azure как части службы. Разработчики Windows 365 тесно взаимодействует с разработчиками Azure, выбирая регионы, которые соответствуют требованиям службы Windows 365 к доступности и емкости. При выборе региона Корпорация Майкрософт настоятельно рекомендует использовать параметр **Автоматически** . Такая автоматизация снижает вероятность сбоя подготовки, увеличивая возможные регионы, в которые будут установлены CloudPC. При доступности мы используем такие функции, как зоны доступности в Azure, чтобы обеспечить устойчивость в регионе в качестве встроенного преимущества службы. Вы можете создать виртуальную сеть или использовать сеть, размещенную на сервере Майкрософт, для подготовки облачных компьютеров в указанных ниже регионах Azure.

- Азия
  - Восточная Азия
  - Юго-Восточная Азия
- Австралия
  - Восток Австралии
- Канада
  - Центральная Канада

- Центральная Америка
  - Центральная Мексика
- Европейский Союз
  - Северная Европа
  - Западная Европа
  - Северная Италия
  - Центральная Польша
  - Центральная Испания
  - Центральная Швеция
- Франция
  - Центральная Франция
- Германия
  - Центрально-Западная Германия
- Индия
  - Центральная Индия
- Япония
  - Восточная Япония
  - Западная Япония
- Средний Восток
  - Центральный Израиль
- Норвегия
  - Восточная Норвегия
- Южная Африка
  - Северная часть Южной Африки
- Южная Америка
  - Южная Бразилия (ограниченное)
- Южная Корея
  - Центральная Корея
- Швейцария
  - Северная Швейцария
- ОАЭ
  - Север ОАЭ
- Великобритания
  - Южная часть Соединенного Королевства
- Центральная часть США
  - Центральная часть США
  - Центрально-южная часть США
- Восточная часть США
  - Восточная часть США
  - Восточная часть США 2
- Западная часть США

- Западная часть США 2 (ограничено)
- Западная часть США 3

Некоторые функции могут быть недоступны в некоторых регионах.

Дальнейшие действия

Просмотр требований к сети

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Требования к сети

Статья • 31.01.2025

Windows 365 — это облачная служба, которая позволяет пользователям подключаться через Интернет с любого устройства и из любого места к рабочему столу Windows, запущенному в Azure. Для поддержки этих подключений к Интернету необходимо соблюдать требования к сети, перечисленные в этой статье.

Каждый клиент имеет свои конкретные требования в зависимости от рабочей нагрузки, используемой для расчета требований к сети среды облачного компьютера.

> **Примечание**
>
> Сведения из этой статьи применяются только для подготовки облачных компьютеров в собственной виртуальной сети Azure, а не в сети, размещенной в Майкрософт.

Общий требования к сети

Windows 365 Корпоративная

Для использования собственной сети и подготовки Microsoft Entra присоединенных облачных компьютеров необходимо выполнить следующие требования:

- Виртуальная сеть Azure: в подписке Azure в том же регионе, где создаются рабочие столы Windows 365, должна присутствовать виртуальная сеть (vNET).
- Пропускная способность сети: см. рекомендации Azure по использованию сети.
- Подсеть в виртуальной сети и доступный диапазон IP-адресов.

Чтобы использовать собственную сеть и подготовить Microsoft Entra гибридных облачных компьютеров, необходимо выполнить указанные выше требования и следующие требования:

- Виртуальная сеть Azure должна обладать возможностью разрешать записи DNS для среды доменных служб Active Directory (AD DS). Для

поддержки этого разрешения определите DNS-серверы доменных служб Active Directory в качестве DNS-серверов для виртуальной сети.
- Виртуальной сети Azure необходимо предоставить сетевой доступ к контроллеру корпоративного домена либо в Azure, либо в локальной среде.

Разрешение подключения к сети

Windows 365 Корпоративная

Необходимо разрешить трафик в конфигурации сети к следующим URL-адресам и портам служб для поддержки подготовки облачных компьютеров и управления ими, а также для удаленного подключения к облачным компьютерам. Хотя большая часть конфигурации связана с сетью облачного компьютера, подключение конечных пользователей происходит с физического устройства. Поэтому необходимо также следовать рекомендациям по подключению в сети физического устройства.

Развернуть таблицу

Устройство или служба	Необходимые URL-адреса и порты для сетевого подключения	Примечания
Физическое устройство	Link	Для подключения и обновлений клиента удаленного рабочего стола.
Служба Microsoft Intune	Link	Для Intune облачных служб, таких как управление устройствами, доставка приложений и аналитика конечных точек.
Виртуальная машина узла сеансов Виртуального рабочего стола Azure	Link	Для удаленного подключения между облачными компьютерами и серверной службой Виртуального рабочего стола Azure.
служба Windows 365	Link	Для подготовки и проверок работоспособности.

служба Windows 365

Для подготовки облачных компьютеров и проверок работоспособности сетевого подключения Azure (ANC) требуются следующие URL-адреса и порты:

- *.infra.windows365.microsoft.com
- *.cmdagent.trafficmanager.net
- Конечные точки для регистрации
  - login.microsoftonline.com
  - login.live.com
  - enterpriseregistration.windows.net
  - global.azure-devices-provisioning.net (исходящие 443 и 5671)
  - hm-iot-in-prod-prap01.azure-devices.net (исходящие 443 и 5671)
  - hm-iot-in-prod-prau01.azure-devices.net (исходящие 443 и 5671)
  - hm-iot-in-prod-preu01.azure-devices.net (исходящие 443 и 5671)
  - hm-iot-in-prod-prna01.azure-devices.net (исходящие 443 и 5671)
  - hm-iot-in-prod-prna02.azure-devices.net (443 & 5671 исходящих)
  - hm-iot-in-2-prod-preu01.azure-devices.net (443 & 5671 исходящий трафик)
  - hm-iot-in-2-prod-prna01.azure-devices.net (443 & 5671 исходящих)
  - hm-iot-in-3-prod-preu01.azure-devices.net (443 & 5671 исходящих)
  - hm-iot-in-3-prod-prna01.azure-devices.net (443 & 5671 исходящих)
  - hm-iot-in-4-prod-prna01.azure-devices.net (443 & 5671 исходящих)

Все конечные точки подключаются через порт 443, если не указано иное.

Порт 3389

Порт 3389 отключен по умолчанию для всех вновь подготовленных облачных компьютеров. Корпорация Майкрософт рекомендует оставить порт 3389 закрытым. Однако если вам нужно, чтобы порт 3389 был открыт для любых повторно подготовленных или недавно подготовленных облачных компьютеров с помощью параметра развертывания сетевого подключения Azure (ANC), можно просмотреть следующие варианты:

- Windows 365 базовые показатели безопасности. Клиенты могут использовать базовые показатели безопасности Windows 365 для эффективного управления портом 3389 для Windows 365 облачных компьютеров. Эти базовые показатели предоставляют комплексные средства и конфигурации, предназначенные для повышения мер безопасности и предоставления необходимого доступа. Изменив параметры брандмауэра и установив для параметра **Действие входящего трафика по умолчанию для общедоступного профиля***значение Разрешить*, организации могут убедиться, что порт 3389 настроен

соответствующим образом в соответствии с операционными потребностями. Просмотрите и настройте эти параметры в соответствии с требованиями вашей организации.

- Создайте настраиваемое правило брандмауэра в Microsoft Intune. Клиенты могут использовать настраиваемые правила брандмауэра в Microsoft Intune для настройки порта 3389 для Windows 365 облачных компьютеров. Этот параметр включает в себя создание настраиваемого правила в политиках безопасности Intune, предназначенных для разрешения входящего трафика через порт 3389, который используется для доступа к облачным компьютерам. Определив параметры правила, такие как номер порта, протокол (TCP) и ограничение определенных IP-адресов или сетей, можно убедиться, что доступ к порту 3389 строго контролируется и ограничивается только авторизованными сущностями.

Эти параметры неприменимы для клиентов, использующих сеть, размещенную в Майкрософт.

Использование тегов FQDN для конечных точек через Брандмауэр Azure

Windows 365 теги полного доменного имени (FQDN) упрощают предоставление доступа к Windows 365 необходимым конечным точкам службы через брандмауэр Azure. Дополнительные сведения см. в разделе Использование Брандмауэр Azure для управления средами Windows 365 и защиты.

Конечные точки службы брокера протокола удаленного рабочего стола (RDP)

Прямое подключение к конечным точкам службы брокера RDP Виртуального рабочего стола Azure очень важно для производительности в удаленном режиме на облачном компьютере. Эти конечные точки влияют как на соединение, так и на задержку. Чтобы соответствовать принципам сетевого подключения Microsoft 365, необходимо классифицировать эти конечные точки как конечные точки **Оптимизации**. Рекомендуется использовать прямой путь к этим конечным точкам из виртуальной сети Azure.

Чтобы упростить настройку элементов управления сетевой безопасностью, используйте теги службы виртуального рабочего стола Azure, чтобы идентифицировать эти конечные точки для прямой маршрутизации с помощью Определяемого пользователем маршрута сети Azure (UDR). UDR приводит к

прямой маршрутизации между виртуальной сетью и брокером RDP с наименьшей задержкой. Дополнительные сведения о тегах служб Azure см. в статье Обзор тегов служб Azure.

Изменение сетевых маршрутов облачного компьютера (на сетевом уровне или на уровне облачного компьютера (например, VPN)) может нарушить соединение между облачным компьютером и брокером RDP виртуальных рабочих столов Azure. В этом случае пользователь отключается от облачного компьютера до тех пор, пока подключение не будет восстановлено.

Требования к DNS

В рамках Microsoft Entra требований к гибридному присоединению облачные компьютеры должны иметь возможность присоединения к локальная служба Active Directory. Для этого необходимо, чтобы облачные компьютеры могли разрешать записи DNS для вашей локальной среды AD.

Настройте виртуальную сеть Azure, в которой будут подготовлены облачные компьютеры, следующим образом.

1. Убедитесь в том, что ваша виртуальная сеть Azure имеет сетевое подключение к DNS-серверам, которые могут разрешать ваш домен Active Directory.
2. В параметрах виртуальной сети Azure выберите "DNS-серверы", а затем "Пользовательские".
3. Введите IP-адреса DNS-серверов, которые могут разрешить ваш домен AD DS.

> **Совет**
>
> Добавление по крайней мере двух DNS-серверов, как и на физическом компьютере, помогает снизить риск единой точки отказа в разрешении имен.

Дополнительные сведения см. в разделе о настройке параметров виртуальных сетей Azure.

Требования к протоколу удаленного рабочего стола

Windows 365 использует протокол удаленного рабочего стола (RDP).

Развернуть таблицу

Сценарий	Режим по умолчанию	Режим H.264/AVC 444	Описание
Бездействие	0,3 Кбит/с	0,3 Кбит/с	Пользователь приостановил работу, и активные обновления экрана отсутствуют.
Microsoft Word	100–150 Кбит/с	200–300 Кбит/с	Пользователь активно работает с Microsoft Word: выполняет ввод данных, вставляет графические объекты и переключается между документами.
Microsoft Excel	150–200 Кбит/с	400–500 Кбит/с	Пользователь активно работает с Microsoft Excel: одновременно обновляются многие ячейки с формулами и диаграммами
Microsoft PowerPoint	4–4,5 Мбит/с	1,6–1,8 Мбит/с	Пользователь активно работает с Microsoft PowerPoint: выполняет ввод, вставляет объекты, изменяет насыщенную графику и использует эффекты смены слайдов.
Просмотр веб-страниц	6–6,5 Мбит/с	0,9–1 Мбит/с	Пользователь активно работает с графически насыщенным веб-сайтом, который содержит множество статических и анимированных изображений. Пользователь прокручивает страницы по горизонтали и по вертикали
Коллекция изображений	3,3–3,6 Мбит/с	0,7–0,8 Мбит/с	Пользователь активно работает с приложением из коллекции изображений: просматривает и масштабирует изображения, изменяет их размер и поворачивает их.
Воспроизведение видео	8,5–9,5 Мбит/с	2,5–2,8 Мбит/с	Пользователь просматривает видеоматериал в стандарте 30 кадров в секунду, который занимает 1/2 экрана.
Воспроизведение полноэкранного видео	7,5–8,5 Мбит/с	2,5–3,1 Мбит/с	Пользователь просматривает видео со разрешением 30 кадров/с, развернутое в полноэкранном режиме.

Требования к Microsoft Teams

Microsoft Teams — это одна из основных служб Microsoft 365 на облачном компьютере. Windows 365 разгружает аудио- и видеотрафик в конечную точку для обеспечения работы с видео, аналогичной Teams на физическом компьютере.

Качество сети важно для каждого сценария. Убедитесь в наличии пропускной способности, достаточной для обеспечения качества, которое вы хотите предложить.

Microsoft Teams на облачных компьютерах не поддерживает разрешение Full HD (1920 x 1080 пикселей).

Развернуть таблицу

Счетчик пропускной способности	Сценарии
30 Кбит/с	Одноранговый голосовой вызов.
130 Кбит/с	Одноранговый голосовой вызов и общий доступ к экрану.
500 Кбит/с	Одноранговый видеовызов с высоким качеством, с разрешением 360 пикселей, с частотой 30 кадров/с.
1,2 Мбит/с	Одноранговый видеовызов высокой четкости (HD), с разрешением 720 пикселей, с частотой 30 кадров/с.
500 Кбит/с / 1 Мбит/с	Групповой видеовызов.

Дополнительные сведения о требованиях к сети Microsoft Teams см. в статье Рекомендации по работе с сетями.

Технологии перехвата трафика

Некоторые корпоративные клиенты используют прослушивание трафика, расшифровку SSL, внимательное отслеживание пакетов и другие аналогичные технологии, позволяющие командам службы безопасности отслеживать сетевой трафик. Для подготовки облачных компьютеров может потребоваться прямой доступ к виртуальной машине. Эти технологии прослушивания трафика могут вызвать проблемы с выполнением локальных проверок сетевых подключений или подготовкой облачных компьютеров. Убедитесь, что для облачных компьютеров, подготовленных в службе Windows 365, не применяется прослушивание сети.

Пропускная способность

Windows 365 использует инфраструктуру сети Azure. Подписка Azure требуется при выборе виртуальной сети во время развертывания Windows 365 Корпоративная. Плата за пропускную способность для использования облачных компьютеров включает:

- За сетевой трафик, поступающий на облачный компьютер, плата не взимается.
- За исходящий трафик взимается плата с подписки Azure для виртуальной сети.
- За данные Office (например, синхронизация файлов электронной почты и OneDrive для бизнеса) выставляются платежи исходящего трафика, если облачный компьютер и данные пользователя находятся в разных регионах.
- За сетевой трафик RDP всегда выставляются платежи исходящего трафика.

Если вы используете собственную сеть, см. раздел Цены на пропускную способность.

Если вы используете сеть, размещенную в Майкрософт, исходящие данные в месяц зависят от ОЗУ облачного компьютера:
– 2 ГБ ОЗУ = 12 ГБ исходящих данных
– 4 или 8 ГБ ОЗУ = 20 ГБ исходящих данных
– 16 ГБ ОЗУ = 40 ГБ исходящих данных
– 32 ГБ ОЗУ = 70 ГБ исходящих данных
Пропускная способность данных может быть ограничена при превышении этих уровней.

Дальнейшие действия

Узнайте об управлении доступом на основе ролей для облачных компьютеров.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Общие сведения о подключении Windows 365

18.09.2025

Windows 365 — это глобально распределенное предложение SaaS, позволяющее организациям предоставлять пользователям в нескольких регионах безопасные, надежные и высокопроизводительные рабочие столы. Важным фактором, определяющим качество работы Windows 365 конечным пользователем, является эффективность сети и минимальная задержка между физическим устройством и облачным компьютером.

Корпорация Майкрософт управляет одной из крупнейших глобальных сетей в мире. Эта сеть подключается к Windows 365 точкам входа служб, включая шлюзы RDP и ретрансляторы TURN, которые распределены между центрами обработки данных по всему миру.

Эта инфраструктура обеспечивает доступность службы рядом с пользователями, чтобы уменьшить задержку, и позволяет корпорации Майкрософт управлять подключением большую часть пути из расположения пользователя к облачному компьютеру. Он также обеспечивает преимущество подключения на обратном пути к пользователю, находясь в глобальной магистрали Майкрософт.

В этой статье объясняется, как работает подключение Windows 365, как эффективно использовать глобальную инфраструктуру и почему требуется другой подход к оптимизации, отличный от стандартного интернет-трафика.

цели подключения Windows 365

Ключевой целью Windows 365 подключения является оптимизация взаимодействия с конечными пользователями путем обеспечения оптимизированного подключения между клиентами и ближайшей инфраструктурой подключения. Качество взаимодействия с конечным пользователем напрямую связано с производительностью и скоростью реагирования подключения между конечным пользователем и облачным компьютером.

Windows 365 имеет важный элемент с точки зрения службы SaaS, так как подключение к этой инфраструктуре настраивается клиентом по *обе* стороны подключения. При использовании служб SaaS поставщик обычно управляет стороной службы, как и в Случае с Microsoft 365.

Windows 365 предлагает простые варианты развертывания, которые значительно сокращают количество элементов на стороне службы, необходимых для настройки и

управления ими. Однако при настройке среды по-прежнему необходимо учитывать определенные конфигурации облачных компьютеров, которые могут повлиять на подключение.

Такие факторы, как неправильно настроенные VPN, защищенные веб-шлюзы (SWG) или параметры прокси-сервера, могут значительно нарушить производительность и надежность службы.

Основной целью структуры сети должно быть обеспечение безопасного подключения к службе с минимальной возможной задержкой. Ключевым фактором в достижении этого результата является сокращение времени кругового пути (RTT) между клиентскими устройствами и глобальной сетью Майкрософт, высокопроизводительной общедоступной магистралью Майкрософт, которая соединяет ее глобальные центры обработки данных. Эта сеть обеспечивает низкую задержку, поэтому данные быстро перемещаются между конечными точками с минимальной задержкой и высоким уровнем доступности, то есть службы остаются доступными даже во время сбоев или обслуживания. Windows 365 также использует глобально распределенные точки входа на границе сети, размещая их рядом с пользователями для повышения производительности. Дополнительные сведения о глобальной сети Майкрософт см. в статье Как Майкрософт строит свою быструю и надежную глобальную сеть.

Windows 365 можно настроить для максимально возможной производительности, следуя нескольким ключевым принципам:

- Подготовьте облачный компьютер как можно ближе к пользователю, если это возможно.
- Определение Windows 365 сетевого трафика.
- Разрешите локальный исходящий трафик Windows 365 из каждого расположения, где пользователи подключаются к службе.
- Разрешите трафику Windows 365 ключей обходить прокси-серверы и средства проверки и направлять его непосредственно в инфраструктуру Майкрософт.

Дополнительные сведения о принципах Windows 365 сетевого подключения Windows 365 см. в статье Принципы подключения Windows 365.

Традиционные сетевые архитектуры и SaaS

Традиционные локальные сетевые архитектуры для рабочих нагрузок клиента или сервера основаны на предположении, что трафик между клиентами и конечными точками остается в пределах периметра корпоративной сети. На многих предприятиях

весь исходящий интернет-трафик проходит через корпоративную сеть. Он завершает работу в централизованной точке исходящего трафика, обычно (модуль) безопасности, например прокси-сервер. Это устройство проверяет и фильтрует трафик, прежде чем он достигнет Интернета.

В традиционных сетевых архитектурах более высокая задержка для универсального интернет-трафика является необходимым компромиссом для обеспечения безопасности периметра сети. Оптимизация производительности интернет-трафика обычно включает обновление или масштабирование оборудования в точках исходящего трафика сети. Однако такой подход не отвечает требованиям к производительности служб SaaS, таких как Windows 365. Это становится еще сложнее из-за дополнительных элементов подключения в Azure. Таким образом, для обеспечения высокой производительности и надежности конечных пользователей требуется оптимизация подключения для конкретных служб.

Вы уже можете использовать аналогичные оптимизации для таких служб, как Microsoft 365. Windows 365 можно легко согласовать с тем же подходом.

Определение сетевого трафика Windows 365

Корпорация Майкрософт упрощает идентификацию Windows 365 сетевого трафика и упрощает управление идентификацией сети.

Теперь в документации по требованиям к конечным точкам мы выделим, какие конечные точки требуют специальной обработки с точки зрения оптимизации, а какие из них могут пройти стандартный путь к Интернету без специальной обработки. Требования к конечной точке для службы можно найти на странице Требования к конечной точке сети .

Защита Windows 365 подключений

Цель традиционной системы сетевой безопасности — укрепить защиту периметра корпоративной сети от вторжений и вредоносных эксплойтов. Большинство корпоративных сетей обеспечивают безопасность сети для интернет-трафика с помощью таких технологий, как прокси-серверы, брандмауэры, прерывание и проверка tls, глубокая проверка пакетов и системы защиты от потери данных. Эти технологии обеспечивают важное устранение рисков для универсальных интернет-запросов, но могут значительно снизить производительность, масштабируемость и качество взаимодействия с конечными пользователями при применении к критически важным конечным точкам Windows 365.

Некоторые конечные точки не получают преимуществ от проверки ИЛИ маршрутизации TLS через прокси-серверы, VPN или защищенные веб-шлюзы (SWG). Вместо этого эти методы могут повредить надежности службы и взаимодействию с пользователем, если их не избежать.

Дополнительные сведения о том, как обеспечивается подключение RDP, см. в документации по безопасности протокола удаленного рабочего стола (RDP). Проверка трафика RDP по протоколу TLS не требуется и не обеспечивает никаких преимуществ.

Чем отличается сеть Windows 365?

Windows 365 предназначена для оптимальной производительности с использованием безопасности конечных точек и зашифрованных сетевых подключений, что снижает потребность в принудительном применении безопасности периметра. Windows 365 работает в глобальной инфраструктуре Майкрософт. Служба использует несколько методов для подключения клиентов к ближайшим и наиболее производительным конечным точкам службы.

Эта локальная входная дверь для службы обеспечивает подключение пользователя к инфраструктуре Майкрософт и высокопроизводительной глобальной магистрали с низкой задержкой, независимо от расположения облачного компьютера.

Распространенные проблемы с производительностью возникают, когда некоторые Windows 365 трафик подвергается проверке пакетов и централизованному исходящему трафику:

- Неэффективная маршрутизация, прокси-серверы или проверка увеличивают задержку. Эта задержка приводит к низкой производительности рабочего стола, низкой пропускной способности и задержке ввода данных пользователем, что приводит к плохому взаимодействию с пользователем.

- Маршрутизация подключений из нелокального расположения обходит динамическую маршрутизацию и эффективность microsoft, что увеличивает задержку и время кругового пути. Это также может привести к частым отключениям, так как путь не оптимизирован для больших расстояний.

- Расшифровка и повторное шифрование трафика TLS для Windows 365 не дает никаких преимуществ, представляет угрозу безопасности и может привести к ошибкам протокола. Это также повышает вероятность отключения сеанса RDP и оказывает большую нагрузку на проверяющее устройство. По этим причинам проверка TLS Windows 365 трафика RDP не поддерживается.

Когда облачный компьютер инициирует подключение, конечные точки, находящиеся в инфраструктуре Майкрософт, такие как RDP, могут полностью избежать общедоступного Интернета, если трафик выходит локально. Маршрутизация этого трафика через прокси-сервер, безопасный веб-шлюз или VPN не только приводит к значительному снижению производительности, но и сводит на нет этот прямой путь, избегая Интернета.

В приведенном примере компания Contoso настраивает оптимальное Windows 365 подключение в соответствии с рекомендациями. Локальный и прямой исходящий трафик для RDP в расположении Contoso India и на стороне облачного компьютера, развернутого в США, означает, что происходит несколько положительных оптимизаций.

1. Локальный и прямой исходящий трафик — это наиболее эффективный путь через локального поставщика услуг Интернета (ISP) для подключения к глобальной сети Майкрософт в Течение нескольких миллисекунд в Индии.

2. Для подключения можно использовать локальные шлюзы RDP и ретрансляторы TURN, что означает низкую задержку от пользователя до этих входных дверей службы. В этом примере пользователь подключается к точке входа службы примерно за 10 мс.

3. Географическое расстояние от Индии до расположения облачного компьютера в США полностью проходит по управляемой магистрали Майкрософт, обеспечивая максимально высокий уровень производительности и надежности.

4. Этот трафик не проходит через глобальную глобальную глобальную сеть Contoso. Эта емкость остается доступной для рабочих нагрузок, которым она требуется.

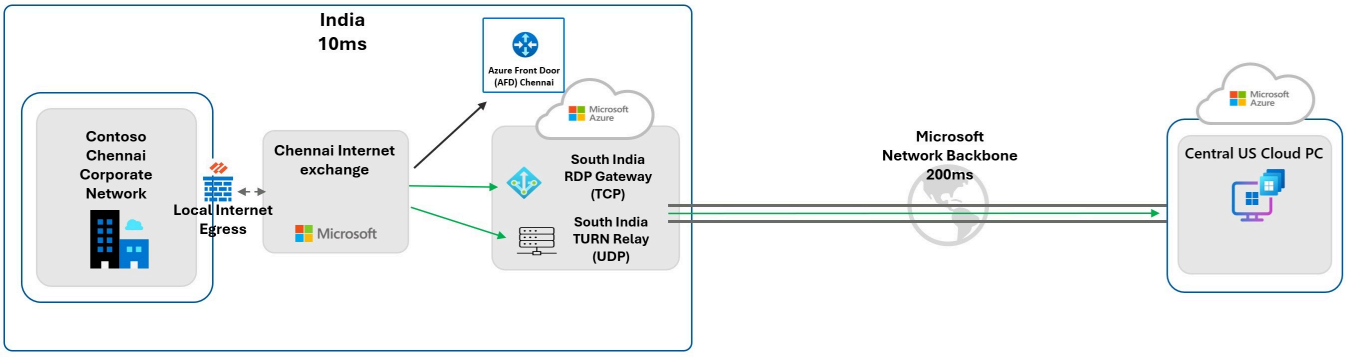


Схема 1. Оптимизация RDP с локальным прорывом

На этом изображении показано следующее:

- Локальный исходящий трафик RDP в Ченнаи гарантирует, что трафик попадает в глобальную сеть Майкрософт в расположении пиринга Ченнаи.
- Локальные входные двери службы (шлюзы удаленных рабочих столов и ретрансляторы TURN) сокращают задержку, сохраняя подключения близко к

пользователю.

- Элемент междугородней обратной связи от входной двери службы до облачного компьютера в центральной части США работает полностью в сети Майкрософт, обеспечивая оптимизированный путь с высокой пропускной способностью и низкой задержкой с избыточными каналами.
- Эта конструкция обеспечивает наименьшую возможную задержку, высокую производительность, снижение риска отключения и отличный пользовательский интерфейс, избегая общедоступного Интернета на протяжении большей части пути.
- При правильной настройке трафик RDP с облачного компьютера к передней двери службы полностью остается в сети Майкрософт и никогда не проходит через общедоступный Интернет.

Сводка

Оптимизация Windows 365 сетевого подключения сводится к устранению ненужных препятствий и использованию глобальной инфраструктуры Майкрософт. Настройте подключения Windows 365 ключей в качестве доверенного трафика, чтобы поддерживать низкую задержку и предотвращать состязание по пропускной способности прокси-серверов. Разрешение локальных подключений между физическим устройством и облачным компьютером в инфраструктуру Майкрософт позволяет динамически направлять трафик через глобальную сеть Майкрософт и использовать преимущества локальных входных дверей службы.

Принципы подключения Windows 365

18.09.2025

Прежде чем планировать сеть для Windows 365, важно понять принципы подключения, которые обеспечивают пользователям безопасный, надежный и высокопроизводительный доступ к облачному компьютеру. Эта статья поможет вам понять последние рекомендации по безопасной оптимизации этого критического трафика.

Традиционные корпоративные сети в основном предназначены для предоставления доступа к приложениям и данным, размещенным в центре обработки данных, управляемом компанией. Эти сети используют безопасность периметра, которая включает брандмауэры, системы обнаружения вторжений и средства проверки трафика для защиты от ненадежного внешнего мира. Эта традиционная модель предполагает, что пользователи получают доступ к приложениям и данным из корпоративной сети либо непосредственно с корпоративных сайтов, либо удаленно через подключения виртуальной частной сети (VPN). Эта архитектура оптимизирована для централизованных элементов управления и защиты, но может привести к задержке и сложности при доступе к облачным службам.

Windows 365 может предоставлять полностью интерфейс на основе SaaS для облачного компьютера, позволяя организациям предоставлять пользователям по всему миру безопасные, надежные и высокопроизводительные классические среды. Поэтому для подключения к инфраструктуре, предоставляемой для обеспечения этого глобального беспроблемного подключения, требуется специальная оптимизация для обеспечения максимально возможной производительности и качества для конечных пользователей.

Архитектура Windows 365

Windows 365 — это географически распределенная служба "программное обеспечение как услуга" (SaaS). Облачные компьютеры можно развернуть в нескольких глобальных регионах в соответствии с потребностями пользователей и организаций.

Подключение между пользователем и его облачным компьютером должно быть разработано в соответствии с предоставленными рекомендациями. Этот подход помогает оптимизировать производительность, используя глобальную сеть и инфраструктуру пограничных служб Майкрософт, ближайшую к пользователю и облачному компьютеру, а не основываясь на расположении целевого объекта.

- Корпорация Майкрософт управляет одной из крупнейших глобальных сетей, предлагая высокодоступные подключения с высокой пропускной способностью и

низкой задержкой между центрами обработки данных и пограничным интернет-подключением. Благодаря 185 точкам присутствия глобальной сети и растущему росту эта инфраструктура обеспечивает подключение пользователей.

- Windows 365 использует глобально распределенные точки входа службы, включая службу шлюза для подключений по протоколу удаленного рабочего стола (RDP) на основе TCP и ретрансляторы TURN для подключений по протоколу UDP. Эти точки входа расположены рядом с пользователями, где бы они ни находились, чтобы обеспечить оптимальное подключение.

- Облачные компьютеры могут напрямую обращаться к магистральной сети Майкрософт, чтобы достичь этих входных дверей службы после подключения пользователя к ним. При правильной маршрутизации трафик к конечным точкам, размещенным корпорацией Майкрософт, никогда не касается Интернета с облачного компьютера.

Правильное использование всех трех элементов помогает обеспечить быстрое и надежное подключение между пользователями и их облачными компьютерами независимо от расположения пользователей.

Элементы подключения для понимания

Windows 365 требования к подключению можно разделить на три категории:

A. Подключение по протоколу RDP

Трафик RDP формирует основное соединение между конечным пользователем и облачным компьютером. Он использует одни и те же исходящие конечные точки как на физическом устройстве, так и на облачном компьютере. Оптимизация этого трафика необходима для обеспечения надежного и высокопроизводительного подключения.

Б. **Подключение к облачной службе**

Этот трафик необходим для подготовки облачных компьютеров и работы службы. Большинство конечных точек размещаются в магистральной сети Майкрософт, поэтому маршрутизация трафика непосредственно к ним повышает производительность и надежность. Он также обеспечивает наивысший уровень безопасности, так как трафик не проходит через общедоступный Интернет.

c. Подключение физического клиента

Помимо описанных здесь подключений по протоколу RDP, все остальные требования к физической конечной точке на стороне клиента могут рассматриваться как обычный веб-трафик и управляться в соответствии со стандартными методиками вашей организации.

принципы подключения Windows 365

Корпорация Майкрософт рекомендует следующие принципы для достижения оптимального подключения и производительности. Основной целью проектирования сети для Windows 365 является минимизация задержки за счет сокращения времени кругового пути (RTT) между вашей сетью и глобальной сетью Майкрософт. Эта магистральная сеть соединяет все центры обработки данных Корпорации Майкрософт и обеспечивает низкую задержку как между расположениями центров обработки данных, так и между пограничными сетями, расположенными рядом с пользователями. Для обеспечения максимальной производительности и надежности при подключении с облачного компьютера используйте следующие оптимизации:

1. Развертывание облачного компьютера как можно ближе к пользователю

Размещение облачного компьютера как можно ближе к расположению конечного пользователя помогает свести к минимуму задержку. Корпорация Майкрософт предлагает варианты развертывания во многих регионах Azure по всему миру. Выбор региона, ближайшего к пользователю, сокращает задержку между пользователем и облачным компьютером, обеспечивая наилучшую производительность.

В некоторых случаях развертывание локального облачного компьютера может оказаться невозможным из-за требований к соответствию или ограничений задержки данных приложения. Если локальное развертывание невозможно, оптимизация на уровне сети становится более важной для поддержания производительности на больших расстояниях.

Независимо от того, где развернут облачный компьютер, следуйте этим принципам сети, чтобы обеспечить максимальную производительность и надежность.

2. Определение и дифференциация Windows 365 трафика

Определение Windows 365 сетевого трафика — это первый шаг в том, чтобы при необходимости отличить этот трафик от универсального сетевого трафика, связанного с Интернетом. Windows 365 подключения можно оптимизировать путем реализации сочетания таких подходов, как:

Оптимизация сетевого маршрута

- Обход VPN-шлюза или безопасного веб-шлюза (SWG)
- Правила брандмауэра

- Параметры прокси-сервера браузера.
- Обход устройств проверки сети для определенных конечных точек.

Сведения о конечных точках, необходимых для службы, можно свести к одной из следующих трех категорий.

A. RDP — идентичные требования как на стороне облака, так и на стороне физического устройства.

Б. Подключение к облачной службе

c. Требования к физическому подключению клиента

Трафик в областях (a) и (b) нуждается в специальной оптимизации, тогда как трафик в (c) — нет. Разбивку конечных точек в этих категориях можно найти по указанным ссылкам. Подробные сведения об этих конечных точках см. в документации по требованиям к сети.

3. Исходящие сетевые подключения локально

Для рекомендуемых конечных точек трафик должен быть исходящим локально и напрямую.

- На стороне облачного компьютера трафик должен направляться непосредственно из виртуальной сети в сеть Azure, избегая vpn-туннелей, защищенных веб-шлюзов, прокси-серверов или локальных исходящих подключений.
- Для физических клиентских устройств разрешите трафику службы ключей выйти как можно ближе к пользователю (например. через локальный исходящий трафик SD-WAN или домашнего поставщика услуг Интернета (ISP) вместо того, чтобы сначала отправлять его обратно на центральный сайт.

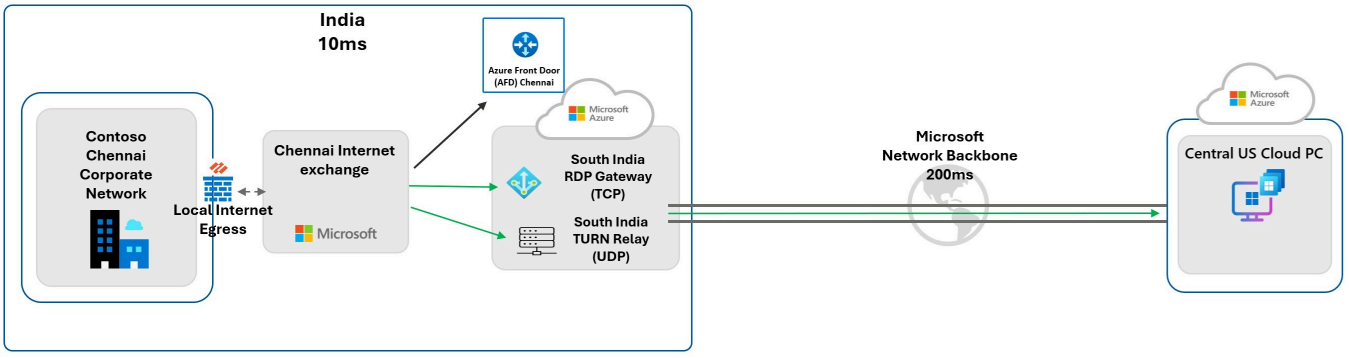


Схема 1. Оптимизация RDP с локальным прорывом

На этом изображении показано следующее:

- Локальный исходящий трафик RDP в Ченнаи гарантирует, что трафик попадает в глобальную сеть Майкрософт в расположении пиринга Ченнаи.
- Локальные входные двери службы (шлюзы удаленных рабочих столов и ретрансляторы TURN) сокращают задержку, сохраняя подключения близко к пользователю.
- Элемент междугородней обратной связи от входной двери службы до облачного компьютера в центральной части США работает полностью в сети Майкрософт, обеспечивая оптимизированный путь с высокой пропускной способностью и низкой задержкой с избыточными каналами.
- Эта конструкция обеспечивает наименьшую возможную задержку, высокую производительность, снижение риска отключения и отличный пользовательский интерфейс, избегая общедоступного Интернета на протяжении большей части пути.
- При правильной настройке трафик RDP с облачного компьютера к передней двери службы полностью остается в сети Майкрософт и никогда не проходит через общедоступный Интернет.

Используйте локальный интернет-прорыв рядом с пользователем, чтобы трафик быстро вошел в глобальную сеть Майкрософт. Такой подход позволяет близлежащим точкам входа Майкрософт оптимизировать подключение и обеспечить надежный доступ к облачному компьютеру, независимо от расположения размещения.

Эта инфраструктура включает в себя:

- Более 185 точек присутствия на границе Интернета
- Более 165 000 миль оптоволоконных и подводных кабелей, соединяющих пользователей с Microsoft Cloud
- Шлюзы RDP для RDP на основе TCP в более чем 40 регионах Azure
- TURN Relays for UDP на основе RDP в более чем 40 регионах Azure

Локальные интернет-прорывы подключают пользователей к Windows 365 инфраструктуре рядом с их расположением. Оттуда весь трафик на облачный компьютер проходит через безопасную, высокоскоростную глобальную сеть Майкрософт с низкой задержкой.

3. Оцените обход прокси-серверов, VPN, защищенных веб-шлюзов и устройств проверки трафика.

Корпоративные клиенты должны проверить свои средства управления безопасностью для Windows 365 трафика и разрешить прямой путь для трафика ключевой службы. Это снижает зависимость от дорогостоящих и навязчивых средств безопасности, которые

могут повредить производительности и надежности. Большинство корпоративных сетей обеспечивают безопасность сети для интернет-трафика с помощью таких технологий, как прокси-серверы, проверка TLS, проверка пакетов и системы защиты от потери данных. Эти технологии обеспечивают важное снижение рисков для универсальных интернет-запросов, но могут значительно снизить производительность, масштабируемость и качество взаимодействия с конечными пользователями при применении к определенным конечным точкам Windows 365. Для всех выделенных конечных точек Windows 365 рекомендуется использовать следующие оптимизации сети:

Для трафика RDP:

- Обход трафика от расшифровки, перехвата, глубокой проверки пакетов и сетевых пакетов & фильтрации содержимого на стороне облачного компьютера *и* физического устройства. Проверка этого трафика не поддерживается и не дает никаких преимуществ.
- В Azure используйте определяемый пользователем маршрут (UDR) для отправки трафика RDP напрямую в Интернет, избегая устройства проверки, например брандмауэра. Например, отправьте прямо в шлюз NAT, избегая пути брандмауэра. Подробный пример см. в документации по Windows 365 Брандмауэр Azure.
- Исключите трафик RDP из VPN, защищенного веб-шлюза (SWG) и туннелей прокси-сервера, настроенных как на облачных компьютерах, так и на физических устройствах.
- Предоставьте прямой путь для трафика, который достигнет Интернета на стороне физического клиента так же, как это делается для трафика мультимедиа Teams.
- Предоставьте локальный интернет-прорыв для физического трафика RDP клиента, а не обратной передачи в центральный или удаленный исходящий трафик, чтобы использовать инфраструктуру служб и глобальную сеть Майкрософт поблизости.

Требования к подключению на стороне облака:

- Убедитесь, что маршрут по умолчанию отправляет трафик в точку исходящего трафика Azure (например, Брандмауэр Azure), а не отправляет его в локальную сеть.
- Исключите Windows 365 трафик из расшифровки, перехвата, глубокой проверки пакетов и фильтрации содержимого, чтобы избежать проблем с производительностью и надежностью. Если требуется фильтрация, разрешите ее непосредственно через Брандмауэр Azure.

- Обход конфигураций VPN, защищенного веб-шлюза (SWG) и прокси-сервера для Windows 365 трафика.

Для подключения физического клиента

- Исключите трафик RDP из VPN, защищенного веб-шлюза (SWG) и туннелей прокси-сервера, настроенных на устройстве.
- Предоставьте прямой локальный интернет-прорыв для всего трафика RDP, чтобы свести к минимуму задержку и повысить надежность.
- Отключите проверку TLS для исходящего пути для трафика RDP, чтобы предотвратить прерывание сеанса.
- Обработка всех остальных конечных точек в качестве стандартного веб-трафика в соответствии с обычной моделью внешнего подключения вашей организации.

Windows 365 вопросы безопасности

При реализации оптимизации Windows 365 подключения учитывайте следующие моменты:

- Большинство обязательных конечных точек — только служба. Они существуют для работы службы Windows 365 и не содержат созданные пользователем данные.
- Трафик протокола удаленного рабочего стола (RDP) является исключением. Данные, такие как перенаправление буфера обмена, осуществляется внутри этого трафика, но его путь изолирован к соединению между физическим устройством и облачным компьютером.
- Проверка или неоптимизированная маршрутизация может повредить производительности. Такие методы, как глубокая проверка пакетов, перехват TLS или обратная маршрутизация, часто снижают задержку и снижают надежность.
- Проверка TLS не обеспечивает никаких преимуществ для этих конечных точек. Конечные точки уже используют ПРОТОКОЛ TLS для безопасного обмена данными, а данные связаны со службой.
- Трафик RDP шифруется в два раза. Традиционные встроенные средства проверки не могут расшифровать его.
- Большой объем трафика может перегружать устройства безопасности. При возникновении этого сценария могут быть нарушены другие критически важные службы, которые совместно используют одну и ту же инфраструктуру.

- Большинство конечных точек размещаются в инфраструктуре Майкрософт.
- Прямой локальный исходящий трафик в магистраль Azure — это наиболее эффективный и безопасный путь. С облачного компьютера трафик остается в глобальной сети Майкрософт без обхода общедоступного Интернета.
- Большая часть трафика уже зашифрована по протоколу TLS, что защищает конфиденциальность при передаче.
- Трафик через TCP-порт 80 не содержит частные данные. Он необходим для определенных функций, таких как проверка взаимодействия с Azure Fabric и списка отзыва сертификатов (CRL).

Все исключения четко задокументированы. Трафик, который не соответствует этим критериям, определяется в требованиях к конечной точке Windows 365 и может соответствовать стандартным путям к Интернету.

Упрощение развертывания

Windows 365 предлагает два варианта сетевого подключения. Выбор правильного может значительно снизить сложность, затраты и риски.

- **Сетевое подключение Azure (ANC):** С помощью ANC вы управляете базовым подключением. Реализация этих требований часто включает недели или месяцы работы по настройке сети, правил брандмауэра, определяемых пользователем, ExpressRoute и групп безопасности сети (NSG), а также текущее обслуживание. Он отражает традиционное расширение корпоративной сети, от которого многие организации отходят.
- **Размещенная сеть Майкрософт:** Параметр Размещенная сеть Майкрософт обеспечивает быстрое развертывание с минимальными сетевыми издержками. Корпорация Майкрософт разрабатывает, обслуживает и защищает среду для обеспечения оптимального подключения. Основная задача заключается в том, чтобы основной трафик обходить туннели VPN или SWG, что обычно быстро настраивается. Эта модель соответствует принципам "Никому не доверяй" и хорошо работает с современными решениями SWG и частного доступа.

Многие организации уже используют аналогичный подход для удаленных сотрудников, предоставляя ноутбуки, управляемые с помощью современного управления конечными точками и "Никому не доверяй". Размещенная сеть Майкрософт применяет ту же концепцию к облачным компьютерам, рассматривая их как защищенные домашние устройства, которые делают только исходящие подключения. Такая конструкция сокращает сроки проекта, повышает гибкость и упрощает текущее управление.

Дополнительные сведения об этом варианте проектирования см. в документации по параметрам развертывания Windows 365.

Параметры сетевого развертывания

18.09.2025

Windows 365 предоставляет два варианта развертывания сетевых подключений, используемых облачным компьютером.

- Размещенная сеть Майкрософт — (рекомендуется)
- Сетевое подключение Azure (ANC) — (для устаревших или специализированных требований)

Размещенная сеть Майкрософт — это рекомендуемый вариант развертывания для большинства сценариев. Она проста, современна и соответствует принципам "Никому не доверяй". Этот подход предпочтителен, так как он снижает сложность и затраты на управление. Сетевое подключение Azure (ANC) — это альтернатива, если нельзя избежать устаревших требований, таких как гибридное Azure AD присоединения или прямая связь с корпоративной сетью.

Размещенная сеть Майкрософт — рекомендуемый вариант развертывания

При развертывании облачных компьютеров следует выбрать параметр Размещенная сеть Майкрософт. Только отменить изменения к развертываниям ANC в крайнем случае.

Размещенная сеть Майкрософт — это полностью управляемый вариант, в котором корпорация Майкрософт настраивает базовую сеть для облачных компьютеров и управляет ею. Такой подход обеспечивает полное развертывание Windows 365 SaaS, упрощая управление сетью, повышая безопасность и сокращая затраты. Это идеальный выбор для организаций, которым требуется современное, простое, безопасное и масштабируемое развертывание Windows 365.

При выборе размещенной сети Майкрософт единственной необходимой настройкой инфраструктуры является выбор региона для развертывания. Корпорация Майкрософт берет на себя все остальное, включая любые будущие требования к управлению и обслуживанию.

Преимущества параметра Размещенная сеть Майкрософт

Выбор **размещенной сети Майкрософт** снижает сложность, ускоряет время получения ценности и повышает надежность Windows 365.

- **Простой по дизайну** - Нет управляемых клиентом виртуальная сеть Azure, брандмауэров, маршрутов и определяемых пользователем маршрутов, шлюзов NAT или правил для создания и обслуживания. Все, что требуется, — выбрать регион для развертывания; Чтобы обеспечить оптимальную подготовку, выберите **Автоматически**.

- **Быстрое развертывание** — Минимальные зависимости от сетевых элементов клиента позволяют быстро развертывать облачные компьютеры.

- **Эластичная емкость** — Корпорация Майкрософт управляет масштабированием, поэтому вы можете добавлять большое количество облачных компьютеров по запросу, не расширяя сначала сетевую инфраструктуру. Например, аварийное восстановление между регионами не требует предварительно подготовленной сети, если выбрана размещенная сеть Майкрософт.

- **Более низкая стоимость инфраструктуры** — Вы не платите за запуск виртуальных сетей, сетевых виртуальных устройств, пропускной способности или шлюзов NAT для облачных компьютеров. Корпорация Майкрософт управляет базовой сетью от вашего имени.

- **Снижение эксплуатационных накладных расходов** — Для настройки или обслуживания этой среды не требуется выделенная команда по работе с сетями Azure.

- **Подписка Azure не требуется .** Корпорация Майкрософт предоставляет инфраструктуру Azure, необходимую для работы облачных компьютеров, и управляет ею.

- **Согласовано с "Никому не доверяй"** - Доступ основан на удостоверениях, устройствах, рабочей нагрузке и сигналах данных, а не на сетевом расположении. Современные безопасные веб-шлюзы (SWG) и средства частного доступа на устройстве хорошо интегрируются с этой моделью.

- **Подключение с высокой пропускной способностью** — Облачные компьютеры имеют высокоскоростное подключение и прямой вход в глобальную сеть Майкрософт для таких служб, как Microsoft 365.

- **Защита по умолчанию** — Разрешены только исходящие подключения, входящее или боковое подключение не допускается. Примените стандартный VPN или SWG на устройстве так же, как это делается с управляемыми ноутбуками.

- **Более простые операции** — Устранение неполадок проще и соответствует современному управлению устройствами с помощью политик Intune, элементов управления безопасностью и встроенных отчетов.

- **Более высокий уровень надежности —** Управляемая стандартизированная сеть снижает риск неправильной настройки и повышает общую надежность облачных компьютеров.

Рекомендации по размещенной сети Майкрософт

Прежде чем выбрать **размещенную сеть Майкрософт**, ознакомьтесь с этими пунктами, чтобы убедиться, что она соответствует вашим целям развертывания.

- **Несовместимо с гибридным присоединением Microsoft Entra.** Эта модель поддерживает только облачные компьютеры и не имеет прямого подключения к локальная служба Active Directory Доменные службы (AD DS). Если вы зависите от групповая политика, перенесите эти политики в Microsoft Intune с помощью каталога параметров, приема ADMX или базовых показателей безопасности.

- **Нет клиентского контроля над виртуальной сетью.** Виртуальная сеть полностью управляется корпорацией Майкрософт. Примените элементы управления исходящим трафиком на **облачном компьютере** (например, правила VPN/SWG на основе устройств, брандмауэр Windows, веб-элементы управления Microsoft Defender для конечной точки) или на выходе из Интернета организации, а не в виртуальной сети.

- **VPN или решение частного доступа, необходимое для доступа к локальным ресурсам.** Используйте решение VPN или частного доступа/ZTNA для доступа к локальным приложениям. Требуется раздельное туннелирование, поэтому трафик RDP и другой трафик службы для Windows 365 не проходит через VPN. Этот шаблон соответствует подходу "Никому не доверяй".

- **Требуется управление на основе облака.** Планируйте современное управление конечными точками с помощью Intune, а не операций, ориентированных на объект групповой политики.

Ограничения сети по умолчанию.

- **Порт 25 (SMTP) заблокирован.**

- **ICMP/ping заблокирован.**

- **Нет бокового (облачного компьютера с облачным компьютером) связи.**

- **Нет прямого входящего подключения к облачным компьютерам.**

- **IP-адресация управляется службой.** Вы не можете выбрать частные диапазоны IP-адресов или пространство адресов NAT для исходящего трафика. Windows 365

автоматически назначает IP-адресацию и управляет ими.

Схема: параметр Размещенная сеть (Майкрософт)

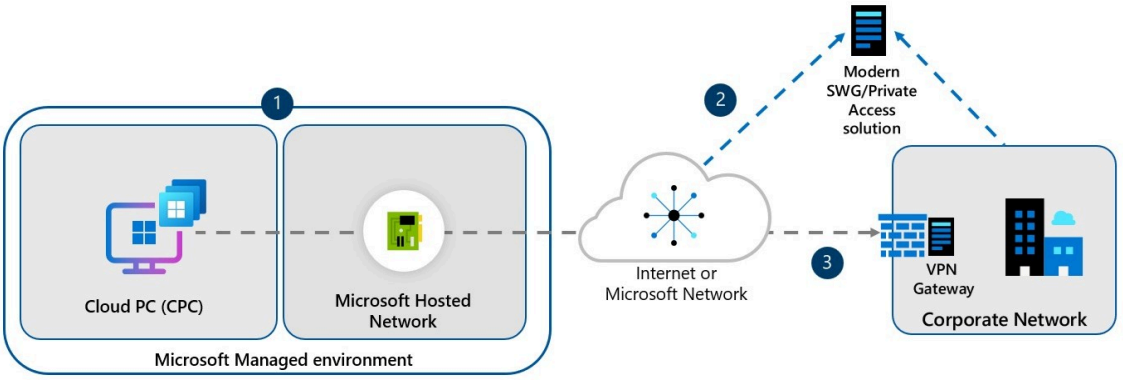


Схема 1. Пример развертывания размещенной сети Майкрософт

На этой схеме показаны три ключевых элемента размещенной сети Майкрософт:

1. Облачный компьютер и его базовое сетевое подключение развертываются в среде, полностью управляемой корпорацией Майкрософт.
2. Исходящим подключением можно управлять с помощью современного безопасного веб-шлюза и решения для частного доступа, развернутого на облачном компьютере.
3. Кроме того, можно использовать традиционный VPN.

Оба 2 & 3 могут быть предоставлены идентичными способами для перемещаемых устройств пользователей.

Вариант развертывания сетевого подключения Azure

Когда следует выбрать сетевое подключение Azure (ANC)

Используйте **ANC** , если у вас есть определенные устаревшие или сетевые требования, которые не могут быть решены, и таким образом предотвратить использование размещенной сети Майкрософт, например:

- **Microsoft Entra требуется гибридное соединение**.
- **Приложениям и службам требуется прямая прямая видимость локальных ресурсов** (например, AD DS, Kerberos/NTLM, общие папки SMB, устаревшие

протоколы).

- **Вы не готовы полностью перейти к модели "Никому не доверяй"**, и вам потребуется больше времени для перехода.
- **Требуется управляемое частным образом подключение** из локальных сетей к облачным компьютерам (например, VPN типа "сеть — сеть", ExpressRoute, фиксированные IP-адреса исходящего трафика, частные DNS).

Рекомендация: Использовать размещенную сеть Майкрософт по умолчанию. Используйте ANC только для пользователей и сценариев, для которых это строго требуется. Обе модели могут работать параллельно.

Что предоставляет ANC

- **Полный элемент управления виртуальная сеть (виртуальная сеть).** Виртуальная сетевая карта облачного компьютера (vNIC) находится в подписке Azure и виртуальной сети. Вы управляете группами безопасности сети (NSG), определяемыми пользователем маршрутами (UDR), таблицами маршрутизации, Брандмауэр Azure, шлюзом NAT и ведением журнала.
- **Прямое подключение к локальной среде.** Используйте VPN-подключение типа "сеть — сеть" или ExpressRoute для доступа к AD DS, общим папкам, серверам печати и локальным приложениям.
- **Поведение в сети.** Расширение корпоративной сети до виртуальной сети позволяет облачным компьютерам работать так, как если бы они были внутри вашей сети.
- **Пиринг с другими виртуальными сетями.** Пиринг между виртуальными сетями облачного компьютера с другими виртуальными сетями Azure и напрямую обращаться к ресурсам, размещенным в Azure (в том числе через Приватный канал, если применимо).

Компромиссы и обязанности

Выбор ANC переключит ответственность за сеть на вашу команду и повышает сложность:

- **Требуется подписка Azure.** Все сетевые сети находятся в вашей подписке (и выставляются счета за нее).
- **Вы владеете проектированием и операциями.** Вы несете ответственность за адресацию, маршрутизацию, DNS, элементы управления безопасностью, ведение журнала, высокий уровень доступности и аварийное восстановление для

виртуальных сетевых устройств (NVA), установку исправлений, управление емкостью и изменениями.

- **Более высокий профиль затрат.** Ваша организация несет ответственность за расходы на пропускную способность сети, виртуальные сетевые устройства (NVA), Брандмауэр Azure, шлюз NAT и хранилище журналов в дополнение к затратам на персонал для контроля инфраструктуры подключения.
- **Более длинные временные шкалы.** Дополнительные предварительные требования и утверждения обычно значительно расширяют развертывание по сравнению с размещенной сетью Майкрософт.
- **Более высокий риск неправильной настройки.** Более движущиеся части могут привести к более высокому риску подключения или проблемам с производительностью, если не тщательно управлять.

Схема: параметр "Сетевое подключение Azure"

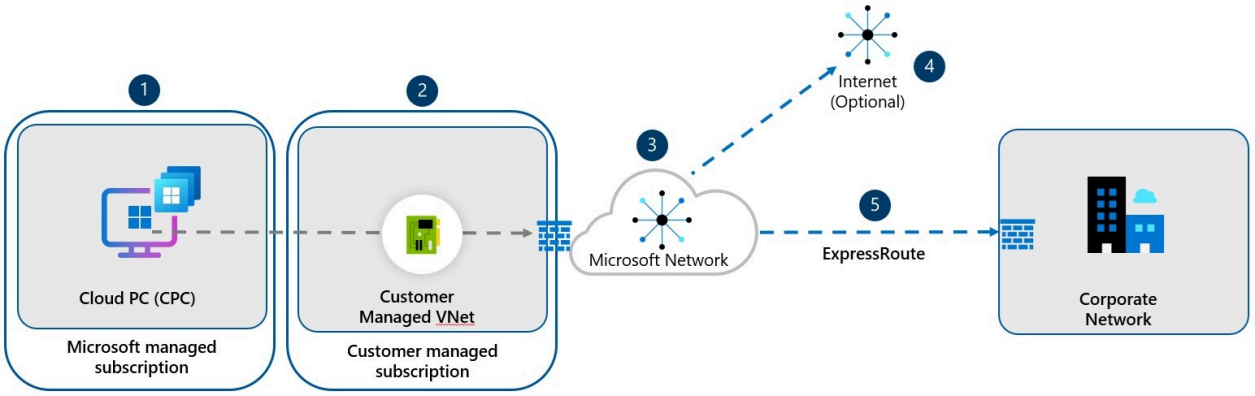


Схема 2. Пример развертывания ANC

Ключевые элементы, показанные на этой схеме:

1. **Облачный компьютер** развертывается в среде Azure, управляемой корпорацией Майкрософт.
2. В развертываниях **сетевого подключения Azure (ANC)** сетевой интерфейс облачного компьютера помещается в управляемую клиентом **виртуальную сеть в** рамках подписки клиента. Клиент несет ответственность за предоставление всех необходимых сетевых подключений к этой виртуальной сети.
3. **Подключение к службе** должно направляться непосредственно в сеть Майкрософт. Не следует направлять этот трафик через локальные точки исходящего трафика.

4. Высокоскоростное подключение к Интернету можно предоставить непосредственно из Azure. Такой подход обеспечивает значительно более высокую производительность, чем маршрутизация через локальные расположения исходящего трафика.

5. Используйте ExpressRoute или VPN типа "сеть — сеть" для подключения виртуальной сети к корпоративной сети.

Варианты одновременного развертывания

Вы можете запустить размещенную сеть Майкрософт и сетевое подключение Azure (ANC) параллельно. Используйте ANC только для подмножества пользователей или рабочих нагрузок, которые имеют строгие устаревшие потребности, например для финансовой команды, для которых требуется прямая видимость локальных данных. Для всех остальных пользователей, не имеющих этих требований, используйте размещенную сеть Майкрософт, чтобы свести к минимуму сложность, затраты и время.

Сравнение вариантов развертывания

Развернуть таблицу

Категория	Размещенная сеть Майкрософт	Сетевое подключение Azure (ANC)
Рекомендуемый вариант использования	Вариант по умолчанию и предпочтительный параметр для большинства пользователей	Только для устаревших или определенных вариантов использования, требующих локального доступа
Управление инфраструктурой	Полностью управляется корпорацией Майкрософт	Управляется клиентом
Требуется подписка Azure	Нет	Да
Сложность развертывания	Низкий — требуется минимальная настройка	Высокий — требуется настройка виртуальных сетей, брандмауэров, маршрутизации и т. д.
Масштабируемость	Высокий — автоматический и гибкий	Ограниченный — зависит от инфраструктуры, управляемой клиентом.
Модель безопасности	Выравнивание "Никому не доверяй"	Традиционная модель сетевого доверия

Категория	Размещенная сеть Майкрософт	Сетевое подключение Azure (ANC)
Подключение к локальной среде	Требуется VPN или SWG	Прямая прямая видимость через VPN-подключение типа "сеть — сеть" или ExpressRoute. Или VPN-подключение типа "точка — сеть" или SWG
Последствия для затрат	Отсутствие затрат на сетевую инфраструктуру или управление	Затраты на инфраструктуру, исходящий трафик и управление сетью
Устранение неполадок с надежностью &	Проще и надежнее благодаря управляемой настройке	Более сложный и склонный к неправильной настройке
Примеры вариантов использования	Облачные пользователи, удаленные сотрудники, современное управление удостоверениями	Пользователи гибридного присоединения, устаревшие приложения, нуждающиеся в прямом доступе к локальным ресурсам
Ограничения	Не контролирует диапазоны IP-адресов или базовую сеть.	Требуется опыт работы с сетями Azure, более длительные сроки развертывания

Общие сведения о сетевых потоках — протоколе удаленного рабочего стола

17.10.2025

Чтобы обеспечить оптимальную производительность и надежность развертывания Windows 365, важно понимать основные требования к подключению. Эти требования делятся на три основные категории:

- **Подключение по протоколу удаленного рабочего стола (RDP)** — применяется в равной степени как к облачной среде, так и к физическим клиентским устройствам.
- **Подключение к облачной службе** — охватывает требования к сети от самого облачного компьютера к службе.
- **Подключение к клиентскому устройству** — включает конфигурацию сети для физических конечных точек, обращающихся к службе.

Правильная настройка каждого элемента подключения необходима для обеспечения простого Windows 365 взаимодействия. В этом документе рассматриваются доступные варианты подключения по протоколу RDP и способы их оптимизации для обеспечения максимальной производительности и надежности.

> ⓘ **Примечание**
>
> Подключение по протоколу RDP требует особого внимания. Одни и те же принципы конфигурации применяются как к размещенным в облаке, так и к физическим устройствам.

Подключение по протоколу RDP

Подключение по протоколу RDP является критически важным компонентом Windows 365 взаимодействия. Это позволяет пользователям легко подключаться к облачным компьютерам и требует тщательной настройки сети для обеспечения производительности и надежности.

Характеристики трафика RDP

Трафик RDP имеет несколько важных элементов, требующих особого внимания:

- **С учетом задержки:** Трафик RDP должен быть доставлен с минимальной задержкой. Хотя RDP и опытен в решении сложных сетевых условий, оптимизация для как можно более низкой задержки помогает поддерживать адаптивный пользовательский интерфейс.
- **В режиме реального времени:** Как и трафик мультимедиа Microsoft Teams, трафик RDP работает в режиме реального времени. Любая задержка может нарушить сеанс пользователя.

- **Большой объем:** Сеансы RDP могут генерировать значительный объем трафика. Эффективная маршрутизация этого трафика и предотвращение дорогостоящих операций, таких как проверка TLS, помогает сохранить производительность и предотвратить перегрузку сетевых устройств.
- **Долговечный:** Подключения RDP часто остаются активными в течение длительного периода времени. Эффективная маршрутизация снижает влияние на устройства, выполняющие преобразование сетевых адресов (NAT), и поддерживает масштабируемость.

Чтобы обеспечить высококачественный пользовательский интерфейс, трафик RDP должен направляться по наиболее прямому и эффективному пути к глобальной инфраструктуре Майкрософт. Важно обеспечить предотвращение ненужных проверок, фильтрации или обходов.

> ⓘ **Важно!**
>
> Сбой оптимизации трафика RDP может привести к снижению производительности, нестабильности сеанса и низкой надежности для конечных пользователей.

Традиционные RDP и Windows 365 RDP

Windows 365 использует модернизированную версию протокола удаленного рабочего стола (RDP), предназначенную для облачных сред и предназначенную для обеспечения безопасного и простого взаимодействия с различными сетевыми условиями. Этот современный протокол RDP значительно отличается от RDP, используемого в традиционных средах удаленных рабочих столов.

Традиционный протокол RDP

Традиционный протокол RDP, обычно используемый в локальных средах, использует входящее подключение через tcp-порт 3389 для создания сеансов удаленного рабочего стола. Этот подход вызывает проблемы безопасности, так как он требует открытия входящих портов в периметре сети.

Современный протокол RDP в Windows 365

Windows 365 использует современную облачную реализацию RDP, которая значительно отличается от традиционных моделей. Он не требует входящего подключения и использует исходящий трафик по следующим протоколам и портам, которые должны работать в любой правильно настроенной сети:

- **TCP-порт 443**
- **UDP-порт 3478**

Эти подключения устанавливаются с облачного компьютера и клиентского устройства к глобальной инфраструктуре подключения Майкрософт. Другие методы подключения RDP также могут быть доступны в зависимости от среды. Они также описаны в этой статье.

Эта современная модель RDP повышает безопасность, упрощает развертывание и поддерживает надежное удаленное отображение и ввод данных в различных условиях сети.

> ⓘ **Важно!**
>
> Windows 365 не использует традиционный протокол RDP. Для доступа к облачному компьютеру не требуется входящее подключение.

Методы подключения RDP в Windows 365

Windows 365 поддерживает несколько методов подключения по протоколу RDP для обеспечения надежной производительности даже в сложных условиях сети. Эти методы можно разделить на варианты подключения к общедоступной и частной сети.

Методы подключения к общедоступной сети

Windows 365 поддерживает следующие варианты общедоступного подключения. По умолчанию для службы используются следующие методы:

- **Обратное подключение на основе TCP:** Это основной метод для всех подключений. Для установки сеанса используется исходящий протокол RDP через TCP-порт 443.
- **Ретрансляция RDP на основе RDP Shortpath:** Этот метод использует исходящий RDP через UDP-порт 3478 и подключается через инфраструктуру ретранслятора Майкрософт для повышения производительности мультимедиа.
- **Direct UDP-based RDP Shortpath:** Этот параметр устанавливает прямое подключение "один к одному" через UDP, уменьшая задержки и повышая скорость реагирования. Этот метод использует сервер STUN для поиска рабочего пути прямого подключения между пользователем и его облачным компьютером.

Метод подключения к частной сети

1. **Прямая UDP через частные сети** Включает UDP-подключение "один к одному" через частную сеть. Этот метод применим только для развертываний с использованием сетевого подключения Azure (ANC). Этот метод технически может быть возможен через VPN-каналы, но вряд ли будет выбран в качестве транспортного варианта Windows 365 из-за низкой производительности.

> ⓘ **Примечание**
>
> Корпорация Майкрософт автоматически выбирает наиболее оптимальный метод в зависимости от условий сети и типа развертывания. Для большинства сценариев не требуется настраивать вручную. Windows 365 поддерживает несколько методов подключения по

протоколу RDP для обеспечения надежной производительности даже в сложных условиях сети.

Подключение по протоколу RDP общедоступной сети

Обратное подключение на основе TCP

Обратное подключение — это метод по умолчанию, используемый для подключений по протоколу RDP в Windows 365. Он инициирует исходящее подключение через TCP-порт 443 и не требует прослушивателя ни на стороне клиента, ни на стороне облачного компьютера. Такой подход упрощает развертывание и повышает безопасность, устраняя потребность в входящих подключениях, и используется для каждого подключения независимо от используемого метода.

Принцип работы обратного подключения

1. **Установка агента RD:** Во время подготовки агент RD устанавливается на облачном компьютере для управления подключением.
2. **Сеанс постоянной сигнализации:** При запуске агент удаленных рабочих столов устанавливает постоянный исходящий сеанс передачи сигналов с шифрованием TLS в инфраструктуру Windows 365. Этот процесс выполняется автоматически и не требует настройки вручную.
3. **Вход пользователя:** На физическом клиентском устройстве пользователь входит в систему с помощью поддерживаемого клиента, например Windows App.
4. **Проверка подлинности:** Microsoft Entra идентификатор проверяет подлинность пользователя и возвращает маркер, перечисляющий доступные ресурсы пользователя.
5. **Проверка маркера.** Клиент передает маркер в службу подписки канала, которая проверяет его.
6. **Перечисление ресурсов:** Служба возвращает список доступных облачных компьютеров для пользователя в виде конфигураций подключения с цифровой подписью.
7. **Хранилище конфигурации подключения:** Клиент сохраняет эти конфигурации в виде `.rdp` файлов для каждого ресурса.
8. **Инициация подключения:** Когда пользователь выбирает облачный компьютер, клиент подключается к Azure Front Door (AFD) через прослушиватель anycast. Ближайший узел AFD выбирается автоматически в зависимости от исходящего сетевого трафика.
9. **Выбор шлюза:** AFD оценивает задержку для всех доступных шлюзов и выбирает тот, с наименьшей задержкой и наименьшим количеством активных подключений.

10. **Безопасное подключение к шлюзу.** Клиент подключается к выбранному шлюзу с помощью безопасного подключения TLS 1.3. Шлюз проверяет запрос и связывается с брокером.

11. **Оркестрация брокера:** Брокер определяет целевой облачный компьютер и использует существующий сигнальный канал для запуска сеанса.

12. **Подключение узла сеансов:** Стек удаленного рабочего стола на облачном компьютере инициирует исходящее подключение TLS 1.3 к тому же экземпляру шлюза.

13. **Ретранслятор данных:** После подключения обеих конечных точек шлюз передает данные между ними и формирует базовый транспорт Reverse Connect с помощью вложенного туннеля и максимальной взаимно поддерживаемой версии TLS (до TLS 1.3).

14. **Подтверждение RDP** Клиент начинает подтверждение RDP, чтобы установить сеанс.

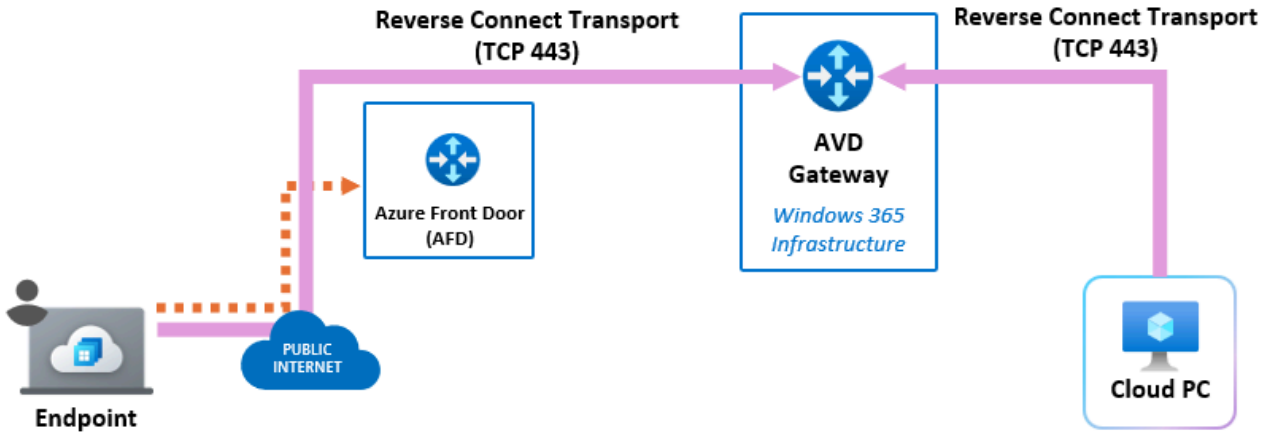


Схема 1. Обратное подключение RDP через TCP-порт 443

Direct UDP-based RDP Shortpath (Using STUN)

Windows 365 также использует подключение RDP на основе UDP для повышения производительности сеанса, надежности и пропускной способности. После установки сеанса обратного подключения на основе TCP Windows 365 пытается обновить транспорт до UDP одним из двух способов:

- **Direct RDP Shortpath:** Устанавливает одно-к-одному UDP-подключение с помощью STUN для упрощения.
- **Ретрансляция RDP Shortpath:** Использует TURN для ретрансляции трафика UDP через известный IP-адрес и порт.

Принцип работы Shortpath с прямым UDP

1. **Начальное TCP-подключение:** Сеанс RDP начинается через транспорт обратного подключения на основе TCP через шлюз, как описано в этом документе.

2. **Создание сокета UDP:** Если RDP Shortpath включен на облачном компьютере (включен по умолчанию), служба создает сокеты UDP во всех жизнеспособных сетевых интерфейсах.

3. **Обнаружение STUN:** Облачный компьютер пытается подключиться к серверу STUN Windows 365 через UDP-порт 3478. Это временное подключение определяет внешний IP-адрес и порт устройства NAT. Трафик RDP не направляется через сервер STUN.

4. **Обмен кандидатами:** Облачный компьютер предоставляет клиенту сведения о своих потенциальных IP-адресах и портах через установленный сеанс TCP. Клиент также отправляет собственный список кандидатов.

5. **Попытка подключения:** Обе конечные точки пытаются установить прямое UDP-подключение одновременно. Так как оба инициируют исходящий трафик, этот метод часто завершается успешно даже через ограничивающие брандмауэры с поддерживаемым типом NAT.

6. **Оценка транспорта.** Если прямое подключение выполнено успешно и определено как самый быстрый путь, все динамические виртуальные каналы, такие как графика, ввод и перенаправление устройств, переключитесь на новый транспорт UDP.

7. **Перейти к TURN:** Если установить подключение на основе STUN невозможно, система пытается подключиться к серверам TURN через UDP-порт 3478. Это обеспечивает ретрансляционное подключение UDP, которое имеет более высокий показатель успешности в различных условиях сети из-за возможности работать с любым типом NAT и известной IP-подсетью & портом.

> ⓘ **Примечание**
>
> Этот метод подключения не проходит через сервер STUN. Сервер STUN используется только на начальном этапе подключения для определения конфигурации NAT с обеих сторон и включения подключения "один к одному".
>
> RDP Shortpath на основе UDP повышает производительность и надежность. Он автоматически выполняет попытки после обратного подключения на основе TCP и не требует настройки вручную, кроме оптимизации трафика.

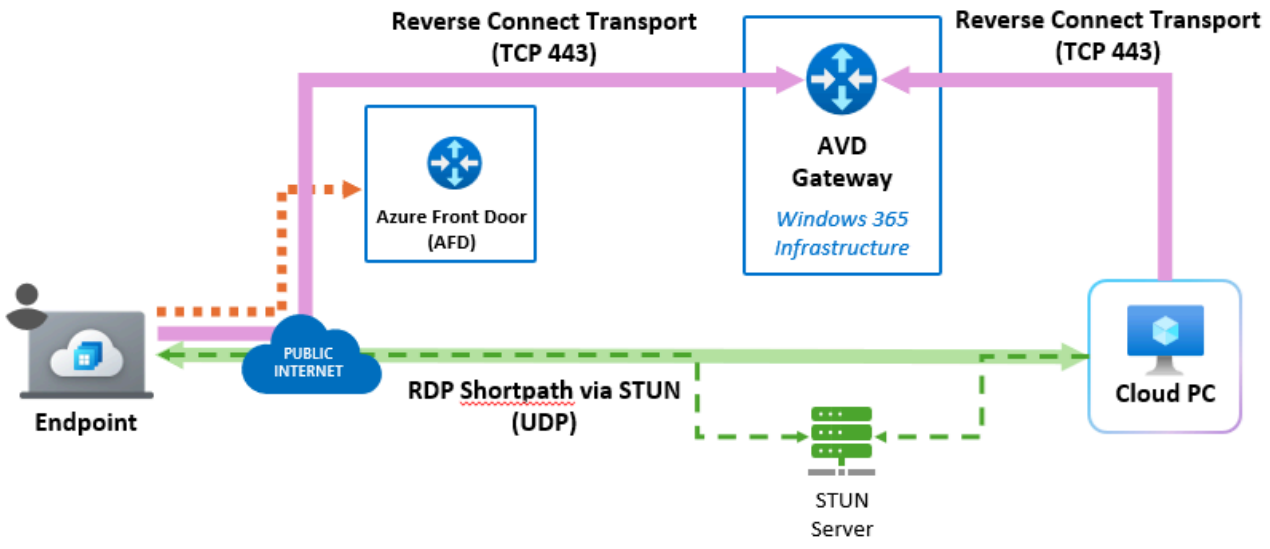


Схема 2. Подключение RDP к RDP Shortpath с помощью STUN

Известные проблемы с Direct RDP Shortpath (использование STUN)

Direct RDP Shortpath использует STUN для установки UDP-подключения "один к одному". Хотя этот метод обеспечивает значительные преимущества производительности по сравнению с подключением RDP на основе TCP, он может не быть успешным в некоторых сетевых средах из-за ограничений в поведении NAT и конфигурациях брандмауэра. Чтобы эта модель подключения была успешной, тип NAT в сетях физического устройства и облачного компьютера должен иметь поддерживаемый тип.

Также часто бывает сложно заранее определить IP-адреса, необходимые для этого типа подключения, например при настройке обхода VPN или безопасного веб-шлюза (SWG) для удаленных пользователей.

Сценарии, в которых direct RDP Shortpath может завершиться сбоем

Прямое подключение может не работать в следующих условиях, многие из которых распространены в корпоративных сетях:

- **Двойной NAT:** Например, трафик, направляемый через безопасный веб-шлюз (SWG) или прокси-сервер, дважды применяет преобразование сетевых адресов (NAT), один раз на исходящий трафик Azure и снова в конечной точке VPN или SWG.
- **Интернет-прокси или устройства проверки:** Маршрутизация через прокси-серверы или устройства, проверяющие трафик, может помешать подключению на основе STUN. Обход этих устройств может быть затруднительным из-за отсутствия знаний об IP-адресе NAT.
- **Симметричное NAT:** Как правило, в корпоративных сетях симметричный NAT на облачном компьютере или на стороне клиента предотвращает успешное согласование STUN. Шлюз NAT

Azure использует этот тип NAT, как и многие другие распространенные корпоративные устройства NAT.

- **Ограниченный доступ UDP:** Сети, которые блокируют или ограничивают трафик UDP или ограничивают доступ к определенным портам или диапазонам IP-адресов, предотвращают прямое подключение и часто используются в корпоративных сетях. Обход этого ограничения затруднен из-за отсутствия предварительного знания о портах и IP-адресах, используемых для подключения.
- **NAT класса носителя (CGN):** Если несколько сетей совместно используют общедоступный IP-адрес, STUN не может установить уникальный путь.

Из-за этих ограничений относитесь к этому методу как к оптимальному подходу и избегайте значительных усилий, чтобы заставить его работать. Вместо этого определите приоритеты оптимизации ретранслятора UDP через TURN, который надежно работает почти во всех сетевых условиях.

Дополнительные сведения о краткой инструкции по протоколу RDP см. здесь.

> **Совет**
>
> Используйте **средство avdnettest**, чтобы проверка тип NAT, используемый в сетевой среде.

Использование ретранслятора RDP Shortpath

Из-за этих ограничений Direct RDP Shortpath — это наиболее подходящая модель подключения. Если его не удается установить, Windows 365 автоматически возвращается к ретранслятору RDP Shortpath, который использует серверы TURN и имеет значительно более высокий показатель успешности. Этот метод работает надежно, так как требования к подсети и портам для исходящего трафика известны заранее и поэтому могут быть открыты и легко оптимизированы.

> **Примечание**
>
> Ретрансляция RDP Shortpath обеспечивает согласованное подключение в более широком диапазоне сетевых условий, а также не требует входящего доступа.

Ретрансляция RDP shortpath на основе UDP (с помощью TURN)

Ретрансляция RDP Shortpath предоставляет надежный метод подключения по протоколу RDP на основе UDP, если прямой Shortpath невозможен. Этот метод использует глобально распределенные серверы TURN в инфраструктуре Майкрософт для ретрансляции трафика RDP между клиентом и облачным компьютером. Эта модель подключения работает автоматически и не

требует никакой конфигурации, кроме оптимизации требуемого трафика. Очень важно, чтобы этот метод подключения был настроен и оптимизирован в сетевых средах.

Основные преимущества

- **Обход ограничений NAT:** В отличие от прямых подключений на основе STUN, ретрансляторы TURN не зависят от двойного NAT, симметричного NAT или ограничений брандмауэра.
- **Глобальный охват:** Серверы TURN развернуты в более чем 47 регионах по всему миру, что позволяет передавать трафик через расположение, близкое к пользователю, для оптимальной производительности.
- **Предсказуемая конфигурация:** Ретрансляемый трафик использует известные IP-подсети и порты, что обеспечивает оптимизацию брандмауэра и сети, включая прокси-сервер, безопасный веб-шлюз (SWG) и обход VPN.

Как работает ретрансляция RDP Shortpath

- **Обратное подключение на основе TCP:** Сеанс RDP начинается через TCP-порт 443 с помощью метода Обратного подключения.
- **Прямая попытка RDP Shortpath:** Система пытается установить прямое UDP-подключение с помощью STUN.
- **Настройка подключения TURN:** В случае сбоя прямого подключения клиент и облачный компьютер пытаются подключиться к инфраструктуре TURN через UDP-порт 3478, в частности, для выделенной подсети 51.5.0.0/16.
- **Оценка транспорта.** Если ретрансляция подключения выполнена успешно и определена как самый быстрый путь, все динамические виртуальные каналы, такие как графика, ввод и перенаправление устройств, переключитесь на новый транспорт.
- **Сохраняемость TCP:** Если метод UDP не выполнен успешно, сеанс RDP продолжается через существующее TCP-подключение.
- **RDP Multipath:** При использовании RDP Multipath установлено несколько UDP-подключений, чтобы обеспечить непрерывное непрерывное подключение при возникновении проблем в активном пути.

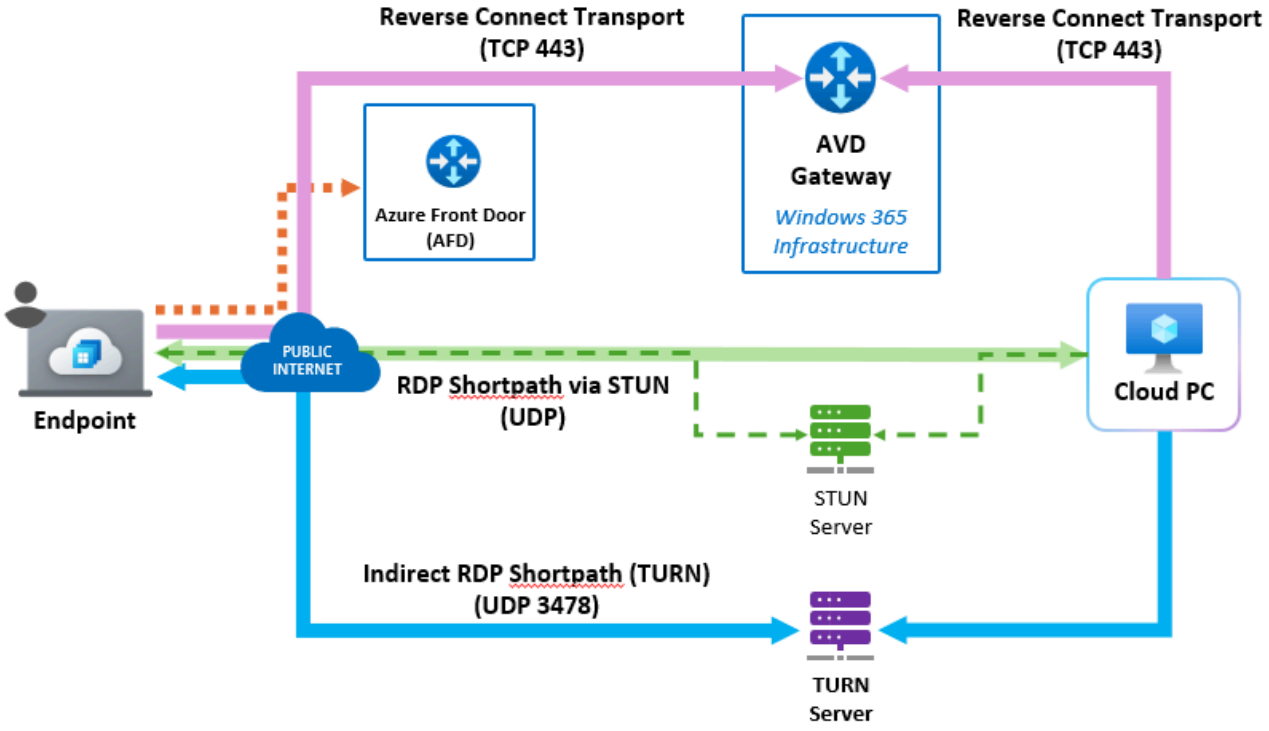


Схема 3. Все параметры общедоступного RDP

> ⓘ **Примечание**
>
> Ретрансляция RDP Shortpath включается автоматически и не требует настройки вручную. Это обеспечивает согласованное подключение к широкому спектру сетевых сред. Дополнительные сведения о краткой дорожке по протоколу RDP для общедоступных сетей можно найти здесь.

Подключение по протоколу RDP частной сети

RDP Shortpath для управляемых сетей

Windows 365 поддерживает четвертый метод подключения по протоколу RDP для управляемых частных сетей. Этот параметр доступен только в определенных сценариях развертывания и обеспечивает прямое UDP-подключение между клиентским устройством и облачным компьютером.

> ⓘ **Важно!**
>
> Этот метод не требуется для обеспечения высокопроизводительного подключения к службе. Основными методами и методами по умолчанию являются открытые методы, описанные в этой статье.

Условия доступности

RDP Shortpath для управляемых сетей поддерживается только в следующих случаях:

- В развертывании используется сетевое подключение Azure (ANC). Этот метод подключения недоступен для развертываний сети, размещенных в Майкрософт.
- Между физическим устройством и облачным компьютером существует **прямая линия видимости** через ExpressRoute или VPN-подключение типа "сеть — сеть".
- Сетевой путь позволяет трафику успешно проходить. Правила брандмауэра должны разрешать необходимые порты, протоколы и диапазоны IP-адресов.

Методы подключения

Это подключение можно установить одним из двух способов:

1. **Прослушиватель Shortpath по протоколу RDP:** После настройки облачный компьютер прослушивает UDP-порт 3390 для входящих подключений.
2. **ICE/STUN Discovery:** Если метод прослушивателя не является жизнеспособным, ice/STUN используется для обнаружения доступных IP-адресов и согласования динамического порта. При необходимости диапазон портов можно настроить.

После успешного установления UDP-подключения общедоступный путь на основе TCP удаляется, и сеанс продолжается через частную сеть.

Дополнительные сведения см. в документации по RDP Shortpath для частных сетей.

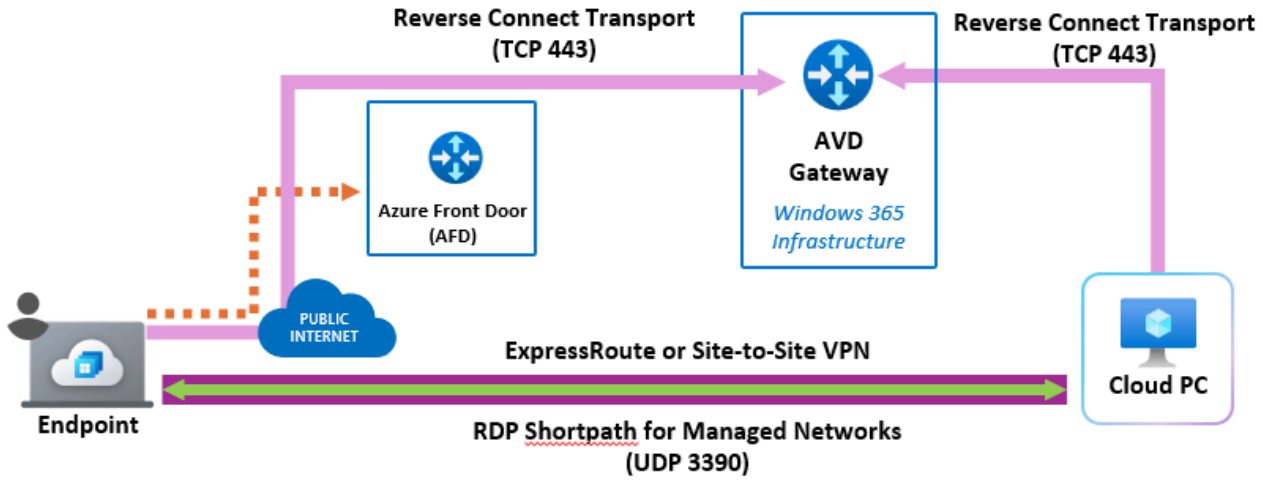


Схема 4. RDP Shortpath для частных сетей

> ⓘ **Примечание**
>
> Этот метод обеспечивает прямое подключение в управляемых сетевых средах, но требует определенных конфигураций и сетевых условий. Для установки этого типа подключения по-

прежнему требуется открытый метод на основе TCP.

RDP Multipath

RDP Multipath — это инновационное улучшение подключения для Windows 365, которое повышает надежность и производительность сеанса за счет интеллектуального управления несколькими сетевыми путями. Он основан на RDP Shortpath и использует интерактивное создание подключения (ICE) для обнаружения и оценки нескольких маршрутов UDP в режиме реального времени, в том числе с использованием протоколов STUN и TURN.

Эта функция гарантирует, что если активный путь становится нестабильным или сбоем, система автоматически переключается на путь резервного копирования, не прерывая сеанс пользователя. Маршрутизация с несколькими маршрутами особенно полезна в средах с изменяющимися сетевыми условиями, обеспечивая более плавный и более устойчивый интерфейс удаленного рабочего стола.

Подробные сведения см. в документации по RDP Multipath.

Сводка по методу подключения RDP

В следующей таблице приведена сводка методов RDP, доступных для безопасного подключения к облачному компьютеру.

Убедитесь, что вы проверка на странице Требования к сети полные требования к подключению.

Развернуть таблицу

Метод RDP	Протокол или порт	Полное доменное имя	IP	Метод общедоступной и частной сети	Примечания
TCP RDP (обратное подключение)	TCP/443	*.wvd.microsoft.com	40.64.144.0/20 охватывает элемент подключения RDP в этом домене	Общедоступное	Протокол RDP на основе TCP, ретранслируемый через глобальную инфраструктуру шлюза RDP корпорации Майкрософт. Во всех случаях используется метод первоначального подключения.

Метод RDP	Протокол или порт	Полное доменное имя	IP	Метод общедоступной и частной сети	Примечания
Непрямая UDP RDP (RDP через TURN)	UDP/3478	н/д	51.5.0.0/16	Общедоступное	RDP на основе UDP, ретранслируется через глобальную инфраструктуру TURN корпорации Майкрософт. Работает в любом сетевом сценарии, если доступны необходимые конечные точки.
Прямая маршрутизация по протоколу RDP с помощью STUN	UDP/1024-65535 (по умолчанию 49152-65535)	н/д	51.5.0.0/16 для элемента STUN. Общедоступный IP-адрес NAT, используемый по обе стороны подключения	Общедоступное	Не во всех сетевых сценариях. Требуется открытый доступ к любому общедоступному IP-адресу, если IP-адрес NAT не известен заранее.
RDP Shortpath для управляемых сетей	UDP/3390 (настраиваемый)	н/д	Частные IP-адреса физического клиента и облачного компьютера	Частный	Требуется прямая линия видимости между физическим устройством и облачным компьютером. Возможно только при развертывании ANC.
RDP Shortpath для управляемых сетей, использующих ICE/STUN	UDP/1024-65535 (по умолчанию 49152-65535)	н/д	51.5.0.0/16 для STUN, а затем частный IP-адрес физического устройства и облачного компьютера	Частный	Требуется доступ к диапазону серверов STUN, а также прямая линия видимости между физическим устройством и облачным компьютером. Возможно только при

Метод RDP	Протокол или порт	Полное доменное имя	IP	Метод общедоступной и частной сети	Примечания
					развертывании ANC

Определение используемого транспорта RDP.

Дополнительные сведения о том, как определить, какой метод транспорта используется для определенного подключения, см. в статье Проверка работы RDP Shortpath.

Оптимизация трафика RDP

Трафик протокола удаленного рабочего стола (RDP) имеет решающее значение для Облачный компьютер Windows 365 производительности и надежности. Чтобы оптимизировать подключение, необходимо настроить сетевой путь как на физическом устройстве, так и на облачном компьютере. Трафик RDP ведет себя как трафик мультимедиа Teams: он работает в режиме реального времени, учитывает задержки и большой объем с длительными подключениями. Таким образом, методы оптимизации тесно зеркало методами, используемыми для Teams.

Хотя в этом руководстве рассматриваются следующие основные методы RDP, которые работают во всех сетевых средах, они также применимы к любому доступному параметру.

- Обратное подключение на основе TCP
- Непрямая RDP Shortpath через TURN

Дополнительные сведения о различных параметрах RDP, доступных для Windows 365, и о том, как они работают, см. в статье Общие сведения о сетевых потоках — подключение RDP.

Если трафик RDP не оптимизирован, сетевой путь по умолчанию для веб-трафика во многих корпоративных сетях может значительно повлиять на взаимодействие с пользователем. Ниже перечислены распространенные проблемы.

- Снижение производительности
- Частые отключения
- Отключения во время первоначального входа
- Медленный входной ответ

Действия по оптимизации применяются как к физическому клиенту, так и к облачному компьютеру с незначительными различиями в реализации.

Основные этапы оптимизации

1. Отключение проверки TLS

Проверка трафика RDP не поддерживается. Отключите проверку TLS для всех необходимых конечных точек.

Зачем отключать проверку TLS?

- **Двойное шифрование**: трафик RDP использует вложенное шифрование. Транспортный сеанс TLS 1.3 (DTLS с UDP) имеет зашифрованный сеанс RDP. Проверка сеанса транспорта не обеспечивает никаких преимуществ в области безопасности, но оказывает значительное негативное воздействие.

- **Выделенная инфраструктура**: RDP на основе TCP через шлюзы и UDP через ретрансляторы TURN используют глобально распределенную инфраструктуру Майкрософт. Эта инфраструктура использует выделенное пространство IPv4 исключительно для Windows 365, Azure Виртуального рабочего стола и Devbox.

- **Не влияет на безопасность**: RDP подключает только физическое устройство к облачному компьютеру. Вы по-прежнему можете проверить интернет-трафик на обоих устройствах в соответствии с обычными стандартами.

Влияние инспекции

- **Добавляет дрожание:** Изменение времени поступления пакетов снижает качество.

- **Добавляет задержку:** Увеличенное время обхода пакетов влияет на скорость реагирования рабочего стола.

- **Снижает пропускную способность:** Из-за характера проверки TLS она может значительно снизить пропускную способность подключения, что влияет на производительность.

- **Увеличивает нагрузку на устройство:** Трафик RDP является большим. Проверка является вычислительным ресурсоемким и может привести к ухудшению другого трафика с помощью устройства, выполняющего проверку. Масштабирование для обработки проверки повышает затраты без преимуществ.

2. Обход туннелей VPN и безопасного веб-шлюза

Многие развертывания Windows 365 и Azure виртуальных рабочих столов (AVD) используют клиенты виртуальной частной сети (VPN) или защищенного веб-шлюза (SWG) для обеспечения безопасного доступа к локальным ресурсам и защищенного доступа к Интернету. Такая конфигурация особенно распространена в рекомендуемой модели размещенной сети Майкрософт , где облачные компьютеры имеют прямое высокоскоростное подключение к Интернету и где применяемые сетевые элементы управления могут быть практически идентичны элементам управления, используемым для перемещаемых пользователей.

Современные решения SWG соответствуют принципам "Никому не доверяй" и, как правило, превосходят традиционные подходы к VPN, которые направляют интернет-трафик через локальные прокси-серверы. Однако эти решения по-прежнему представляют проблемы для трафика с учетом задержки, например RDP.

Если туннели VPN или SWG настроены неправильно, пользователи могут столкнуться с:

- Увеличение задержки и снижение производительности
- Отключения во время первоначального входа
- Сеанс удаляется при сбросе туннелей
- Частое отключение RDP

Пример проблемы: подключение RDP падает при первоначальном входе:

Распространенный симптом трафика по протоколу RDP, направляемого через безопасный веб-шлюз (SWG) или VPN-туннель, заключается в отключении во время первоначального входа в облачный компьютер, когда включены туннели на основе пользователей.

Что происходит

- Пользователь запускает подключение, и облачный компьютер отвечает. Экран входа отображается в обычном режиме.
- После ввода учетных данных клиентское программное обеспечение создает туннели на основе пользователей в SWG или VPN.
- На этом этапе экран входа зависает. Подключение падает, и клиент должен повторно подключиться к облачному компьютеру.
- После повторного подключения сеанс обычно работает без дополнительных проблем. Однако если туннель удаляется позже, удаленный сеанс снова отключается.

Это приводит к плохому взаимодействию, особенно при первоначальном входе.

Почему происходит отключение

Туннели на основе пользователей часто направляют весь трафик, связанный с Интернетом, через SWG или VPN, если конечная точка не настроена для обхода. Эта

конфигурация называется принудительным туннелем или обратным разделенным туннелем, и туннель становится путем по умолчанию.

Первоначальный вход завершается успешно, так как туннель еще не активен. Когда туннель запускается при входе пользователя, трафик RDP перенаправляется в туннель, что приводит к повторному подключению. Если туннель удаляется и повторно подключается во время работы, сеанс RDP также должен повторно подключиться внутри восстановленного туннеля.

На следующей схеме показано упрощенное представление этого косвенного подключения с принудительным туннелем. Трафик RDP проходит через ресурсы VPN или SWG до достижения шлюза. Эта маршрутизация допустима для общего веб-трафика, но не является оптимальной для трафика с учетом задержки, такого как мультимедиа Teams или RDP. На стороне облачного компьютера отсутствие оптимизации также означает, что трафику RDP может потребоваться покинуть сеть Майкрософт и снова пройти из расположения РЕШЕНИЯ SWG или VPN.

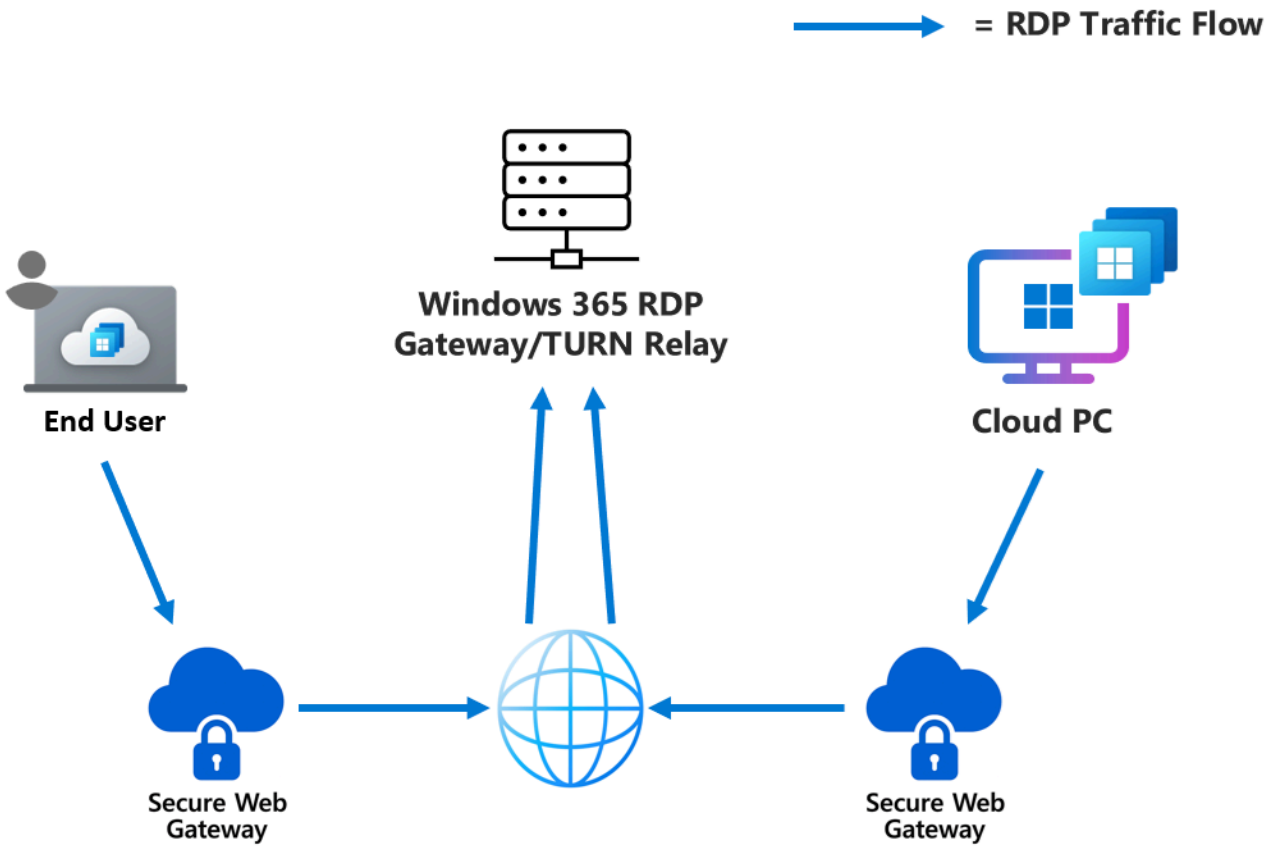


Схема 1. Неоптимизированный трафик RDP, закрепленный через Безопасный веб-шлюз

Решение: обход трафика RDP из vpn-туннелей или туннелей SWG

Исключения принудительного туннеля для трафика RDP имеют важное значение. Эта конфигурация обеспечивает следующее:

- **Прямая маршрутизация трафика с учетом задержки** для поддержания согласованной и высокой производительности
- **Отсутствие зависимости от состояния туннеля** для надежного подключения

На стороне облачного компьютера трафик остается в сети Майкрософт и не должен проходить через Интернет.

После обхода трафик, связанный с интернетом, по-прежнему использует туннель SWG или VPN, но RDP принимает оптимизированный путь, как показано на следующей схеме.

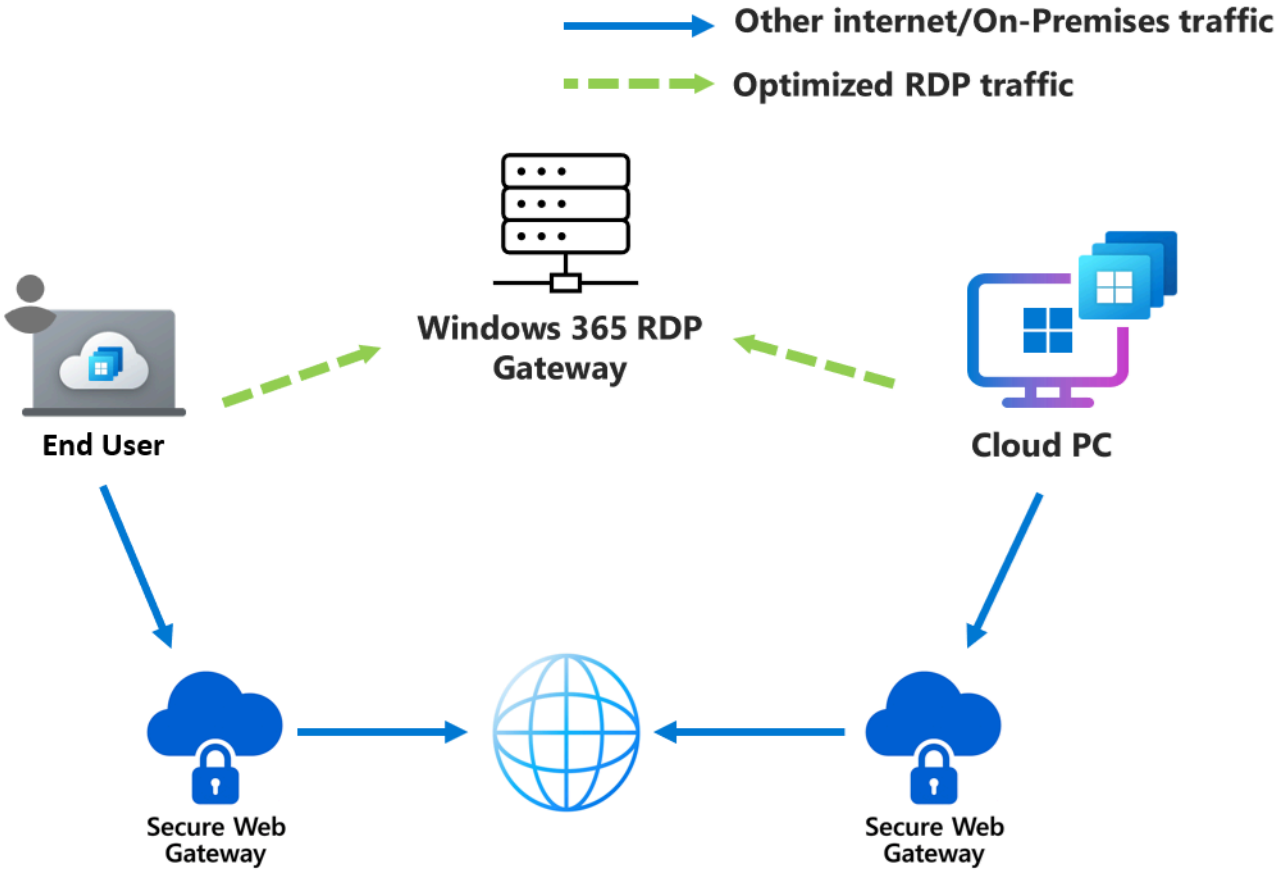


Схема 2. Оптимизированный трафик RDP на основе TCP, отправленный напрямую в шлюз Windows 365

3. Исходящий трафик локальной сети

Локальный исходящий трафик является ключевым шагом в оптимизации трафика RDP. Это гарантирует, что трафик принимает наиболее прямой маршрут в граничную сеть Майкрософт.

Облачная сторона

Локальный исходящий трафик из Azure сокращает время кругового пути, избегая ненужных прыжков через удаленные расположения. Такой подход повышает скорость отклика и стабильность сеанса. При локальном исходящем трафике RDP непосредственно в сеть Майкрософт через шлюз NAT, например, трафик остается в сети Майкрософт к шлюзу или ретранслятору TURN для его полного пути.

Физическая сторона

Локальный прорыв в Интернет как можно ближе к пользователю предотвращает передачу трафика через корпоративные сети, VPN и защищенные веб-шлюзы (SWG). С помощью этой оптимизации можно использовать ближайший шлюз или ретранслятор TURN, чтобы избежать маршрутизации через нелоконные шлюзы RDP или ретрансляторы TURN, которые ближе к расположению VPN или SWG, чем конечный пользователь. Использование этих удаленных шлюзов или ретрансляторов может привести к значительной задержке и проблемам с надежностью.

Преимущества

Включив локальный исходящий трафик, вы минимизируете задержку, уменьшаете потери пакетов, вызванные перегруженными туннелями, а также обеспечиваете более плавный и надежный пользовательский интерфейс.

Когда трафик RDP отправляется локально, он подключается к ближайшему шлюзу RDP или ретранслятору TURN, обычно близко к расположению пользователя. Оттуда трафик проходит через управляемую магистральную сеть Майкрософт к облачному компьютеру и обратно. Это означает, что трафик находится в общедоступном Интернете только на короткое расстояние, что повышает безопасность и производительность.

Дополнительные сведения о глобально распределенной инфраструктуре Майкрософт для оптимизации RDP см . в этой статье.

Реализация оптимизации

Способ реализации этих оптимизаций может немного отличаться в зависимости от того, на какой стороне настраиваемого подключения.

Оптимизация физического Device-Side

Выполните следующие действия, чтобы обеспечить наиболее прямой, надежный и высокопроизводительный трафик RDP.

1. **Определите основные сведения о конечной точке RDP:** Эти сведения отображаются в следующей таблице, но одинаковы для физических и облачных компьютеров. Последние сведения всегда см. в документации по требованиям к сети .

Развернуть таблицу

ИД	Полное доменное имя	IP	Протокол или порт	Назначение
1	*.wvd.microsoft.com	40.64.144.0/20 (охватывает поток RDP в полном доменном имени, но не все в домене с подстановочными знаками)	TCP/443	Подключение RDP на основе TCP
2	н/д	51.5.0.0/16	UDP/3478	RDP на основе UDP через TURN

> **Примечание.**
>
> Подсеть 40.64.144.0/20 охватывает поток RDP, связанный с *.wvd.microsoft.com но не каждую конечную точку в *.wvd.microsoft.com

1. **Обход туннелей VPN и безопасного веб-шлюза (SWG).** Маршрутизация трафика RDP непосредственно в Интернет. Избегайте отправки через прокси-серверы, VPN или группы SWG. Корпорация Майкрософт владеет ip-подсетями, перечисленными в таблице, и управляет ими, и они предназначены для Windows 365 и Azure Виртуального рабочего стола.

2. **Включение локальных исходящих данных** Убедитесь, что трафик выходит из сети как можно ближе к пользователю. Избегайте обратной передачи трафика на большие расстояния, прежде чем добраться до Интернета. Это позволяет использовать ближайший шлюз или ретранслятор TURN, что обеспечивает максимальную производительность.

3. **Отключение проверки TLS** Не проверяйте трафик RDP в брандмауэре исходящего трафика. Проверка TLS обеспечивает задержку и ухудшает качество сеанса, не предоставляя никаких преимуществ. Внутри сеанса зашифрованного транспорта TLS находится вложенный сеанс зашифрованных данных TLS. Дополнительные сведения см. в документации по безопасности подключений.

4. **Определение приоритета трафика RDP** Если применимо, приоритезировать трафик RDP в сети, чтобы поддерживать скорость реагирования на сеанс. Относитесь к нему

так же, как обрабатывается мультимедийный трафик Microsoft Teams.

Пример результата:

Компания Contoso использовала сведения о конечной точке RDP в строках 1 и 2 для маршрутизации трафика по оптимизированной схеме (отображается пунктирной линией). Этот путь отправляется локально в Интернет через прямой маршрут из корпоративной сети. Проверка TLS отключена для этого трафика в брандмауэре.

Следуя этому подходу, компания Contoso достигла следующего:

- Минимальная возможная задержка в службе Windows 365
- Высочайшая надежность подключения
- Максимальная пропускная способность для удаленных сеансов
- Снижение нагрузки на путь прокси-сервера
- Локальные шлюзы RDP и ретрансляторы TURN рядом с пользователями, обеспечивая максимально раннее поступление трафика в глобальную магистраль Майкрософт для обеспечения комплексной производительности

Из локального шлюза или ретранслятора трафик проходит через магистральную сеть Майкрософт к облачному компьютеру и обратно, что снижает доступность общедоступного Интернета и повышает стабильность.

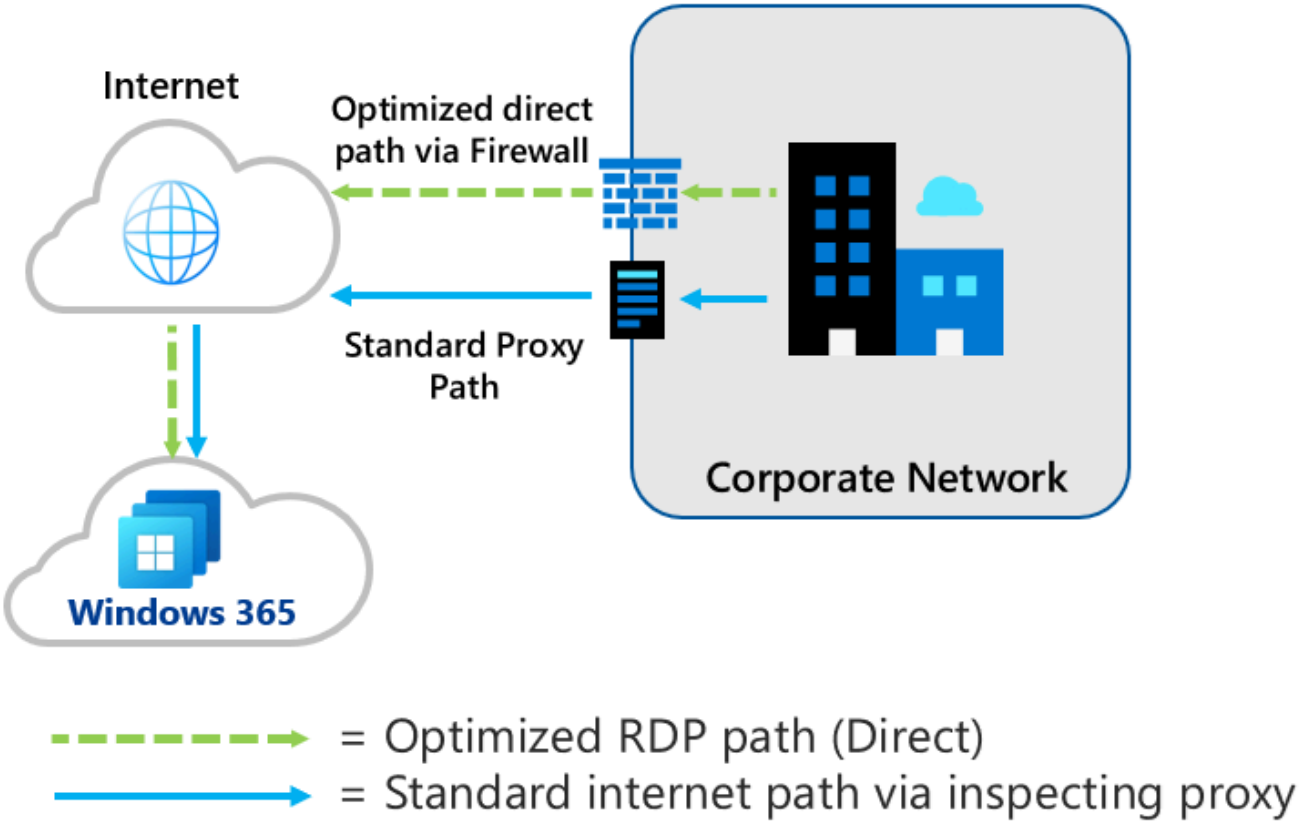


Схема 3. Оптимизация RDP из корпоративной сети

В следующем примере показана конфигурация мобильной рабочей сети Contoso. Программное обеспечение VPN, используемое мобильными рабочими, настроено для обхода трафика RDP из VPN принудительного туннеля с помощью показанной информации (пунктирная линия).

Эта оптимизация позволяет трафику RDP, например трафику мультимедиа Teams, использовать прямой интернет-путь пользователя к Корпорации Майкрософт вместо маршрутизации через корпоративную сеть.

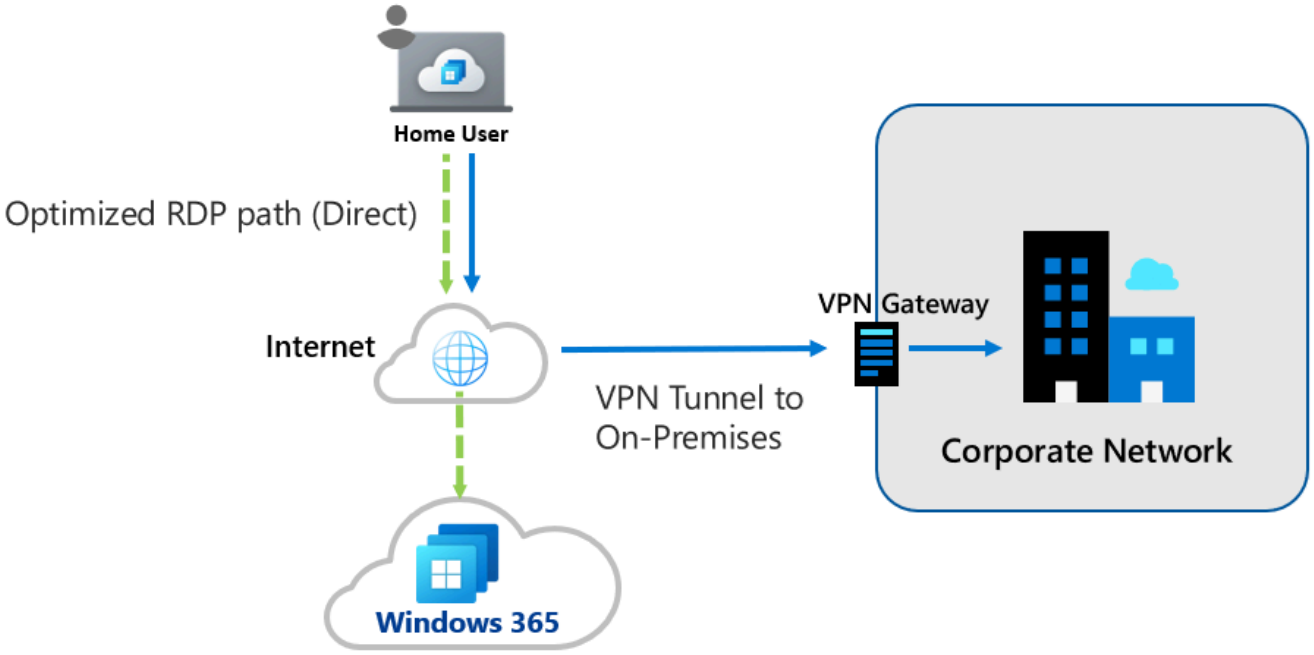


Схема 4. Оптимизация RDP от удаленного пользователя

Оптимизация на стороне облачного компьютера

Конечные точки RDP, используемые на стороне облачного компьютера, совпадают с конечными точками, используемыми на стороне физического устройства, и они также являются исходящими. При правильной конфигурации трафик RDP с облачного компьютера остается в магистрали Майкрософт к целевому шлюзу или ретранслятору TURN вместо обхода общедоступного Интернета. Такой подход повышает надежность и производительность.

Шаги по достижению этой оптимизации на стороне облачного компьютера могут немного отличаться от физического устройства в зависимости от выбранного варианта развертывания .

Развертывания размещенной сети Майкрософт

В модели размещенной сети Майкрософт, которая является рекомендуемым вариантом развертывания, корпорация Майкрософт предварительно настраивает и оптимизирует основное подключение от вашего имени. Вам не нужно выполнять дополнительную настройку, чтобы обеспечить оптимальное подключение к базовой сети.

Когда требуется дополнительная настройка

При установке сетевого программного обеспечения на облачном компьютере, например VPN-клиента или агента безопасного веб-шлюза (SWG), эти компоненты могут изменить путь трафика RDP, чтобы он не использовал предоставленную базовую сеть напрямую. В этом случае требуется настройка для обхода трафика RDP, поэтому он направляется непосредственно в сеть Майкрософт по указанному пути, а не через РЕШЕНИЕ VPN или SWG.

Эти конечные точки соответствуют требуемым в физической сети и перечислены в следующей таблице:

Развернуть таблицу

ИД	Полное доменное имя	IP	Протокол или порт	Назначение
1	*.wvd.microsoft.com	40.64.144.0/20 (охватывает поток RDP в полном доменном имени, но не все в домене с подстановочными знаками)	TCP/443	Подключение RDP на основе TCP
2	н/д	51.5.0.0/16	UDP/3478	RDP на основе UDP через TURN

Некоторые поставщики безопасного веб-шлюза (SWG), например Zscaler, предоставляют упрощенные варианты обхода трафика RDP. Дополнительные сведения см. в соответствующей записи Techcommunity.

Кроме того, необходимо убедиться, что следующие **конечные точки, отличные от RDP, не отправляются через какой-либо прокси-сервер** , VPN или туннель SWG на стороне облачного компьютера. Если этот трафик направляется за пределы Azure или блокируется, подключение завершается ошибкой.

Развернуть таблицу

ИД	Полное доменное имя	IP	Протокол или порт	Назначение
3	azkms.core.windows.net	20.118.99.224/32, 40.83.245.53/32, 23.102.135.246/32 (сведения об обновлениях см. в документации по KMS Azure)	TCP/1688	Azure трафика KMS
4	н/д	169.254.169.254	TCP/80	Взаимодействие Azure Fabric
5	н/д	168.63.129.16	TCP/80	Взаимодействие

ИД	Полное доменное имя	IP	Протокол или порт	Назначение
				Azure Fabric

> ⓘ **Внимание**
>
> **Убедитесь, что трафик RDP обошел для всех типов туннелей**: туннели VPN и SWG обычно основаны на пользователях, но убедитесь, что все туннели на основе компьютера также исключают необходимые конечные точки RDP. Этот обход имеет решающее значение, так как для входа пользователя на облачный компьютер требуется исходящее подключение к этим конечным точкам.

развертывания Azure сетевого подключения (ANC)

Для развертываний Azure сетевого подключения (ANC), где облачный компьютер использует собственную виртуальную сеть Azure, настройте оптимизированный исходящий путь для RDP, чтобы трафик использовал магистраль Корпорации Майкрософт без необходимости проверки или привязки волос. Реализуйте следующие рекомендации, чтобы обеспечить максимальную производительность и надежность.

- **Определяемый пользователем маршрут (UDR) для трафика RDP.** Используйте маршрут, предназначенный для тега `WindowsVirtualDesktop` службы в **Интернет**, в идеале через шлюз NAT, связанный с подсетью. Такой подход позволяет сохранить потоки RDP от виртуальных сетевых устройств (NVA), сохраняя согласованный исходящий путь.

- **Группы безопасности сети (NSG):** Убедитесь, что группы безопасности сети разрешают исходящий трафик TCP/443 и UDP/3478 для соответствующих конечных точек служб. Не блокируйте тег службы.

- **Нет проверки TLS или проверки подлинности прокси-сервера в потоках RDP:** Отключите перехват или проверку подключения по протоколу RDP, если оно проходит через устройство, предоставляющее эту функцию.

- **Другой трафик:** При необходимости трафик, отличный от RDP, можно направлять по маршруту по умолчанию (например, в Брандмауэр Azure).

- **Будьте осторожны с NVA для RDP:** NVA, включая Брандмауэр Azure, могут увеличить задержку и нарушить длительные сеансы UDP/TCP во время операций масштабирования. Используйте шлюз NAT для трафика с длительным сроком действия ключей, таких как трафик RDP и Microsoft 365.

- **Проверьте базовое подключение:** Используйте предоставленные рекомендации и проверьте с помощью проверок работоспособности сетевого подключения (ANC) Azure.

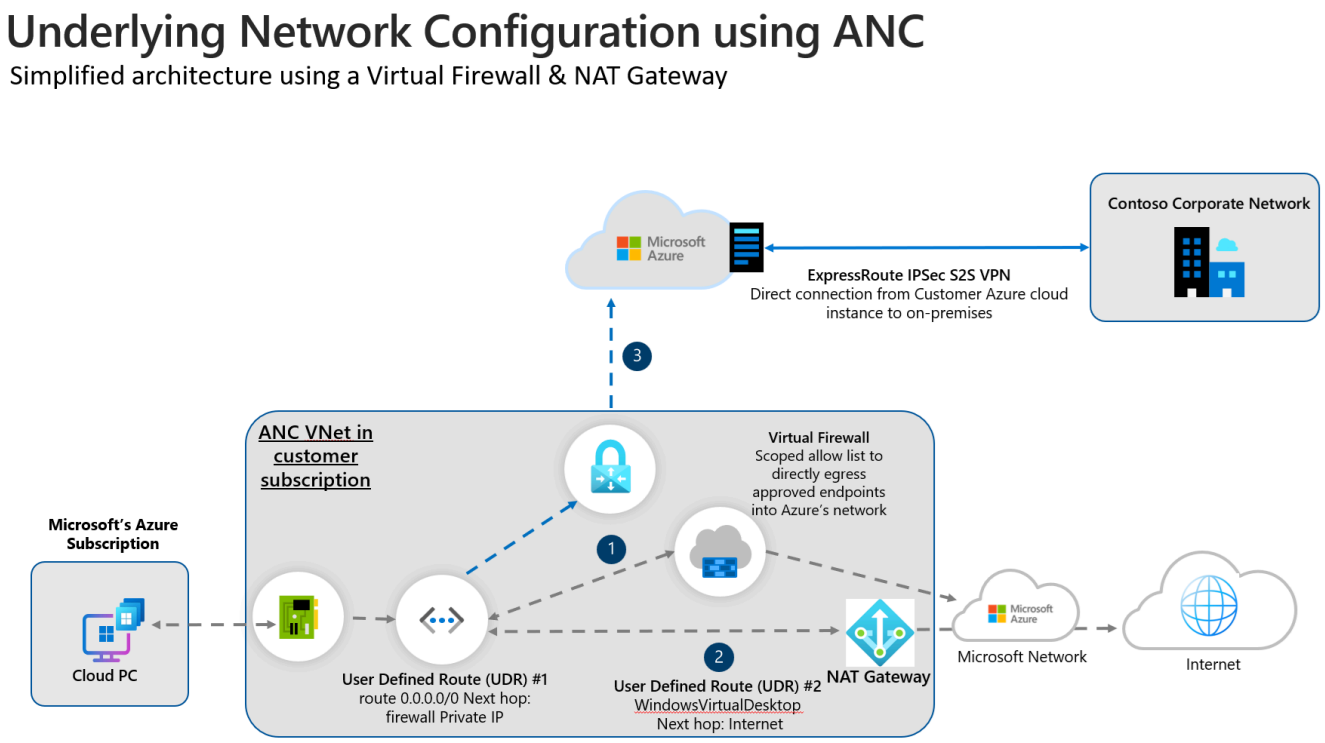


Схема 5. Упрощенное развертывание ANC с оптимизацией трафика RDP

На этой схеме показаны три основных маршрута, настроенные из виртуальной сети Azure:

1. **Маршрут по умолчанию (0.0.0.0/0 определяемый пользователем маршрут UDR)** Отправляет весь трафик на частный IP-адрес Брандмауэр Azure, который становится путем по умолчанию. Брандмауэр разрешает утвержденный трафик в сеть Майкрософт и Интернет по мере необходимости. Используйте этот путь для других конечных точек службы Windows 365, которые не требуют специальной обработки.

2. **Оптимизированный маршрут для трафика RDP** Более конкретный UDR отправляет `WindowsVirtualDesktop` тег службы в **Интернет**, который в этом примере использует шлюз NAT. Этот путь оптимизирован для RDP и также должен использоваться для трафика с длительным сроком жизни или с учетом задержки, который не должен проходить через брандмауэр. "Интернет" не означает, что этот трафик достигает общедоступного Интернета.

3. **Локальный маршрут** Шлюз ExpressRoute предоставляет более конкретный маршрут для локального трафика, например для всего `10.0.0.0/8` диапазона.

Дополнительные сведения см. в документе Использование Брандмауэр Azure для управления средами Windows 365 и защиты.

> **Совет**
>
> Доверенный трафик, такой как потоки Microsoft 365, туннели VPN/SWG или другой трафик с большим объемом, чувствительный к задержке, также может извлечь выгоду из использования оптимизированного пути. Это снижает нагрузку на брандмауэр для трафика, которому действительно требуются его службы.

Часто задаваемые вопросы об оптимизации RDP

Вопрос. Нужно ли выполнять что-либо еще в развертывании размещенной сети Майкрософт?

A: После настройки обхода конечных точек, перечисленных в этой статье, в решениях прокси-сервера, VPN или SWG дополнительная настройка обычно не требуется. Виртуальная сеть карта автоматически настраивается для использования магистрали Майкрософт для прямого и высокоскоростного подключения.

Вопрос. Нужно ли настраивать обход только на облачном компьютере?

A: Нет. Примените обход к облачному компьютеру и подключаемого клиента, если клиент использует прокси-сервер, SWG или VPN. Если оба устройства используют один и тот же профиль конфигурации, этот обход должен выполняться автоматически. Строки 3–5 в таблице этого документа применяются только к облачному компьютеру.

Вопрос. Как часто IP-адреса меняются?

A: Мы объединили конечные точки RDP в две выделенные подсети для службы по всему миру. Размер этих подсетей позволяет свести к минимуму риск частого изменения IP-адресов. Такая конструкция помогает поддерживать стабильность и упрощает конфигурации брандмауэра и маршрутизации. Тег службы можно отслеживать `WindowsVirtualDesktop` на наличие обновлений. Мы также работаем над включением этих требований в веб-службу Microsoft 365 для упрощения мониторинга и автоматизации.

Вопрос. Можно ли добавить в обход больше трафика по протоколу RDP?

A: В настоящее время корпорация Майкрософт предоставляет IP-адреса только для подключения по протоколу RDP. Если решение поддерживает конфигурацию на основе полного доменного имени, можно добавить другие конечные точки службы. См. страницу Документация Майкрософт, связанную с этой статьей. Кроме того, рекомендуется обойти трафик Microsoft 365 .

Вопрос. Я использую настоящий разделенный туннель. Влияет ли это на меня?

A: Нет. Это руководство применяется к сценариям принудительного туннелирования (обратный разделенный туннель), в которых весь трафик проходит через туннель, кроме определенных исключений. В настоящем разделенном туннеле, где путь по умолчанию — Интернет, а через туннель проходят только определенные конечные точки, трафик RDP должен следовать интернет-пути по умолчанию, если иначе не настроено вручную.

Вопрос. Относится ли этот совет также к Azure Виртуальному рабочему столу (AVD)?

A: Да. Windows 365 и AVD имеют те же требования к подключению, что и Devbox.

Вопрос. Снижает ли обход безопасность?

A: Нет. Подключение остается сквозным шифрованием TLS. Обход изменяет только сетевой путь, но не проверку подлинности или шифрование. Сохраняйте политики защиты конечных точек, условного доступа и соответствия устройств.

Last updated on 21.11.2025

Использование Брандмауэр Azure для управления средами Windows 365 и защиты

Статья • 22.04.2025

В этой статье объясняется, как упростить и защитить среду Windows 365 с помощью Брандмауэр Azure. Пример архитектуры, описанный здесь, обеспечивает низкий уровень обслуживания и автоматический доступ к требуемым конечным точкам через прямой и оптимизированный путь подключения. Для репликации этого примера архитектуры в среде можно использовать правила сети Брандмауэр Azure и теги полного доменного имени (FQDN).

> **Примечание**
>
> Эта статья относится к клиентам, которые развертывают Windows 365 с помощью сетевых подключений Azure (ANC). Эта статья не относится к средам, в которых используются размещенные майкрософт сети, так как корпорация Майкрософт управляет базовой безопасностью и подключением. Дополнительные сведения о каждом из них см. в разделе варианты развертывания сети Windows 365.

Служба Windows 365 требует оптимизированного и непроксимированного подключения к критически важным конечным точкам служб, многие из которых находятся в инфраструктуре Майкрософт. Подключение к этим ресурсам с помощью локальных сетей через Интернет является неэффективным и не рекомендуется. Такие подключения также могут быть сложными для настройки и управления.

Например, некоторые клиенты Windows 365, использующие модель развертывания ANC, могут иметь прямое подключение к локальной среде, которая использует ExpressRoute или VPN типа "сеть — сеть". Исходящий трафик может маршрутизироваться с помощью существующего прокси-сервера так же, как и локальный трафик. Эта стратегия подключения не оптимизирована для Windows 365 сред и может оказать значительное влияние на производительность.

Вместо этого можно использовать Брандмауэр Azure со средами WINDOWS 365 ANC, чтобы обеспечить оптимизированный, безопасный, низкий уровень обслуживания и автоматический доступ. Вы также можете использовать прямой путь для оптимизации трафика RDP и других длительных подключений, например к защищенному веб-шлюзу.

Необходимые конечные точки для Windows 365

Windows 365 требуется доступ к следующим конечным точкам:

1. Windows 365
2. Виртуальный рабочий стол Azure
3. Intune

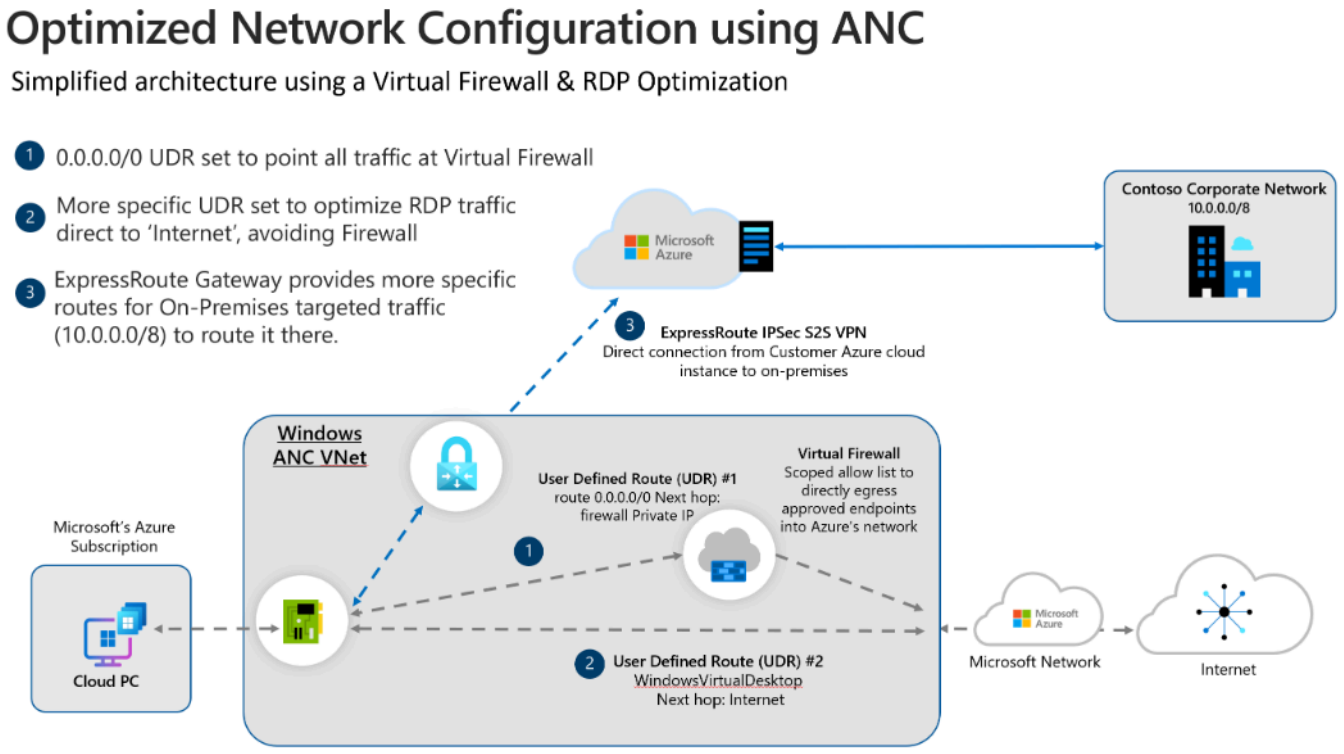
Вы также можете рассмотреть возможность доступа к другим службам Майкрософт (например, Office 365) при настройке оптимизированного подключения из среды.

Теги FQDN для определенных служб доступны для Брандмауэр Azure, чтобы помочь в настройке и обслуживании этих правил простым способом, и они рассматриваются далее в этом документе.

Пример архитектуры с использованием тегов Брандмауэр Azure и FQDN

Существует множество способов настройки сети в Azure. Здесь мы используем:

- Одна виртуальная сеть с Брандмауэр Azure управления исходящим доступом.
- Оптимизация трафика RDP для отправки его напрямую в Корпорацию Майкрософт.
- Канал ExpressRoute для подключения виртуальной сети к локальной среде.



Поток трафика на этой схеме:

1. Корпоративная сеть Contoso. Эта локальная IP-подсеть объявляется в виртуальной сети через шлюз ExpressRoute. Весь трафик в этот диапазон (10.0.0.0/8) отправляется через канал ExpressRoute.
2. Весь остальной трафик из подсети Windows 365 отправляется в брандмауэр Azure через определяемый пользователем маршрут (UDR) 0.0.0.0/0. В качестве IP-адреса следующего прыжка задается частный IP-адрес Брандмауэр Azure.
3. Брандмауэр содержит правила приложений (и теги FQDN) и сетевые правила, настроенные для Windows 365 необходимых конечных точек. Трафик, соответствующий правилам, разрешен. Любой другой трафик, явно не разрешенный, блокируется.
4. Другой UDR указывает на тег службы "WindowsVirtualDesktop", который содержит диапазоны IP-адресов для подключения по протоколу RDP, для которого для следующего прыжка задано значение "Интернет". Этот UDR не позволяет трафику RDP проходить через брандмауэр и помещается непосредственно в сеть Майкрософт.

Оптимизация подключения RDP

В этом примере конфигурации RDP настраивается с определенным UDR, чтобы указать тег службы "WindowsVirtualDesktop" на "интернет". Такая конфигурация означает, что этот трафик с высоким объемом и задержкой имеет прямой и высокоэффективный путь к инфраструктуре и позволяет

избежать ненужной нагрузки на брандмауэр. Рекомендуется реализовать эту конфигурацию для предоставления наиболее эффективного и надежного пути для RDP. Хотя назначением для этого UDR является Интернет, так как этот трафик направляется к конечным точкам Майкрософт, этот трафик с облачного компьютера в инфраструктуру RDP не попадает в Интернет, а остается в магистрали Майкрософт.

> **Примечание**
>
> В этом примере используется исходящий доступ по умолчанию. В сентябре 2025 г. исходящий доступ по умолчанию будет прекращен для новых развертываний. Он будет по-прежнему доступен для существующих развертываний. Дополнительные сведения о выходе из эксплуатации см. в официальном объявлении. После сентября в новых развертываниях можно использовать явную форму NAT, например шлюз NAT, чтобы предоставить эту функцию. Добавление шлюза NAT в используемую подсеть означает, что шлюз NAT используется для трафика, направленного в Интернет, а не для исходящего доступа по умолчанию.

правила приложений Брандмауэр Azure

Среда на схеме была настроена с помощью следующих Брандмауэр Azure правил приложения (примененных в выноске 3). Весь трафик, не предназначенный для локальной подсети Contoso, направляется в брандмауэр. Эти правила разрешают определенному трафику исходящий трафик к месту назначения. Дополнительные сведения о развертывании Брандмауэр Azure см. в статье Развертывание и настройка Брандмауэр Azure с помощью портал Azure.

Развернуть таблицу

Описание правила	Тип назначения	Имя тега FQDN	Протокол	Проверка tls	Обязательный или необязательный
полные доменные имена Windows 365	Тег FQDN	Windows365	HTTP: 80, HTTPS: 443	Не рекомендуется	Обязательный
полные доменные имена Intune	Тег FQDN	MicrosoftIntune	HTTP: 80, HTTPS: 443	Не рекомендуется	Обязательный
полные доменные имена Office 365	Тег FQDN	Office365	HTTP: 80, HTTPS: 443	Не рекомендуется оптимизировать & разрешенные категории	Необязательно, но рекомендуется
Центр обновления Windows	Тег FQDN	WindowsUpdate	HTTP: 80, HTTPS: 443	Не рекомендуется	Необязательный
Citrix HDX Plus	Тег FQDN	CitrixHDXPlusForWindows365	HTTP: 80, HTTPS: 443	Не рекомендуется	Необязательный (требуется только при использовании Citrix HDX Plus)

Брандмауэр Azure можно связать с общедоступными IP-адресами для обеспечения исходящего подключения к Интернету. Первый общедоступный IP-адрес выбирается случайным образом для предоставления исходящего преобразования сетевых адресов источника (SNAT). Следующий доступный общедоступный IP-адрес будет использоваться после исчерпания всех портов SNAT из первого IP-адреса. В сценариях, требующих высокой пропускной способности, рекомендуется использовать шлюз Azure NAT. Шлюз NAT динамически масштабирует исходящие подключения и может быть интегрирован с Брандмауэр Azure. Дополнительные сведения см. в руководстве по интеграции шлюза NAT с Брандмауэр Azure.

Тег Windows365

Тег Windows365 включает необходимые конечные точки Виртуального рабочего стола Azure (AVD), за исключением конечных точек с нестандартными портами, которые необходимо ввести вручную (см. раздел Сетевые правила).

Тег Windows365 не содержит Intune. Тег MicrosoftIntune можно использовать отдельно.

Тег FQDN Windows365 включает все необходимые конечные точки, кроме конечных точек, перечисленных как *обязательные* в отдельных строках этого документа, которые необходимо настроить отдельно. Теги FQDN отличаются от тега службы. Например, тег службы WindowsVirtualDesktop включает только IP-адреса, по которым разрешается *.wvd.microsoft.com.

Правила сети

Брандмауэр Azure в настоящее время не обрабатывает нестандартные порты в теге FQDN. Windows 365 имеет несколько нестандартных требований к портам, поэтому следующие правила необходимо добавить вручную в качестве сетевых правил в дополнение к тегам FQDN.

Развернуть таблицу

Описание правила	Тип назначения	Полное доменное имя/IP-адрес	Протокол	Порт/с	Проверка TLS	Обязательный или необязательный
Активация Windows	Полное доменное имя	azkms.core.windows.net	TCP	1688	Не рекомендуется	Обязательный
Регистрация	Полное доменное имя	global.azure-devices-provisioning.net	TCP	443, 5671	Не рекомендуется	Обязательный
Регистрация	Полное доменное имя	hm-iot-in-prod-preu01.azure-devices.net	TCP	443,5671	Не рекомендуется	Обязательный
Регистрация	Полное доменное имя	hm-iot-in-prod-prap01.azure-devices.net	TCP	443,5671	Не рекомендуется	Обязательный

Описание правила	Тип назначения	Полное доменное имя/IP-адрес	Протокол	Порт/с	Проверка TLS	Обязательный или необязательный
Регистрация	Полное доменное имя	hm-iot-in-prod-prna01.azure-devices.net	TCP	443,5671	Не рекомендуется	Обязательный
Регистрация	Полное доменное имя	hm-iot-in-prod-prau01.azure-devices.net	TCP	443,5671	Не рекомендуется	Обязательный
Регистрация	Полное доменное имя	hm-iot-in-prod-prna02.azure-devices.net	TCP	443,5671	Не рекомендуется	Обязательный
Регистрация	Полное доменное имя	hm-iot-in-2-prod-prna01.azure-devices.net	TCP	443,5671	Не рекомендуется	Обязательный
Регистрация	Полное доменное имя	hm-iot-in-3-prod-prna01.azure-devices.net	TCP	443,5671	Не рекомендуется	Обязательный
Регистрация	Полное доменное имя	hm-iot-in-2-prod-preu01.azure-devices.net	TCP	443,5671	Не рекомендуется	Обязательный
Регистрация	Полное доменное имя	hm-iot-in-3-prod-preu01.azure-devices.net	TCP	443,5671	Не рекомендуется	Обязательный
Подключение к пользовательскому протоколу datagram (UDP) через TURN	IP	20.202.0.0/16	UDP	3478	Не рекомендуется	Обязательный
Регистрация	Полное доменное имя	hm-iot-in-4-prod-prna01.azure-devices.net	TCP	443, 5671	Не рекомендуется	Обязательный

Варианты решений для обеспечения безопасности партнеров

Другие способы защиты среды Windows 365 — это варианты решений для обеспечения безопасности партнеров, которые предоставляют автоматические наборы правил для доступа к необходимым конечным точкам для службы Windows 365. К таким вариантам относятся:

- Обновляемые объекты Check Point Software Technologies

Дальнейшие действия

Дополнительные сведения об архитектуре Windows 365.

Дополнительные сведения о FQDNS см. в статье Общие сведения о тегах FQDN.

Дополнительные сведения о тегах служб см. в статье Теги службы виртуальной сети.

Управление доступом на основе ролей

Статья • 31.01.2025

Управление доступом на основе ролей (RBAC) помогает управлять доступом пользователей к ресурсам вашей организации и выполнению операций с этими ресурсами. Вы можете назначить роли для облачных компьютеров с помощью центра администрирования Microsoft Intune.

Когда пользователь с ролью владельца подписки или администратора доступа пользователей создает, изменяет или повторяет ANC, Windows 365 прозрачно назначает необходимые встроенные роли следующим ресурсам (если они еще не назначены):

- Подписка на Azure
- Группа ресурсов
- Виртуальная сеть, связанная с ANC

Если у вас есть только роль читателя подписки, эти назначения не являются автоматическими. Вместо этого необходимо вручную настроить необходимые встроенные роли для приложения Windows First Party в Azure.

Дополнительные сведения см. в статье Управление доступом на основе ролей (RBAC) с помощью Microsoft Intune.

Роль администратора Windows 365

Windows 365 поддерживает роль администратора Windows 365, доступную для назначения ролей через Центр Администратор Майкрософт и Microsoft Entra ID. Эта роль позволяет управлять облачными компьютерами в Windows 365 для бизнеса и Windows 365 Корпоративная. Роль администратора Windows 365 может предоставлять больше разрешений, чем другие Microsoft Entra роли, например глобальный администратор. Дополнительные сведения см. в разделе Microsoft Entra встроенных ролей.

Встроенные роли для облачных компьютеров

Для облачного компьютера доступны следующие встроенные роли:

Администратор облачного компьютера

Управляет всеми аспектами облачных компьютеров, например:

- управление образами ОС;
- Конфигурация сетевого подключения Azure
- Подготовка

Читатель облачного компьютера

Просматривает данные облачного компьютера, доступные в узле Windows 365 в Microsoft Intune, но не может вносить изменения.

Участник сетевого интерфейса Windows 365

Роль участника сетевого интерфейса Windows 365 назначается группе ресурсов, связанной с сетевым подключением Azure (ANC). Эта роль позволяет службе Windows 365 создавать сетевые карты и присоединяться к ней, а также управлять развертыванием в группе ресурсов. Эта роль представляет собой коллекцию минимальных разрешений, необходимых для работы Windows 365 при использовании ANC.

Развернуть таблицу

Тип действия	Разрешения
actions	Microsoft.Resources/subscriptions/resourcegroups/read Microsoft.Resources/deployments/read Microsoft.Resources/deployments/write Microsoft.Resources/deployments/delete Microsoft.Resources/deployments/operations/read Microsoft.Resources/deployments/operationstatuses/read Microsoft.Network/locations/operations/read Microsoft.Network/locations/operationResults/read Microsoft.Network/locations/usages/read Microsoft.Network/networkInterfaces/write Microsoft.Network/networkInterfaces/read Microsoft.Network/networkInterfaces/delete Microsoft.Network/networkInterfaces/join/action Microsoft.Network/networkInterfaces/effectiveNetworkSecurityGroups/action Microsoft.Network/networkInterfaces/effectiveRouteTable/action
NotActions	Нет
dataActions	Нет

Тип действия	Разрешения
notDataActions	Нет

пользователь сети Windows 365

Роль пользователя сети Windows 365 назначается виртуальной сети, связанной с ANC. Эта роль позволяет службе Windows 365 присоединить сетевой адаптер к виртуальной сети. Эта роль представляет собой коллекцию минимальных разрешений, необходимых для работы Windows 365 при использовании ANC.

Развернуть таблицу

Тип действия	Разрешения
actions	Microsoft.Network/virtualNetworks/read Microsoft.Network/virtualNetworks/subnets/read Microsoft.Network/virtualNetworks/usages/read Microsoft.Network/virtualNetworks/subnets/join/action
NotActions	Нет
dataActions	Нет
notDataActions	Нет

Настраиваемые роли

Вы можете создать настраиваемые роли для Windows 365 в Центре администрирования Microsoft Intune. Дополнительные сведения см. в статье Создание настраиваемой роли.

При создании настраиваемых ролей доступны следующие разрешения.

Развернуть таблицу

Разрешение	Описание
Аудит данных и чтения	Чтение журналов аудита ресурсов облачного компьютера в клиенте.
Connections сети Azure или создание	Создайте локальное подключение для подготовки облачных компьютеров. Для создания локального подключения также

Разрешение	Описание
	требуется роль Azure владельца подписки или администратора доступа пользователей.
Connections и удаление сети Azure	Удалите определенное локальное подключение. Напоминание. Вы не можете удалить используемое подключение. Для удаления локального подключения также требуется роль Azure владельца подписки или администратора доступа пользователей.
Connections и чтение сети Azure	Чтение свойств локальных подключений.
Connections и обновление сети Azure	Обновите свойства определенного локального подключения. Для обновления локального подключения также требуется роль Azure владельца подписки или администратора доступа пользователей.
Connections сети Azure/RunHealthChecks	Выполните проверки работоспособности для определенного локального подключения. Для выполнения проверок работоспособности также требуется роль Azure владельца подписки или администратора доступа пользователей.
Connections сети Azure/UpdateAdDomainPassword	Обновление пароля домена Active Directory для определенного локального подключения.
Облачные компьютеры и чтение	Чтение свойств облачных компьютеров в клиенте.
Облачные компьютеры/повторная подготовка	Повторное создание облачных компьютеров в клиенте.
Облачные компьютеры/изменение размера	Изменение размера облачных компьютеров в клиенте.
Облачные компьютеры/EndGracePeriod	Окончание льготного периода для облачных компьютеров в клиенте.
Облачные компьютеры/восстановление	Восстановление облачных компьютеров в клиенте.
Облачные компьютеры/перезагрузка	Перезагрузите облачные компьютеры в клиенте.
Облачные компьютеры/переименование	Переименуйте облачные компьютеры в клиенте.

Разрешение	Описание
Облачные компьютеры и устранение неполадок	Устранение неполадок облачных компьютеров в клиенте.
Облачные компьютеры/ChangeUserAccountType	Измените тип учетной записи пользователя между локальным администратором и стандартным пользователем облачного компьютера в клиенте.
Облачные компьютеры/PlaceUnderReview	Настройка облачных компьютеров в клиенте.
Облачные компьютеры/RetryPartnerAgentInstallation	Попытка переустановки сторонних агентов партнеров на облачном компьютере, который не удалось установить.
Облачные компьютеры/ApplyCurrentProvisioningPolicy	Примените текущую конфигурацию политики подготовки к облачным компьютерам в клиенте.
Облачные компьютеры/CreateSnapshot	Вручную создайте snapshot для облачных компьютеров в клиенте.
Образы устройств и создание	Отправьте пользовательский образ ОС, который позже можно подготовить на облачных компьютерах.
Изображения и удаление устройств	Удаление образа ОС с облачного компьютера.
Изображения и чтение устройств	Чтение свойств образов облачных компьютеров.
Параметры внешнего партнера/чтение	Чтение свойств параметра внешнего партнера облачного компьютера.
Параметры внешнего партнера/Создание	Создайте новый параметр внешнего партнера облачного компьютера.
Параметры и обновление внешних партнеров	Обновите свойства параметра внешнего партнера облачного компьютера.
Параметры организации/чтение	Ознакомьтесь со свойствами параметров организации облачного компьютера.
Параметры организации/обновление	Обновите свойства параметров организации облачного компьютера.
Отчеты о производительности и чтение	Ознакомьтесь с отчетами, связанными с Облачный компьютер Windows 365 удаленными подключениями.

Разрешение	Описание
Политики подготовки и назначение	Назначьте политику подготовки облачных компьютеров группам пользователей.
Политики подготовки/создание	Создайте новую политику подготовки облачных компьютеров.
Политики подготовки/удаление	Удалите политику подготовки облачных компьютеров. Вы не можете удалить используемую политику.
Политики подготовки/чтение	Чтение свойств политики подготовки облачных компьютеров.
Политики подготовки и обновление	Обновите свойства политики подготовки облачных компьютеров.
Отчеты и экспорт	Экспорт Windows 365 связанных отчетов.
Назначение ролей или создание	Создайте назначение роли облачного компьютера.
Назначения ролей и обновление	Обновите свойства определенного назначения роли облачного компьютера.
Назначения ролей и удаление	Удалите определенное назначение роли облачного компьютера.
Роли/Чтение	Просмотр разрешений, определений ролей и назначений ролей для роли облачного компьютера. Просмотр операции или действия, которые можно выполнить для ресурса (или сущности) облачного компьютера.
Роли/Создание	Создайте роль для облачного компьютера. Операции создания можно выполнять с ресурсом (или сущностью) облачного компьютера.
Роли/Обновление	Роль обновления для облачного компьютера. Операции обновления можно выполнять для ресурса (или сущности) облачного компьютера.
Роли/Удаление	Удаление роли для облачного компьютера. Операции удаления можно выполнять с ресурсом (или сущностью) облачного компьютера.

Разрешение	Описание
План обслуживания и чтение	Ознакомьтесь с планами обслуживания облачного компьютера.
SharedUseLicenseUsageReports/Read	Ознакомьтесь с отчетами об использовании лицензий Облачный компьютер Windows 365 общего использования.
SharedUseServicePlans/Read	Ознакомьтесь со свойствами планов общего использования облачных компьютеров.
Моментальный снимок и чтение	Прочтите моментальный снимок облачного компьютера.
Моментальный снимок или общий доступ	Общий доступ к моментальному снимку облачного компьютера.
Поддерживаемый регион и чтение	Ознакомьтесь с поддерживаемыми регионами облачного компьютера.
Параметры пользователя/назначение	Назначьте параметр пользователя Cloud PC группам пользователей.
Параметры пользователя/создание	Создайте новый параметр пользователя облачного компьютера.
Параметры пользователя/удаление	Удаление параметра пользователя облачного компьютера.
Параметры пользователя/чтение	Чтение свойств параметра пользователя облачного компьютера.
Параметры пользователя/обновление	Обновите свойства параметра пользователя облачного компьютера.

Для создания политики подготовки администратору необходимы следующие разрешения:

- Политики подготовки/чтение
- Политики подготовки/создание
- Connections и чтение сети Azure
- Поддерживаемый регион и чтение
- Изображения и чтение устройств

Перенос существующих разрешений

Для ACS, созданных до 26 ноября 2023 г., роль участник сети используется для применения разрешений как для группы ресурсов, так и для виртуальная сеть. Чтобы применить к новым ролям RBAC, можно повторить проверка работоспособности ANC. Существующие роли необходимо удалить вручную.

Чтобы вручную удалить существующие роли и добавить новые роли, см. следующую таблицу для существующих ролей, используемых в каждом ресурсе Azure. Перед удалением существующих ролей убедитесь, что назначены обновленные роли.

Развернуть таблицу

Ресурс Azure	Существующая роль (до 26 ноября 2023 г.)	Обновленная роль (после 26 ноября 2023 г.)
Группа ресурсов	Участник сети	Участник сетевого интерфейса Windows 365
Виртуальная сеть	Участник сети	пользователь сети Windows 365
Подписка	Читатель	Читатель

Дополнительные сведения об удалении назначения ролей из ресурса Azure см. в статье Удаление назначений ролей Azure.

Теги области

Для RBAC роли являются только частью уравнения. Хотя роли хорошо определяют набор разрешений, область теги помогают определить видимость ресурсов вашей организации. Теги области наиболее полезны при организации клиента, чтобы пользователи были ограничены определенными иерархиями, географическими регионами, подразделениями и т. д.

Используйте Intune для создания тегов область и управления ими. Дополнительные сведения о создании и управлении тегами область см. в статье Использование управления доступом на основе ролей (RBAC) и тегов область для распределенных ИТ-служб.

В Windows 365 область теги можно применять к следующим ресурсам:

- Политики подготовки
- Сетевые подключения Azure (ANC)
- Облачные компьютеры

- Пользовательские образы
- Windows 365 назначения ролей RBAC

Чтобы убедиться, что в списке всех **устройств**, принадлежащих Intune, и в списке **все облачные компьютеры**, принадлежащие Windows 365, отображаются одни и те же облачные компьютеры на основе область, выполните следующие действия после создания тегов область и политики подготовки.

1. Создайте динамическую группу устройств Microsoft Entra ID с правилом enrollmentProfileName, равным точному имени созданной политики подготовки.
2. Назначьте созданный тег область динамической группе устройств.
3. После подготовки и регистрации облачного компьютера в Intune в списке Все устройства и Все облачные компьютеры должны отображаться одни и те же облачные компьютеры.

При добавлении новых тегов область в политику подготовки убедитесь, что вы также добавили теги область в динамическую группу Intune. Это дополнение делает так, чтобы динамическая группа учитывала новые теги область. Кроме того, проверка на любых облачных компьютерах, на которых могут быть добавлены уникальные теги область, чтобы убедиться, что они все еще существуют после любых обновлений.

Чтобы убедиться, что Windows 365 могут учитывать изменения тегов Intune область, эти данные синхронизируются из Intune. Дополнительные сведения см. в разделе Конфиденциальность, данные клиента и содержимое клиента в Windows 365.

Чтобы администраторы с ограниченной областью просматривали, какие область теги назначены им и объекты в их область, им должна быть назначена одна из следующих ролей:

- Intune только для чтения
- Читатель или администратор облачного компьютера
- Настраиваемая роль с похожими разрешениями.

Дальнейшие действия

Управление доступом на основе ролей (RBAC) с помощью Microsoft Intune

Общие сведения об определениях ролей Azure

Что такое управление доступом на основе ролей Azure (Azure RBAC)?

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Управление доступом на основе ролей (RBAC) в Microsoft Intune

20.08.2025

Защита доступа к организации — это важный шаг безопасности. В этой статье представлены основные сведения об использовании элементов управления доступом на основе ролей Microsoft Intune (RBAC), которые являются расширением элементов управления RBAC Microsoft Entra идентификатора. Последующие статьи помогут вам развернуть Intune RBAC в организации.

С помощью Intune RBAC вы можете предоставить администраторам детализированные разрешения, чтобы контролировать, кто имеет доступ к ресурсам вашей организации и что они могут делать с этими ресурсами. При назначении ролей RBAC Intune и выполнении принципов доступа с минимальными привилегиями администраторы могут выполнять назначенные им задачи только на тех пользователях и устройствах, которыми они должны иметь право управлять.

Роли RBAC

Каждая роль RBAC Intune задает набор разрешений, доступных пользователям, назначенным этой роли. Разрешения состоят из одной или нескольких категорий управления, таких как *конфигурация устройства* или *данные аудита*, а также наборы действий, которые можно выполнить, например *чтение*, *запись*, *обновление* и *удаление*. Вместе они определяют область административного доступа и разрешений в Intune.

Intune включает как встроенные, так и пользовательские роли. Встроенные роли одинаковы во всех клиентах и предоставляются для решения распространенных административных сценариев, в то время как создаваемые настраиваемые роли разрешают определенные разрешения, необходимые администратору. Кроме того, несколько Microsoft Entra ролей включают разрешения в Intune.

Чтобы просмотреть роль в **Центре администрирования Intune**, **перейдите в раздел Администрирование**> клиента**Все**>**роли**> и выберите роль. Затем вы можете управлять этой ролью на следующих страницах:

- **Свойства**. Имя, описание, тип, разрешения и теги области для роли. Вы также можете просмотреть имя, описание и разрешения встроенных ролей в этой документации в разделе Разрешения встроенных ролей.
- **Назначения**. Выберите назначение для роли, чтобы просмотреть сведения о нем, включая группы и области, которые включает назначение. Роль может иметь

несколько назначений, а пользователь может получать несколько назначений.

> ⓘ **Примечание**
>
> В июне 2021 г. Intune начала поддерживать **нелицензированных администраторов**. Учетные записи пользователей, созданные после этого изменения, могут администрировать Intune без назначенной лицензии. Учетным записям, созданным до этого изменения, и учетным записям администраторов во вложенной группе безопасности, назначенной роли, по-прежнему требуется лицензия на управление Intune.

Встроенные роли

Администратор Intune с достаточными разрешениями может назначать любую из ролей Intune группам пользователей. Встроенные роли предоставляют определенные разрешения, необходимые для выполнения административных задач, которые соответствуют назначению роли. Intune не поддерживает изменения описания, типа или разрешений встроенной роли.

- **Диспетчер приложений**. Управляет мобильными и управляемыми приложениями. Может читать информацию об устройстве и просматривать его профили конфигурации.
- **Endpoint Privilege Manager**. Управляет политиками Управление привилегиями на конечных точках в консоли Intune.
- **Читатель привилегий конечной точки**. Средства чтения привилегий конечных точек могут просматривать политики Управление привилегиями на конечных точках в консоли Intune.
- **Endpoint Security Manager**. Управляет функциями безопасности и соответствия, такими как базовые показатели безопасности, соответствие устройств, условный доступ и Microsoft Defender для конечной точки.
- **Оператор службы технической поддержки**. Выполняет удаленные задачи для пользователей и устройств, а также может назначать пользователям и устройствам приложения или политики.
- **Администратор ролей Intune**. Управляет пользовательскими ролями Intune и добавляет назначения для встроенных ролей Intune. Это единственная роль Intune, позволяющая назначать разрешения для администраторов.
- **Диспетчер политик и профилей**. Управляет политикой соответствия требованиям, профилями конфигурации, регистрацией Apple, идентификаторами корпоративных устройств и базовыми показателями безопасности.

- **Оператор с правами "только чтение"**. Просматривает сведения о пользователях, устройствах, регистрации, конфигурации и приложениях. Не может вносить изменения в Intune.
- **Администратор учебного заведения**. Администраторы учебных заведений управляют приложениями, параметрами и устройствами для своих групп в Intune для образовательных учреждений. Они могут выполнять удаленные действия на устройствах, в том числе удаленно блокировать их, перезапускать и выходить из управления.

Если клиент включает подписку на Windows 365 для поддержки облачных компьютеров, в Центре администрирования Intune также отображаются следующие роли облачных компьютеров. Эти роли недоступны по умолчанию и включают разрешения в Intune для задач, связанных с облачными компьютерами. Дополнительные сведения об этих ролях см. в статье Встроенные роли облачного компьютера в документации по Windows 365.

- **Администратор облачных компьютеров**. Администратор облачных компьютеров имеет доступ на *чтение* и *запись* ко всем функциям облачного компьютера, расположенным в области облачных компьютеров.
- **Средство чтения облачных компьютеров**. Средство чтения облачных компьютеров имеет доступ на *чтение* ко всем функциям облачных компьютеров, расположенным в области облачных компьютеров.

Настраиваемые роли

Вы можете создать собственные настраиваемые роли Intune, чтобы предоставить администраторам только определенные разрешения, необходимые для их задач. Эти настраиваемые роли могут включать любое разрешение Intune RBAC, что обеспечивает улучшенный доступ администратора и поддержку принципа доступа с наименьшими привилегиями в организации.

См . статью Создание настраиваемой роли.

Microsoft Entra роли с доступом Intune

Разрешения RBAC Intune — это подмножество Microsoft Entra разрешений RBAC. В качестве подмножества существуют некоторые Microsoft Entra роли, которые включают разрешения в Intune. Большинство Entra ID ролей, имеющих доступ к Intune, считаются привилегированными ролями. Использование и назначение привилегированных ролей должно быть ограничено и не должно использоваться для повседневных административных задач в Intune.

Корпорация Майкрософт рекомендует следовать принципу минимальных разрешений, назначая администратору только минимальные необходимые разрешения для выполнения своих обязанностей. Для поддержки этого принципа используйте встроенные роли RBAC Intune для ежедневных административных задач Intune и избегайте использования Microsoft Entra ролей, имеющих доступ к Intune.

В следующей таблице указаны Microsoft Entra роли, имеющие доступ к Intune, и разрешения Intune, которые они включают.

Развернуть таблицу

роль Microsoft Entra	Все данные в Intune	Данные аудита Intune
PRIVILEGED глобального администратора	Чтение и запись	Чтение и запись
PRIVILEGED администратор службы Intune"	Чтение и запись	Чтение и запись
PRIVILEGED администратора условного доступа	Нет	Нет
PRIVILEGED администратора безопасности	Только чтение (полные административные разрешения для узла Endpoint Security)	Только чтение
PRIVILEGED оператора безопасности	Только чтение	Только чтение
PRIVILEGED читатель безопасности"	Только чтение	Только чтение
Администратор соответствия требованиям	Нет	Только чтение
Администратор данных соответствия требованиям	Нет	Только чтение
PRIVILEGED читатель" (эта роль эквивалентна роли *оператора службы технической поддержки* Intune)	Только чтение	Только чтение
PRIVILEGED (эта роль эквивалентна роли *оператора службы технической поддержки* Intune)	Только чтение	Только чтение
Читатель отчетов	Нет	Только

роль Microsoft Entra	Все данные в Intune	Данные аудита Intune
		чтение

Помимо Microsoft Entra ролей с разрешениями в Intune, следующие три области Intune являются прямыми расширениями Microsoft Entra: **пользователи**, **группы** и **условный доступ**. Экземпляры этих объектов и конфигураций, сделанных из Intune, существуют в Microsoft Entra. Как Microsoft Entra объектами, ими могут управлять администраторы Microsoft Entra с достаточными разрешениями, предоставленными ролью Microsoft Entra. Аналогичным образом администраторы Intune с достаточными разрешениями для Intune могут просматривать эти типы объектов, созданные в Microsoft Entra, и управлять ими.

Роли глобального администратора и администратора Intune

Роль **глобального администратора** является встроенной ролью в Microsoft Entra и имеет полный доступ к Microsoft Intune. Глобальные администраторы имеют доступ к функциям администрирования в идентификаторе Microsoft Entra и службам, которые используют Microsoft Entra удостоверения, включая Microsoft Intune.

Чтобы снизить риск, выполните приведенные далее действия.

- Не используйте роль глобального администратора в Intune. Корпорация Майкрософт не рекомендует использовать роль глобального администратора для администрирования Intune или управления ими.

  В Intune есть некоторые функции, которым требуется роль глобального администратора, например некоторые соединители защиты от угроз на мобильных устройствах (MTD). В таких случаях используйте роль глобального администратора только при необходимости, а затем удалите ее после завершения задачи.

- Используйте встроенные роли Intune или создайте настраиваемые роли для администрирования Intune и управления ими.

- Назначьте роль Intune с наименьшими привилегиями, необходимую администратору для выполнения своих задач.

Дополнительные сведения о роли глобального администратора Microsoft Entra см. в статье Microsoft Entra встроенные роли — глобальный администратор.

Роль **администратора Intune** — это встроенная роль в Microsoft Entra, а также роль **администратора службы Intune**. Он имеет ограниченный область разрешений на администрирование Intune и управление ими, а также управление связанными функциями, такими как управление пользователями и группами. Эта роль подходит для администраторов, которым нужно только администрировать Intune.

Чтобы снизить риск, выполните приведенные далее действия.

- Назначьте роль администратора Intune только по мере необходимости. Если есть встроенная роль Intune , которая соответствует потребностям администратора, назначьте ее вместо роли администратора Intune. Всегда назначайте роль Intune с наименьшими привилегиями, необходимую администратору для выполнения своих задач.
- Создайте настраиваемые роли, чтобы дополнительно ограничить область разрешений для администраторов.

Расширенные элементы управления безопасностью:

Утверждение нескольких Администратор теперь поддерживает управление доступом на основе ролей. Если этот параметр включен, второй администратор должен утвердить изменения ролей. Эти изменения могут включать обновления разрешений ролей, групп администраторов или назначений групп участников. Изменение вступает в силу только после утверждения. Этот процесс двойной авторизации помогает защитить организацию от несанкционированных или случайных изменений управления доступом на основе ролей. Дополнительные сведения см. в разделе Использование утверждения нескольких Администратор в Intune.

Дополнительные сведения о роли администратора Intune Microsoft Entra см. в статье Microsoft Entra встроенных ролей — администратор Intune.

управление привилегированными пользователями для Intune

При использовании Entra ID управление привилегированными пользователями (PIM) можно управлять тем, когда пользователь может использовать привилегии, предоставляемые ролью Intune RBAC или ролью администратора Intune из Entra ID.

Intune поддерживает два метода повышения ролей. Между этими двумя методами существуют различия в производительности и минимальных привилегиях.

- **Метод 1**. Создайте JIT-политику с Microsoft Entra управление привилегированными пользователями (PIM) для Microsoft Entra встроенной роли **администратора Intune** и

назначьте ей учетную запись администратора.

- **Метод 2**. Используйте управление привилегированными пользователями (PIM) для групп с назначением роли RBAC Intune. Дополнительные сведения об использовании PIM для групп с ролями RBAC Intune см. в статье Настройка JIT-доступа администратора Microsoft Intune с помощью Microsoft Entra PIM для групп | Центр сообщества Майкрософт

При использовании повышения прав PIM для роли администратора Intune из Entra ID повышение прав обычно происходит в течение 10 секунд. Повышение прав на основе групп PIM для встроенных или пользовательских ролей Intune обычно занимает до 15 минут.

Сведения о назначениях ролей Intune

Как пользовательские, так и встроенные роли Intune назначаются группам пользователей. Назначенная роль применяется к каждому пользователю в группе и определяет:

- какие пользователи назначены этой роли;
- какие ресурсы они могут видеть;
- какие ресурсы они могут менять.

Каждая группа, которым назначена роль Intune, должна включать только пользователей, которым разрешено выполнять административные задачи для этой роли.

- Если встроенная роль с наименьшими привилегиями предоставляет чрезмерные привилегии или разрешения, рекомендуется использовать пользовательскую роль для ограничения область административного доступа.
- При планировании назначений ролей учитывайте результаты пользователя с несколькими назначениями ролей.

Для назначения роли Intune и доступа к администрированию Intune пользователю не требуется лицензия Intune, *если* его учетная запись была создана в Entra после июня 2021 г. Учетным записям, созданным до июня 2021 г., требуется назначить лицензию на использование Intune.

Чтобы просмотреть существующее назначение ролей, выберите **Intune**>**Администрирование**> клиента**Роли**>**Все роли**> выбирают роль >**Назначения**> выберите назначение. На странице **свойств** назначений можно изменить:

- **Основные сведения**: имена и описание назначений.

- **Участники**. Участники — это группы, которые настраиваются на странице *группы Администратор* при создании назначения ролей. Все пользователи в

перечисленных группах безопасности Azure имеют разрешение на управление пользователями и устройствами, перечисленными в *разделе Область (группы)*.

- **Область (группы)**. Используйте область (группы), чтобы определить группы пользователей и устройств, которыми может управлять администратор с этим назначением роли. Пользователи с правами администратора с этим назначением роли могут использовать разрешения, предоставленные ролью, для управления каждым пользователем или устройством в рамках назначений ролей, определенных область группами.

  > **Совет**
  >
  > При настройке группы область ограничьте доступ, выбрав только группы безопасности, включающие пользователей и устройства, которыми должен управлять администратор с назначением этой роли. Чтобы администраторы с этой ролью не могли ориентироваться на всех пользователей или все устройства, не выбирайте *Добавить всех пользователей* или *Добавить все устройства*.
  >
  > Если вы указываете группу исключений для назначения, например политики или приложения, она должна быть либо вложена в одно из назначений RBAC область групп, либо должна быть отдельно указана в качестве область группы в назначении ролей RBAC.

- **Теги области. Пользователи** с правами администратора, которым назначена эта роль, могут просматривать ресурсы с одинаковыми область тегами.

> **Примечание**
>
> Теги области — это текстовые значения свободной формы, которые администратор определяет, а затем добавляет к назначению роли. Тег область, добавленный в роль, управляет видимостью самой роли. Тег область, добавленный в назначение ролей, ограничивает видимость объектов Intune, таких как политики, приложения или устройства, только администраторами в этом назначении ролей, так как назначение роли содержит один или несколько соответствующих тегов область.

Несколько назначений ролей

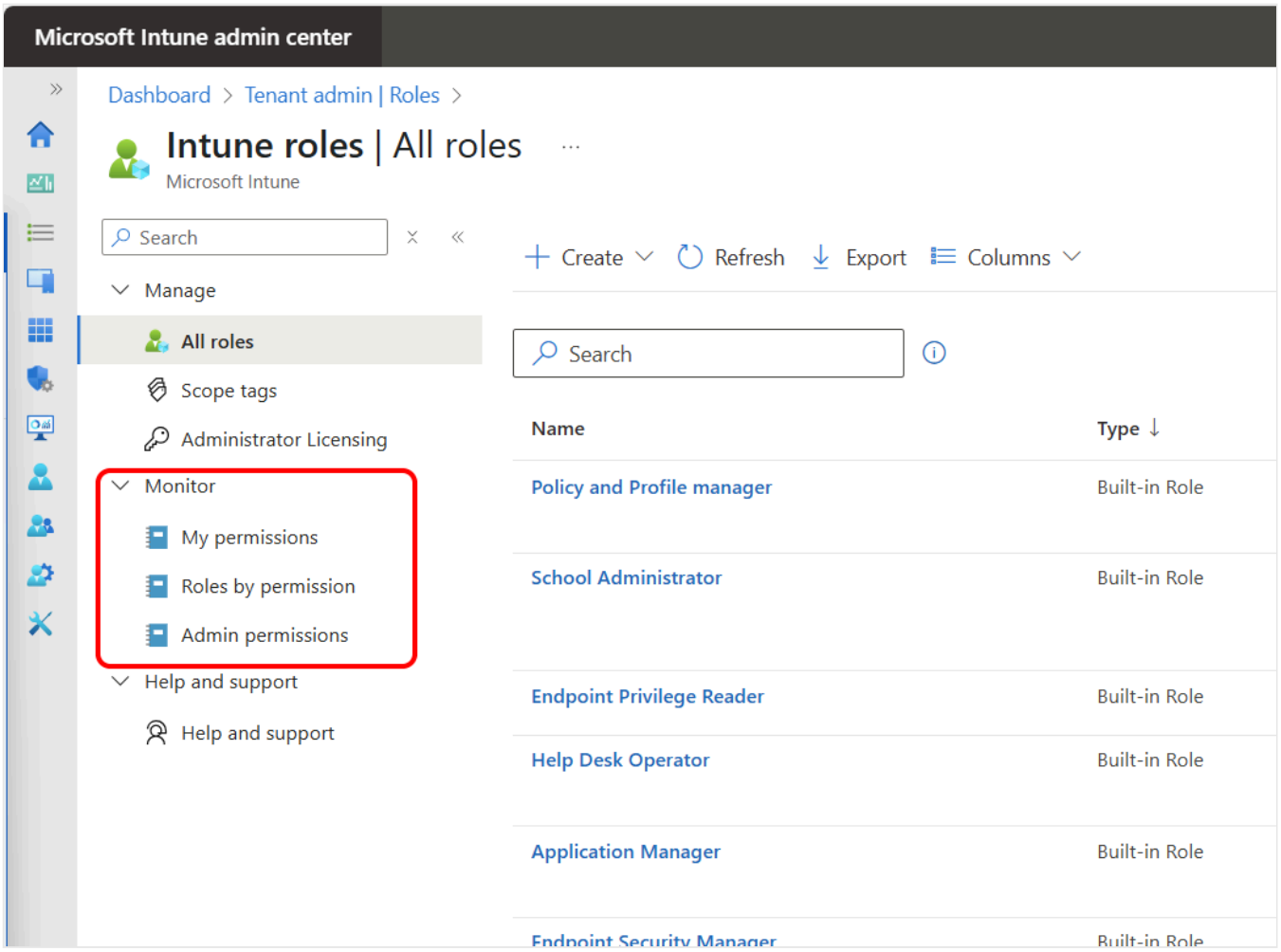
Если пользователь имеет несколько назначений ролей, разрешений и тегов области, эти назначения ролей распространяются на разные объекты следующим образом:

- Разрешения бывают добавочными в случае, когда две или более ролей предоставляют разрешения для одного и того же объекта. Например, пользователь с разрешениями на чтение от одной роли и чтение и запись из другой роли имеет действующее разрешение на чтение и запись (при условии, что назначения для обеих ролей предназначены для одного и того же область тегов).
- Разрешения назначений и теги области применяются только к объектам (например, политикам или приложениям) в области (группах) назначений этой роли. Разрешения назначений и теги области не применяются к объектам в других назначениях ролей, если другие назначения явно не предоставляют их.
- Другие разрешения (такие как создание, чтение, обновление, удаление) и теги областей применяются ко всем объектам одного типа (например, ко всем политикам или всем приложениям) в любых назначениях пользователей.
- Разрешения и теги области для объектов различных типов (например, политик или приложений) не применяются друг к другу. Например, разрешение на чтение для политики не предоставляет разрешение на чтение в приложениях в назначениях пользователя.
- Если нет тегов область или некоторые область теги назначены из разных назначений, пользователь может видеть только устройства, которые являются частью некоторых тегов область и не могут видеть все устройства.

Мониторинг назначений RBAC

Этот и три подраздела находятся в процессе выполнения

В Центре администрирования Intune можно перейти к**разделу Ролиадминистратора**> клиента и развернуть **элемент Монитор**, чтобы найти несколько представлений, которые помогут вам определить разрешения, которые разные пользователи имеют в вашем клиенте Intune. Например, в сложной административной среде можно использовать представление **разрешений Администратор**, чтобы указать учетную запись, чтобы просмотреть ее текущую область административных привилегий.



Мои разрешения

При выборе этого узла отображается объединенный список текущих категорий и разрешений Intune RBAC, предоставленных вашей учетной записи. В этом объединенном списке содержатся все разрешения от всех назначений ролей, но не то, какие назначения ролей предоставляют их или каким членством в группах они назначены.

Роли по разрешениям

В этом представлении можно просмотреть сведения о конкретной категории и разрешениях RBAC Intune, а также о назначениях ролей и группах, которым предоставляется доступ к этой комбинации.

Чтобы приступить к работе, выберите категорию разрешений Intune, а затем конкретное разрешение из этой категории. Затем в Центре администрирования отображается список экземпляров, которые приводят к назначению этого разрешения, в том числе:

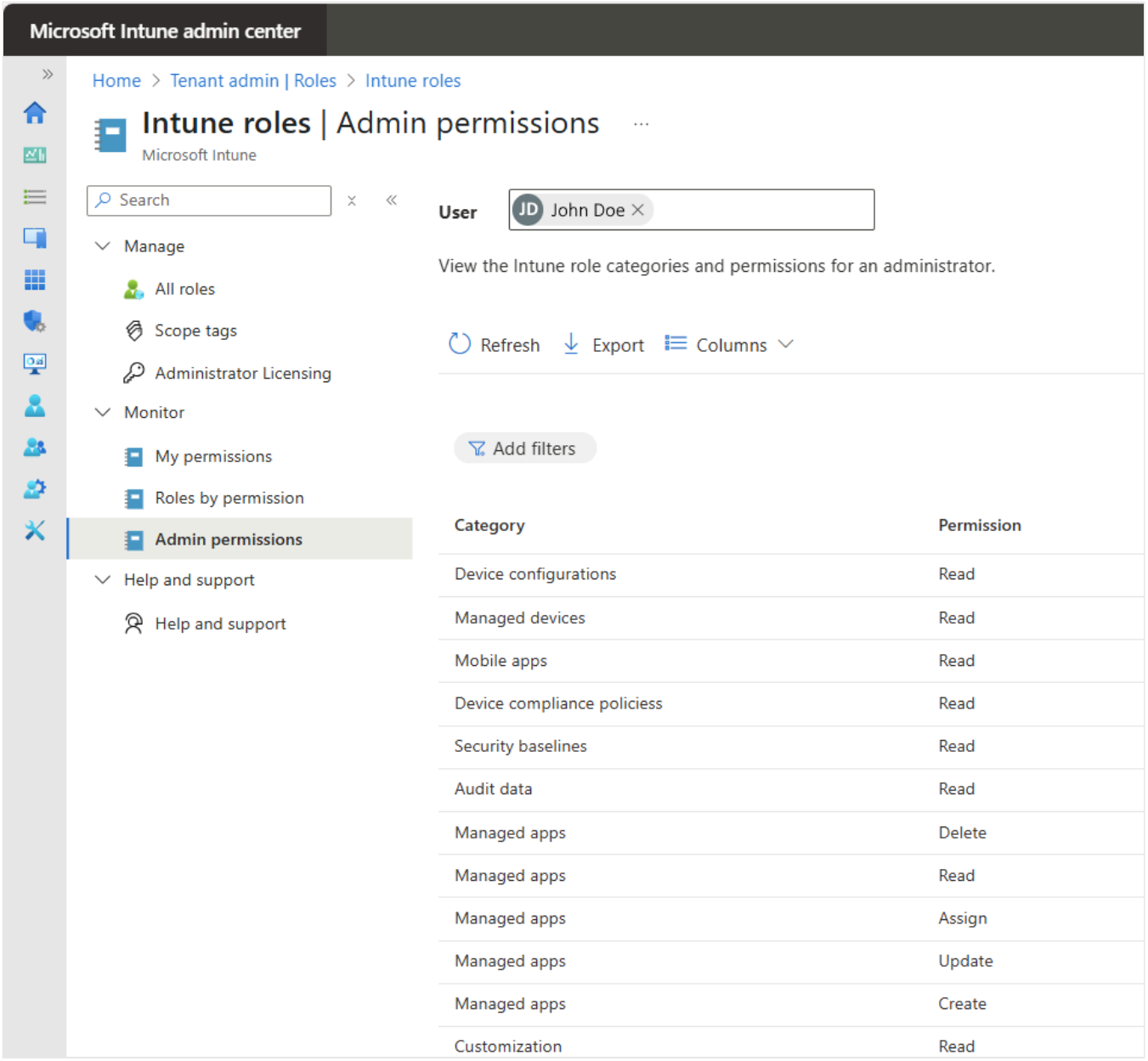
- **Отображаемое имя роли** — имя встроенной или настраиваемой роли RBAC, которая предоставляет разрешение.

- **Отображаемое имя назначения роли** — имя назначения роли, которая назначает роль группам пользователей.
- **Имя группы** — имя группы, которая получает это назначение роли.

разрешения Администратор

Используйте узел Администратор разрешений, чтобы определить конкретные разрешения, предоставленные учетной записи в данный момент.

Начните с указания учетной записи **пользователя** . Пока пользователю назначены разрешения Intune для его учетной записи, Intune отображает полный список этих разрешений, определенных *по категориям* и *разрешениям*.



Дальнейшие действия

- Назначение роли пользователю
- Создание настраиваемой роли

Рекомендации о размере облачного компьютера

Статья • 31.01.2025

Windows 365 предлагает лицензирование с фиксированной ценой (с помощью Microsoft 365) для различных размеров Облачных компьютеров. Необходимо оценить бизнес-требования, чтобы определить, какие размеры лучше подходят для ваших пользователей.

Если для Облачного компьютера требуются дополнительные ресурсы, администратор или конечный пользователь могут легко увеличить размер Облачного компьютера. Дополнительные сведения см. в разделе Изменение размера Облачного компьютера.

Сведения о требованиях к оборудованию пользователя см. в статье Требования к оборудованию пользователей.

В этой таблице приведены примеры различных размеров, доступных для Облачных компьютеров:

Развернуть таблицу

ЦП, ОЗУ и хранилище для Облачных компьютеров	Примеры сценариев	Рекомендуемые приложения
2 виртуальных ЦП/4 ГБ/256 ГБ 2 виртуальных ЦП/4 ГБ/128 ГБ 2 виртуальных ЦП/4 ГБ/64 ГБ	Сотрудники первой линии, центры обработки вызовов, доступ к образованию, обучению/ доступ к CRM, слияния и приобретения, краткосрочные и сезонные, обслуживание клиентов.	Приложения Microsoft 365, Microsoft Teams (только аудио), OneDrive, Adobe Reader, Microsoft Edge, бизнес-приложения, поддержка Defender.
2 виртуальных ЦП/8 ГБ/256 ГБ 2 виртуальных ЦП/8 ГБ/128 ГБ	Использование собственных компьютеров, работа из дома, исследования рынка, государственные организации, консультанты.	Приложения Microsoft 365, Microsoft Teams, Outlook, Excel, Access, PowerPoint, OneDrive, Adobe Reader, Microsoft Edge, бизнес-приложения, поддержка Defender.
4 виртуальных ЦП/16 ГБ/512 ГБ 4 виртуальных ЦП/16 ГБ/256 ГБ	Финансы, государственные	Приложения Microsoft 365, Microsoft Teams, Outlook,

ЦП, ОЗУ и хранилище для Облачных компьютеров	Примеры сценариев	Рекомендуемые приложения
4 виртуальных ЦП/16 ГБ/128 ГБ	учреждения, консультанты, медицинские услуги, собственные ПК, работа из дома.	Excel, Access, PowerPoint, Power BI, Dynamics 365, OneDrive, Adobe Reader, Microsoft Edge, бизнес-приложение, поддержка Defender.
8 виртуальных ЦП/32 ГБ/512 ГБ 8 виртуальных ЦП/32 ГБ/256 ГБ 8 виртуальных ЦП/32 ГБ/128 ГБ	Разработчики программного обеспечения, инженеры, создатели контента, рабочие станции для проектирования.	Приложения Microsoft 365, Microsoft Teams, Outlook, Access, OneDrive, Adobe Reader, Microsoft Edge, Power BI, Visual Studio Code, рабочие нагрузки на основе виртуализации: поддержка Hyper-V, подсистемы Windows для Linux (WSL), бизнес-приложений и Defender.
GPU Standard 4vCPU/16GB/4GBvRAM/512 ГБ GPU Super 8CPU/56GB/12GBvRAM/1TB Gpu Max 16vCPU/110GB/16GBvRAM/1TB Дополнительные сведения см. в разделе Облачные компьютеры с GPU.	Графический дизайн, отрисовка изображений и видео, трехмерные моделирование, игры, обработка данных и визуализация	Приложения Microsoft 365, Microsoft Teams, Outlook, Excel, Access, Adobe, Figma, Autodesk, Revit, Illustrator, Blender, Unity, ArcGIS, Microsoft Edge, Power BI, Visual Studio Code, бизнес-приложения, поддержка Defender.
16 в ЦП/64 ГБ/512 ГБ ЦП 16 в/64 ГБ/1TB	Разработка программного обеспечения, проектирование, анализ и визуализация данных, финансовые услуги и управление активами.	Приложения Microsoft 365, Microsoft Teams, Outlook, Excel, Access, Adobe Reader, Microsoft Edge, Power BI, Tableau, Visual Studio Code, Blackrock Aladdin, Bloomberg, Eclipse, бизнес-приложения, поддержка Defender.

Рекомендуемый образ из коллекции доступен в marketplace политик подготовки. Дополнительные сведения см. в разделе Общие сведения об образах устройств.

Проверка производительности

Чтобы обеспечить соблюдение требований, протестируйте развертывание с помощью средств моделирования. Вы можете отслеживать пользовательский опыт

и потребление ресурсов с помощью таких служб, как служба Аналитики конечных точек.

Дальнейшие действия

Дополнительные сведения см. в разделе Общие сведения об образах устройств.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Облачные компьютеры GPU в Windows 365

06.06.2025

Windows 365 предлагает облачные компьютеры с поддержкой GPU, которые подходят для интенсивных графических рабочих нагрузок, которые должны быть оптимизированы для производительности. Эти предложения могут помочь в графическом дизайне, отрисовке изображений и видео, трехмерном моделировании, а также в приложениях для обработки и визуализации данных, которым требуется GPU.

Для Windows 365 Enterprise (включая FedRamp) и Windows 365 Frontline облачных компьютеров в выделенном режиме доступны три предложения GPU:

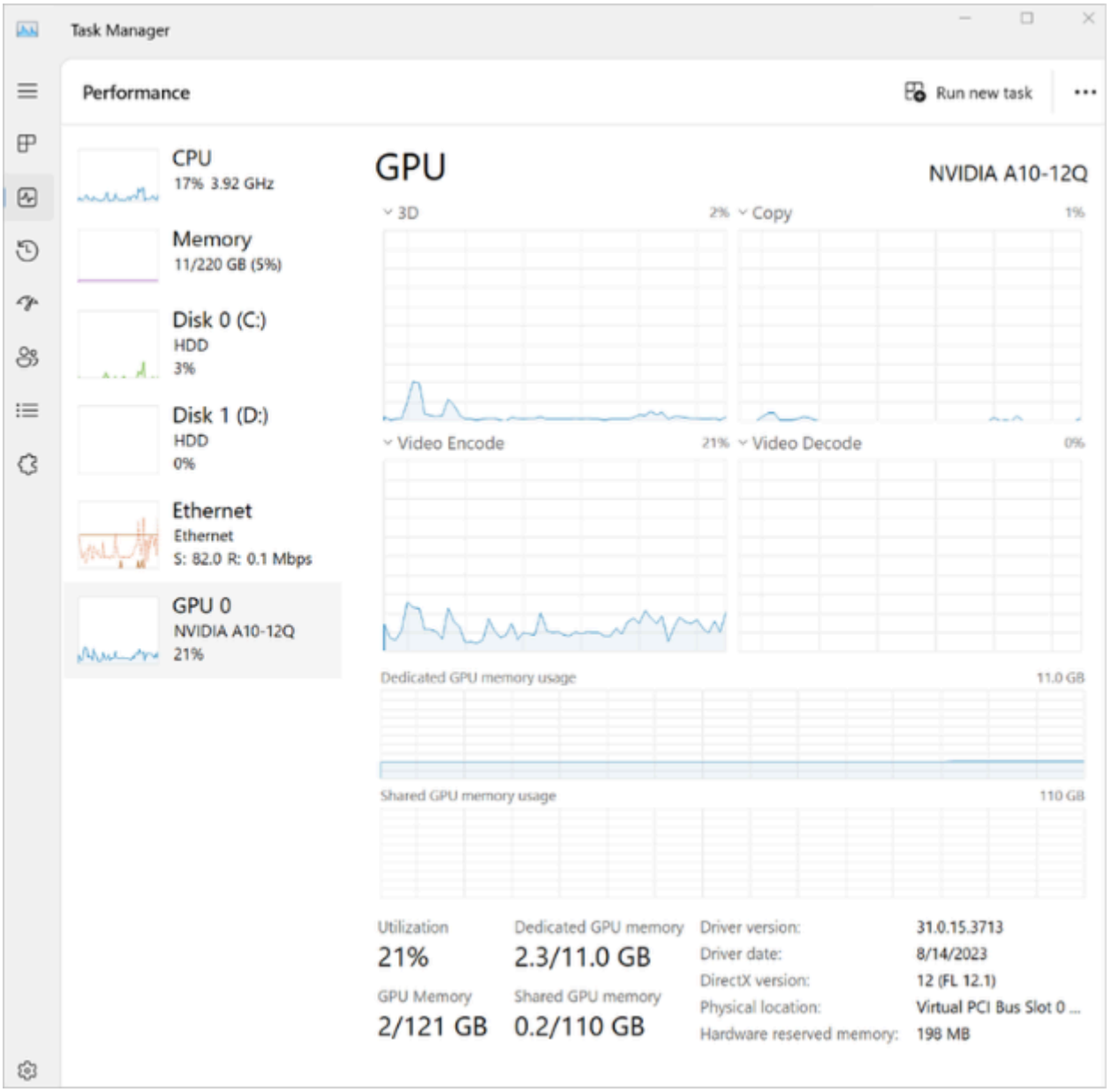
Развернуть таблицу

Предложение GPU	Минимальные спецификации	Руководствовался	Назначение
Standard GPU Windows 365 Корпоративная	4 виртуальных ЦП, 16 ГБ ОЗУ, 8 ГБ виртуальной памяти, 512 ГБ (с временным хранилищем 176 ГБ)	NVIDIA и AMD	Приложения, использующие базовое ускорение графики на одном дисплее 3840x2160 или до двух дисплеев с разрешением 1920x1080p.
Windows 365 Корпоративная GPU Super	8 виртуальных ЦП, 56 ГБ ОЗУ, 12 ГБ виртуальной памяти, 1 ТБ (с временным хранилищем 352 ГБ)	NVIDIA	Приложения с более высокими требованиями к спецификациям и высокопроизводительными графическими рабочими нагрузками на четырех дисплеях 3840x2160.
Максимальное число GPU Windows 365 Корпоративная	16 виртуальных ЦП, 110 ГБ ОЗУ, 16 ГБ виртуальной памяти, 1 ТБ (с временным хранилищем 352 ГБ)	NVIDIA	Графические рабочие нагрузки, требующие высокой производительности и строгие требования к задержке.

Дополнительные сведения об этих предложениях см. в статье Рекомендации по размеру облачных компьютеров.

Так как региональная емкость является динамической, корпорация Майкрософт использует доступную емкость, когда она необходима. Иногда это может привести к превышению минимальных спецификаций облачных компьютеров GPU. Чтобы

просмотреть спецификации GPU облачного компьютера, перейдите на вкладку производительности диспетчера задач.



Облачные компьютеры GPU не поддерживают вложенную виртуализацию. Дополнительные сведения см. в статье Настройка рабочих нагрузок на основе виртуализации на Облачный компьютер Windows 365.

Чтобы приобрести предложения GPU, обратитесь в свою группу учетных записей. Предложения GPU недоступны в прямом веб-канале.

Размещение облачных компьютеров GPU и d: сведения о хранилище диска

Корпорация Майкрософт размещает Windows 365 облачных компьютерах с поддержкой GPU, используя последнюю версию Microsoft Hyper-V.

Каждый из этих облачных компьютеров поставляется с накопителем SSD (c:) для данных и приложений, а также большим временным диском (d:).

Временный диск (d: диск) удаляется и повторно создается при каждой перезагрузке облачного компьютера. Никогда не используйте его для хранения данных. Вместо этого его можно использовать в качестве диска кэша для хранения временных файлов. Эта стратегия полезна для повышения производительности приложений, которым требуются временные диски для обработки больших наборов данных.

Разделы реестра и драйверы на облачных компьютерах GPU

Разделы реестра задаются автоматически в процессе подготовки.

Поддерживаемые драйверы устанавливаются автоматически в процессе подготовки. Вам не нужно устанавливать драйверы вручную. Однако драйверы не обновляются автоматически, поэтому при необходимости необходимо вручную обновить драйверы.

Список разрешенных

На каждом Windows 365 облачном компьютере GPU необходимо разрешить следующие URL-адреса:

Развернуть таблицу

URL-адрес	Оборудование
download.microsoft.com	Nvidia, AMD
go.microsoft.com	Nvidia, AMD
raw.githubusercontent.com/Azure/azhpc-extensions/master/NvidiaGPU/resources.json (файл ресурсов драйвера Nvidia)	Nvidia
raw.githubusercontent.com/Azure/azhpc-extensions/master/AmdGPU/resources.json (файл ресурсов драйвера AMD)	AMD

Поддерживаемые регионы

Предложения GPU доступны во всех поддерживаемых регионах Windows 365, за исключением следующих регионов:

- Центральная часть США

- Восточная Норвегия
- Западная Европа (Windows 365 Корпоративная Standard GPU доступен в этом регионе)

Регион "Западная часть США 2" поддерживается, но является ограниченным регионом.

Рекомендации по использованию облачных компьютеров GPU

Чтобы обеспечить оптимальную производительность облачных компьютеров с поддержкой GPU, ознакомьтесь со следующими рекомендациями:

- Убедитесь, что сеть настроена для включения UDP по умолчанию. Дополнительные сведения о UDP см. в разделе RDP Shortpath.

- Убедитесь, что вы используете облачный компьютер GPU в полноэкранном режиме. Свернутые окна требуют дополнительной обработки и координации с локальным устройством, что может помешать производительности сеанса.

- Используйте приложение Windows для оптимального подключения.

- Используйте Windows 11 облачных компьютеров.

- Облачные компьютеры с поддержкой GPU предварительно подготовлены с правильным драйвером, необходимым для оптимальной работы. Сведения об установке драйверов см. в разделах Установка драйверов GPU NVIDIA на виртуальных машинах серии N под управлением Windows и Установка драйверов AMD GPU на виртуальных машинах серии N под управлением Windows (для Standard SKU только в ограниченных регионах). Использование любых внешних драйверов, включая драйверы с веб-сайтов NVIDIA и AMD, не поддерживается.

- Не используйте расширение перенаправления мультимедиа для браузера или Teams. По умолчанию это расширение удаляется для облачных компьютеров с поддержкой GPU во время подготовки.

- Предложения GPU не предназначены для разработки игр. Эти предложения оптимизированы для графических приложений, которые обычно используются в корпоративных сценариях. Дополнительные сведения о сценариях разработки игр см. в статье Создание виртуальной машины разработки игр с помощью других игровых движков.

- Если вы хотите гарантировать, что все пользователи имеют одинаковую конфигурацию BPU, вместо облачных компьютеров можно использовать

Виртуальный рабочий стол Azure (AVD). AVD может помочь клиентам, которые предпочитают конфигурации конкретного оборудования, а не конфигурации, ориентированные на рабочую нагрузку. Полный список предложений GPU Azure см. в статье Размеры виртуальных машин в Azure с ускорением GPU.

- По умолчанию облачные компьютеры с поддержкой GPU подготавливаются для использования удаленного кодирования кадров с ускорением GPU. Дополнительные сведения о различных профилях кодирования графики с аппаратным ускорением и управлении ими на облачных компьютерах с поддержкой GPU см. в разделе Включение ускорения GPU.
  - В следующей таблице приведена совместимость номеров SKU Облачный компьютер Windows 365 с двумя различными профилями кодирования графики с ускорением GPU.

Развернуть таблицу

Windows 365 Корпоративная GPU	Поддерживаемые удаленные кодировщики кадров с ускорением GPU
Max	HEVC/H.265 AVC/H.264
Супер	HEVC/H.265 AVC/H.264
Стандартный	AVC/H.264

Дальнейшие действия

Дополнительные сведения о предложениях облачных компьютеров см. в статье Рекомендации по размеру облачных компьютеров.

Windows 365 производительность облачного компьютера с поддержкой GPU

Статья • 31.01.2025

Windows 365 предоставляет следующие конфигурации облачных компьютеров с поддержкой графического процессора (GPU) для Windows 365 Корпоративная и Windows 365 Frontline:

- Standard GPU Windows 365
- Windows 365 GPU Super
- Максимальное число GPU Windows 365

Эти предложения поддерживаются NVIDIA и AMD для удовлетворения следующих вопросов:

- графический дизайн
- отрисовка изображений и видео
- Трехмерные модели
- рабочие нагрузки визуализации и обработки данных

Обновления

Windows 365 облачные компьютеры с поддержкой GPU подготавливаются с использованием высокопроизводительного оборудования. Однако инфраструктура со временем развивается, что может привести к обновлению базовых виртуальных машин и оборудования, доступных клиентам. Эти корректировки необходимы для реализации улучшений, поддержания производительности и улучшения взаимодействия с конечными пользователями. Команда разработчиков Windows 365 продуктов регулярно проводит тщательное тестирование, чтобы каждое обновление способствовало повышению производительности Windows 365 облачных пк с поддержкой GPU. В этой статье рассматривается, как мы тестируем производительность облачных компьютеров с поддержкой GPU Windows 365, а также относительные целевые показатели рабочей нагрузки трех предложений.

Тестирование производительности графики

Чтобы оценить производительность облачных компьютеров с Windows 365 с поддержкой GPU, мы проводим различные отраслевые стандартные графические

тесты:

- Отрисовка тестов производительности для оценки стабильности и производительности GPU. Мы используем различные примеры файлов для измерения скорости и качества отрисовки. Эти тесты помогают понять, насколько хорошо GPU обрабатывает сложные визуальные задачи.
- Тест разрешения отрисовки для оценки частоты кадров и задержки. Мы тестируем различные разрешения (например, 1080p и 4K), чтобы понаблюдать за тем, как GPU работает при различных требованиях к дисплею. Высокое разрешение может повысить нагрузку на GPU.
- Тесты ЦП, чтобы понять влияние производительности ЦП на графические задачи. Мы анализируем, насколько хорошо выгружается ЦП на GPU во время отрисовки и других операций с большим объемом графики.
- Стресс-тесты для оценки общей производительности и надежности системы. Система подвергается тяжелым рабочим нагрузкам, имитируя реальное использование. Эти тесты помогают выявить все узкие места или проблемы.

Все конфигурации облачных компьютеров с поддержкой GPU тестируются в одной рабочей среде в одном регионе. Конкретные сторонние агенты, развернутые клиентами, не учитываются при обычном тестировании, так как у них могут быть собственные требования к ресурсам, влияющие на производительность.

Проведение собственного тестирования может предоставить ценные сведения, которые очень похожи на потребности ваших пользователей в графике. Включите графические приложения, которые используют пользователи, и проверьте результаты теста, чтобы принять обоснованные решения для пользователей. Дополнительные сведения см. в руководстве по планированию для Windows 365.

Целевые объекты рабочей нагрузки графики

Хотя программная отрисовка не с поддержкой GPU Windows 365 облачных компьютеров отлично подходит для большинства приложений, некоторые приложения могут требовать производительности прямых вызовов API, использующих GPU. К числу распространенных примеров относятся продукты Adobe, ArcGIS, Autodesk и Dassault Systèmes. Другие продукты могут потребовать использования выделенного GPU или оптимизированы для более эффективной работы с ним в соответствии с требованиями к системе, опубликованными на соответствующих веб-сайтах.

Развернуть таблицу

Предложение GPU	Назначение	Поддерживаемые дисплеи	Сравнимо с	Поддержка разработки ИИ
Standard GPU Windows 365	Графическим приложениям требуется не более 8 ГБ виртуальной памяти.	Один дисплей 3840x2160 или до двух дисплеев 1920x1080.	Устройства с выделенными графическими графическими процессорами начального уровня.	Нет.
Windows 365 GPU Super	Для рабочих нагрузок высокопроизводительной графики требуется не более 12 ГБ виртуальной памяти.	До четырех дисплеев 3840x2160.	Настольные устройства с выделенными графическими GPU.	Нет.
Максимальное число GPU Windows 365	Максимальная производительность, требующая до 24 ГБ виртуальной памяти.	Поддержка нескольких дисплеев с более высоким разрешением.	Рабочие станции классической графики, обслуживающие самые требовательные графические рабочие нагрузки.	Да, с vsCode AI Toolkit, Phi-3 с ONNX и многое другое.

Все облачные компьютеры с поддержкой GPU совместимы с функциями ИИ, интегрированными в широко используемые программные приложения, такие как Copilot, и поддерживают их. Для разработки ИИ или для выполнения задач ИИ, требующих интенсивной обработки GPU, используйте Windows 365 GPU Max.

Корпорация Майкрософт размещает облачные компьютеры с поддержкой GPU с помощью последней итерации Microsoft Hyper-V. Каждый облачный компьютер оснащен диском хранилища (C:) для файлов и программ, а также значительным временным диском (D:). Рекомендуется использовать диск D: для кэширования временных файлов, что может повысить производительность приложений, требующих "с нуля" дисков для обработки обширных наборов данных.

Обязательно ознакомьтесь с требованиями к системе поставщиков программного обеспечения, прежде чем принимать решение о том, какой облачный компьютер с поддержкой GPU лучше всего подходит для вас. Если вы обнаружите, что текущий размер облачного компьютера с поддержкой GPU не соответствует вашим потребностям, вы можете выбрать предложение с более высокой конфигурацией.

Дальнейшие действия

Дополнительные сведения о предложениях облачных компьютеров GPU см. в статье Облачные компьютеры GPU в Windows 365.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Общие сведения о развертывании Windows 365

Статья • 31.01.2025

После приобретения вашей организацией одной или нескольких лицензий Windows 365 узел Windows 365 в Microsoft Intune станет активным для управления. На этом этапе вы можете подготовить облачные компьютеры.

Чтобы настроить систему для подготовки Облачных компьютеров для пользователей по требованию, выполните следующие действия:

1. Назначьте лицензии пользователям.
2. Создайте сетевое подключение Azure (необязательно).
3. Предоставьте локализованный интерфейс Windows (необязательно).
4. Добавьте образы устройств (необязательно).
5. Создайте политику подготовки.

Далее вы узнаете, как назначать лицензии пользователям.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Назначение лицензий

Статья • 31.01.2025

Windows 365 лицензии должны быть назначены, прежде чем пользователи смогут использовать облачный компьютер.

Windows 365 Корпоративная

Чтобы пользователь мог работать с облачным компьютером, необходимо назначить пользователю лицензию Windows 365. Лицензии можно назначить с помощью любого из следующих методов:

- Центр администрирования Microsoft 365 для отдельных пользователей. Инструкции по назначению лицензий с помощью Центра администрирования см. в статье Назначение лицензий пользователям.
- Центр администрирования Microsoft Entra для назначений лицензий групп. Дополнительные сведения о назначениях лицензий групп см. в статье Назначение лицензий пользователям по членству в группах в Microsoft Entra ID.
- Чтобы назначить прямые лицензии списку отдельных пользователей, см. статью Назначение лицензий для Windows 365 или назначение лицензии для выполнения с помощью Graph.

Windows 365 Frontline

Лицензии на Windows 365 Frontline назначаются клиенту и совместно используются на облачных компьютерах, подготовленных в выделенном и общем режиме. Лицензии назначаются путем выбора Microsoft Entra группы во время создания политик подготовки.

Дальнейшие действия

Создание сетевого подключения Azure.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

облачные приложения Windows 365 (предварительная версия)

26.09.2025

Функция Windows 365 Cloud Apps позволяет администраторам предоставлять пользователям безопасный доступ к отдельным приложениям, размещенным на облачном компьютере, не требуя выделенного облачного компьютера для каждого пользователя. Windows 365 Frontline лицензии дают организациям право выполнять потоковую передачу Windows 365 облачных приложений при работе с облачными компьютерами в общем режиме.

Этот компонент находится в состоянии общедоступной предварительной версии.

Предварительные требования

Для создания облачных приложений требуется лицензия на Windows 365 Frontline.

Создание облачных приложений

1. Сначала создайте политику подготовки Windows 365 и выполните следующие действия.

    a. На вкладке **Общие** в разделе **Взаимодействие** выберите "Доступ только к приложениям". При выборе по умолчанию для параметра Тип лицензии заданы режимы Frontline и Shared.

    b. При необходимости на вкладке **Изображение** просмотрите приложения, доступные на изображении, которые можно опубликовать после подготовки.

2. После создания политики облачные компьютеры frontline в режиме общего доступа с типом интерфейса "Облачное приложение" начинают подготовку на **всех облачных компьютерах**. После подготовки первого облачного компьютера приложения, доступные на изображении, будут отображаться как "Готовы к публикации" во **всех облачных приложениях**.

3. Во **всех облачных приложениях** можно публиковать, изменять, сбрасывать и отменять публикацию облачных приложений.

    a. При публикации облачных приложений состояние приложения изменяется с "Готово к публикации" на "Публикация" на "Опубликовано". Публикация

приложения делает его доступным в Windows App для всех пользователей, назначенных политике подготовки.

i. Если приложение находится в состоянии "Сбой", попробуйте отменить публикацию и повторно опубликовать.

b. Вы можете изменить отдельные сведения о Cloud App, включая отображаемое имя, описание, командную строку и индекс пути значка. Теги и назначения область Cloud App наследуются из политики подготовки. Изменения публикуются немедленно в Windows App.

c. Сведения об облачном приложении можно сбросить в исходное состояние обнаружения из образа устройства.

d. При отмене публикации облачных приложений состояние приложения изменяется с "Опубликовано" на "Готово к публикации", и приложение больше не доступно в Windows App. Сведения о приложении также сбрасываются.

4. Чтобы удалить облачные приложения, необходимо удалить назначение политики подготовки облачных приложений.

> ⓘ **Примечание**
>
> Так как облачные приложения работают на **облачных компьютерах Frontline в режиме общего доступа**, те же возможности управления и конечных пользователей, которые применяются к общим облачным компьютерам frontline, также применяются к облачным приложениям.
>
> - Максимальное число активных сеансов Windows 365 Cloud App для политики подготовки равно количеству Windows 365 Frontline лицензий, назначенных этой конкретной политике. Вы можете отслеживать параллелизм в отчете Подключенные облачные компьютеры frontline.
> - Все параметры, применяемые к базовым облачным компьютерам Frontline, такие как перенаправление или параметры времени ожидания простоя, также применяются к облачным приложениям.

Доступ к облачным приложениям

Конечные пользователи получают доступ к опубликованным приложениям через Windows App. Обратите внимание, что опубликованные приложения также могут открывать другие приложения, которые находятся на облачном компьютере. Например,

Microsoft Outlook в качестве облачного приложения может запускать Microsoft Edge через внедренные ссылки в сообщениях электронной почты, даже если Microsoft Edge не опубликован как облачное приложение. Чтобы полностью контролировать доступ к приложениям, используйте управление приложениями для Windows.

Если на облачных компьютерах установлены поддерживаемые версии Windows (Windows 11 Корпоративная, версии 24H2 или 22H2 или 23H2 с установленным накопительным обновлением 2024-07 для Windows 11 (KB5040442) или более поздней версии), облачные приложения автоматически запускают OneDrive.

Известные ограничения

- Облачные приложения обнаруживают только исполняемые файлы приложений в меню "Пуск " образа устройства, которые не установлены пакетами Appx или MSIX. В результате облачные приложения в настоящее время не поддерживают Microsoft Teams. В разработке: вы сможете обнаруживать и публиковать приложения Appx и MSIX как облачные приложения.
- В предварительной версии вы не можете изменить путь к значку облачного приложения. В разработке: вы сможете изменить путь к значку.
- В предварительной версии вы можете связать политику подготовки устройств Autopilot, но вы не можете публиковать приложения Intune как облачные приложения. В процессе разработки: вы сможете обнаруживать и публиковать приложения, установленные Intune, которые включены в политику подготовки устройств Autopilot, связанную с политикой подготовки облачных приложений.
- В предварительной версии, если вы хотите опубликовать приложения, которые не установлены в Windows 365 образах коллекции, необходимо использовать пользовательский образ.
- При отправке пользовательского образа Windows 365 Cloud Apps использует скрипт PowerShell для сканирования приложений в меню "Пуск". Однако если клиент применяет политики безопасности, требующие дополнительной проверки подлинности для PowerShell, мы не сможем обнаружить приложения. Кроме того, если пользовательский образ не поддерживается, мы не сможем обнаружить приложения.

Создание сетевого подключения Azure

Статья • 08.05.2025

Сетевые подключения Azure (ANC) позволяют подготовить облачные компьютеры, которые присоединяются к управляемой вами виртуальной сети.

Для каждого клиента может быть до 50 АНК.

В рамках процесса подключения службе Windows 365 предоставляются следующие разрешения:

- Разрешение читателя на подписку Azure.
- Windows 365 роль участника сетевого интерфейса в указанной группе ресурсов.
- Windows 365 роль пользователя сети в виртуальной сети.

Требования

Чтобы создать ANC, необходимо выполнить следующие требования:

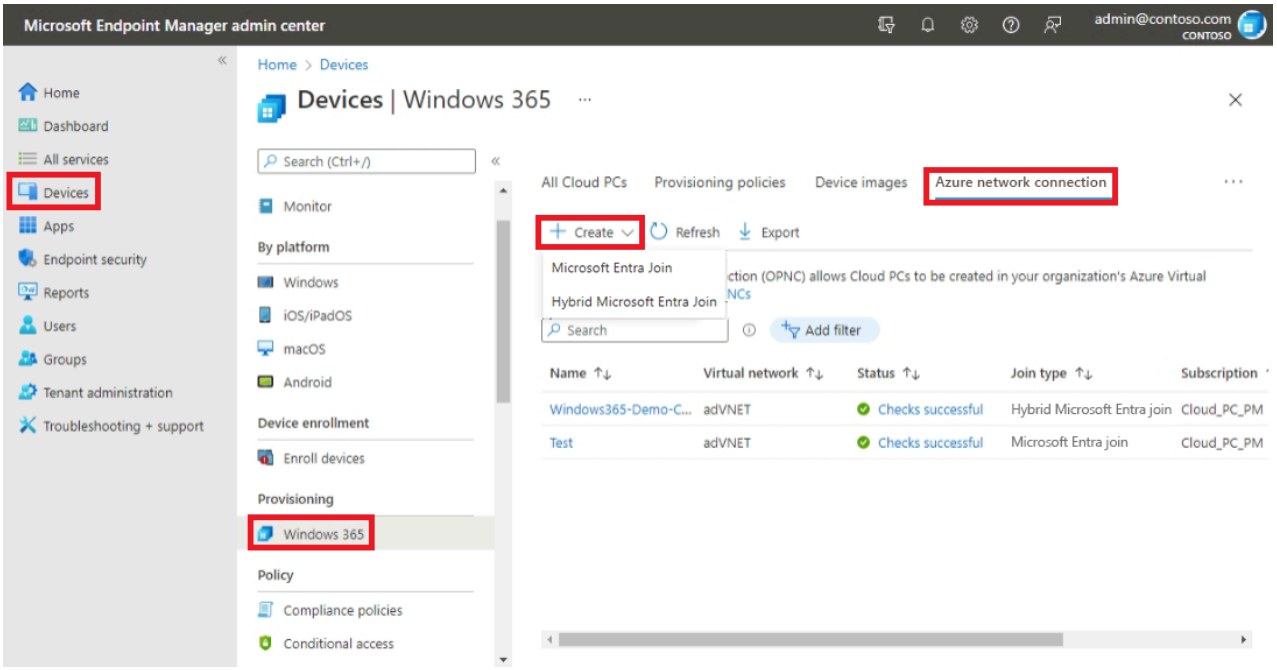
- У вас есть роль администратора Intune или администратора Windows 365.
- У вас есть учетная запись пользователя Active Directory с достаточными разрешениями для присоединения домена AD к этому подразделению (гибридное Microsoft Entra присоединение только к ANCs).
- Укажите роль читателя подписки в подписке Azure, где была размещена виртуальная сеть, связанная с ANC.
- Если вы хотите создать ANC с сетью или группой ресурсов, которые никогда не использовались при создании ANC ранее, необходимо иметь роль владельца подписки или администратора пользователей.
- В целях аварийного восстановления убедитесь, что в подсети доступно по меньшей мере 50 % IP-адресов. Если для аварийного восстановления требуется повторная подготовка, для каждого облачного компьютера, подготовленного в подсети, необходимо достаточное количество новых IP-адресов.
- Для Windows 365 для государственных организаций — облако сообщества для государственных организаций (GCC) и не GCC-High — обязательно выполните параметры сценария, перечисленные в разделе Настройка клиентов для Windows 365 государственных организаций.
- Если вы не используете Azure CloudShell, убедитесь, что политика выполнения PowerShell настроена для разрешения сценариев RemoteSigned. Если вы используете групповая политика для задания политики выполнения, убедитесь, что объект групповая политика, предназначенный для подразделения, определенного в ANC, настроен на разрешение сценариев RemoteSigned. Дополнительные сведения см. в разделе Set-ExecutionPolicy.

При планировании виртуальных сетей ANC с использованием ExpressRoute в качестве локальной модели подключения см. документацию Azure по ограничениям виртуальных машин. Для SKU шлюза ExpressRoute убедитесь, что у вас есть правильный размер шлюза для количества облачных компьютеров, запланированных в виртуальной сети. Превышение этого ограничения может привести к нестабильности подключения.

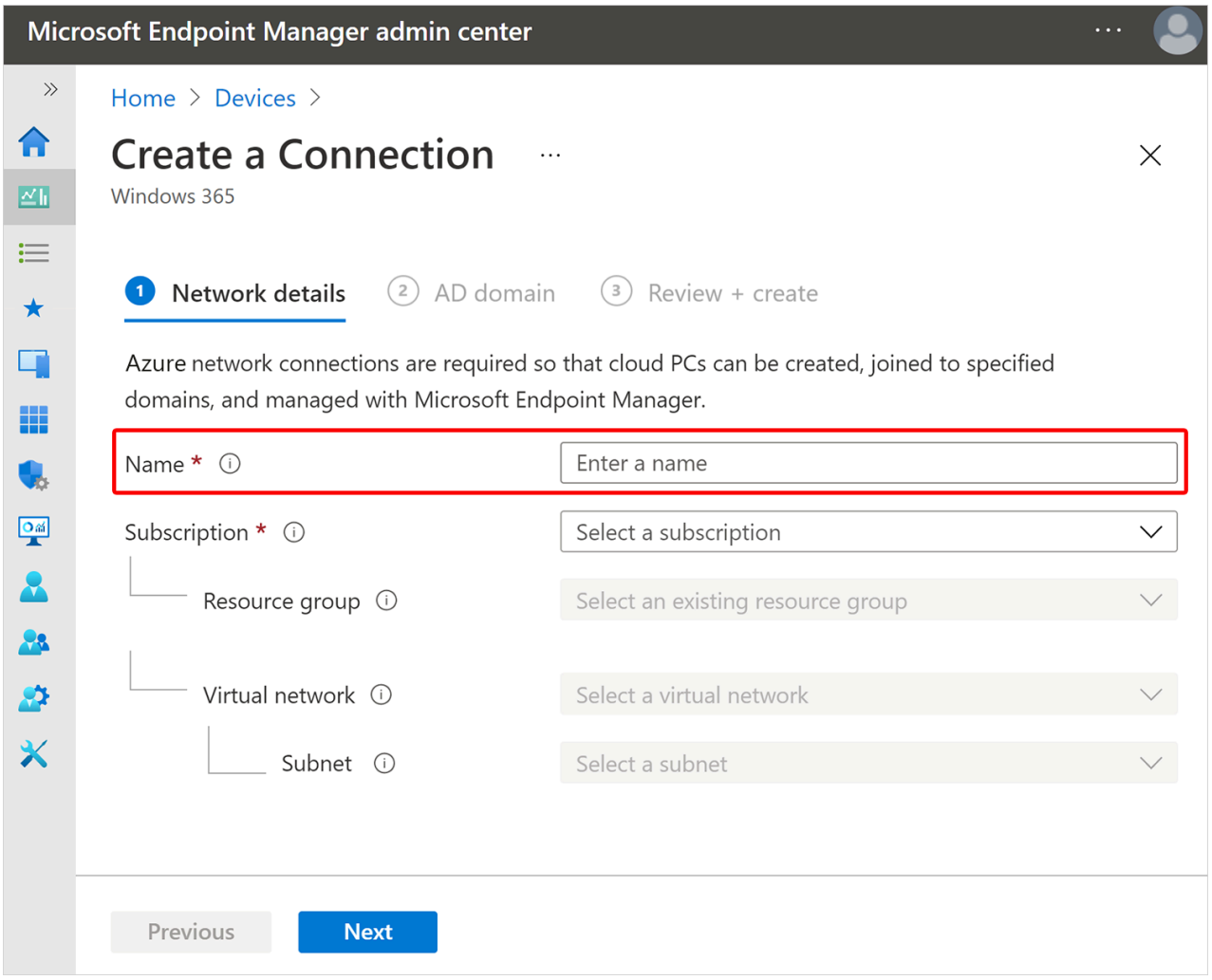
Создание ANC

1. Войдите в Центр администрирования Microsoft Intune, выберите **Устройства**>**Windows 365** (в разделе **Подготовка**) >**сетевое подключение**> Azure**Создать**.

2. В зависимости от типа ANC, который требуется создать, выберите **Microsoft Entra Присоединение** или **Гибридное Microsoft Entra присоединение**.



3. На странице **Сведения о сети** введите **имя** нового подключения. Имя подключения должно быть уникальным в арендаторе заказчика.



4. Выберите **подписку** и **группу ресурсов** для нового подключения. Создайте новую группу ресурсов для размещения ресурсов Облачного компьютера. При необходимости можно выбрать существующую группу ресурсов в списке (чтобы предоставить разрешения Windows 365 имеющейся группе ресурсов). Если у вас нет работоспособного ANC, вы не можете продолжить.

5. Выберите **виртуальную сеть** и **подсеть**. При выборе виртуальной сети:

   - Чтобы обеспечить стабильное и производительное подключение, убедитесь, что виртуальная сеть находится в регионе, ближайшем к Windows 365 пользователей.
   - Чтобы разместить все необходимые облачные компьютеры, убедитесь, что в подсети виртуальной сети достаточно IP-адресов. Кроме того, рассмотрите будущие потребности роста и изменения размера .
   - Убедитесь, что виртуальная сеть имеет прямой доступ к контроллеру домена. Эта линия видимости необходима для первоначальной подготовки и успешного входа в систему для гибридных облачных компьютеров.
   - Убедитесь, что все необходимые конечные точки разрешены через виртуальную сеть и не заблокированы брандмауэром, прокси-сервером или шлюзами программного обеспечения.

6. Нажмите кнопку **Далее**.

7. Для гибридных Microsoft Entra присоединения к ANCs на странице **домена AD** укажите следующие сведения:

   - **Доменное имя AD**. DNS-имя домена Active Directory, который вы хотите использовать для подключения и подготовки Облачных компьютеров. Например, corp.contoso.com.

     > ⓘ **Примечание**
     >
     > Если среда локальная служба Active Directory имеет несколько доменов или доменов типа "родители-потомки", обязательно введите конкретный домен, в котором должны быть присоединены облачные компьютеры.

   - **Подразделение** (необязательно). Подразделение (OU) — это контейнер в домене Active Directory, в котором могут размещаться пользователи, группы и компьютеры. Убедитесь, что это подразделение включено для синхронизации с Microsoft Entra Connect. Подготовка завершается сбоем, если это подразделение не синхронизируется.

   - **Имя пользователя домена AD**. Имя пользователя в формате имени участника-пользователя (UPN), которое будет использоваться для подключения Облачных компьютеров к домену Active Directory. Например, svcDomainJoin@corp.contoso.com. Эта учетная запись службы должна иметь разрешение на присоединение компьютеров к домену и, если задано, целевому подразделению.

   - **Пароль домена AD**: пароль пользователя.

   - **Подтвердите пароль домена AD**: пароль пользователя.

   Облачные компьютеры, использующие определенный ANC, присоединяются к указанному домену и подразделению. Убедитесь, что выбранный домен является нужным доменом для присоединения компьютеров.

8. Нажмите **Далее**.

9. На странице **Проверка + создание** нажмите кнопку **Создать**.

Если anC используется, его нельзя удалить, и некоторые параметры конфигурации не могут быть изменены. Дополнительные сведения см. в разделах Изменение сетевого подключения Azure и Удаление сетевого подключения Azure.

Дальнейшие действия

Изменение сетевого подключения Azure.

Изменение сетевого подключения Azure

Статья • 05.02.2025

Все сетевые подключения Azure (ANC) периодически проверяются, чтобы убедиться в готовности среды к подготовке облачных компьютеров. В случае сбоя этих проверок вам может потребоваться исправить настройку сети в Azure или изменить одно из указанных свойств.

Требования

Чтобы изменить ANC, необходимо иметь роль администратора Intune или администратора Windows 365. У вас также должна быть роль читателя подписки в подписке Azure, где расположена виртуальная сеть, связанная с ANC.

Изменение сетевого подключения Azure

Чтобы изменить сетевое подключение Azure:

1. Войдите в центр >администрирования Microsoft Intune устройства >**Windows 365** (в разделе **Подготовка**) >**сетевое подключение**> Azure выберите подключение, которое вы хотите изменить > свойства.
2. Для всех ANC вы можете изменить **общие** параметры, выбрав **Изменить** рядом с каждым заголовком. Вы можете изменить все параметры, кроме **типа присоединения**. Для Microsoft Entra гибридных подключений можно также изменить параметры **домена AD**.

После сохранения изменений выполняются проверки ANC для проверки конфигурации.

Вы не можете изменить ANC, если для него выполняются проверки. Дождитесь успешного завершения или сбоя проверок, чтобы функция изменения стала доступной.

Параметры конфигурации (кроме имени) нельзя изменить для ACS, которые:

- На который ссылается политика подготовки, в том числе в качестве альтернативного ANC.
- Используется облачным компьютером.

- Настроено в качестве резервных anCs для аварийного восстановления между регионами.

Если для изменения ANC, к которому подключен облачный компьютер, необходимо внести изменения, см. документацию по перемещению облачного компьютера.

Дальнейшие действия

Удаление сетевого подключения Azure.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

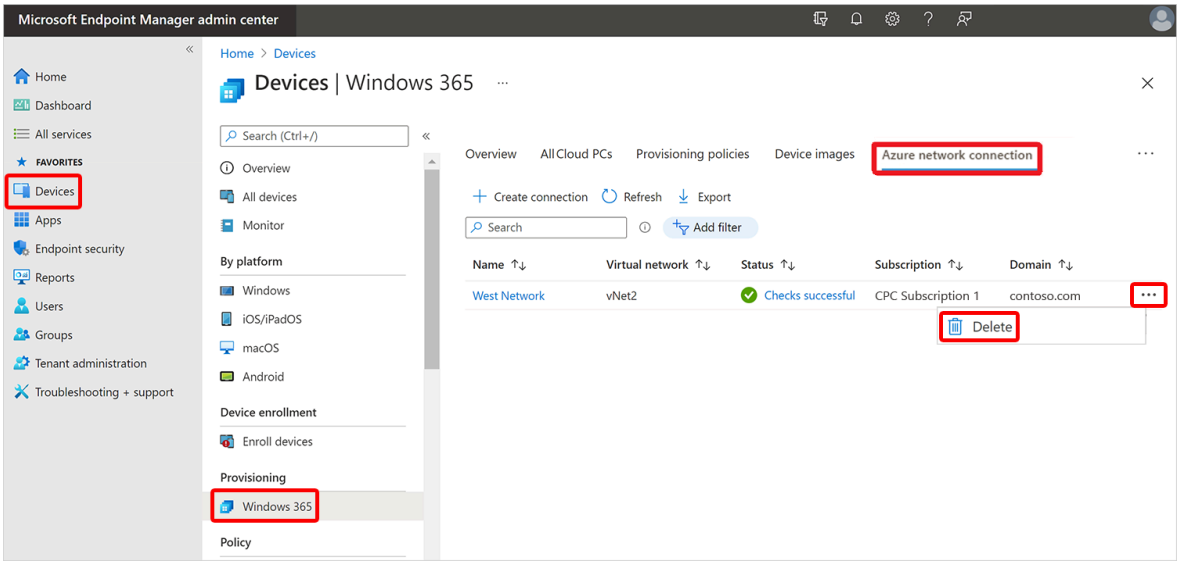
Удаление сетевого подключения Azure

Статья • 31.01.2025

Удалить можно только неиспользуемое сетевое подключение Azure (ANC).

Чтобы удалить неиспользуемый ANC, выполните приведенные далее действия.

1. Войдите в центр администрирования > Microsoft Intune**устройства**>**Windows 365** (в разделе **Подготовка)**>**сетевое подключение Azure**. У вас должны быть разрешения администратора Intune или администратора Windows 365.



2. Выберите многоточие (...) рядом с подключением, которое нужно удалить >**Удалить**.
3. Выберите **Подтвердить** при запросе на удаление подключения.

Используемые АНК

AnCs, которые используются, не могут быть удалены. К используемым ANCs относятся:

- На который ссылается политика подготовки, в том числе в качестве альтернативного ANC.
- Используется облачным компьютером.
- Настроено в качестве резервных anCs для аварийного восстановления между регионами.

Если используется ANC, необходимо выполнить одно из следующих действий, прежде чем его можно будет удалить:

- Удалите ANC из всех политик подготовки.
- Переместите облачные компьютеры в другой ANC или отзыв облачных компьютеров.
- Удалите ANC из всех параметров пользователя аварийного восстановления в разных регионах.

Дальнейшие действия

Добавление образов устройств.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Обеспечьте локализованное взаимодействие с Windows

Статья • 31.01.2025

Чтобы пользователи могли работать на своих Облачных компьютерах Windows 365, важно, чтобы в Windows использовался удобный для них язык интерфейса. Пользователи в любой момент могут самостоятельно изменить язык интерфейса с помощью приложения "Параметры" в Windows. Тем не менее интерфейс Windows будет более доброжелательным, если для пользователя будет отображаться нужный язык с первого входа в систему.

Существует два различных способа предоставления локализованного интерфейса Windows при первом входе пользователей:

- Используйте политику подготовки. Если вы планируете использовать образ из галереи, вы можете выбрать язык при создании политики поиска. При использовании этого метода для развертывания языковых пакетов необходимое содержимое автоматически устанавливается в процессе подготовки. Это содержимое загружается из конечных точек, перечисленных на странице Сетевые конечные точки для Microsoft Intune. Эти Intune конечные точки являются обязательными для работы Windows 365, поэтому, если сеть настроена правильно, они уже доступны в вашей среде. Убедитесь, что tcp-порт 80 открыт для этих конечных точек. Как объясняется требованиями Intune, этот порт используется для скачивания элементов содержимого.
- Создание пользовательского образа устройства. Если вы планируете использовать собственный образ и управлять своими облачными компьютерами с помощью групповой политики, вы можете включить язык как часть пользовательского образа. Ссылки на скачивание содержимого для этого метода развертывания см. в следующем разделе.

URL-адреса для развертывания пользовательского образа

Для развертываний пользовательских образов можно скачать языки отображения из следующих полных доменных имен:

- Все версии Windows
  - http://*.delivery.mp.microsoft.com

    - http://*.windowsupdate.com
    - Дополнительные сведения см. в статье Конечные точки содержимого и служб подключенного кэша Майкрософт.
- Windows 11 21H2
    - Языковой пакет:https://software-download.microsoft.com/download/sg/22000.1.210604-1628.co_release_amd64fre_CLIENT_LOF_PACKAGES_OEM.iso
    - FodToLP: https://download.microsoft.com/download/7/6/0/7600F9DC-C296-4CF8-B92A-2D85BAFBD5D2/Windows-10-1809-FOD-to-LP-Mapping-Table.xlsx
- Windows 10 21H2 и 21H1
    - Языковой пакет:https://software-download.microsoft.com/download/pr/19041.1.191206-1406.vb_release_CLIENTLANGPACKDVD_OEM_MULTI.iso
    - FOD: https://software-download.microsoft.com/download/pr/19041.1.191206-1406.vb_release_amd64fre_FOD-PACKAGES_OEM_PT1_amd64fre_MULTI.iso
    - Входящие приложения: https://software-download.microsoft.com/download/sg/19041.928.210407-2138.vb_release_svc_prod1_amd64fre_InboxApps.iso
- Windows 10 21H2
    - Языковой пакет:https://software-download.microsoft.com/download/pr/19041.1.191206-1406.vb_release_CLIENTLANGPACKDVD_OEM_MULTI.iso
    - FOD: https://software-download.microsoft.com/download/pr/19041.1.191206-1406.vb_release_amd64fre_FOD-PACKAGES_OEM_PT1_amd64fre_MULTI.iso
    - Входящие приложения: https://software-download.microsoft.com/download/pr/19041.508.200905-1327.vb_release_svc_prod1_amd64fre_InboxApps.iso
- Windows 10 1909
    - Языковой пакет:https://software-download.microsoft.com/download/pr/18362.1.190318-1202.19h1_release_CLIENTLANGPACKDVD_OEM_MULTI.iso
    - FOD: https://software-download.microsoft.com/download/pr/18362.1.190318-1202.19h1_release_amd64fre_FOD-PACKAGES_OEM_PT1_amd64fre_MULTI.iso
    - Входящие приложения: https://software-download.microsoft.com/download/pr/18362.1.190318-1202.19h1_release_amd64fre_InboxApps.iso

Дальнейшие действия

Использование политики подготовки или создание настраиваемого образа устройства для настройки языка интерфейса.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Используйте политику подготовки для настройки языка интерфейса по умолчанию на облачных ПК

Статья • 31.01.2025

Чтобы обеспечить доступность правильных языковых пакетов на облачном компьютере при первом входе, вы можете настроить политику подготовки:

- Создайте политику подготовки и выберите **язык & регион** в разделе **Конфигурация**. Для Windows 365 доступно 38 языковых пакетов Windows. Windows 365 автоматически использует для языкового пакета стандартный макет удаленной клавиатуры.

Для всех облачных компьютеров, подготовленных с этой политикой, в интерфейсе первого входа будет использоваться выбранный языковой пакет.

Кроме того, вы можете отредактировать политики подготовки, чтобы изменить конфигурацию языка и региона. После применения политики и переподготовки связанных облачных компьютеров выбранный языковый пакет будет доступен на облачных компьютерах.

Дальнейшие действия

Обязательные URL-адреса для языковых пакетов

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Создание пользовательского образа устройства с уже установленными языками

Статья • 31.01.2025

Чтобы создать настраиваемый образ устройства, предоставляющий пользователям локализованный интерфейс Windows, выполните следующие действия.

1. Создание настраиваемого образа устройства.
2. Настройте язык по умолчанию с помощью групповой политики.

Облачные компьютеры, подготовленные с использованием этого образа, будут полностью настроены для работы на любом из установленных языков без каких-либо действий со стороны пользователя. Когда пользователь выполняет вход в Облачный компьютер, групповая политика оценивает устройство и выбирает соответствующий предварительно установленный язык в качестве предпочтительного языка пользователя для Windows.

Создание пользовательского образа

Создание пользовательского образа с установленными языками — лучший способ обеспечить доступность нужных языков на Облачном компьютере при входе пользователя в систему.

Прежде чем создавать пользовательский образ, проверьте, поддерживается ли используемый вами язык скриптом установщика языков Windows 365. Если:

- язык, который необходимо предоставить пользователям, поддерживается скриптом PowerShell, добавьте языки в Windows с помощью скрипта и сохраните образ. Поддерживаются только пользовательские образы Windows 10;
- язык, который вы хотите предоставить пользователям, не поддерживается скриптом PowerShell, добавьте языки в Windows вручную и сохраните образ.

Добавление языков в Windows с помощью скрипта и сохранение образа

Чтобы добавить язык с помощью скрипта установщика языков Windows 365, выполните указанные ниже действия.

1. Войдите в виртуальную машину, над которой вы работаете для создания пользовательского образа.
2. Выполните один из **вариантов установки**, описанный для скрипта установщика языков Windows 365.
3. Запустите скрипт и введите номер, соответствующий языку, который необходимо установить в пользовательском образе.

> **Примечание**
>
> С помощью скрипта можно установить в пользовательском образе нужное количество языков. Для этого запустите этот скрипт один раз для каждого языка.

После того как вы добавите нужные языки и будете готовы сохранить образ, выполните действия по завершению настройки образа.

Добавление языков в Windows вручную и сохранение образа

Чтобы вручную установить нужные языки в пользовательский образ Windows 10 Корпоративная или Windows 11 Корпоративная, выполните действия, описанные в статье Добавление языковых пакетов в образ Windows 10 или Windows 11 с многосеансной поддержкой до пункта об окончании настройки образа включительно.

> **Примечание**
>
> Несмотря на то что эти инструкции написаны специально для Windows 10 Корпоративная или Windows 11 Корпоративная с многосеансной поддержкой, эти же действия можно использовать и для Windows 10 Корпоративная или Windows 11 Корпоративная.

Отправка пользовательского образа

Чтобы отправить пользовательский образ в службу Windows 365 после его сохранения в качестве управляемого образа Azure, выполните действия, указанные в статье Добавление и удаление образов устройств.

Настройка языка по умолчанию с помощью групповой политики

После установки языков в образ, который получат пользователи, необходимо создать групповую политику, чтобы по умолчанию применять нужные предварительно установленные языки для пользователей.

С помощью указанных ниже действий настройте параметры групповой политики, чтобы задать значение реестра PreferredUILanguages и региональные параметры Windows. Группа безопасности будет назначать эти параметры наборам пользователей. Каждый объект группы безопасности и групповой политики настраивает один язык в качестве языка по умолчанию для этих пользователей. Чтобы удовлетворить потребности пользователей с различными требованиями к языкам по умолчанию, можно использовать один образ с несколькими языками и различные объекты групповой политики, предназначенные для различных групп пользователей.

1. В домене Active Directory создайте группу безопасности, которая будет сопоставлять языки с определенными наборами пользователей в этой группе.

2. Добавьте всех пользователей Облачных компьютеров, которые должны получить этот язык в новой группе безопасности.

3. В диспетчере сервера откройте раздел **Управление групповыми политиками** и добавьте новый объект групповой политики, связанный с подразделением или доменом, который будет содержать Облачные компьютеры для этих пользователей.

4. Щелкните правой кнопкой мыши новый объект групповой политики и выберите пункт **Изменить...**

5. Перейдите в раздел **Конфигурация пользователя**>**Параметры**>**Параметры Windows**, правой кнопкой мыши щелкните пункт **Реестр** и выберите пункты **Создать**>**Элемент реестра**.

6. На вкладке **Общие** введите указанные ниже сведения. В примере ниже показан испанский язык (Испания) с языковым кодом es-ES.

    - Действие: замена
    - Куст: HKEY_CURRENT_USER
    - Путь к разделу: Панель управления\Рабочий стол
    - Имя значения: PreferredUILanguages
    - Тип значения: REG_SZ

- Данные значения: [тег языка и региона]. Пример: **ar-SA** для арабского языка (Саудовская Аравия).

> ⓘ **Примечание**
>
> Найти код языка для нужного сочетания языка и региона можно в [списке языковых пакетов](#).

7. Перейдите на вкладку **Общие** и проверьте три указанных ниже параметра.

   - **Запускать в контексте безопасности пользователя, выполнившего вход в систему (параметр политики пользователей)**
   - **Применить один раз и не применять повторно**

> ⓘ **Примечание**
>
> Этот параметр позволяет пользователям самостоятельно изменять параметры языка позже.

   - **Нацеливание на уровень элемента**

8. Выберите пункты **Нацеливание...**, **Создать элемент** и **Группа безопасности**.

9. Выберите пункт **...** рядом с элементом "Группа", выполните поиск новой группы безопасности, выберите новую группу безопасности и нажмите кнопку **OK**.

10. Выберите пункт **Пользователь в группе**, затем нажмите кнопки **OK** и **OK**, чтобы завершить процесс создания реестра.

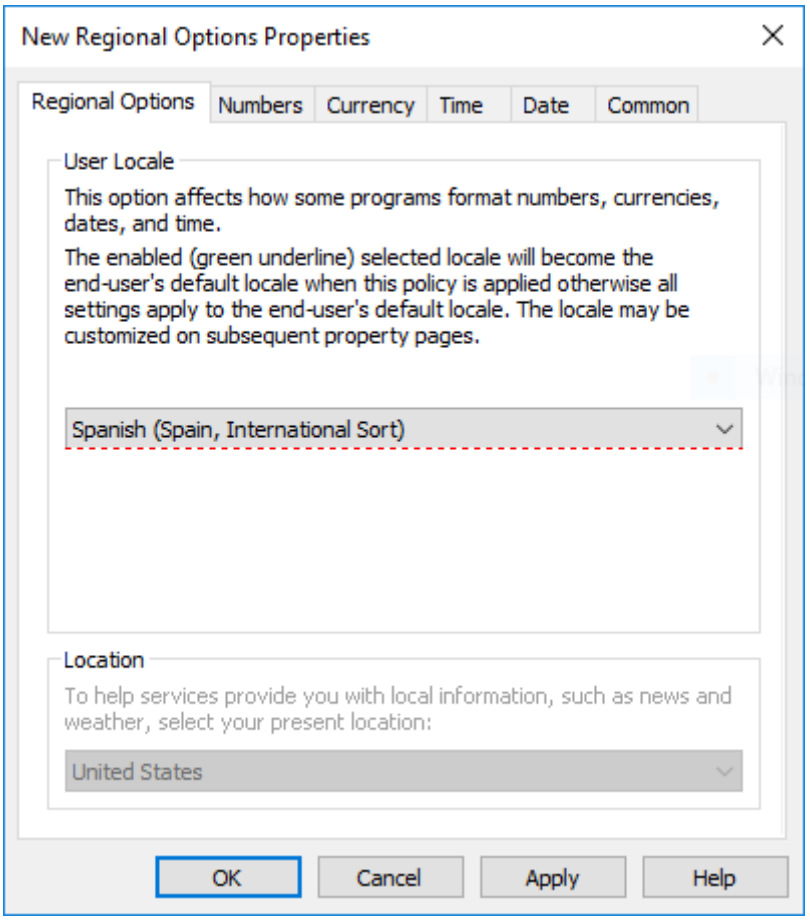
11. В редакторе "Управление групповыми политиками" перейдите в раздел **Конфигурация пользователя**>**Параметры**>**Параметры панели управления**, правой кнопкой мыши щелкните пункт **Региональные параметры**, и выберите пункты **Создать**>**Региональные параметры**.

12. В разделе **Язык пользователя** выберите сочетание языка и региона, соответствующее разделу реестра, который вы создали на предыдущем шаге.

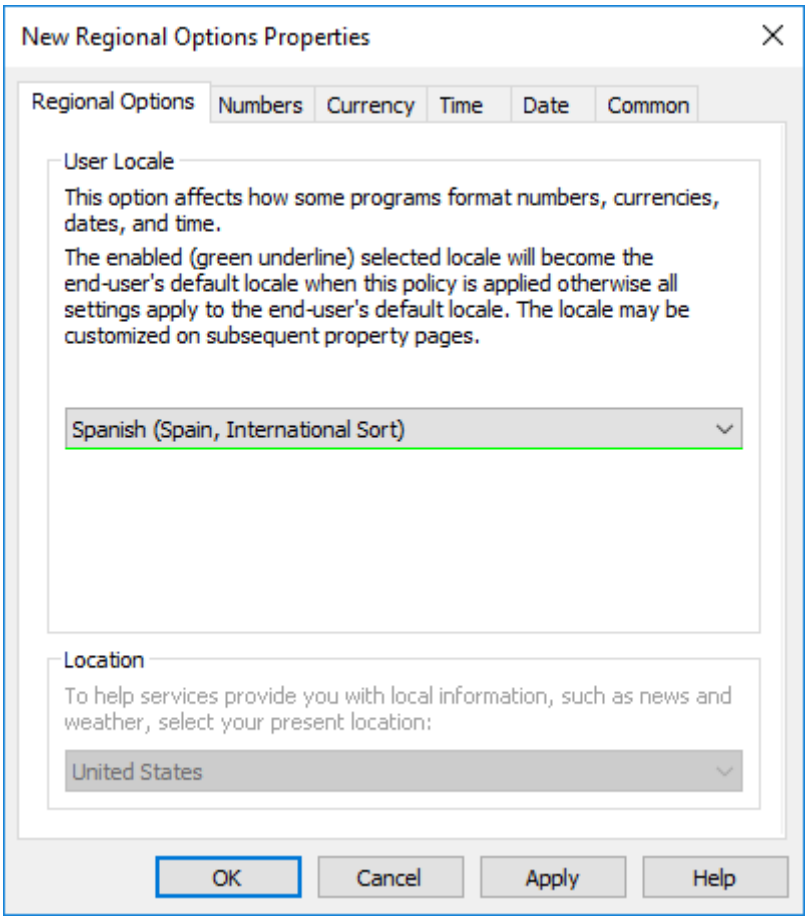
13. После того как вы выберете нужное сочетание языка и региона в раскрывающемся меню, раскрывающемся меню может быть подчеркнуто красным цветом. Это подчеркивание означает, что выбор не подтвержден. Нажмите функциональную клавишу **F5** на клавиатуре, чтобы подтвердить

выбор. После этого раскрывающееся меню будет подчеркнуто зеленым цветом.

Перед нажатием клавиши **F5**:



После нажатия клавиши **F5**:



14. Перейдите на вкладку **Общие** и проверьте три указанных ниже параметра.

    - **Запускать в контексте безопасности пользователя, выполнившего вход в систему (параметр политики пользователей).**
    - **Применить один раз и не применять повторно.**

    > ⓘ **Примечание**
    >
    > Этот параметр позволяет пользователям самостоятельно изменять параметры языка позже.

    - **Нацеливание на уровень элемента.**

15. Выберите пункты **Нацеливание...**, **Создать элемент** и **Группа безопасности**.

16. Выберите пункт **...** рядом с элементом "Группа", выполните поиск новой группы безопасности, выберите новую группу безопасности и нажмите кнопку **OK**.

17. Выберите пункт **Пользователь в группе**, затем нажмите кнопки **OK** и **OK**, чтобы завершить процесс создания реестра.

Вы можете выполнить эти действия для каждого языка, который необходимо предоставить в качестве языка по умолчанию для пользователей. Если у

пользователей есть и Облачные компьютеры, и физические устройства, вам, возможно, потребуется применить замыкание групповой политики, чтобы эти параметры действовали для пользователей, только когда последние входят в систему на своих Облачных компьютерах.

> **Примечание**
>
> В действии 6 выше используется команда "Заменить", которая задает для пользователя только один предпочитаемый язык, указанный в элементе реестра. Если вы создаете несколько объектов групповой политики для назначения различных языков пользователям, убедитесь, что каждый пользователь является членом только одной целевой группы безопасности.

Дальнейшие действия

Обязательные URL-адреса для языковых пакетов

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Добавление или удаление пользовательских образов устройств

17.10.2025

Если вы хотите использовать пользовательский образ устройства, вы можете добавить его в подписку Azure, а затем использовать для подготовки облачных компьютеров. Вы можете использовать стандартные образы из коллекции Azure Marketplace или создать свои настраиваемые управляемые образы. Если в настоящее время вы используете коллекцию вычислений Azure в Microsoft Azure, вы можете преобразовать один из этих образов в управляемый образ. Для преобразования используйте действия по экспорту версии образа на управляемый диск, а затем создайте образ с управляемого диска.

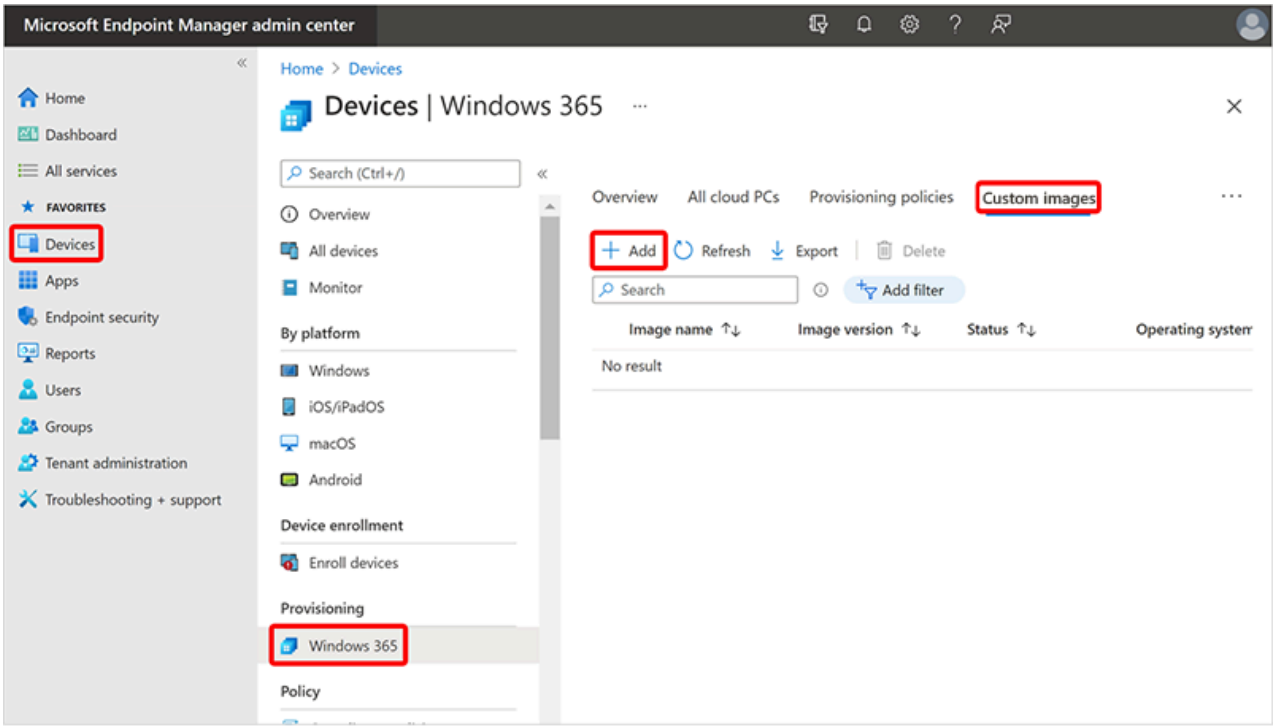
> **Примечание**
>
> - образы Windows 10 и Windows 11 не должны содержать клиентские компоненты Виртуального рабочего стола Azure. Кроме того, нельзя импортировать Windows 10 и Windows 11 многосессионные образы в Windows 365.
> - При развертывании виртуальной машины в Azure для создания настраиваемого образа необходимо выбрать тип безопасности "Standard" при создании виртуальной машины. Управляемые образы не поддерживают виртуальные машины доверенного запуска.
> - Диски данных, подключенные к пользовательскому образу, не поддерживаются в Windows 365.
> - Сведения о поддержке пользовательских образов устройств Windows 11 см. в статье Что нового в Windows 365 Корпоративная.
> - Вы также можете использовать существующие встроенные образы коллекции без настройки для потоковой передачи.

Добавление пользовательского образа устройства

Вы можете передать пользовательский образ в службу Windows 365, выполнив следующие действия:

1. Войдите в Центр администрирования Microsoft Intune.

2. Выберите **Устройства**>**Windows 365**>**Настройки**>**Добавить**.



3. На панели **Добавить образ** укажите следующие сведения:

   - **Имя образа**: имя образа, который вы хотите добавить.
   - **Версия образа**: номер версии образа в формате основной (целое число).дополнительный (целое число).исправления (целое число). Например: 0.0.1, 1.5.13.
   - **Подписка**. Выберите подписку Azure, из которой был получен образ.
   - **Исходный образ**: выберите добавляемый образ. Список будет заполнен всеми пользовательскими изображениями из выбранной подписки, которые соответствуют предварительным требованиям.

4. Нажмите кнопку **Добавить**, чтобы добавить образ в список образов устройства.

После успешной отправки образа вы увидите отправленное изображение при выборе образа для создания политики подготовки.

Удаление пользовательского образа устройства

Вы можете удалить пользовательский образ из Windows 365, выполнив следующие действия:

1. Войдите в Центр администрирования Microsoft Intune, выберите **Устройства**>**Windows 365**>**Настройка образов**.
2. На странице **Образы устройств** выберите поле проверка рядом с изображением >**Удалить**.

3. Нажмите кнопку **Да** во всплывающем окне подтверждения, чтобы окончательно удалить образ.

Образы устройств, используемые в политике подготовки, невозможно удалить. Сначала удалите политику подготовки, а затем связанный образ устройства.

Дальнейшие действия

Создайте политику подготовки.

Дополнительные сведения о виртуальных машинах и создании пользовательских образов в Azure см. в статье Виртуальные машины в Azure.

Преобразование существующего пользовательского образа устройства в виртуальную машину поколения 2

Статья • 31.01.2025

Для поддержки Windows 11 пользовательские образы устройств должны основываться на виртуальных машинах поколения 2 (2-го поколения). Если у вас уже есть пользовательские образы устройств на основе виртуальных машин поколения 1 (1-го поколения), эти пользовательские образы устройств можно преобразовать, выполнив приведенные ниже действия. После выполнения этих действий все будущие облачные компьютеры, подготовленные из преобразованного образа устройства, будут основаны на виртуальных машинах 2-го поколения.

Windows 365 не помешает подготовить новые облачные компьютеры из существующих пользовательских образов на основе виртуальных машин поколения 1. Однако если вы хотите добавить новые пользовательские образы, Windows 365 будут принимать только образы на основе 2-го поколения. Для поддержки Windows 11 требуются виртуальные машины 2-го поколения.

Для этого процесса предусмотрено четыре основных шага:

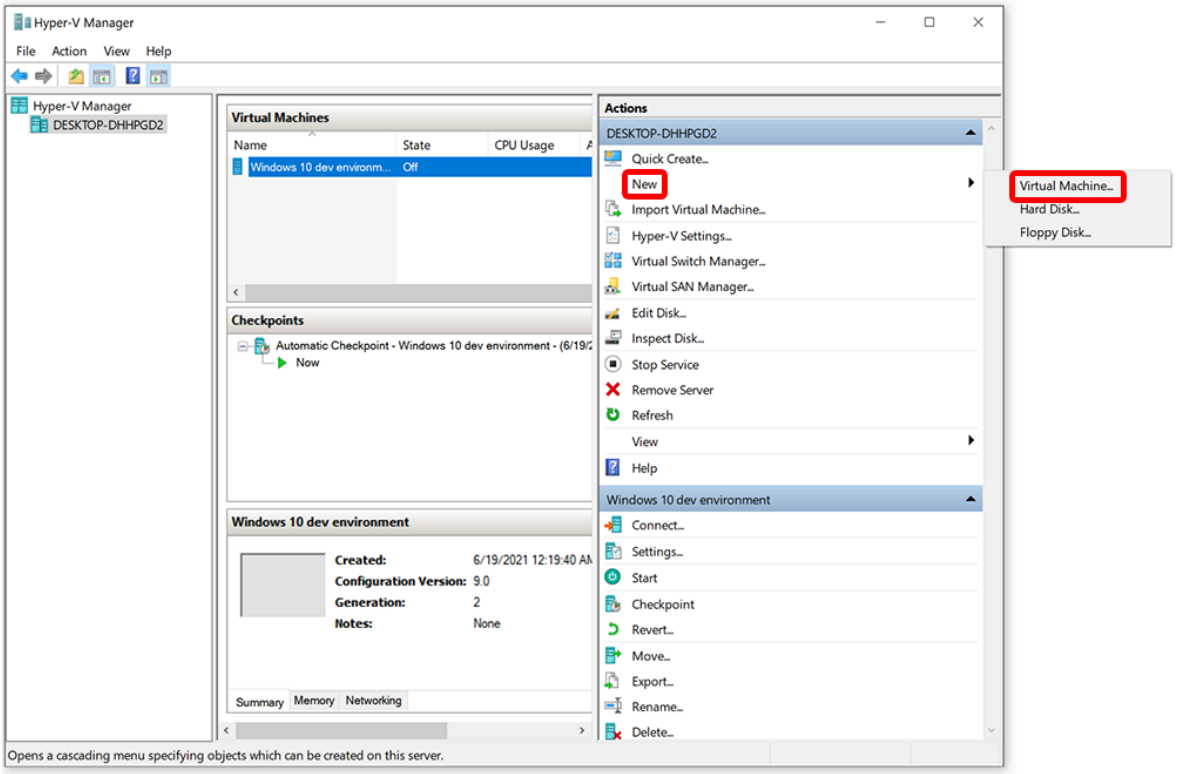
1. Создание новой виртуальной машины
2. Преобразование основной загрузочной записи в раздел GUID
3. Преобразование диска в фиксированный размер и формат VHD
4. Отправка преобразованной виртуальной машины в Azure

Создание новой виртуальной машины

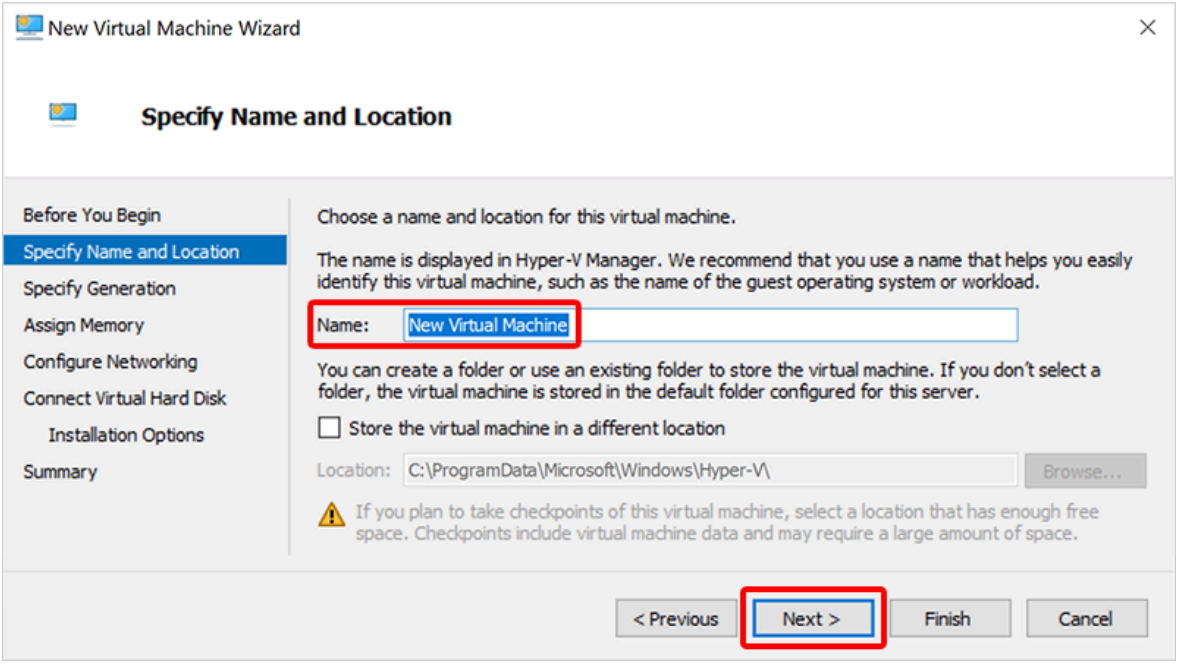
1. Убедитесь, что на вашем управляющем компьютере установлена система Hyper-V. Сведения об установке Hyper-V см. в статье Установка Hyper-V в Windows.
2. Скачайте файл виртуального жесткого диска (VHD) вашего пользовательского образа с URL-адреса BLOB-файлов Azure на свой компьютер с установленной системой Hyper-V. Файл VHD имеет точный размер диска ОС, который может быть очень большим. Убедитесь, что для скачивания файла VHD используется быстрое и стабильное подключение к Интернету, и подготовьтесь к длительной загрузке. Информацию о загрузке управляемого диска см. в статье Загрузка файла VHD из Azure. Вы также можете скачать файл VHD

непосредственно с помощью Обозревателя службы хранилища Azure либо как управляемый диск, либо как BLOB-объект хранилища.

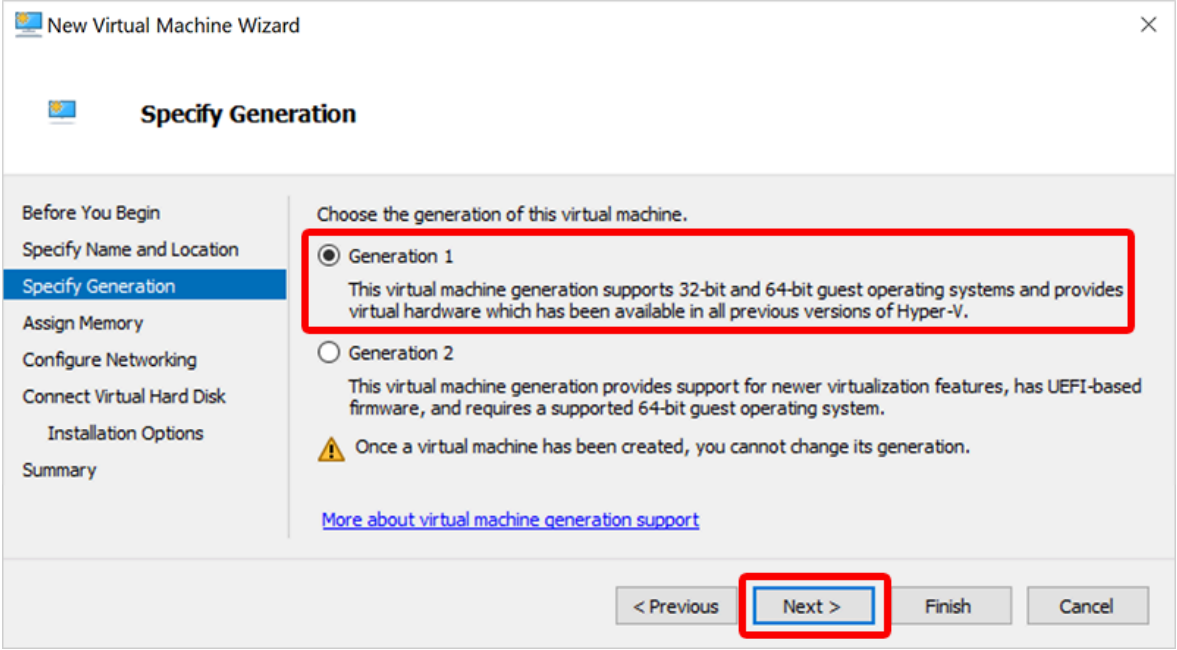
3. Перейдите на свой локальный компьютер и откройте диспетчер Hyper-V.
4. В разделе **Действия** выберите пункт **Новая**>**виртуальная машина**.



5. На странице **Перед началом работы** нажмите кнопку **Далее**.
6. На странице **Задание имени и расположения** введите понятное имя, например CustomFinanceImageg2, и нажмите **Далее**.

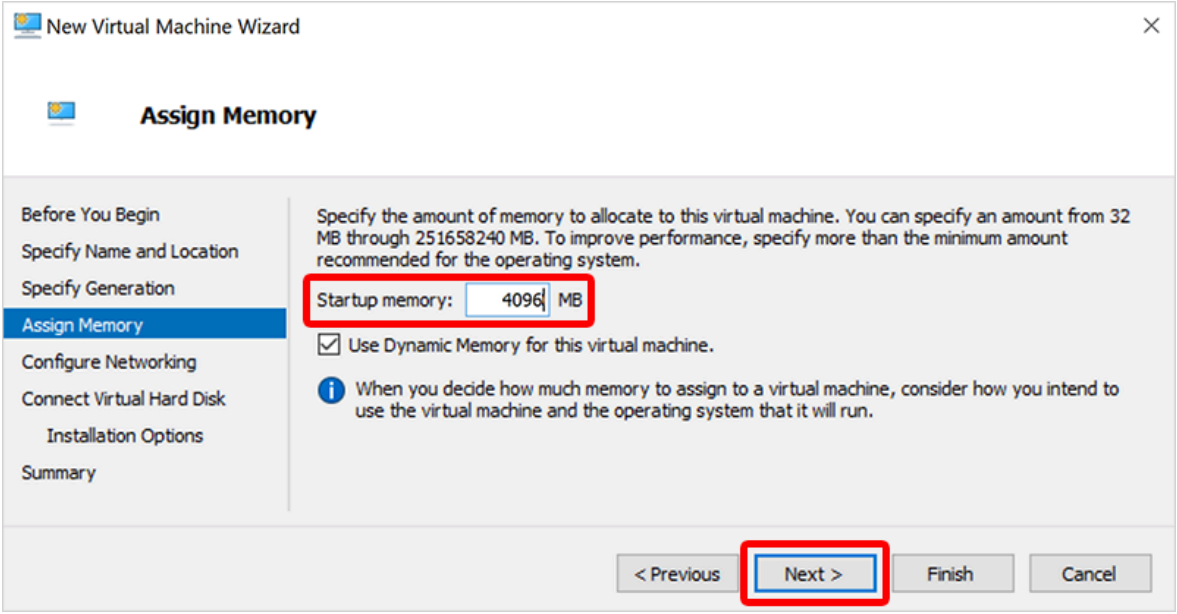


7. На странице **Задание поколения** выберите **поколение 1** (не **поколение 2**). Здесь необходимо поколение 2, чтобы подключить диск и изменить модель секционирования на GUID Partition Table (GPT). Нажмите кнопку **Далее**.

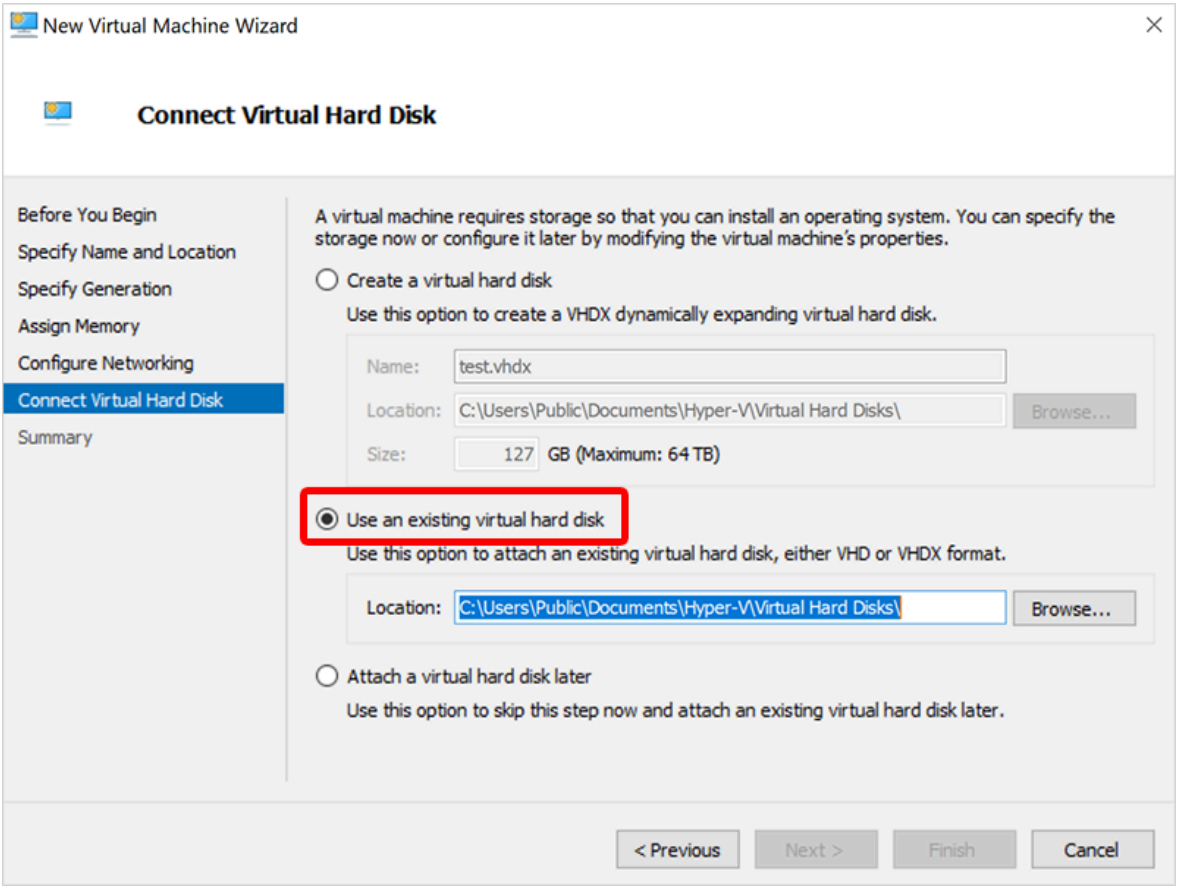


Hyper-V поддерживает только образы поколения 2 в VHDX и образы поколения 1 в VHD. Azure поддерживает только образы поколения 2 в виртуальном жестком диске. Поэтому мы создадим здесь образ VHD поколения 1, чтобы преобразовать его в образ VHD поколения 2.

8. На странице **Назначение памяти** задайте объем **памяти для запуска** не менее 1024 МБ, желательно 4096 МБ. Нажмите кнопку **Далее**.



9. На странице **Настройка сети** выберите **Переключатель по умолчанию**>**Далее**.
10. На странице **Подключение виртуального жесткого диска** выберите **Использование существующего виртуального жесткого диска**.



11. Чтобы указать **расположение**, выберите **Обзор** и VHD, который был загружен ранее.
12. Нажмите **Далее**, а на странице **Сводка** выберите **Готово**.

Преобразование основной загрузочной записи в раздел GUID

1. Создание ISO с WinPE на носителе. Инструкции по созданию ISO см. в статье Создание загрузочного носителя с WinPE. Или выполните загрузку из ISO Windows 11 и нажмите клавиши SHIFT+F10, чтобы отобразить подсказку CMD.
2. В разделе **виртуальные машины** диспетчера Hyper-V выберите новую виртуальную машину, а затем в разделе **Действия** выберите **Параметры**.
3. В области навигации слева зайдите в раздел **контроллер IDE 1** и выберите **DVD-диск**.
4. В разделе **DVD-диск** зайдите в секцию **Контроллер** и выберите **контроллер IDE 1**.
5. Выберите **файл образа** и перейдите к созданному вами новому файлу ISO.
6. Нажмите кнопку **OK**.
7. В разделе **Действия** щелкните **Запустить**.
8. Подождите, пока откроется командная строка wpeinit.
9. Чтобы преобразовать основную загрузочную запись (MBR) по модели таблицы разделов GUID (GPT), запустите в окне wpeinit следующие две

команды. GPT — это новый стандарт для виртуальных машин на основе 2-го поколения.

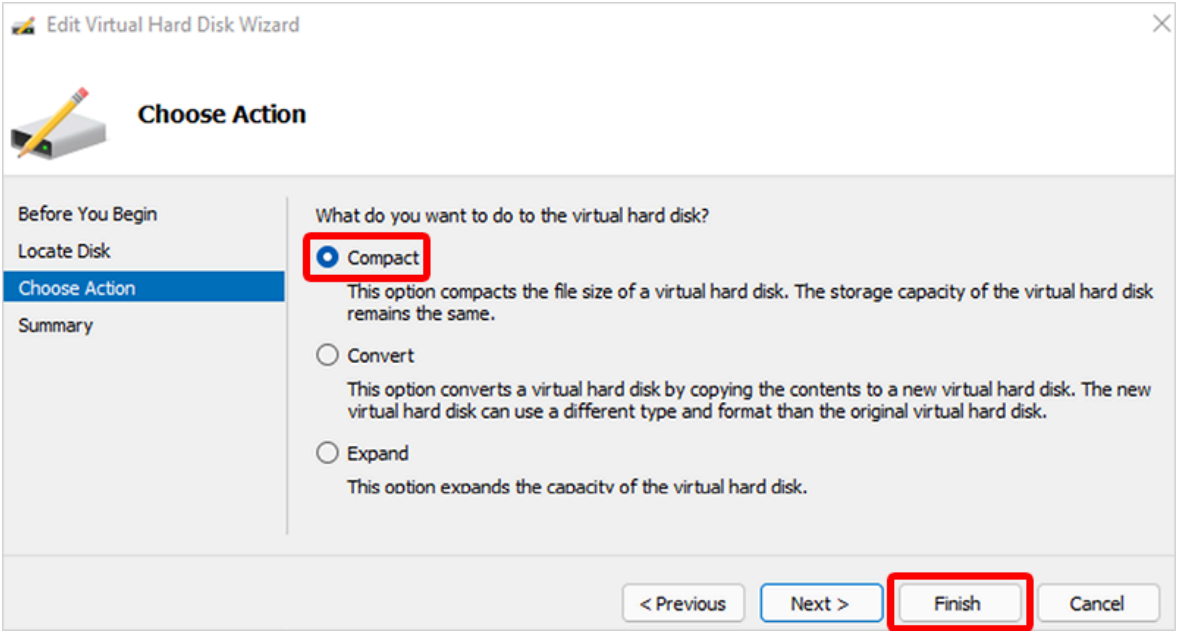
a. Чтобы определить нужный диск для преобразования и проверить его, запустите `mbr2gpt /validate /disk:0`.

b. Чтобы преобразовать диск в соответствии с таблицей разделов GUID (GPT), запустите `mbr2gpt /convert /disk:0`. Дополнительную информацию о MBR2GPT см. в разделе Документация о MBR2GPT.exe.

10. После успешного выполнения команд переходите к следующему шагу.

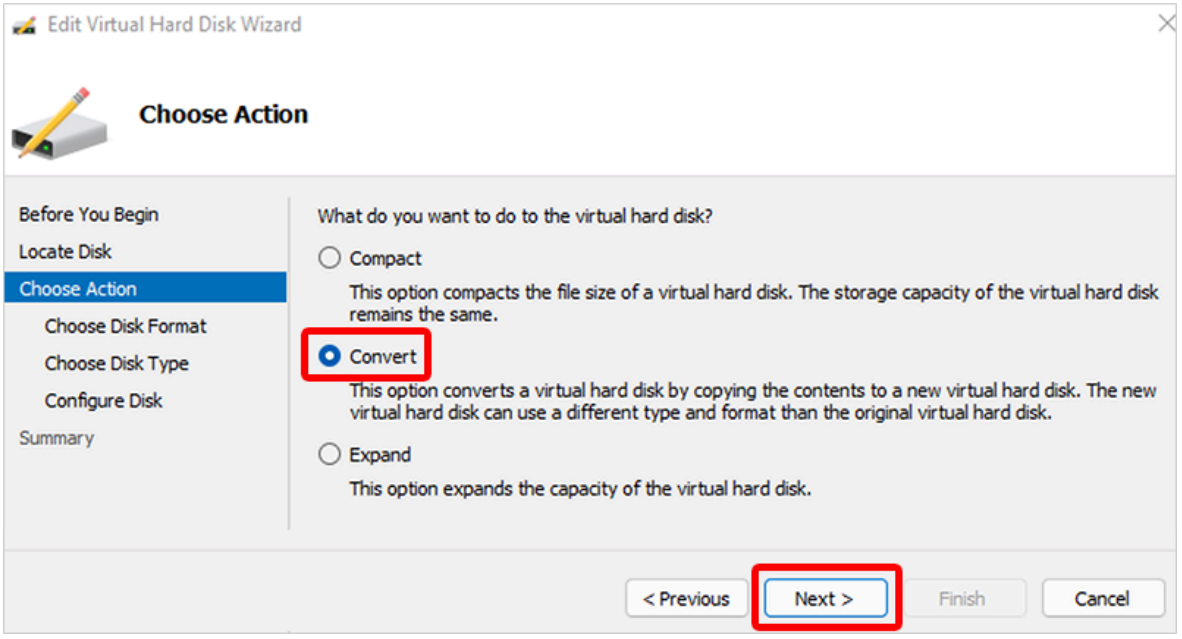
Преобразование диска в фиксированный размер и формат VHD

1. Отключение виртуальной машины.
2. В диспетчере Hyper-V выберите новую виртуальную машину >**Изменить диск** (в разделе **Действия**).
3. На странице **Перед началом работы** нажмите кнопку **Далее**.
4. На странице **Поиск дискаперейдите** к расположению преобразованного диска >**Далее**.
5. На странице **Выбор действия** выберите **Сжать**>**Готово**.

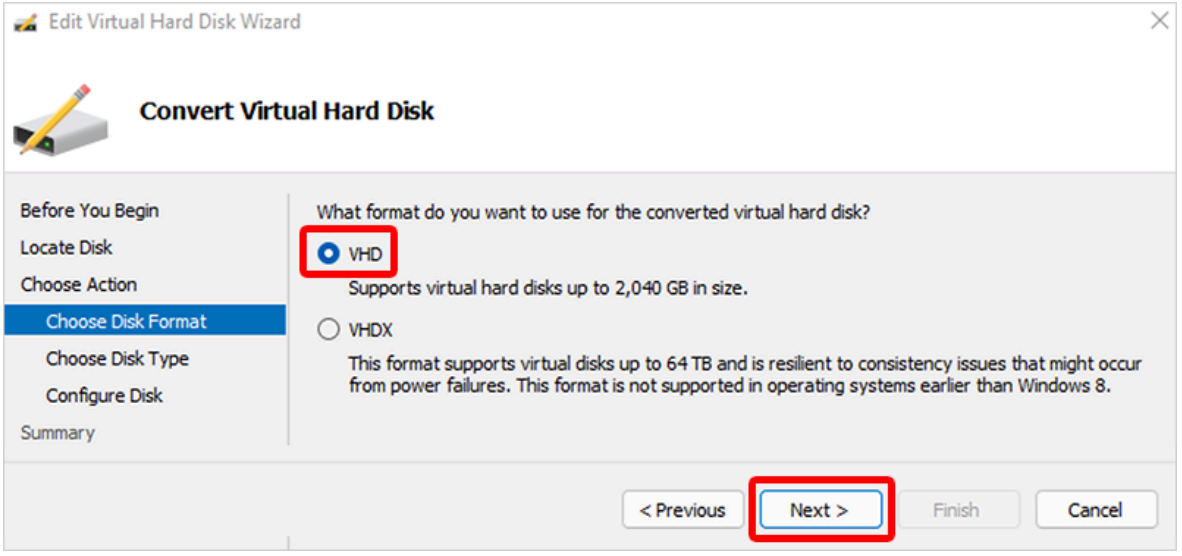


6. После завершения процесса выберите новую виртуальную машину еще раз >**Изменить диск**.
7. На странице **Перед началом работы** нажмите кнопку **Далее**.
8. На странице **Поиск дискаперейдите** к расположению преобразованного диска >**Далее**.

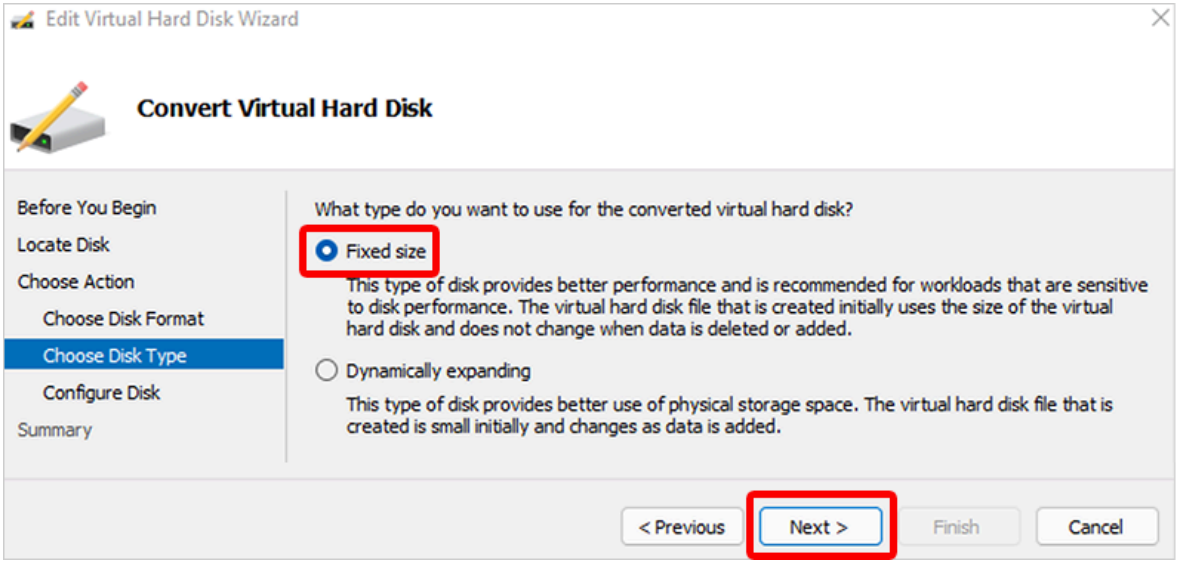
9. На странице **Выбор действия** выберите **Преобразовать**>**Далее**.



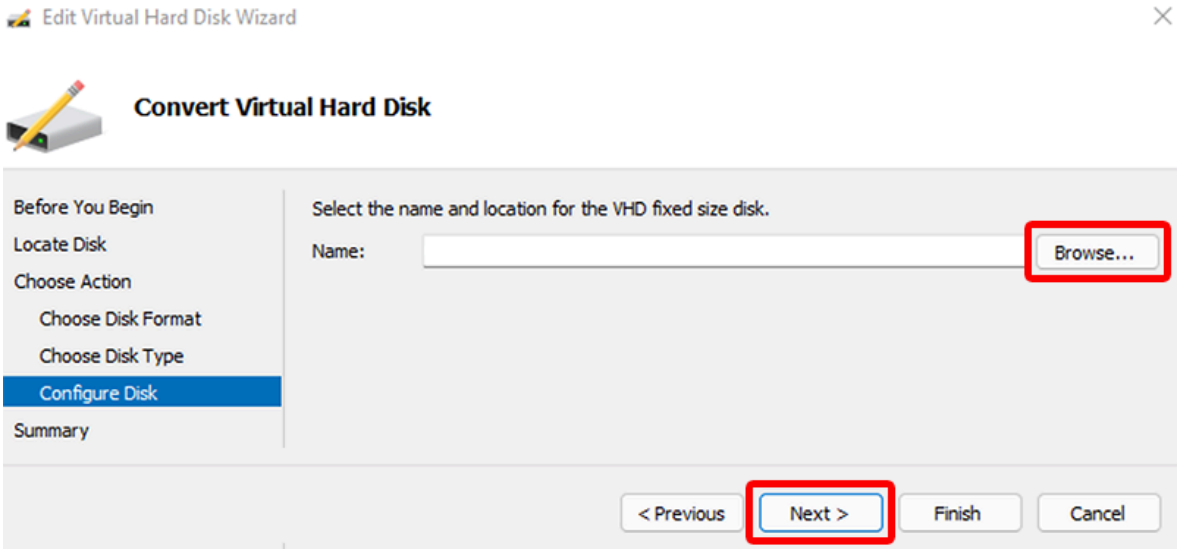
10. На странице **Выбор формата диска** выберите **VHD**>**Далее**.



11. На странице **Выбор типа диска** выберите **Фиксированный размер**>**Далее**.



12. На странице **Настройка дискаперейдите** к новому расположению диска, который будет создан >**Далее**.



13. На странице **Сводка** подтвердите правильность всех сведений и нажмите **Готово**.
14. После завершения процесса отключите ISO WinPE следующим образом.
    a. В разделе **виртуальные машины** диспетчера Hyper-V выберите новую виртуальную машину, а затем в разделе **Действия** выберите **Параметры**.
    b. В области навигации слева выберите **контроллер IDE 1**.
    c. В разделе **DVD-диск** зайдите в секцию **Контроллер** и выберите **контроллер IDE 1**.
    d. Нажмите кнопку **OK**.

Отправка преобразованного VHD в Azure

1. Отправьте преобразованный VHD обратно в Azure. Вы можете использовать Обозреватель службы хранилища Azure. Другие варианты отправки см. в разделе Отправка обобщенного VHD для Windows и создание с его помощью новых виртуальных машин в Azure.

> ⓘ **Примечание**
>
> Убедитесь, что VHD остается **VHD фиксированного размера**. **VHDX как формат** в Azure не поддерживается.

2. Перейдите на портал Azure, откройте **Образы**>**Создать**.
3. Заполните обязательные поля и выберите значение **Gen 2** для параметра **поколение VM**.
4. Нажмите **Проверить и создать**.
5. (Необязательно) После создания образа его можно отправить. Инструкции по отправке см. в статье Отправка виртуального жесткого диска в Azure или копирование управляемого диска в другой регион — Azure PowerShell.

6. Теперь можно добавить образ устройства в Windows 365. Информацию об отправке пользовательских образов см. в статье Добавление пользовательского образа устройства.

Дальнейшие действия

Дополнительные сведения о конфигурации устройств.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Настройка клиентов для Windows 365 государственных организаций

Статья • 31.01.2025

Самый быстрый способ использования Windows 365 — использовать AADJ, образы из коллекции и параметр Microsoft Hosted Network. Инструкции на этой странице приведены только в том случае, если необходимо использовать один из следующих вариантов:

- **Пользовательские образы**. Windows 365 предоставляет оптимизированные образы коллекции, включая образы с предустановленными приложениями Microsoft 365. После развертывания образа коллекции Intune можно использовать для дальнейшей настройки общих параметров и развертывания приложений. Если необходимо использовать существующий пользовательский образ, дополнительные сведения см. в разделе Добавление пользовательского образа.
- **Connections сети Azure (ANC).** ACS позволяют подготавливать облачные компьютеры, подключенные к управляемой виртуальной сети. Вот некоторые примеры.
  - Azure виртуальная сеть (виртуальная сеть).
  - Azure VPN-шлюз или выделенное подключение через ExpressRoute.
  - Другие ресурсы Azure, включая ресурсы облачных компьютеров.
- Дополнительные сведения см. в статье Создание сетевого подключения Azure.

Только для клиентов облака сообщества для государственных организаций (GCC) приведенные ниже инструкции позволяют Intune работать в Azure для управления облачными компьютерами, работающими в Azure для государственных организаций регионах.

> ⓘ **Примечание**
>
> - Для использования Windows 365 государственных организаций не требуется подписка на Azure для государственных организаций. Эти инструкции предназначены специально для GCC и только в том случае, если требуются пользовательские образы и (или) сетевые Connections Azure. Инструкции на этой странице не применяются к GCC High.
> - Для государственных организаций, у которых нет подписки на Azure для государственных организаций или требуется интеграция с Azure, рассмотрите возможность использования Windows 365 Корпоративная.

Убедитесь, что это соответствует вашим требованиям к соответствию. Windows 365 Корпоративная соответствует FedRAMP. См. описание службы Windows 365

Подготовка к работе

Для сопоставления клиентов и предоставления разрешений для пользовательских образов и (или) подключения к собственным сетям необходимо:

- Подписка Azure для государственных организаций.
- Учетные данные пользователя, имеющего:
  - Роль *глобального администратора* в клиенте Azure (заканчивается onmicrosoft.com).
- Учетные данные пользователя, имеющего:
  - Роль *владельца* в подписке Azure для государственных организаций, И
  - Роль *глобального администратора* в клиенте Azure для государственных организаций (заканчивается onmicrosoft.us).
- Для удовлетворения требований к лицензированию.
- (Если применимо) Ниже приведены сведения о применении разрешений для настройки сетевого подключения Azure. Виртуальная сеть и подсеть уже должны существовать.
  - Идентификатор подписки.
  - Группа ресурсов.
  - виртуальная сеть.
  - Подсеть.

Примечание

В то время как облачные компьютеры пользователей GCC размещаются и защищены в Azure для государственных организаций облаке, конечные точки для администраторов и конечных пользователей находятся в коммерческом домене Azure. Пользователи будут входить в облачные компьютеры, используя учетные данные, синхронизированные с Microsoft Entra ID.

параметры Microsoft Entra

Если вы хотите использовать Microsoft Entra присоединение или Microsoft Entra гибридное соединение, рассмотрите следующие возможности.

Microsoft Entra присоединенных облачных компьютеров. Если вы хотите использовать инфраструктуру Microsoft Entra присоединения и собственную сеть, вам потребуется клиент и подписка Azure в Azure для государственных организаций облаке. Клиент в домене azure .com должен быть сопоставлен с клиентом в домене Azure для государственных организаций (US).

Облачные компьютеры, присоединенные к гибридным Microsoft Entra. Если вы хотите использовать инфраструктуру гибридного присоединения Microsoft Entra, перед созданием виртуальных сетей Azure необходимо настроить свой коммерческий клиент (.com) и арендаторы для государственных организаций (US).

Подготовка к Windows 365 средству установки GCC

Чтобы средство установки GCC Windows 365 завершило сопоставление клиентов, приложению Windows 365 Microsoft Entra должно быть предоставлено разрешение на доступ к клиенту Azure для государственных организаций AD через субъект-службу. Объект субъекта-службы определяет, что приложение может делать в клиенте, кто может получить доступ к приложению и к каким ресурсам приложение может получить доступ. Перед первым запуском средства установки GCC Windows 365 необходимо выполнить следующие действия.

1. Если это еще не сделано, установите Azure CLI на компьютере, где будет создан субъект-служба. Дополнительные сведения см . в статье Установка Azure CLI.
2. Войдите в клиент Azure для государственных организаций AD, выполнив действия Azure CLI, описанные в разделе Вход с помощью Azure CLI. Для создания субъекта-службы для Windows App требуются разрешения глобального администратора.
3. Дополнительные сведения о работе с субъектами-службами в Azure см. в статье Работа с субъектом-службой Azure с помощью Azure CLI. Предоставьте клиенту разрешения приложения Windows 365 Microsoft Entra, выполнив следующую команду PowerShell: `az ad sp create --id 0af06dc6-e4b5-4f28-818e-e78e62d137a5`.
4. После успешного выполнения команды вы сможете просмотреть сведения о субъекте-службе, выполнив следующую команду PowerShell: `az ad sp show --id 0af06dc6-e4b5-4f28-818e-e78e62d137a5`. Вы должны увидеть Windows App, перечисленные в представлении **Все приложения** в колонке Корпоративное приложение в портал Azure.

Субъект-служба Windows App может получить доступ только к ресурсам Azure, необходимым для настройки пользовательского образа и поддержки сетевого подключения Azure (ANC) в Windows 365. После создания субъект-службу можно удалить только после отзыва пользовательских образов, объектов ANC и соответствующих облачных компьютеров, использующих их. В противном случае задачи подготовки облачных компьютеров могут завершиться сбоем, а существующие облачные компьютеры могут стать недоступными.

Начало работы со средством установки GCC Windows 365

Выполните следующие действия, чтобы настроить сопоставление клиентов с помощью средства установки GCC Windows 365.

1. Запустите GCCSetupTool.exe. Это средство доступно в Windows 365 для государственных организаций — средство установки GCC для Windows 10/11.
2. На странице **Начало работы** нажмите кнопку **Далее**.
3. Войдите с помощью учетной записи Azure. Эта учетная запись должна иметь разрешения глобального администратора.
4. Подтвердите, что вы хотите продолжить работу с коммерческой **учетной записью**> Далее.
5. Войдите с помощью учетной записи > Azure для государственных организаций **Далее**> введите свои учетные данные.
6. Подтвердите, что вы хотите продолжить работу с учетной записью для государственных организаций >**Далее**.
7. На **экране Выберите функцию для включения** убедитесь, что выбран параметр **Пользовательские изображения** . Этот параметр выбран по умолчанию, так как нет причин для запуска средства установки Windows 365 GCC, если вам не нужна хотя бы одна из перечисленных ниже функций.

   > **Примечание**
   >
   > ANC включает разрешения для пользовательских образов.

8. Выберите **сетевые подключения Azure** , а затем выберите **Подписка**, **Виртуальная сеть** и **Подсеть** , которые требуется настроить. Нажмите кнопку **Далее**.
9. На странице **Проверка параметров** просмотрите выбранные вами параметры и нажмите **кнопку Предоставить**.
10. После завершения настройки можно закрыть средство.

Устранение неполадок

Если у вас возникли проблемы с запуском средства установки GCC Windows 365:

1. В той же папке, где выполняется GCCSetupTool.exe, перейдите в папку **Log** и просмотрите `GCCAdminTool.log` файл.
2. Если у вас по-прежнему возникают проблемы, обратитесь в службу поддержки и предоставьте файл GCCADminTool.log.

Последующее использование средства установки GCC

Средство установки GCC Windows 365 можно запустить снова после начальной настройки. Возможно, вам потребуется снова использовать средство установки GCC, если вы:

- Не настроили ancs ранее или
- Требуется расширить использование ANCs в других сетях.

Альтернативный сценарий

В качестве альтернативы использованию средства установки GCC для настройки ANC можно также использовать следующий скрипт для настройки разрешений для дополнительных AHO.

> ⓘ **Примечание**
>
> Сопоставление клиента должно быть успешно выполнено, прежде чем приступить к выполнению скрипта для настройки ANCs.

Azure PowerShell

```
connect-azaccount -usedeviceauthentication
curl https://raw.githubusercontent.com/microsoft/Windows365-PSScripts/main/Windows%20365%20GCC/Grant%20Service%20Principal%20Roles%20in%20Tenant/Grant%20W365%20SP%20Roles%20In%20Tenant.ps1 -o GrantW365SProles.ps1
& ./GrantW365SProles.ps1
```

1. Если у вас нет Cloud Shell (требуется учетная запись хранения Azure), можно запустить скрипт двумя способами:

    - Выберите **Копировать** в скрипте и запустите сценарий PowerShell локально на компьютере.

- Выберите **Открыть Cloudshell**> вставьте скрипт в Azure для государственных организаций подписке Cloud Shell > запустите скрипт.

2. После выполнения скрипта в командной строке выберите вариант **2**. Этот параметр настраивает разрешения для ANC.
3. В списке Azure для государственных организаций подписок выберите подписку, для которой требуется предоставить разрешения.
4. В списке групп ресурсов выберите группу ресурсов, которую вы хотите использовать.
5. Выберите виртуальную сеть.
6. Скрипт предоставляет разрешения и перечисляет настроенные параметры.

Дальнейшие действия

Узнайте больше о Windows 365 государственных организаций.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Что такое Windows 365 boot?

19.09.2025

Windows 365 загрузка позволяет администраторам настраивать Windows 11 физических устройств, чтобы пользователи могли:

- Избегайте входа на физическое устройство.
- Войдите непосредственно в Облачный компьютер Windows 365 на физическом устройстве.

Когда пользователь включает физическое устройство и входит в систему, Windows 365 boot входит в систему непосредственно на своем облачном компьютере, а не на физическом устройстве. Если единый вход включен для облачного компьютера, им не нужно повторно входить на облачный компьютер. Благодаря этому ускоренная процедура входа сокращает время, необходимое пользователю для доступа к облачному компьютеру.

Windows 365 Boot поддерживает сценарии как выделенных, так и общих компьютеров.

Windows 365 общий режим загрузки поддерживает проверку подлинности FIDO. Дополнительные сведения см. в разделе Практическое руководство. Вход с ключом безопасности FIDO2 без пароля для Windows 10 устройств HAADJ.

Сценарий общего компьютера

Несколько пользователей могут использовать одно физическое устройство для входа на собственные личные облачные компьютеры. Когда каждый пользователь входит на физическое устройство, его уникальное удостоверение переносит его на назначенный и безопасный облачный компьютер. Такая гибкость делает Windows 365 Boot хорошим решением для таких работников, как медсестры, продавцы и колл-центры, которые совместно используют физические устройства компании. Такие рабочие роли могут часто переключаться между физическими задачами и взаимодействием с компьютером. Windows 365 Boot позволяет обходить длительный процесс запуска и загружаться непосредственно на защищенный облачный компьютер, чтобы выбрать место, где они вышли.

Такие работники могут:

1. Выйдите из облачного компьютера на физическом устройстве.
2. Передайте физическое устройство следующему сотруднику во время смены.
3. Следующая рабочая роль смены может использовать то же физическое устройство для входа на свой облачный компьютер.

Выход из Облачный компьютер Windows 365 возвращает устройство на экран Windows 11 входа, готовый для следующего пользователя.

Сценарий выделенного компьютера

В этом сценарии физическое устройство назначается конкретному пользователю для подключения к облачному компьютеру. выделенный режим загрузки Windows 365 поддерживает Windows Hello.

Доступ к физическому устройству

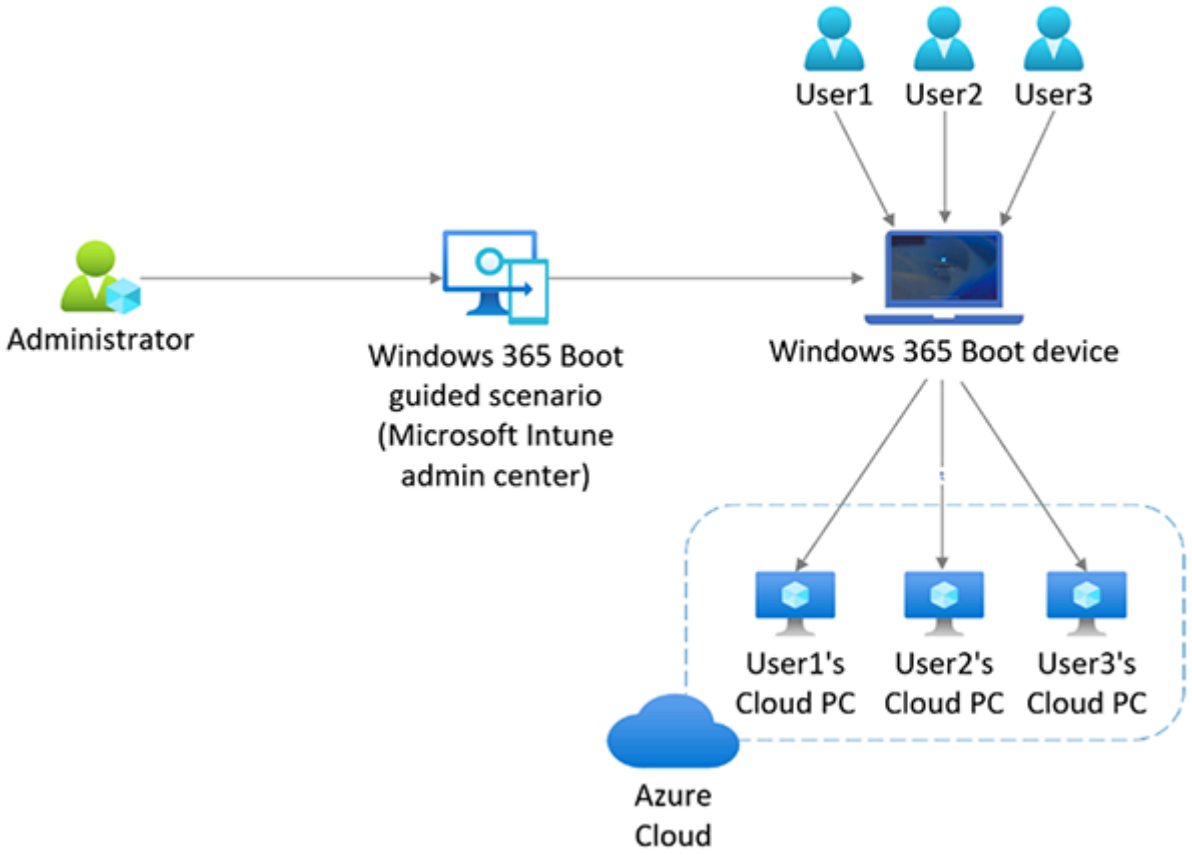
Windows 365 Загрузочные физические устройства предназначены для взаимодействия пользователей со своими облачными компьютерами без возможности взаимодействия с физическим устройством. Для достижения этой цели необходимо задать некоторые политики поставщика служб конфигурации (CSP).

Windows 365 загрузка не настраивает эти политики автоматически, чтобы полностью ограничить доступ конечных пользователей к определенным ресурсам на физическом устройстве. Ознакомьтесь с политиками конфигурации, которые можно применить к устройствам загрузки Windows 365, чтобы обеспечить безопасность вашей организации для предотвращения доступа к физическому устройству. Дополнительные сведения об этих профилях конфигурации см. в разделе Ограничение доступа пользователей к физическому устройству Windows 365 загрузки.

Основное намерение заключается в том, что пользователи не могут войти на физический компьютер. Сведения об элементах управления для предоставления физического доступа см. в разделе Включение или ограничение доступа к физическому устройству.

Обзор процесса

1. С помощью интерактивного сценария загрузки Windows 365 в Центре администрирования Microsoft Intune настройте физическое устройство для Windows 365 загрузки.
2. (Необязательно) Рассмотрите возможность ограничения доступа пользователей к физическим устройствам Windows 365 загрузки.
3. Настройте каждое физическое устройство для Windows 365 конфигурации загрузки.
4. После настройки устройства несколько пользователей могут получить доступ к выделенным облачным компьютерам с одного и того же Windows 365 загрузочного физического устройства.



Режимы проверки подлинности при входе пользователя

Поддержка Windows 365 режимов проверки подлинности загрузки при входе пользователей на облачные компьютеры показана в следующей таблице:

Развернуть таблицу

Режим проверки подлинности	Поддержка выделенного режима	Поддерживается общий режим
Имя пользователя и пароль	Да	Да
Windows Hello для бизнеса	Да	Нет
Ключ FIDO	Да	Да
Удобный контакт	Нет	Нет

Центр подключений при входе в систему

Если у вас несколько облачных компьютеров и по умолчанию облачный компьютер не задан, вы увидите **Центр подключений** при входе в систему. Центр подключений — это экран выбора, на который перечислены все доступные облачные компьютеры, связанные с учетной записью пользователя.

- В центре подключений можно выбрать, какой облачный компьютер следует запустить для этого сеанса.
- Если вы хотите избежать запроса каждый раз, можно задать один из облачных компьютеров по умолчанию непосредственно в центре подключений, щелкнув меню с многоточием (...) и выбрав **Подключиться автоматически**.
- После установки по умолчанию облачного компьютера он будет автоматически использоваться для последующих входов.
- Если вы хотите изменить значение по умолчанию на другой облачный компьютер, это необходимо сделать из веб-клиента, обновив параметр по умолчанию из карта Cloud PC.

Изменение облачного компьютера по умолчанию с веб-клиента

Если у пользователя несколько облачных компьютеров, он может выбрать облачный компьютер по умолчанию для использования при каждом входе. Чтобы задать это значение по умолчанию, выполните следующее:

1. Перейдите к **веб-клиенту** (https://windows.cloud.microsoft).
2. В карта для облачного компьютера, который вы хотите задать по умолчанию, выберите многоточие (...). >**Параметры**.
3. На вкладке **Интегрированные возможности** в разделе **Загрузка на этом облачном компьютере** выберите **Подключиться при входе на устройство**.
4. Нажмите кнопку **Обновить**.

Улучшения обработки ошибок

1. Если возникнет ошибка, при нажатии кнопки **Отмена** в диалоговом окне вы откроете **центр подключений**.
2. В карта облачного компьютера, который вы хотите устранить, выберите многоточие (...), чтобы перезапустить или устранить неполадки облачного компьютера.

Поддержка аварийного восстановления между регионами

Windows 365 Boot теперь поддерживает аварийное восстановление между регионами. См. статью Аварийное восстановление между регионами в Windows 365

Поддержка Bluetooth

Чтобы подключиться к устройствам Bluetooth с Windows 365 загрузить облачный компьютер, выполните следующие действия.

1. Откройте **bluetooth быстрых**> параметров.
2. В окне **Параметры** свяжите и подключитесь к устройствам Bluetooth.

Перенаправление батареи

В режиме загрузки Windows 365 на панели задач на рабочем столе облачного компьютера отображается состояние батареи локального компьютера.

Дальнейшие действия

Windows 365 сценарии загрузки.

Windows 365 требования к физическому устройству загрузки.

Ограничьте доступ пользователей к физическому устройству Windows 365 загрузки.

Устранение неполадок Windows 365 загрузки.

Посетите блог технического сообщества Майкрософт.

Интерактивный сценарий: развертывание Windows 365 загрузки на физических устройствах

01.06.2025

Следуя этому интерактивному сценарию, можно развернуть Windows 365 загрузки на общих Windows 11 Pro или физических устройствах enterprise. Windows 365 загрузка позволяет пользователям физических устройств выполнять вход непосредственно на облачные компьютеры без входа на физические устройства.

В этом руководстве описано, как определить:

1. Шаблоны имен устройств Autopilot и префиксы имен ресурсов.
2. Параметры обновления Windows.
3. Профиль VPN, профиль Wifi и языковые параметры.
4. Группирование назначений для определения физических устройств, настроенных для Windows 365 загрузки.

Дополнительные сведения о интерактивных сценариях в целом см. в Intune обзоре интерактивных сценариев.

Предварительные условия

- Каждое физическое устройство и облачный компьютер должны работать Windows 11 Корпоративная или Professional версии 22621.3374 или более поздней.
- У вас должна быть роль администратора службы Intune.

Перед добавлением физических устройств в группу необходимо убедиться, что они соответствуют требованиям Windows 365 загрузки.

Вы можете выполнить интерактивный сценарий, пока в группу еще не добавлены устройства. После добавления устройств в группу и доступа к Интернету они автоматически обновляются с помощью параметров загрузки Windows 365, определенных в интерактивном сценарии.

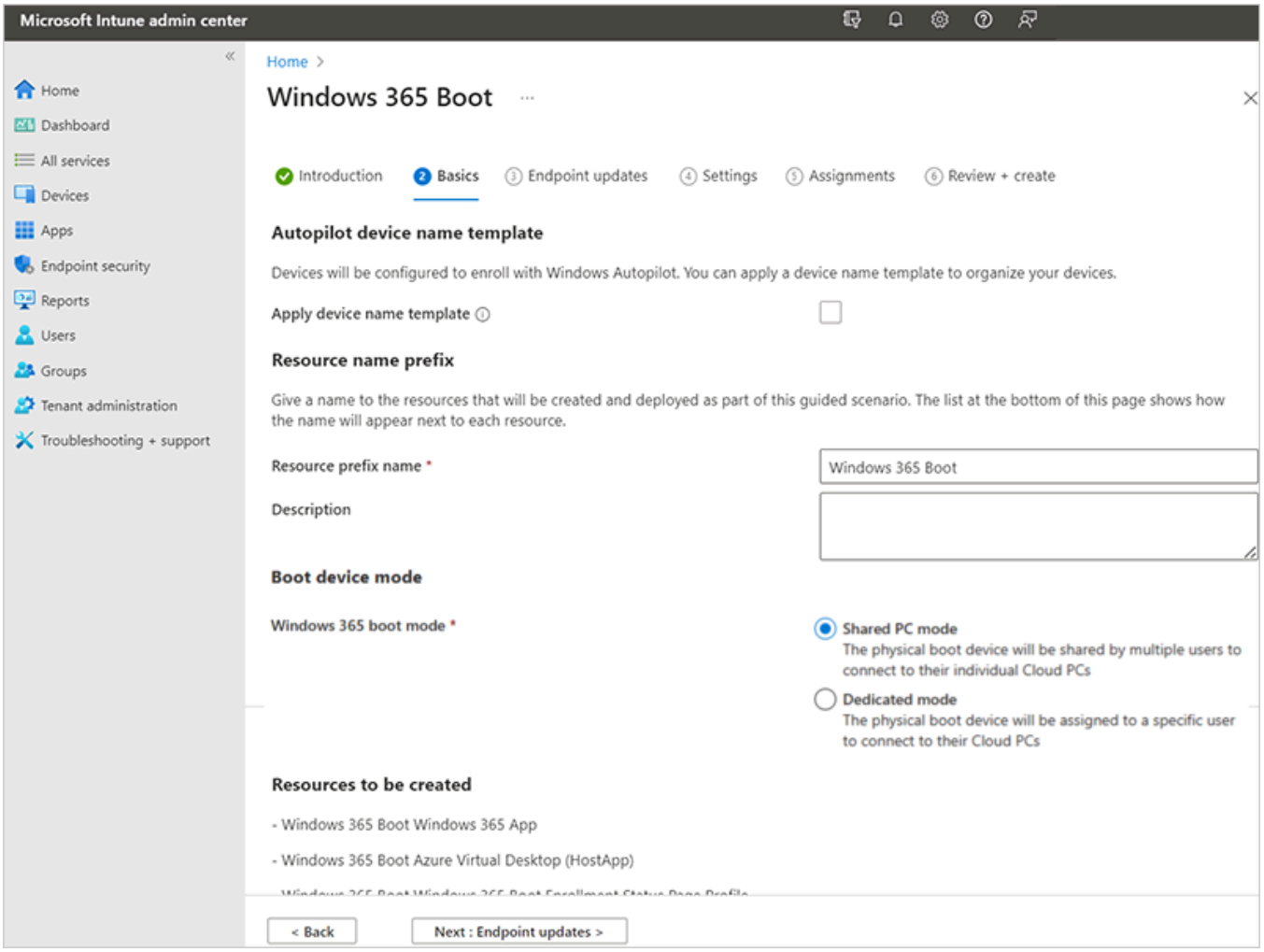
Шаг 1. Введение

1. Войдите в Центр администрирования Microsoft Intune как пользователь с ролью администратора службы Intune.

2. Выберите **Устройства**>**Windows 365** (в разделе **Обзор**) >**Windows 365 Загрузка** (в Windows 365 руководствах).
3. На странице **Введение** выберите **Далее: основные сведения**.

Шаг 2. Основные сведения

Выберите, какие имена получат устройства при регистрации, и выберите префикс для имен всех создаваемых ресурсов.



1. **Autopilot device name template** (Шаблон имени для устройства Autopilot): этот интерактивный сценарий регистрирует устройства в Windows Autopilot. Вы можете присваивать имена устройствам при регистрации с помощью уникального шаблона, который применяется ко всем устройствам. Доступны следующие параметры:

    - **Применить шаблон имени устройства**. Если вы не проверка это поле, при именовании устройств не создается шаблон или шаблон. Устройство получает имя OEM, например DESKTOP-, за которым следует несколько случайных символов. Установите флажок, чтобы создать уникальный шаблон для присвоения устройству имени. Например, введите Contoso-%RAND:7%, чтобы назвать все устройства Contoso, а затем семь случайных символов.

Имена должны соответствовать следующим требованиям:
    - Должны иметь длину не более 15 символов.
    - Могут включать латинские буквы (a–z, A–Z), цифры (0–9) и дефисы.
    - Не могут состоять из одних цифр и не могут содержать пробелы.
    - Можно использовать макрос %SERIAL% для добавления серийного номера оборудования.
    - Можно использовать макрос %RAND:x% для добавления случайной строки символов, где x равно количеству добавляемых символов.

- **Префикс имени ресурса**: при развертывании этого интерактивного сценария автоматически создаются несколько ресурсов. Чтобы различать элементы, используемые в этом развертывании, добавьте префикс.

2. **Введите имя префикса ресурса**. Введите текст, который будет помещен в начало созданных элементов. Например, введите `Windows 365 Boot`. Все созданные ресурсы называются **примерно так: Windows 365 Загрузка Виртуального рабочего стола Azure (HostApp).**

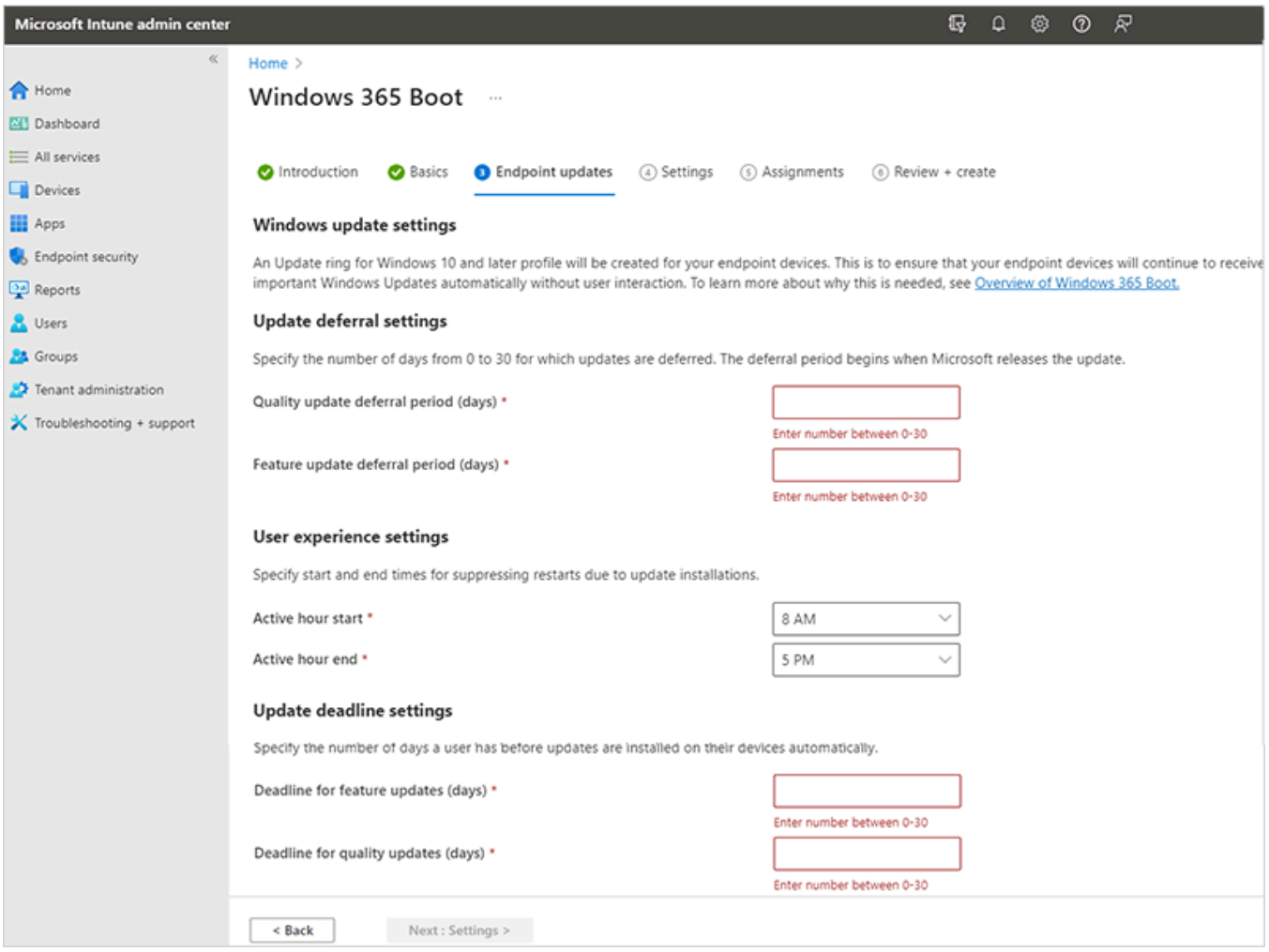
3. **Режим загрузки устройства**. Выберите один из следующих параметров:

    - **Режим общего компьютера**: для физических устройств, совместно используемых несколькими пользователями
    - **Выделенный режим**: для физического устройства, используемого одним конкретным пользователем.

4. Выберите **Далее: обновления конечной точки**.

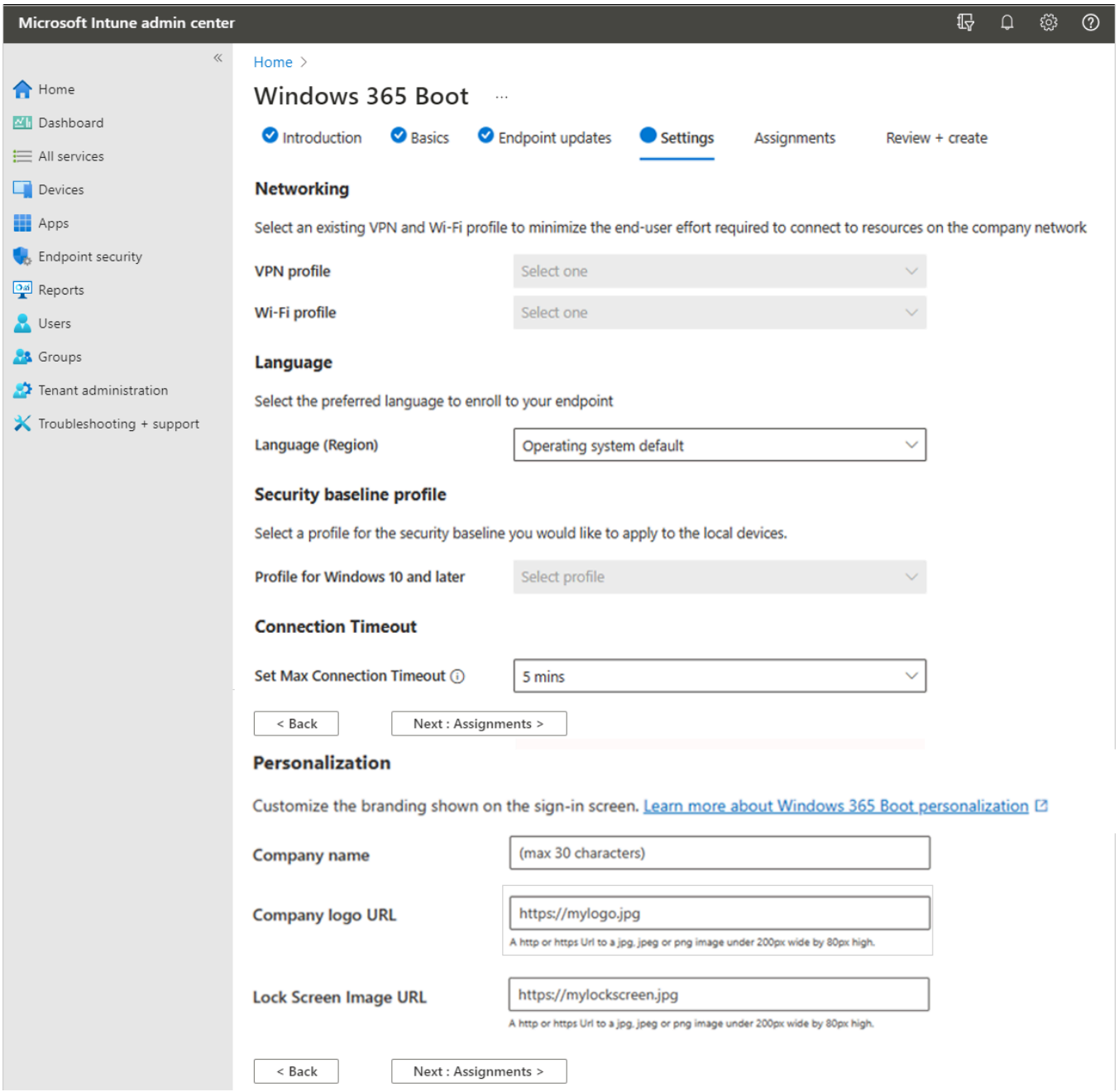
Шаг 3. Обновления конечной точки

На странице **Обновления конечной точки** задайте параметры, которые нужно использовать для Windows Обновления на физических устройствах. Убедитесь, что выбранные варианты соответствуют требованиям безопасности вашей организации. Выберите **Далее: Параметры**.



Windows 365 загрузка поддерживает автоматическое исправление Windows для автоматизации управления исправлениями для Windows 365 загрузочных физических устройств. Если вы используете эту автоматизацию, ее следует настроить вне этого интерактивного сценария.

Шаг 4. Параметры



1. (Необязательно) На странице **Параметры** выберите **профиль VPN** и **профиль Wi-Fi**, которые будут использоваться для Windows 365 загрузочных физических устройств. При выборе существующего профиля Wi-Fi или VPN, если профиль уже назначен **всем пользователям** или **всем устройствам**, это назначение удаляется и заменяется новым назначением, предназначенным только для Windows 365 группы, созданной или выбранной в этом интерактивном сценарии.
2. (Необязательно) Если вы не хотите использовать язык операционной системы по умолчанию, выберите конкретный **язык (регион)**>**Далее: Назначения**.
3. (Необязательно) Выберите **профиль базовых показателей безопасности**, который будет использоваться для Windows 365 загрузки физических устройств.
4. (Необязательно) Выберите значение для **параметра Задать максимальное время ожидания подключения** для Windows 365 загрузки. Операционная система ожидает подключения, пока не будет достигнуто выбранное значение времени ожидания.

Дополнительные сведения см. в разделе Поставщик службы конфигурации политики (CSP) SetMaxConnectionTimeout.

5. (Необязательно) Если вы хотите настроить фирменную символику, отображаемую в верхней части экрана входа, укажите любую или все из следующих сведений:

   - **Название компании**
   - **URL-адрес логотипа компании**
   - **URL-адрес изображения экрана блокировки**

Шаг 5. Назначения

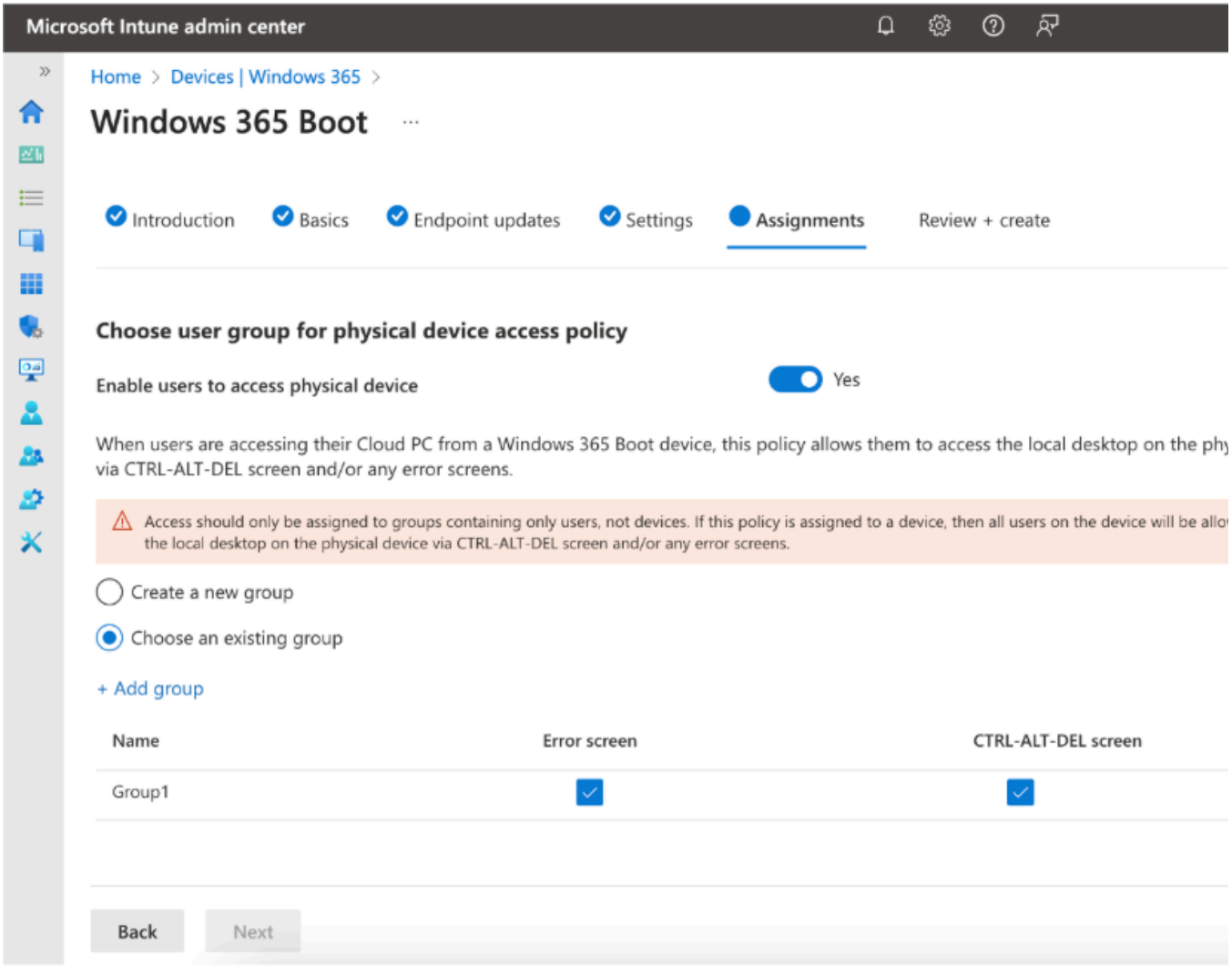
Выберите группы, которые вы хотите получить в этом интерактивном сценарии, и все ресурсы, которые он создает. Вы можете назначить существующие группы или создать новые группы и назначить их.

- **Создать новую группу**: создает новую группу и развертывает в ней политики интерактивного сценария. По мере добавления устройств в эту группу они получают ресурсы из этого интерактивного сценария.
  - **Имя группы**: введите имя для новой группы. Например, введите `Windows 365 boot physical devices`.

- **Выбрать существующую группу**: выберите нужную группу. Ресурсы интерактивного сценария развертываются в этой группе.

Вы также можете выбрать группы пользователей для назначения политики доступа к физическому устройству. Эта политика позволяет пользователям получать доступ к локальному рабочему столу на физическом устройстве с помощью экрана CTRL-ALT-DEL или любых экранов ошибок. Вы можете применить доступ к экрану CTRL-ALT-DEL, доступ к экрану ошибки, нет или и то, и другое, к любой группе пользователей. Эту политику можно назначить существующей группе или создать новую группу для нее.

Дополнительные сведения о функции доступа к физическому устройству см. в разделе Включение или ограничение доступа к физическому устройству.



Завершив назначение групп, выберите **Далее: Проверка и создание**.

Вы можете выполнить интерактивный сценарий, пока в группу еще не добавлены устройства. Когда устройства добавляются в группу и имеют доступ к Интернету, они автоматически начинают получать политики в этом интерактивном сценарии.

Вы также можете добавить в группу предварительно зарегистрированные устройства Windows Autopilot. добавить их в группу перед регистрацией или применением каких либо политик; Инструкции по настройке новых устройств с Помощью Windows Autopilot см. в разделе Windows 365 Требования к физическому устройству загрузки.

Шаг 6. Проверка и создание

Отображаются сводные данные о параметрах и значениях, которые вы настроили. Вы можете вернуться на любую вкладку и изменить добавленные значения.

Когда параметры вас устраивают, нажмите кнопку **Создать**.

Шаг 7 (необязательно) — режим самостоятельного развертывания

Режим самостоятельного развертывания — это конфигурация в Windows Autopilot, которая позволяет развертывать устройство без вмешательства пользователя. Он идеально подходит для таких сценариев, как общие устройства или настройки в стиле киоска.

Если вы уже выполнили интерактивный сценарий, создается профиль **Autopilot, управляемый пользователем**, для подготовки Windows 365 загрузочных устройств. Чтобы переключиться в **режим саморазвертывания**, выполните следующие действия.

1. Создайте новый профиль развертывания Autopilot:

   a. В Центре администрирования Microsoft Intune перейдите в раздел**Профили развертыванияWindows Autopilot>для регистрации устройств**>>.

   b. Выберите **+ Создать профиль**, а затем — **Компьютер с Windows**.

   c. Введите имя профиля.

   d. В разделе **Режим развертывания** выберите **Самостоятельное развертывание** в раскрывающемся списке.

   e. При необходимости заполните остальные параметры профиля и нажмите кнопку **Далее**.

   f. В разделе **Назначения** оставьте для параметра Включенные группы значение "Группы не выбраны" и нажмите кнопку **Далее** , а затем **создать**.

2. Изменение назначения группы:

   a. Назад к профилю**, управляемому пользователем**, созданному ранее с помощью интерактивного сценария.

   b. В разделе **Назначения свойств**> щелкните **Изменить**.

   c. Запишите имя назначенной в настоящее время группы, а затем нажмите кнопку **Удалить** , чтобы отменить назначение профиля. Нажмите **кнопку Проверить и сохранить** , а затем **Сохранить**.

   d. Откройте созданный профиль **самостоятельного развертывания** .

   e. В разделе **Назначения свойств**> щелкните **Изменить**, а затем добавьте ту же группу, чтобы назначить новый профиль.

Дальнейшие действия

Windows 365 требования к физическому устройству загрузки.

Ограничьте доступ пользователей к физическому устройству Windows 365 загрузки.

Устранение неполадок Windows 365 загрузки.

Дополнительные сведения о интерактивных сценариях см. в Intune обзоре интерактивных сценариев.

Windows 365 настройка и требования к физическому устройству загрузки

Статья • 31.01.2025

Выполните следующие действия и требования, чтобы настроить общие физические устройства для загрузки Windows 365.

Требования к операционной системе

Каждое физическое устройство (и облачный компьютер) должно работать под управлением одной из следующих версий 22621.3374 или более поздней:

- Windows 11 Корпоративная
- Windows 11 Профессиональный
- Windows IoT Enterprise

Настройка физического устройства

1. Откройте **клиентский компонент Центра обновления Windows** и включите **параметр Получать последние обновления, как только они будут доступны**.
2. Войдите вцентр >администрирования Microsoft Intune Устройства >**Все устройства**.
3. Выберите устройство в списке >**Очистка**>**.** Не выбирайте ни один из полей в поле подтверждения очистки.
4. При следующем подключении устройства к Интернету оно будет очищаться. Этот процесс может занять несколько минут.
5. Выполните действия Windows Autopilot, описанные в следующем разделе.

Регистрация физического устройства с помощью Windows Autopilot

Если устройство уже зарегистрировано в Autopilot, пропустите этот раздел.

1. В командной строке физического устройства используйте клавиши SHIFT+F10.

2. В командной строке выполните следующие команды.

```
Azure PowerShell
```

```
PowerShell.exe -ExecutionPolicy Bypass
[Net.ServicePointManager]::SecurityProtocol  =
[Net.SecurityProtocolType]::Tls12
Install-Script -name Get-WindowsAutopilotInfo -Force
Set-ExecutionPolicy -Scope Process -ExecutionPolicy RemoteSigned
Get-WindowsAutopilotInfo -Online
```

3. При появлении запроса войдите в систему с помощью пользователя с ролью администратора Intune. После входа устройство автоматически регистрируется в Intune. Запишите серийный номер.

Добавление физического устройства в группу Microsoft Entra

1. Войдите в Центр администрирования Microsoft Intune как пользователь с ролью администратора службы Intune.
2. Выберите **Группы**>**Все группы**> найдите группу Microsoft Entra, которая использовалась в интерактивном сценарии> загрузки Windows 365 выберите группу.
3. На странице группы выберите **Члены**>**Добавить участников**> поиск по серийному номеру > физического устройства выберите физическое устройство >**Выбрать**.
4. Подождите несколько минут, пока назначения ресурсов будут выполнены.

В течение этого времени просмотрите другие конфигурации устройств, которые могут применяться к устройству. Убедитесь, что они подходят для устройства, которое подключается только напрямую к Облачный компьютер Windows 365. Отмена назначения ненужных приложений и профилей конфигурации, чтобы убедиться, что подключение Windows 365 Boot обеспечивает простое подключение. Также см. раздел Ограничение доступа пользователей к Windows 365 загрузочных физических устройств.

Вход на устройство

1. Завершите готовый запуск (OOBE) для физического устройства, как и для любого пользователя.
2. После запуска запуска перезагрузите устройство.
3. Когда пользователь входит на устройство, он будет доставлен непосредственно в свою Облачный компьютер Windows 365.

Дальнейшие действия

Ограничение доступа пользователей к физическим устройствам Windows 365 загрузки

Устранение неполадок Windows 365 загрузки.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Разрешение или ограничение доступа пользователей к физическому устройству Windows 365 загрузки

Статья • 05.05.2025

Windows 365 Загрузочные физические устройства предназначены для взаимодействия пользователей со своими облачными компьютерами без возможности взаимодействия с физическим устройством. Для достижения этой цели необходимо задать некоторые политики поставщика служб конфигурации (CSP).

Windows 365 загрузка не настраивает эти политики автоматически, чтобы полностью ограничить доступ конечных пользователей к определенным ресурсам на физическом устройстве. Администраторы должны просмотреть следующие поставщики служб безопасности и решить, какие из них следует реализовать на физическом устройстве в соответствии с требованиями к безопасности вашей организации.

Используя политику конфигурации, вы также можете разрешить пользователям доступ к физическому компьютеру с экрана CTRL-ALT-DEL, экранов ошибок облачного компьютера или и того, и другого.

Разрешить пользователю доступ к физическому устройству

С помощью политики доступа к физическому устройству можно разрешить пользователям доступ к физическому компьютеру. Пользователи могут захотеть получить доступ к физическому компьютеру, если они не могут:

- Войдите на облачный компьютер (во время простоя Интернета или простоя службы Майкрософт).
- Войдите в captive Wi-Fi.

Пользователи могут получить доступ к физическому компьютеру с экрана CTRL-ALT-DEL или экранов ошибок, настраиваемых администратором. Когда пользователь нажимает **кнопку Вернуться к физическому компьютеру для входа** на любом экране, он перейдет на экран входа на физическом устройстве. Чтобы вернуться на страницу входа в Cloud PC, пользователи могут заблокировать физический компьютер или выйти из него.

Для любой группы пользователей можно выбрать, имеют ли пользователи доступ к физическому компьютеру с экрана CTRL-ALT-DEL, экраны ошибок, оба или ни один из

них. **Ни один из** вариантов не является значением по умолчанию. После изменения параметра пользователи смогут увидеть кнопки **Вернуться к физическому входу** .

Администраторы настраивают эту политику с помощью интерактивного сценария загрузки на вкладке **Назначения** или вручную. Дополнительные сведения см. в разделах Поставщики служб конфигурации — User/EnablePhysicalDeviceAccessOnCtrlAltDel и Поставщики служб конфигурации — User/EnablePhysicalDeviceAccessOnErrorScreens.

Windows 365 загрузка в облако поддерживает политику доступа к физическому устройству в следующих версиях Windows и более поздних версиях:

- Windows 11 версии 23H2 ОС сборки 22621.4249 или более поздней.

Запрет доступа к диспетчеру задач физического устройства

В Windows 365 загрузки доступ к диспетчеру задач локального устройства можно получить при нажатии клавиш CTRL+ALT+DELETE. Диспетчер задач можно отключить с помощью политики CSP DisableTaskMgr.

Эта политика запрещает использование диспетчера задач в системе для всех пользователей, включая администраторов. Он также предотвращает запуск диспетчера задач с помощью сочетаний клавиш на физическом устройстве. Хотя эта политика повышает безопасность устройства, отсутствие доступа к физическому устройству усложняет устранение неполадок на устройстве.

Запретить пользователям изменять пароль физического устройства

Изменение паролей пользователей не поддерживается для физических устройств Windows 365 загрузки. Если этот параметр используется в вашей среде, его можно отключить, чтобы не запутать пользователей с помощью политики CSP DisableChangePassword.

Настройка поставщика учетных данных по умолчанию

Windows 365 загрузка предназначена для режима общего компьютера. Для этого режима требуется метод проверки подлинности имени пользователя и пароля. В зависимости от среды могут быть настроены другие поставщики проверки подлинности, которые могут

запутать пользователей. Чтобы избежать этой путаницы, рекомендуется задать для поставщика учетных данных по умолчанию имя пользователя и пароль. Чтобы задать это значение по умолчанию, используйте политику CSP DefaultCredentialProvider.

Удаление уведомлений и центра уведомлений с панели задач

Если на устройствах установлены сенсорные экраны, пользователи могут взаимодействовать с центром уведомлений физического устройства и представлением календаря. Эти компоненты также позволяют пользователям запускать приложение "Параметры" для физического устройства Windows 365 Boot. Чтобы удалить у пользователя возможность доступа к этим компонентам, используйте политику DisableNotificationCenter CSP.

Запрет уведомлений о физических устройствах

Уведомления с физического устройства Windows 365 загрузки могут отображаться в сеансе облачного компьютера. Чтобы предотвратить такие уведомления, используйте политику CSP NoToastNotification.

Запрет автоматического запуска приложений во время входа пользователя

Некоторые приложения на физическом устройстве Windows 365 Boot могут быть настроены для автоматического запуска во время входа пользователя. Чтобы избежать этого, используйте политику CSP DisableExplorerRunLegacy_1.

Улучшение входа на устройствах с сенсорным экраном

Устройствам с сенсорным экраном требуется, чтобы во время входа пользователя отображался сенсорный экран. На Windows 365 устройствах с сенсорным экраном загрузки можно улучшить процесс входа с помощью политики CSP EnableTouchKeyboardAutoInvokeInDesktopMode.

Запрет доступа пользователей к физическим дискам устройств

При использовании Windows 365 загрузки физическое устройство пользователя во время входа перенаправляется на облачный компьютер. После этого пользователи облачных компьютеров смогут взаимодействовать с физическим устройством.

Чтобы предотвратить перенаправление дисков для Windows 365 загрузочных подключений, можно включить облачный компьютер в назначение с групповая политика Objects или каталогом параметров. Дополнительные сведения см. в статье Управление перенаправлениями протокола удаленного рабочего стола устройства (RDP) для облачных компьютеров.

Дальнейшие действия

Устранение неполадок Windows 365 загрузки.

Partner, Microsoft, and customer roles and responsibilities for Windows 365

There is a clear divide of responsibilities between Microsoft, third-party partners, and customers.

- Microsoft is responsible for the security and compliance of the cloud infrastructure.
- Partners (Citrix, Omnissa, HP Anyware) are responsible for operating and maintaining their agents, connection protocols, and workspace portals.
- Customers are responsible for managing and configuring security and compliance in the cloud according to their specific needs and risk tolerance.

For complete information about the split responsibilities between Microsoft and customers, reference Microsoft and customer responsibilities for Windows 365 | Microsoft Learn.

Protocol	Component	Responsibility		
		MSFT	Partner	Customer
Windows 365	Gateway connectivity and reliability	✓		
	Web portal access and desktop publishing	✓		
	Brokering of RD connections	✓		
	User authentication			✓
	Cloud PC internet connectivity	✓		✓
	End-client to gateway	✓		✓
	Gateway to Cloud PC	✓		
Windows 365 with Partner protocol	Gateway connectivity and reliability		✓	
	Web portal access and desktop publishing		✓	
	Brokering of RD connections		✓	
	User authentication		✓	✓
	Cloud PC internet connectivity	✓		✓
	End-client to gateway		✓	✓
	Gateway to Cloud PC		✓	✓

Partner Responsibilities

Connection protocol connectivity infrastructure: Partner is responsible for the protocol infrastructure that connects end-users to their Cloud PCs. For Citrix specifically, user connections no longer go through Microsoft's AVD/RDP gateways. Omnissa and HP do not block RDP.

Software (agent and client): Partners are responsible for developing, updating, and maintaining the agents (installed on Cloud PCs) and the workspace portal.

Security and compliance: Partners are responsible for the security, compliance, and reliability of their services and software.

Support and troubleshooting: Partners provide customer support for issues related to their portion of the solution. In general, any connectivity issue over partner protocol is handled by the partner's support team.

Customer Responsibilities

Licensing: Customers must procure, manage, and assign the appropriate licenses for both Windows 365 and partner solutions.

Microsoft, Partner, and Customer Shared Responsibilities

Support and troubleshooting: Microsoft provides platform-level support. Partners provide support specifically towards workspace portals and connection protocols. If an investigation finds that the root cause lies with the partner's service, Microsoft will advise the customer to contact the partner and vice versa. Customers handle OS-level issues, application troubleshooting, and user-related concerns.

User management and authentication: Partners and customers share the responsibilities of managing user accounts, access permissions, and identity security.

Last updated on 29.10.2025

Windows 365 поддерживаемые сценарии интеграции с партнерами

10.10.2025

Следующие сценарии интеграции партнеров поддерживают протоколы партнеров поверх Windows 365, не нарушая простоту и предсказуемость, которые Windows 365 обеспечивает.

Развернуть таблицу

Партнер	Поддерживаемые клиенты	Служба шлюза	Протокол подключения	Поддерживаемые планы обслуживания
Citrix	Веб-клиент Citrix Workspace Настольные клиенты Citrix Workspace для поддерживаемых платформ	Служба шлюза Citrix Cloud	Citrix HDX	Enterprise, Frontline
HP	Веб-клиент HP Anyware Настольные клиенты HP Anyware для поддерживаемых платформ	Служба облачного шлюза HP Anyware	HP Anyware	Enterprise, Enterprise с поддержкой GPU
Omnissa	Веб-клиент Omnissa Workspace ONE Классические клиенты Omnissa ONE для поддерживаемых платформ	Служба облачного шлюза Omnissa	Omnissa Blast	Корпоративная

Хотя сценарии, не перечисленные здесь, могут по-прежнему работать в рабочей среде клиентов, они не поддерживаются корпорацией Майкрософт.

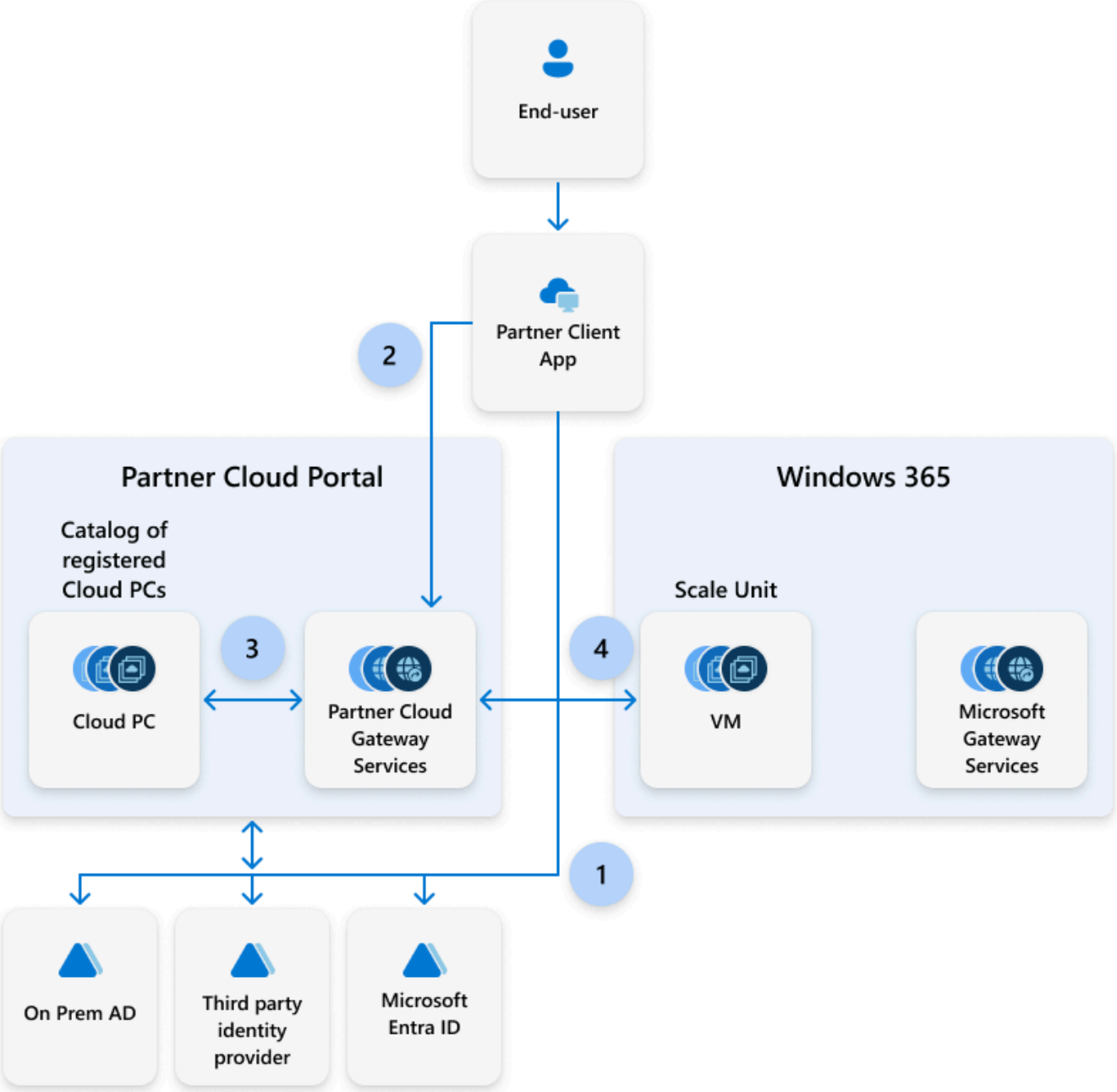
Примечание

Локальные службы шлюзов не поддерживаются.

Важно!

Чтобы агент партнера был в поддерживаемом состоянии, его необходимо установить в рамках стандартного процесса подготовки, назначив пользователям лицензию партнера на портале партнера. Установка агента партнера вручную не поддерживается.

Процесс подключения пользователей с интеграцией партнеров



1. Пользователь проходит проверку подлинности с помощью идентификатора Microsoft Entra, локальная служба Active Directory или стороннего поставщика удостоверений.
2. Windows 365 устанавливает подключение к облачному шлюзу партнера с помощью протоколов партнеров.

3. Облачный компьютер назначается пользователю и доступен на веб-порталах или порталах рабочих областей.
4. Windows 365 устанавливает подключение к облачному компьютеру с помощью протоколов партнеров.

Дальнейшие действия

Настройте Citrix HDX Plus для Windows 365 Корпоративная.

Настройте HP Anywhere для Windows 365 Корпоративная.

Настройте Omnissa Horizon для Windows 365 Корпоративная.

Требования к использованию Citrix HDX Plus для Windows 365 Корпоративная

Статья • 31.01.2025

Чтобы использовать Citrix HDX Plus для Windows 365, необходимо выполнить следующие требования:

Требования Citrix

- Клиент Citrix Cloud с HDX Plus для Windows 365 прав
  - Standard DaaS для Azure
  - DaaS Advanced Plus
  - DaaS Premium
  - DaaS Premium Plus
- Учетная запись администратора Citrix с полными правами администратора
- Облачные компьютеры должны иметь доступ к:
  - https://.. nssvc.net tcp 443 и UDP 443 для сеансов HDX через TCP и EDT соответственно. Если вы не можете разрешить все поддомены таким образом, вместо этого можно использовать https://*.c.nssvc.net и https://*.g.nssvc.net. Дополнительные сведения см. в статье Центра знаний службы поддержки Citrix CTX270584.
  - https://*.xendesktop.net на TCP 443. Если вы не можете разрешить все поддомены таким образом, можно использовать https://<customer_ID.xendesktop.net>, где customer_ID — это идентификатор клиента Citrix Cloud, как показано на портале администрирования Citrix Cloud.
- Для Microsoft Entra гибридных развертываний:
  - Домен Microsoft Entra должен быть синхронизирован с Microsoft Entra домена, к которому принадлежат облачные компьютеры.
  - Облачные соединители, позволяющие Citrix Cloud подключаться к домену Active Directory. Дополнительные сведения см. в разделе Citrix Cloud Connector.
- Конечная точка списка разрешений, необходимая для регистрации VDA: *.apps.cloud.com

Требования Майкрософт

- право Microsoft Intune
- Microsoft Entra домен в том же клиенте, что и Microsoft Intune
- Windows 365 Корпоративная лицензии в том же клиенте, что и Microsoft Intune
- Учетная запись администратора Azure:
  - Intune администратора для необходимых авторизации в Citrix Cloud.
  - Intune администратор для включения соединителя Citrix в Microsoft Intune.
  - Дополнительные сведения о требованиях к Windows 365 см. в разделе требования Windows 365.

Citrix HDX Plus в настоящее время не поддерживает Windows 365 Frontline.

Поддерживаемые конфигурации

Citrix HDX Plus для Windows 365 поддерживает интеграцию с Windows 365 развертываниями для облачных компьютеров, присоединенных к Microsoft Entra, и Microsoft Entra облачных компьютеров с гибридным присоединением. В следующих таблицах подробно описаны конфигурации для каждого сценария.

Поддерживаемые инфраструктуры

Развернуть таблицу

Удостоверение	Citrix Cloud	CVAD (локальная среда)	Рабочая область Citrix	Citrix Storefront	Служба шлюза Citrix	Шлюз Citrix
Microsoft Entra присоединено	Да	Нет	Да	Нет	Да	Нет
Microsoft Entra гибридное присоединение	Да	Нет	Да	Нет	Да	Нет

Поддерживаемые поставщики удостоверений

Развернуть таблицу

Удостоверение	Microsoft Entra ID	Active Directory	Active Directory + токен	Okta	SAML	Шлюз Citrix	Адаптивная проверка подлинности
Microsoft Entra присоединено	Да	Нет	Нет	Нет	Нет	Нет	Нет
Microsoft Entra гибридное присоединение	Да	Да	Да	Да	Да	Да	Да

Примечание

Для развертываний с гибридным присоединением к AD, если вы используете поставщик удостоверений, отличный от Active Directory или Active Directory + Token, вам потребуется служба федеративной проверки подлинности Citrix (FAS). Если вы не используете FAS, вы не сможете использовать единый вход (SSO) на облачном компьютере. Дополнительные сведения см. в **документации FAS**.

Дальнейшие действия

Настройте Citrix HDX Plus для Windows 365 Корпоративная.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Настройка Citrix HDX Plus для Windows 365 Корпоративная

Статья • 31.01.2025

Citrix HDX Plus для Windows 365 позволяет интегрировать Citrix Cloud с Windows 365. Эта интеграция предоставляет доступ к технологиям Citrix HDX для повышения безопасности и управляемости облачных компьютеров.

Общие сведения о настройке

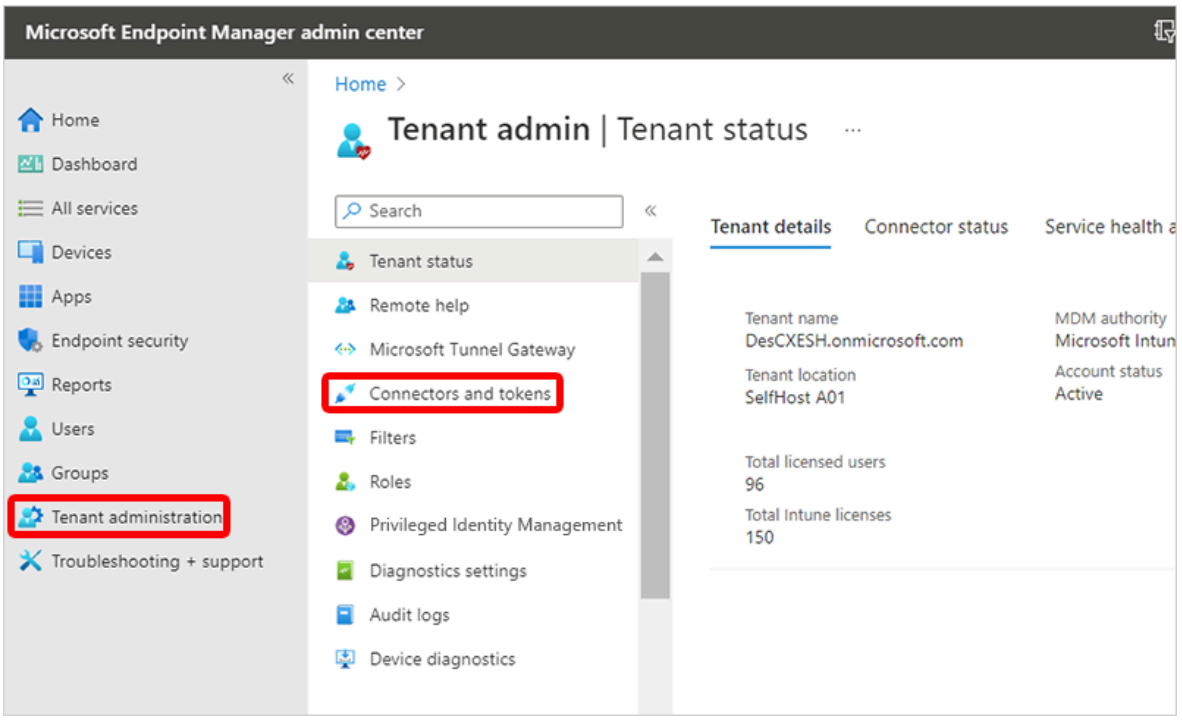
Чтобы настроить Citrix HDX Plus для Windows 365 Корпоративная, выполните следующие действия. Первые два шага описаны здесь на learn.microsoft.com. Остальные действия описаны на веб-сайте citrix.com.

1. Выполнение требований.
2. Включите соединитель Citrix в Intune.
3. Подключите Microsoft Entra ID к Citrix Cloud.
4. Настройте Citrix Workspace.
5. Подключите Windows 365 к Citrix Cloud.
6. Назначьте пользователям лицензии Citrix.
7. Подготовка облачных компьютеров.

Включите соединитель Citrix Windows 365 в Intune

Чтобы включить соединитель Citrix, выполните следующие действия.

1. Как администратор Intune войдите в Центр администрирования Microsoft Intune, выберите**Соединители и маркерыадминистрирования**> клиента.



2. Выберите **Windows Partner Citrix connector**Add (**Добавить** соединитель > Citrix для Windows).

3. В разделе **Добавить соединитель** выберите **Citrix** в раскрывающемся списке.

4. Рядом **с пунктом Разрешить пользователям использовать Citrix для подключения к своим облачным компьютерам** установите переключатель **в значение Добавить**>.

Дальнейшие действия

Перейдите к Citrix Cloud, чтобы завершить интеграцию. Дополнительные сведения о настройке Citrix HDX Plus в Citrix Cloud см. в разделе https://docs.citrix.com/en-us/citrix-hdxplus-w365 .

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Повторная установка агента Citrix

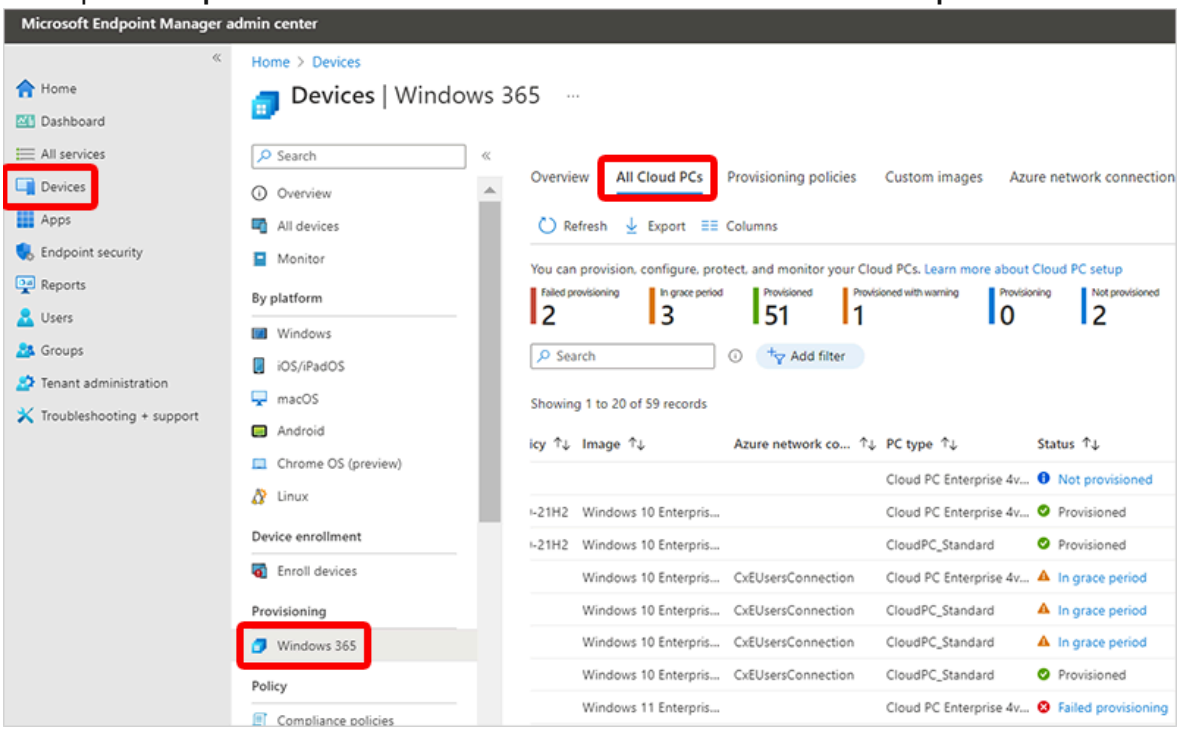
Статья • 24.02.2025

Если подготовка для облачного компьютера Citrix HDX Plus выполнена успешно, но установка агента Citrix завершается сбоем, можно повторить установку агента Citrix. Вам не нужно повторно создавать облачный компьютер.

Чтобы повторить установку агента Citrix, выполните следующие действия.

1. Войдите в Центр администрирования Microsoft Intune.

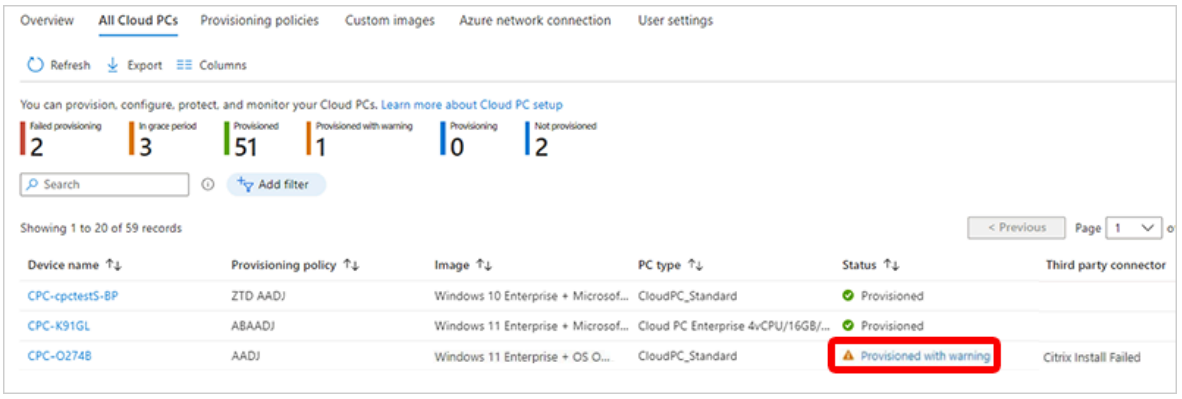
2. Выберите **Устройства**>**Windows 365**>**Все облачные компьютеры**.



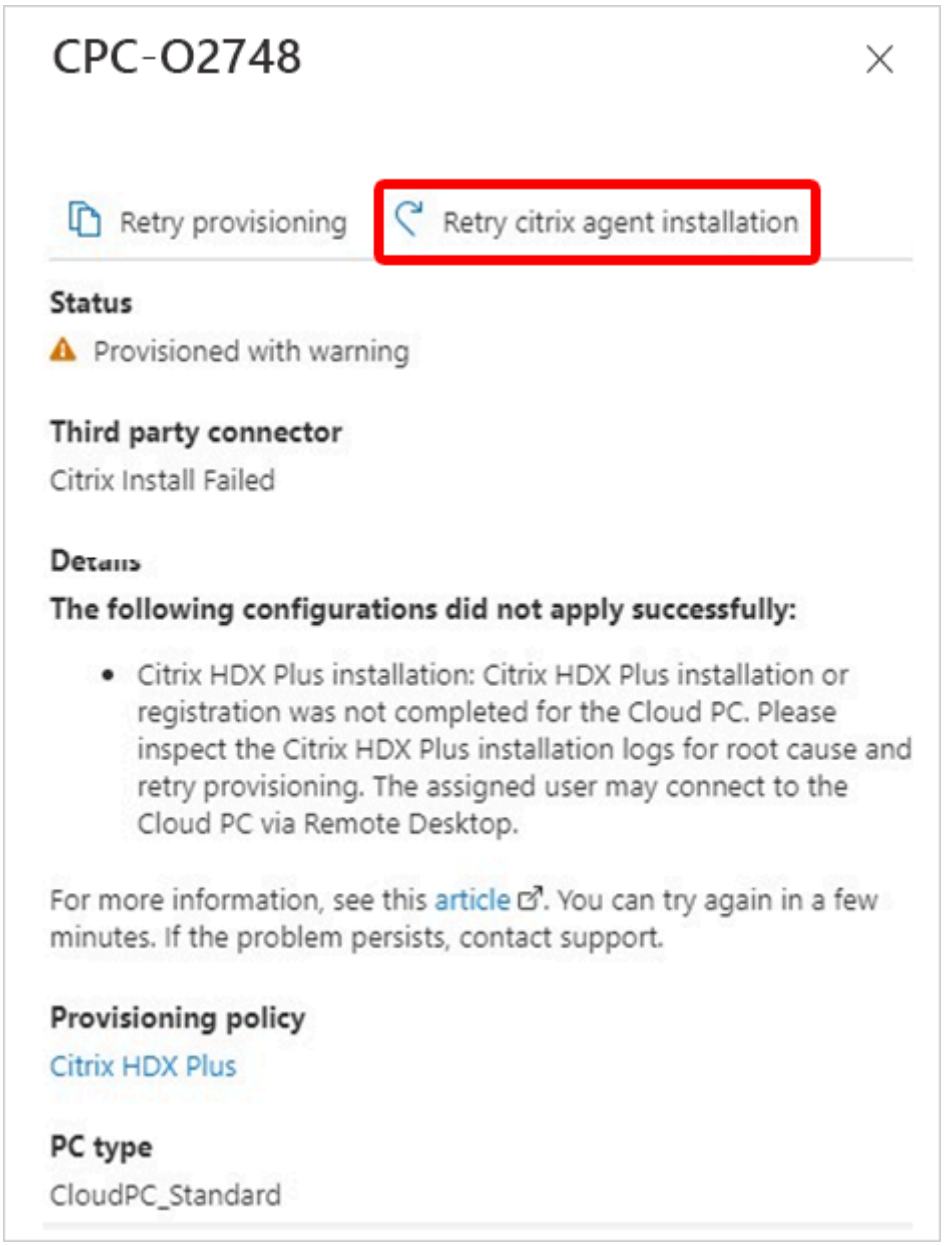
3. Убедитесь, что отображается столбец **Стороннего соединителя** . Этот столбец можно добавить, выбрав **Столбцы**>**Сторонний соединитель**.

4. В столбце **Сторонний соединитель** найдите строку с сообщением о **сбое установки Citrix**.

5. Выберите предупреждение (например , **Подготовлено с предупреждением**) в столбце **Состояние** .



6. В новой области выберите **Повторить установку агента Citrix**. Так как облачный компьютер был успешно подготовлен, вам не нужно повторять подготовку.



Дополнительные сведения о Citrix см. в статье Настройка Citrix HDX Plus для Windows 365 Корпоративная.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Требования к использованию Omnissa Horizon для Windows 365 Корпоративная

Статья • 31.01.2025

Чтобы использовать Omnissa Horizon для Windows 365, необходимо выполнить следующие требования:

Требования Omnissa

- Облачная служба Omnissa Horizon — клиент следующего поколения
- Подписка На облачную службу Horizon, которая включает в себя:
  - Универсальные лицензии Horizon для приложений
  - Horizon Universal License for Desktops and Apps поддерживает брокеры для Windows 365 облачных компьютеров
- Учетная запись Omnissa Cloud Service Portal (CSP)
- Тот же доступ к поставщику удостоверений, используемый клиентом Windows 365
- Подключение клиента к клиенту
- Право пользователей
- Облачный компьютер должен иметь доступ к следующим портам:
  - С агентом: 8444
  - Клиент: 443 и 8443
- Omnissa UAG как услуга (предварительная версия) требуется для брокера для Windows 365 облачных компьютеров. Он включен по умолчанию при включении типа поставщика Windows 365 в Cloud Service Horizon — следующего поколения.
- Клиент должен иметь собственную сеть (BYON) и использовать сетевое подключение Azure.

Требования Майкрософт

- право Microsoft Intune
- Microsoft Entra домен в том же клиенте, что и Microsoft Intune
- Windows 365 Корпоративная лицензии в том же клиенте, что и Microsoft Intune
- Учетная запись администратора Azure:

- Intune администратора для необходимых авторизации в облаке Omnissa.
- Intune администратор для включения соединителя Omnissa в Microsoft Intune.
- Дополнительные сведения о требованиях к Windows 365 см. в разделе требования Windows 365.

Поддерживаемые конфигурации

Omnissa Horizon для Windows 365 поддерживает интеграцию с Windows 365 развертываниями для Microsoft Entra присоединенных облачных компьютеров и Microsoft Entra облачных компьютеров с гибридным присоединением.

Дальнейшие действия

Настройте Omnissa Horizon для Windows 365 Корпоративная.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Настройка Omnissa Horizon для Windows 365 Корпоративная

Статья • 31.01.2025

Omnissa Horizon — это облачная служба, которая позволяет доставлять пользователям Windows 365 Корпоративная рабочих столов с любого устройства и расположения. С помощью Omnissa Horizon можно использовать возможности и безопасность Windows 365 Корпоративная, упрощая при этом управление инфраструктурой виртуальных рабочих столов (VDI) и ее развертывание.

Общие сведения о настройке

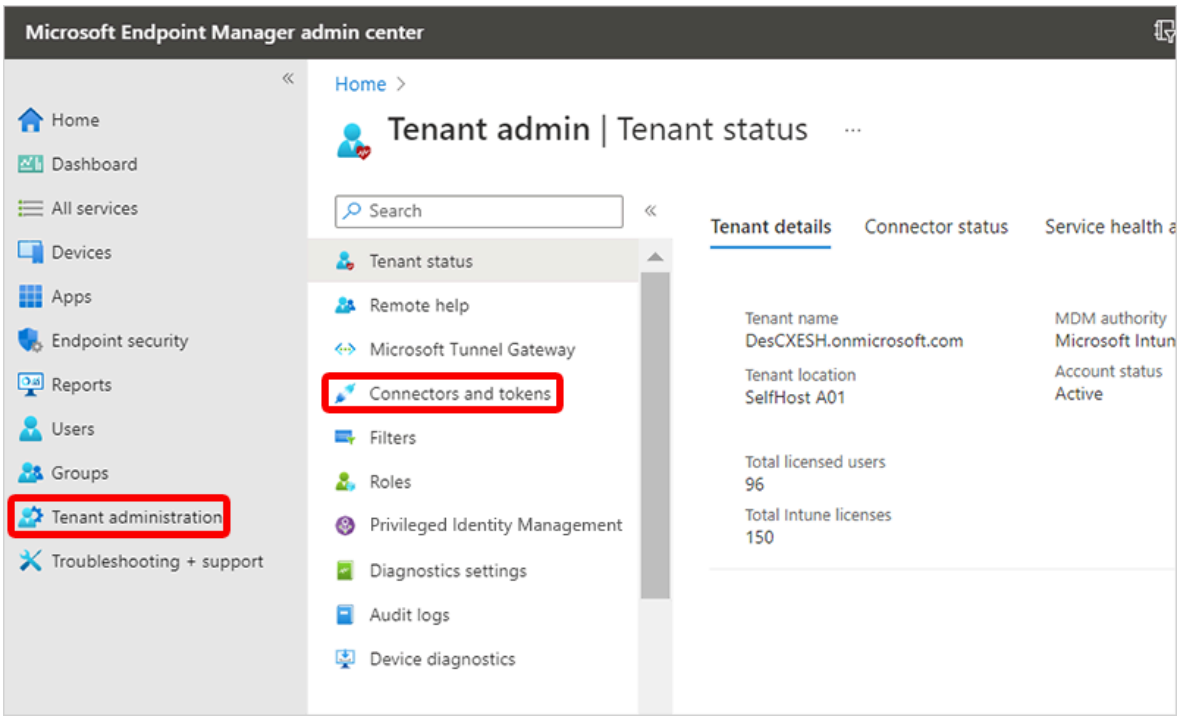
Чтобы настроить Omnissa Horizon для Windows 365 Корпоративная, выполните следующие действия. Первые два шага описаны здесь на learn.microsoft.com. Остальные действия описаны на веб-сайте Omnissa.

1. Выполнение требований.
2. Включите соединитель Windows 365 Omnissa в Intune.
3. Настройте клиент облачной службы Horizon.
4. Настройка поставщика удостоверений.
5. Подключите облачную службу Horizon к Windows 365.
6. Назначьте лицензии Omnissa Microsoft Entra пользователям или группам.

Включите соединитель Windows 365 Omnissa в Intune

Чтобы включить соединитель Omnissa, выполните следующие действия.

1. Как администратор Intune войдите в Центр администрирования Microsoft Intune, выберите**Соединители и маркерыадминистрирования**> клиента.



2. Выберите **Соединители**> партнеров Windows**Добавить**.
3. В разделе **Добавить соединитель** выберите **Omnissa** в раскрывающемся списке.
4. Рядом **с пунктом Разрешить пользователям использовать Omnissa для подключения к своим облачным компьютерам** установите переключатель **в значение Добавить**>.

Дальнейшие действия

Чтобы завершить интеграцию, перейдите к Omnissa Horizon Cloud. Дополнительные сведения о настройке Omnissa Horizon см. в статье Настройка Omnissa Horizon Cloud для интеграции Windows 365.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Требования к использованию HP Anyware для Windows 365 Корпоративная

18.06.2025

Чтобы использовать HP Anyware для Windows 365, необходимо выполнить следующие требования:

Требования к HP Anyware

- HP Anyware Standard или HP Anyware Professional
- Облачные компьютеры должны иметь доступ к:
  - https://cas.teradici.com в TCP 443 для подключения брокера.
- Дополнительные требования см. в руководстве по планированию сеансов Anyware .

Требования Майкрософт

- право Microsoft Intune
- Microsoft Entra домен в том же клиенте, что и Microsoft Intune
- Windows 365 Корпоративная лицензии в том же клиенте, что и Microsoft Intune
- Учетная запись администратора Azure:
  - Intune администратора для необходимых авторизации в службе HP Anyware.
  - Intune администратор для включения соединителя HP Anyware в Microsoft Intune.
  - Дополнительные сведения о требованиях к Windows 365 см. в разделе требования Windows 365.

Поддерживаемые конфигурации

HP Anyware для Windows 365 поддерживает интеграцию с Windows 365 развертываниями для Microsoft Entra присоединенных облачных компьютеров и Microsoft Entra облачных компьютеров с гибридным присоединением. Кроме того, поддерживаемые поставщики удостоверений включают Microsoft Entra ID и Okta.

Дальнейшие действия

Настройка HP AnyWare для Windows 365 Корпоративная.

Настройка HP Anyware для Windows 365 Корпоративная

Статья • 24.04.2025

HP Anyware для Windows 365 — это облачная служба, которая позволяет доставлять Windows 365 Корпоративная рабочих столов по протоколу управления и PCoIP HP Anyware. Инфраструктура и протокол HP Anyware отличаются в средах с низкой пропускной способностью и интенсивных рабочих нагрузках.

HP Anyware для Windows 365 доступно в выбранных регионах. Чтобы зарегистрироваться для интерактивного подключения к HP Anyware для Windows 365 или зарегистрироваться для получения обновлений, см. раздел https://reinvent.hp.com/Anyware-for-windows365 .

Общие сведения о настройке

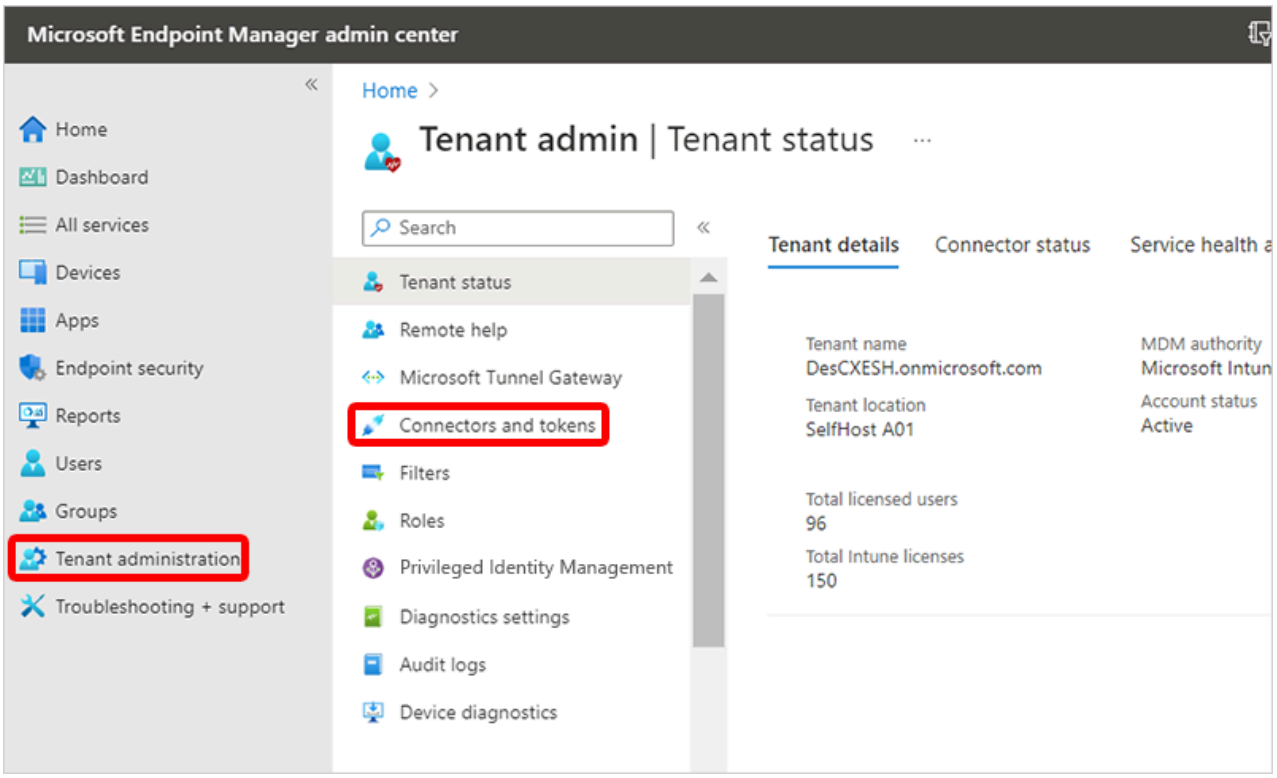
Чтобы настроить HP Anyware для Windows 365 Корпоративная, выполните следующие действия. Первые два шага описаны здесь на learn.microsoft.com. Остальные действия описаны на веб-сайте HP Anyware.

1. Выполнение требований.
2. Включите соединитель WINDOWS 365 HP Anyware в Intune.
3. Подключите Microsoft Entra ID к HP Anyware .
4. Назначьте пользователям лицензии HP Anyware и подготовьте облачные компьютеры .

Включите соединитель WINDOWS 365 HP Anyware в Intune

Чтобы включить соединитель HP Anyware, выполните следующие действия.

1. Как администратор Intune войдите в Центр администрирования Microsoft Intune , выберите**Соединители и маркерыадминистрирования**> клиентов.



2. Выберите **Windows 365 соединители**> партнеров**Добавить**.

3. В разделе **Добавление соединителя** выберите **HP Anyware** в раскрывающемся списке.

4. Рядом **с пунктом Разрешить пользователям использовать HP Anyware для подключения к своим облачным компьютерам** установите переключатель **в значение Добавить**>.

Дальнейшие действия

Чтобы завершить интеграцию, перейдите к HP Anyware Manager. Дополнительные сведения о настройке HP Anyware см. в разделе https://aka.ms/HPAnywareDocConnectEntraIDtoHP .

Создание политик подготовки

Статья • 21.04.2025

Облачные компьютеры создаются и назначаются пользователям на основе политик подготовки. Эти политики содержат основные правила подготовки и параметры, позволяющие службе Windows 365 правильно настроить Облачные компьютеры для пользователей. После создания политик подготовки и назначения Microsoft Entra группам безопасности пользователей или Группы Microsoft 365 служба Windows 365:

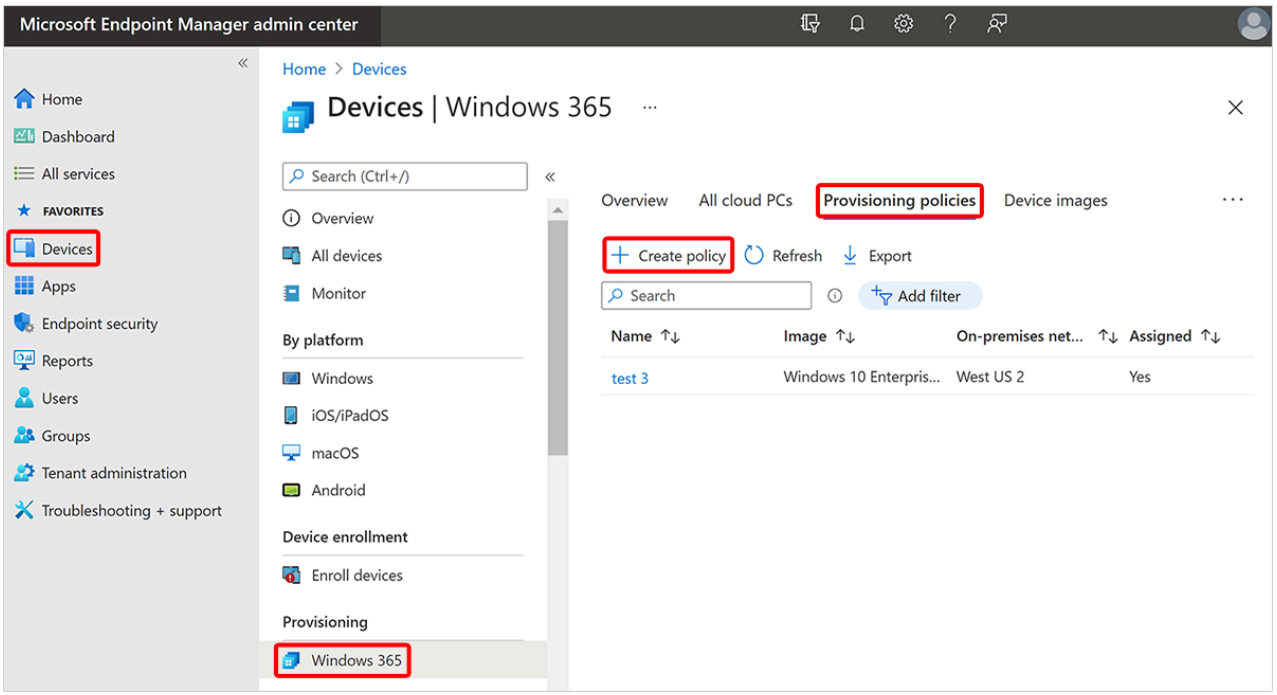
1. Проверяет наличие соответствующего лицензирования.
2. Настраивает облачные компьютеры соответствующим образом.

Рекомендации:

- Windows 365 Корпоративная
  - Если пользователю в назначенной группе не назначена лицензия на Облачный компьютер, Windows 365 не будет подготавливать для него Облачный компьютер.
  - Для каждой лицензии на Облачный компьютер, назначенной пользователю, для настройки используется только одна политика подготовки. Служба Windows 365 всегда использует первую назначенную политику для подготовки Облачного компьютера.
- Windows 365 Frontline в выделенном режиме
  - Если у вас больше пользователей в Microsoft Entra группе пользователей, чем количество облачных компьютеров, доступных для выбранного размера, некоторые пользователи могут не получить свой облачный компьютер.
  - При удалении пользователей из группы пользователей Microsoft Entra облачный компьютер автоматически перемещается в льготный период .
- Windows 365 Frontline в режиме общего доступа
  - При удалении пользователей из группы пользователей Microsoft Entra пользователь теряет доступ к облачному компьютеру.
  - Если удалить группу пользователей Microsoft Entra из назначения, облачные компьютеры автоматически отзываются без перехода на льготный период.

Создание политики подготовки

1. Войдите в Центр администрирования Microsoft Intune , выберите **Устройства**>**Windows 365** (в разделе **Подключение устройств**) > Политики >**подготовкиСоздать политику**.



2. На странице **Общие** введите значения в поля **Имя** и **Описание** (необязательно) для новой политики.

> **Совет**
>
> Имя политики подготовки не может содержать следующие символы: <> & | " ^

3. На странице **Общие** выберите **тип лицензии**:

   - **Enterprise**: подготовка облачных компьютеров для Windows 365 Корпоративная.
   - **Frontline**: подготовка облачных компьютеров для Windows 365 Frontline. Чтобы создать политику подготовки для компьютеров Frontline Cloud, необходимо иметь Windows 365 Frontline лицензии. Если при выборе этого параметра у вас нет таких лицензий, отображается предупреждение.

4. Если выбран вариант **Frontline**, необходимо также выбрать **тип frontline**:

   - **Выделенный**. Подготовка облачных компьютеров в выделенном режиме.
   - **Общий** доступ. Подготовка облачных компьютеров в общем режиме.

5. На странице **Общие** выберите **тип соединения**:

   - **Microsoft Entra присоединение**: у вас есть два варианта **подключения к сети**:
     - **Размещенная сеть Майкрософт**. Выберите **географию** , в которой нужно подготовить облачные компьютеры. Затем для **параметра Регион** можно выбрать:

    - **Автоматический (рекомендуется)** (*не поддерживается для frontline в общем режиме*): служба Windows 365 автоматически выбирает регион в выбранном географическом регионе во время подготовки. Корпорация Майкрософт настоятельно рекомендует использовать параметр **Автоматически** . Такая автоматизация снижает вероятность сбоя подготовки.
    - Конкретный регион. Этот параметр гарантирует, что облачные компьютеры подготовлены только в выбранном вами регионе.
  - **Сетевое подключение Azure**. Выберите сетевое подключение Azure (ANC), используемое для этой политики.
- **Гибридное Microsoft Entra присоединение**. Необходимо выбрать ANC, который будет использоваться для этой политики.

Выбор ANC

Необходимо выбрать ANC для политики подготовки, если в предыдущем разделе вы выбрали один из следующих двух вариантов:

- **Тип** = соединения**Гибридное Microsoft Entra присоединение**
- **Тип** = соединения**Microsoft Entra присоединение исетевое** = **подключение Azure**

Чтобы выбрать ANC, выполните следующие действия.

1. На странице **Общие** для **сетевого подключения Azure** выберите один или несколько ACS. Дополнительные сведения об использовании нескольких АНК см. в разделе Альтернативные anCs.

2. Если выбрать несколько ANC, можно задать порядок приоритета для этих ANC. Для этого наведите указатель мыши на выделенный элемент ANC > и перетащите на три точки > , перетащите ANC в другую позицию в списке.

Пока первый ANC в списке является **работоспособным**, он всегда используется для подготовки облачных компьютеров с помощью этой политики. Если первый anc не работоспособен, политика использует следующий ANC в списке, который является работоспособным.

> ⓘ **Примечание**
>
> Для frontline в общем режиме ANC должен находиться в одном регионе.

Продолжить создание политики подготовки

1. На странице **Общие** можно проверка поле, чтобы пользователи **могли использовать Microsoft Entra единый вход**. Если вы хотите убедиться, что пользователи не получают запросы при каждом подключении к frontline на общем облачном компьютере, см. статью Скрыть диалоговое окно запроса на согласие.

2. Нажмите кнопку **Далее**.

3. На странице **Образ** для параметра **Тип образа** выберите один из следующих вариантов:

   - **Изображение коллекции**: выберите **Выбрать**> Выберите выберите изображение из коллекции >**Выбрать**. Образы из коллекции — это образы по умолчанию, предоставляемые для использования.
   - **Пользовательское изображение**. Выберите **Выбрать**> выберите изображение из списка >**Выбрать**. На странице отображается список изображений, отправленных с помощью рабочего процесса Добавление образов устройств .

4. Нажмите кнопку **Далее**.

5. На странице **Конфигурация** в разделе **Параметры Windows** выберите **Язык и регион**. Выбранный языковой пакет устанавливается на облачных компьютерах, подготовленных с помощью этой политики.

6. Необязательный параметр. Выберите **Применить шаблон имени устройства** , чтобы создать шаблон именования облачных компьютеров, который будет использоваться при именовании всех облачных компьютеров, подготовленных с помощью этой политики. Этот шаблон именования обновляет имя NETBIOS и не влияет на отображаемое имя облачного компьютера. При создании шаблона следуйте следующим правилам:

   - Выделенный режим enterprise и frontline
     - Имена должны содержать от 5 до 15 символов.
     - Имена могут содержать буквы, цифры и дефисы.
     - Имена не могут содержать пустые пробелы или символы подчеркивания.
     - Необязательный параметр. Используйте макрос %USERNAME:X%, чтобы добавить первые X-буквы имени пользователя.
     - Обязательно. Используйте макрос %RAND:Y% для добавления случайной строки символов, где Y равно количеству добавляемых символов. Значение Y должно быть 5 или больше. Имена должны содержать рандомизированную строку.
   - Frontline в общем режиме
     - Имена должны содержать ровно 15 символов.
     - Имена могут содержать буквы, цифры и дефисы.

    - Имена не могут содержать пустые пробелы или символы подчеркивания.
    - Префикс должен содержать не более 7 символов.
    - Обязательно. Используйте макрос %RAND:Y% для добавления случайной строки символов, где Y равно количеству добавляемых символов. Значение Y должно быть 8 или более. Имена должны содержать рандомизированную строку.

  Пример пользовательских шаблонов именования:

  - ABCDEF-%RAND:8%

7. Необязательный параметр. В разделе **Дополнительные службы** выберите службу для установки на облачных компьютерах, подготовленных с помощью этой политики:

   - Выделенный режим enterprise и frontline
     - **Автоматическое исправление Windows** — это облачная служба, которая автоматизирует обновления для Windows, Приложения Microsoft 365 для предприятий, Microsoft Edge и Microsoft Teams на физических и виртуальных устройствах. Дополнительные сведения см. в статье Что такое Автоисправление Windows? и Часто задаваемые вопросы об Автоисправлении Windows. Параметр Автозаставки Windows недоступен для frontline в общем режиме.
     - Если у вас уже настроено автоматическое исправление Windows для управления облачными компьютерами, этот параметр заменяет существующую политику. Эта замена может нарушить любое динамическое распределение, которое уже настроено в автопатруме.
     - Если выбран этот параметр, система назначает устройства новому кольцу в качестве последнего круга группы автозапачка.
     - Чтобы вручную включить динамическое распространение для облачных компьютеров, измените список динамического распространения Групп автозаполнения, чтобы включить группу Entra ID, в которую добавляются облачные компьютеры.
     - **Нет**. Управление облачными компьютерами и обновление их вручную.
   - Общий режим передней линии
     - **Windows Autopilot (предварительная версия)** — это облачная служба, которая обеспечивает установку приложений и сценариев Intune во время начальной регистрации и настройки. При необходимости выберите профиль подготовки устройства в списке.

8. Нажмите кнопку **Далее**.

9. На странице **Назначения** выберите **Выбрать группы**> выберите группы, которым нужно назначить > эту политику**.** Вложенные группы сейчас не поддерживаются.

10. Для Windows 365 Frontline выделенном режиме необходимо также выбрать размер облачного компьютера для каждой группы в политике. Выберите **Выбрать один**> выберите размер в разделе **Доступные**> размеры**Выбрать**. Выбрав размер для каждой группы, нажмите кнопку **Далее**.

11. Необязательно (в общедоступной предварительной версии). При необходимости можно создать назначение для резервирования лицензий для участников группы, выполнив следующие действия.
    a. В разделе **Назначение** введите **имя назначения**.
    b. В поле **Число лицензий** введите количество лицензий, которые нужно зарезервировать для группы. Вы также можете увидеть количество неназначенных лицензий.

12. Для Windows 365 Frontline в режиме общего доступа необходимо:
    a. Выберите **Выбрать один**> выберите размер в разделе **Доступные**> размеры**Выбрать**.
    b. Введите **понятное имя**>, выберите **номер**> облачного компьютера**Далее**. **Понятное имя** отображается в приложении windows конечного пользователя.

13. На странице **Проверка и создание** нажмите кнопку **Создать**. Если вы использовали Microsoft Entra гибридное соединение в качестве типа соединения, процесс создания политики может занять до 60 минут. Время зависит от того, когда в последний раз выполнялась синхронизация Microsoft Entra Connect.

После создания и назначения политики подготовки Windows 365 автоматически начнет подготовку облачных компьютеров.

Windows 365 Frontline в выделенном режиме

Microsoft Entra участники группы не получают облачные компьютеры, если число пользователей в группе пользователей Microsoft Entra превышает максимальное число облачных компьютеров, разрешенных для подготовки (в зависимости от количества приобретенных лицензий).

Администраторы могут подтвердить список участников, которые получили облачные компьютеры, **проверив политику**> подготовки, выбрав политику > проверки пользователей в **группах** в разделе Назначения.

Windows 365 Frontline лицензии предназначены как для облачных компьютеров Frontline в выделенном, так и в общем режиме. При добавлении лицензий облачные компьютеры

передней линии в выделенном режиме имеют приоритет над общим режимом.

Управление параллелизмом (общедоступная предварительная версия)

Если выбрать параметр для создания назначения, назначение определяет максимальное ограничение параллелизма для этой группы пользователей. После достижения ограничения параллелизма последующие пользователи не смогут войти в систему. Они должны ждать освобождения лицензий. Буфер параллелизма привязан к назначению и подсчитывается на основе количества лицензий назначения, а не общего числа лицензий. Сведения об использовании лицензий для разных назначений см. в отчете Подключенные облачные компьютеры frontline. Этот компонент находится в состоянии общедоступной предварительной версии.

Дальнейшие действия

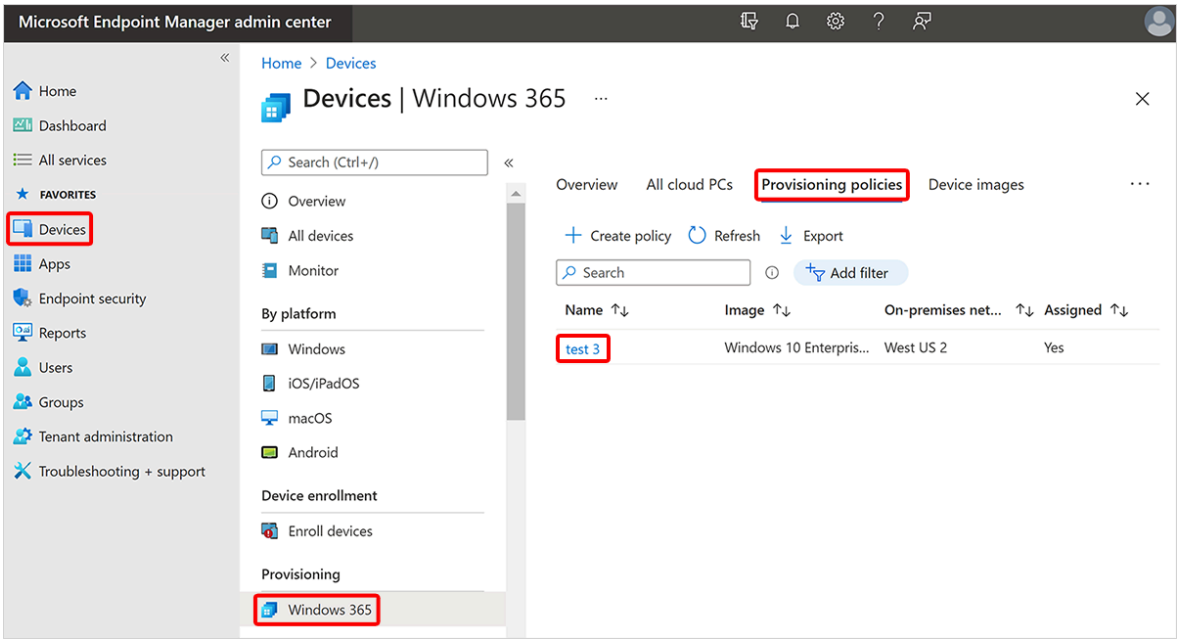
Изменение политики подготовки.

Изменение политик подготовки

Статья • 31.01.2025

Вы можете обновить политики подготовки, чтобы изменить назначения или ключевые атрибуты, такие как изображение и сетевое подключение.

1. Войдите в Центр администрирования Microsoft Intune, выберите **Устройства**>**Windows 365** (в разделе **Подготовка**) > Политики >**подготовки** выберите политику.



2. На странице политики вы можете изменить **общие** сведения, **образ** и **назначения**, выбрав **Изменить** рядом с каждым заголовком.

Если изменить конфигурацию сети, образа, региона или единого входа в политике подготовки, изменения для ранее подготовленных облачных компьютеров не произойдет. Недавно подготовленные или повторно подготовленные облачные компьютеры будут учитывать изменения в политике подготовки. Чтобы изменить сеть или образ ранее подготовленных облачных компьютеров в соответствии с изменениями, необходимо повторно подготовить эти облачные компьютеры. Чтобы изменить регион или единый вход ранее подготовленных облачных компьютеров в соответствии с изменениями, необходимо применить текущую конфигурацию.

Если изменить имя политики подготовки в разделе **Общие** сведения, произойдет следующее:

- На любом облачном компьютере в узле "Все облачные компьютеры" в столбце "политика подготовки" будет обновлено новое имя политики.

- Новые облачные компьютеры, созданные из политики подготовки, будут иметь новое имя, зарегистрированное как enrollmentProfileName устройства в Microsoft Entra ID и Microsoft Intune. Свойство enrollmentProfileName для существующих облачных компьютеров не изменится. Если вы выполнили шаги по созданию динамической группы устройств, содержащей все облачные компьютеры из определенной политики подготовки, измените динамическую группу устройств и добавьте новое правило, чтобы группа содержала как существующие облачные компьютеры, так и любые новые облачные компьютеры из политики подготовки:
  - **Свойство** = "enrollmentProfileName"
  - **Оператор** = "Equals"
  - **Value** = <Новое имя для политики подготовки>

Если вы назначите новым пользователям политику подготовки и у них есть действительная лицензия облачного компьютера, подготовка выполняется автоматически.

При удалении пользователей из назначения политики подготовки:

- Льготный период активируется для корпоративных облачных компьютеров.
- Облачные компьютеры передней линии в выделенном режиме немедленно отзываются.
- Облачные компьютеры передней линии в общем режиме остаются без изменений.

Применение текущей конфигурации для Enterprise и Frontline в выделенном режиме

Чтобы применить изменение конфигурации к существующим облачным компьютерам, выполните указанные действия.

1. Измените и сохраните изменения в существующей политике подготовки.
2. На странице политики выберите **Применить эту конфигурацию**.
3. Выберите изменение конфигурации для применения к существующим облачным компьютерам из списка доступных, включая:
   a. Область.
   b. Единый вход.
4. Нажмите Применить.

> ⓘ **Важно!**

- При применении нового региона облачные компьютеры завершаются во время процесса приложения для целевых облачных компьютеров. Пользователи отключены, и все несохраненные работы теряются.
- При применении единого входа облачные компьютеры, развернутые до апреля 2023 г., завершаются во время процесса приложения. Так как эта операция занимает некоторое время, применение единого входа к большому количеству облачных компьютеров может перезапустить виртуальные машины в течение длительного периода времени и не будет завершено немедленно.

Применение текущей конфигурации для frontline в общем режиме

Чтобы применить конфигурацию к существующим облачным компьютерам, выполните указанные действия.

1. Измените и сохраните изменения в существующей политике подготовки.
2. На странице политики выберите **Повторная подготовка**.
3. Выберите процент облачных компьютеров, которые необходимо убедиться в доступности для подключений пользователей.
4. Нажмите **Продолжить**.

> ⓘ **Важно!**
>
> При применении новой конфигурации облачные компьютеры завершаются во время процесса приложения. Пользователи не будут отключены, если используется облачный компьютер. Перед повторной подготовкой облачные компьютеры ожидают отключения пользователя.

Дальнейшие действия

Узнайте об этапах автоматической подготовки.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

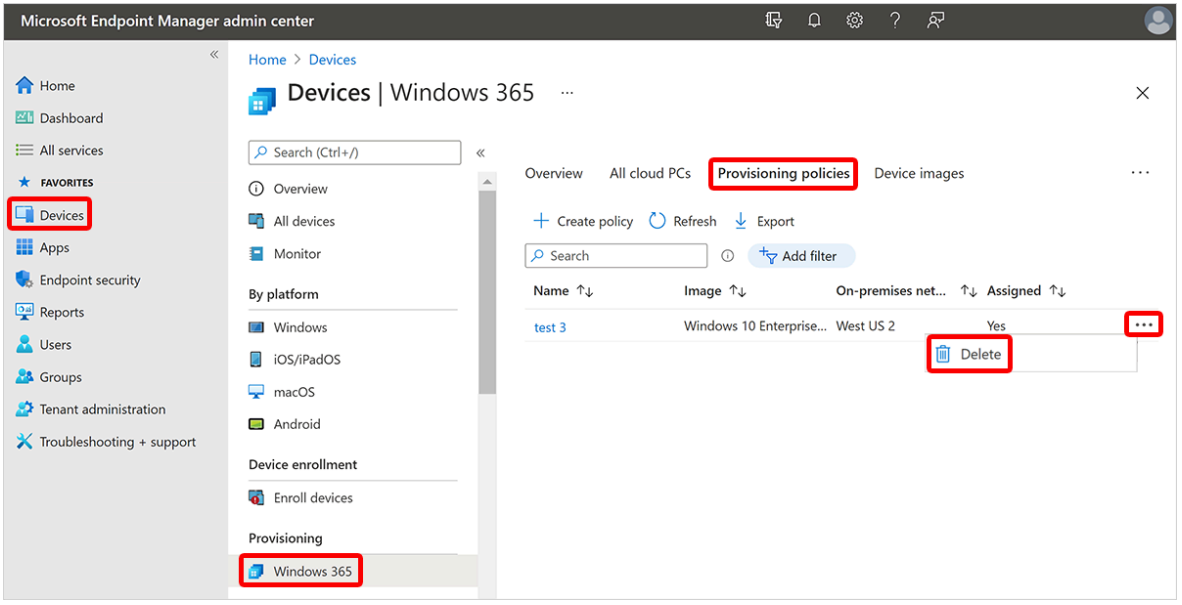
Отзыв о продукте

Удаление политик подготовки с облачных компьютеров

Статья • 31.01.2025

1. **Удалить можно только политику подготовки, которая не имеет назначений**. Поэтому сначала необходимо удалить назначения. Вы можете удалить назначения, выполнив действия, описанные в разделе Изменение политики подготовки. После выполнения этих действий выполните приведенные ниже действия, чтобы удалить политику подготовки.

2. Войдите в центр > администрирования Microsoft Intune**Windows 365**> (в разделе **Подготовка**) >**политики подготовки**.



3. Убедитесь, что **задано** значение **Нет**. Если **состояние Назначено** — **Да**, выберите политику подготовки и удалите назначения.

   Для Windows 365 Корпоративная и Windows 365 Frontline в выделенном режиме при удалении назначений облачные компьютеры перейдут в состояние льготного периода.

4. Выберите многоточие (...) рядом с политикой, которую нужно удалить >**Удалить**.

5. Выберите **Подтвердить** при запросе на удаление политики.

Дальнейшие действия

Дополнительные сведения о подготовке.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Этапы автоматической подготовки

Статья • 31.01.2025

Как администратор вы создаете политики подготовки и сетевые подключения Azure, чтобы настроить Windows 365 для подготовки облачных компьютеров. Используя эти сведения, Windows 365 подготавливает Облачные компьютеры для лицензированных пользователей. В этой статье описаны все этапы, которые автоматически выполняет Windows 365 в процессе подготовки.

Для подготовки Облачных компьютеров Windows 365 автоматически выполняет три этапа:

1. **Подготовка основных ресурсов**. Подготовка core выполняет все задачи, необходимые для того, чтобы настроить виртуальную машину и довести ее до точки успешного входа пользователя.
2. **Конфигурация после подготовки**: Windows 365 вносит изменения в конфигурацию для оптимизации взаимодействия с конечным пользователем облачного компьютера.
3. **Назначение**: Windows 365 назначает пользователя облачному компьютеру, и пользователь теперь может войти в систему.

Базовая подготовка

Windows 365 оптимизирует подготовку ядра только для выполнения необходимых действий, чтобы убедиться, что облачный компьютер успешно подготовлен.

1. **Выделение емкости Azure**. В начале подготовки Windows 365 выделяет емкость Azure в поддерживаемом регионе клиента. Клиентам не нужно управлять емкостью и выделением вручную.

2. **Создание виртуальной машины**: Windows 365 создает виртуальную машину на основе Windows 365 лицензии, назначенной пользователю. Каждая лицензия Windows 365 включает сведения о емкости оборудования. Виртуальная машина создается с этими спецификациями.

3. **Подключение виртуальной машины к соответствующей сети**. Когда Windows 365 создает виртуальную машину, также создается виртуальная сетевая карта. Если в политике подготовки указана сеть, размещенная в Майкрософт, NIC подключается к существующей или новой виртуальной сети в выбранном регионе специально для клиента. Если в политике подготовки указано сетевое подключение Azure, сетевая карта внедряется в предоставленную клиентами

виртуальную сеть. Этот шаг позволяет Облачному компьютеру подключаться к локальной сети клиентов.

4. **Присоединение к Microsoft Entra ID**. После запуска виртуальной машины устройство присоединяется Microsoft Entra ID одним из двух способов:

    - Через Microsoft Entra присоединения: устройство выполняет операцию Microsoft Entra соединения и не имеет Windows Server Active Directory зависимости.
    - Через Microsoft Entra гибридное присоединение: устройство выполняет операцию присоединения к домену в домене клиента, а затем регистрируется для Microsoft Entra ID с помощью синхронизации или федерации. На этом шаге мы дождемся появления объекта computer в Microsoft Entra ID, прежде чем продолжить.

5. **Intune регистрации MDM**. После того как объект Microsoft Entra ID будет доступен, облачный компьютер регистрируется в Intune. Для регистрации устройства не требуются учетные данные пользователя.

6. **Назначение основного пользователя**. Служба Windows 365 назначает пользователя облачного компьютера Intune основному пользователю, чтобы обеспечить бесперебойную работу сценариев самообслуживания и отчетов.

Конфигурация после подготовки

После базовой подготовки Windows 365 оптимизирует конфигурацию, чтобы обеспечить лучшее взаимодействие конечного пользователя с Облачным компьютером.

1. **Скрыть значки питания меню "Пуск"**: скрыть кнопку завершения работы в меню "Пуск" (`HKLM:\Software\Microsoft\PolicyManager\default\Start\HideShutDown\value`) и скрыть кнопку завершения работы на экране входа (`HKLM:\Software\Microsoft\Windows\CurrentVersion\Policies\System\ShutDownWithoutLogon`).

2. **Отключить действие сброса Windows**: reagentc.exe /disable

3. **Назначить пользователя администратором (при необходимости)**: `$Member = 'user@contoso.com' # use OnPremisesUserPrincipalName` `Add-LocalGroupMember -Group "Administrators" -Member $Member`

4. **Настройка режима Teams для VDI**: оптимизация размещенного рабочего стола (`HKLM:\Software\Microsoft\Teams\IsWVDEnvironment`).

5. **Включить перенаправление часовых поясов**: включите параметр (`HKLM:\Software\Policies\Microsoft\Windows NT\Terminal Services\fEnabletimezoneRedirection`).

6. **Изменить размер раздела диска ОС в соответствии с лицензией**: изменить размер диска операционной системы, чтобы он совпадал с размером управляемого диска Azure.

   $DriveLetter

   ```
   $MaxSize = (Get-PartitionSupportedSize -DriveLetter $DriveLetter -
   ErrorAction Stop).SizeMax
   if((Get-Partition -DriveLetter $DriveLetter).Size -lt $MaxSize){
   Resize-Partition -DriveLetter $DriveLetter -Size $MaxSize
   }```
   ```

7. **Отключить порт 3389 по умолчанию**: отключите входящий порт 3389, чтобы предотвратить кражу данных на домашний компьютер пользователя.

В отличие от основной подготовки, если одна или несколько из этих оптимизаций по какой-либо причине завершается сбоем, подготовка по-прежнему будет выполнена успешно. Облачный компьютер будет помечен как **успешный с предупреждениями** , и процесс перейдет на этап назначения.

Если оптимизация завершается сбоем, можно вручную активировать повторную подготовку, если вы хотите, чтобы конфигурация подготовки прошла успешно.

Отключен порт 3389

Чтобы защитить среду Windows 365, по умолчанию Windows 365 отключает открытый входящий порт 3389 на облачных компьютерах. Windows 365 не требуется открытый входящий порт. Если для устранения неполадок необходимо открыть порт 3389, лучше использовать JIT-доступ.

Задание

После завершения рабочих процессов настройки основной подготовки и после подготовки Windows 365 назначит соответствующего пользователя облачному компьютеру.

На этом этапе пользователь может войти в windows365.microsoft.com и получить доступ к своему облачному компьютеру.

Дальнейшие действия

Создайте динамическую группу устройств.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Управление облачными компьютерами Windows 365 с помощью диспетчера конфигураций

Статья • 31.01.2025

По умолчанию облачные компьютеры управляются с помощью Intune. Однако вы также можете управлять облачными компьютерами, используя совместное управление с диспетчером конфигураций. Чтобы использовать диспетчер конфигураций, установите клиент диспетчера конфигураций и включите совместное управление. Управление облачными компьютерами с помощью диспетчера конфигураций в основном совпадает с использованием Autopilot с совместным управлением.

Дополнительные сведения о совместном управлении и его настройке см. в статье Что такое совместное управление?

Требования

Для управления облачными компьютерами с помощью совместного управления диспетчера конфигураций необходимо выполнить следующие требования.

- Назначьте каждому пользователю облачного компьютера лицензию на облачный компьютер и лицензию на Intune. Подготовка облачного компьютера завершится сбоем, если у пользователя нет обеих лицензий. Страница состояния регистрации (ESP) также вызовет сбой.
- Включение совместного управления в диспетчере конфигураций
- Распространите установщик ccmsetup.msi как клиентское бизнес-приложение из Microsoft Intune. Дополнительные сведения см. в статье Как установить клиент диспетчера конфигураций.
- При развертывании Microsoft Entra гибридных облачных компьютеров: в Configuration Manager отключите автоматическую принудительную установку клиента на уровне сайта. Дополнительные сведения см. в статье Как развернуть клиенты на компьютерах с Windows в диспетчере конфигураций.

Для упрощения развертывания клиентского приложения можно создать группу Microsoft Entra на основе типа модели, с помощью фильтров или всех устройств профиля подготовки Windows 365. Дополнительные сведения см. в статье Создание динамической группы устройств с облачными компьютерами.

Рабочие нагрузки совместного управления для облачных компьютеров Windows 365

За несколькими исключениями облачными компьютерами можно управлять аналогично физическим компьютерам. Некоторые функции диспетчера конфигураций не применяются к облачным компьютерам, например OSD и PXE.

Путем переключения рабочих нагрузок администраторы могут контролировать, какая служба будет управлять конкретными областями Windows. Дополнительные сведения см. в статье Рабочие нагрузки совместного управления.

Если у вас много приложений для миграции в Microsoft Intune, рассмотрите возможность направления конечных пользователей в Корпоративный портал. В Корпоративном портале пользователи могут просматривать приложения, назначенные как из диспетчера конфигураций, так и из Microsoft Intune.

Дальнейшие действия

Дополнительные сведения о совместном управлении и его настройке см. в статье Что такое совместное управление?

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Использование страницы состояния регистрации на облачных компьютерах

Статья • 04.04.2025

Когда пользователь впервые входит на устройство, на странице состояния регистрации (ESP) отображается состояние подготовки Intune. Windows 365 поддерживает ESP, который обеспечивает общий интерфейс для пользователей, которые впервые входят на свои физические и облачные компьютеры. Полные сведения о ESP см. в разделе Настройка страницы состояния регистрации.

> ⓘ **Примечание**
>
> Подготовка устройства Autopilot (предварительная версия) для Windows 365 Frontline устройств в общем режиме и ESP несовместимы. Если включить подготовку устройств Autopilot для облачных компьютеров в политиках подготовки, ESP отключается.

Windows 365 и процесс ESP

При подготовке облачного компьютера служба Windows 365:

1. Создает облачный компьютер.
2. Регистрирует облачный компьютер в Intune.
3. Ожидает, пока пользователь впервые войдет на новый облачный компьютер.
    - Во время ожидания облачный компьютер:
        - Продолжает выполнять действие синхронизации для запроса политик Intune.
        - Выполняет фоновые действия, предназначенные для устройства.
4. После первого входа пользователя облачный компьютер выполняет установку и конфигурацию, предназначенные для пользователя.
    - Если ESP включен, пользователю отображается этап **настройки учетной записи** ESP. (Этап **настройки устройства** не поддерживается для облачных компьютеров. Это происходит только во время Autopilot в OOBE.)

Выбор профилей ESP в Windows 365

Windows 365 использует процесс регистрации без пользователя. Предварительная регистрация ресурсов, используемых в Autopilot, отсутствует. Так как профиль ESP задается во время регистрации, группирование и нацеливание чувствительны к времени. По этой причине использование динамических групп Microsoft Entra для целевого профиля ESP не поддерживается.

Существует два способа нацеливать профили ESP на облачные компьютеры:

- Профили ESP по умолчанию, предназначенные для встроенной виртуальной группы "**Все устройства** ".
- Настраиваемые профили ESP, предназначенные для встроенной виртуальной группы "**Все устройства**" и использующие фильтр на основе свойства **enrollmentProfileName (имя профиля регистрации).** Этот фильтр является единственным поддерживаемым типом фильтра для сценария назначения пользовательского профиля ESP. Дополнительные сведения см. в статье Создание фильтра для всех облачных компьютеров с помощью определенной политики подготовки.

Обе стратегии таргетинга поддерживаются для Microsoft Entra типов удостоверений гибридного присоединения и Microsoft Entra присоединения. Дополнительные сведения см. в разделе Типы соединения устройств.

Дальнейшие действия

Дополнительные сведения о странице состояния регистрации.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Использование автоматической подготовки устройств Autopilot с Windows 365 Frontline облачных компьютеров в общем режиме (предварительная версия)

13.09.2025

При подготовке облачных компьютеров можно при необходимости связать подготовку устройства Autopilot, чтобы обеспечить подготовку Windows 365 Frontline облачных компьютеров в общем режиме с помощью важных приложений и сценариев Intune.

Этот компонент находится в состоянии общедоступной предварительной версии.

Связывание политик подготовки устройств с облачными компьютерами

1. Соответствие требованиям к подготовке устройств Windows Autopilot.

2. При создании илиизменении существующей политики подготовки Windows 365 также выполните следующие действия.
   a. На вкладке **Конфигурация** для **политики подготовки устройств Autopilot** выберите политику.
   b. В **поле За минуты, разрешенные до сбоя подготовки устройства**, введите значение, позволяющее установить приложения и скрипты, определенные в политике. Если к этому времени установка приложений и сценариев еще не завершена, подготовка устройства завершается сбоем (но подготовка продолжается).
   c. При необходимости можно выбрать **параметр Запретить подключение пользователей к облачному компьютеру при сбое установки или истечении времени ожидания** , чтобы принудить результат подготовки к **ошибке** в случае истечения времени ожидания или сбоя. Если этот параметр выбран, облачные компьютеры, на которых не удалось завершить установку политики подготовки устройства, помечаются как **Сбой**. В этом случае пользователи не могут подключиться к ним. Если этот параметр не выбран, облачные компьютеры помечаются как **подготовленные с предупреждениями** , и пользователи могут подключаться к своим облачным компьютерам.

3. Выполните оставшиеся действия, чтобы создать илиизменить существующую политику подготовки Windows 365.

Windows 365 завершает процесс подготовки после:

- Приложения и скрипты успешно установлены.
- Время ожидания истекает.

> **Примечание**
>
> Windows 365 поддерживает как присоединение к Entra, так и гибридное присоединение к Entra во время подготовки. Подготовка устройств может использоваться в политиках подготовки с включенными этими функциями.

Мониторинг состояния подготовки устройства на облачных компьютерах

Чтобы просмотреть состояние подготовки устройства к подготовке облачных **компьютеров**, перейдите в раздел Мониторингрегистрации устройств >>>**Windows Autopilot состояние развертывания подготовки устройств**.

Известные ограничения

Для Windows 365 политик подготовки с типом интерфейса Cloud App (предварительная версия) можно связать политику подготовки устройств Autopilot, но вы не сможете публиковать приложения Intune как облачные приложения.

Дальнейшие действия

Узнайте больше о подготовке устройства Windows Autopilot.

Создание динамической группы устройств с вашими облачными ПК

Статья • 31.01.2025

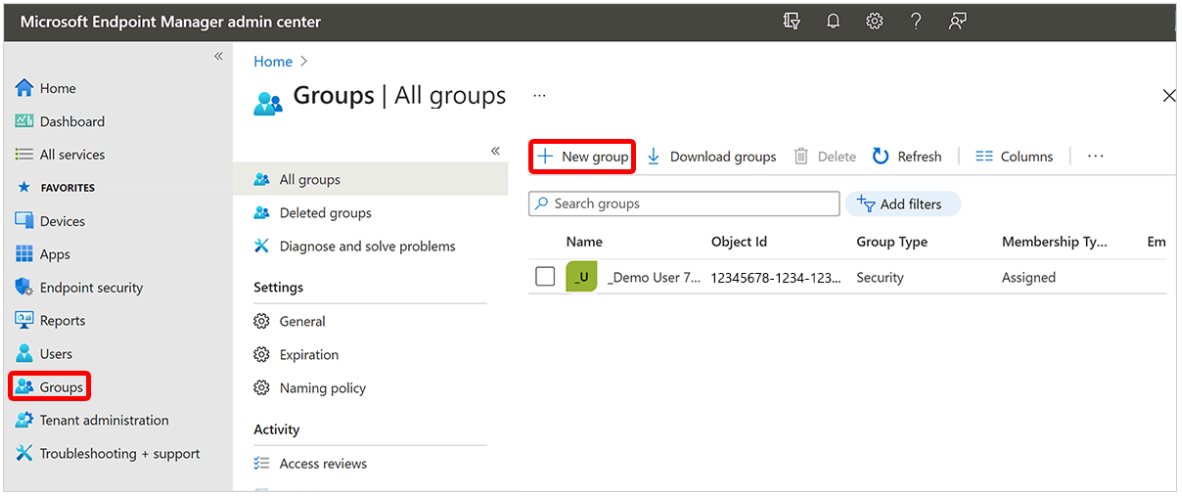
Вы можете создать динамическую группу устройств с вашими облачными ПК. Политики, нацеленные на эту группу устройств, нацелены на все или некоторые облачные компьютеры, в зависимости от настроенных правил. Существуют три различных категории групп, которые можно создать для облачных компьютеров:

- Все облачные компьютеры. Этот тип группы полезен для применения политик и конфигураций ко всем облачным компьютерам в организации.
- Все облачные компьютеры из определенной политики подготовки. Этот тип группы полезен для применения политик и конфигураций к облачным компьютерам на основе одного и того же образа и расположения.
- Все облачные компьютеры с определенной конфигурацией. Этот тип группы полезен для применения политик и конфигураций к облачным компьютерам на основе вычислительной мощности (виртуальный ЦП и ОЗУ) или внутренней памяти.

Создание динамической группы устройств для всех Облачных компьютеров

На этих этапах для создания динамической группы устройств используется свойство устройство "Модель устройства".

1. Войдите в Центр >администрирования Microsoft Intune Группы >**Новая группа**.



2. Выберите **Безопасность** в **поле Тип группы**.
3. Введите следующие сведения.

a. **Имя группы** = "Все Облачные компьютеры" (или другое имя, указывающее на то, что группа будет содержать все Облачные компьютеры).
b. **Описание группы** = "Динамическая группа устройств, содержащая все Облачные компьютеры".

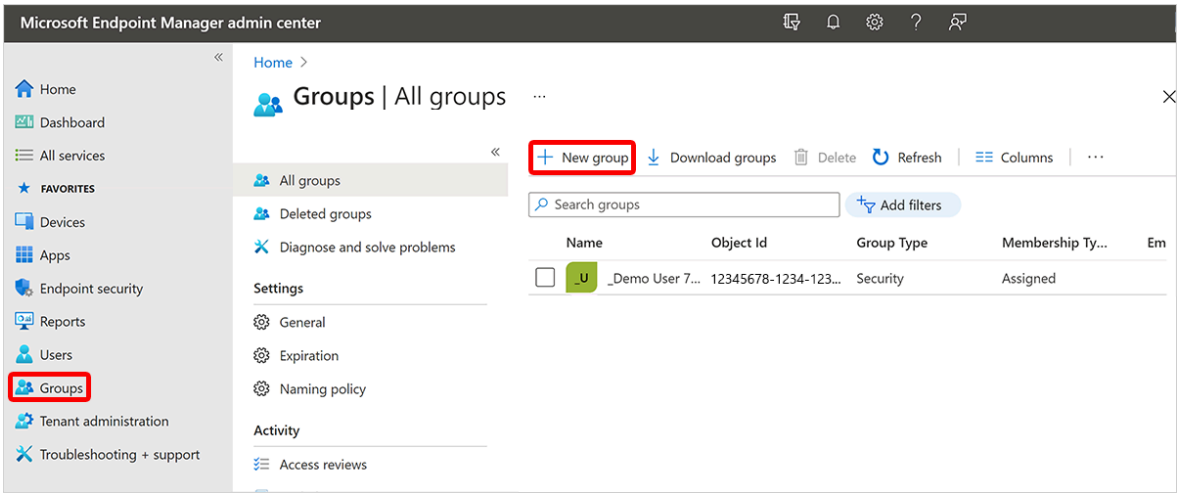
4. В качестве **типа членства** выберите **Динамическое устройство**.
5. Выберите **Добавить динамический запрос**.
6. На странице **Правила членства в динамической группе** введите следующее:
   a. **Свойство** = "deviceModel"
   b. **Оператор** = "Начинается с"
   c. **Значение** = "Облачный компьютер"
7. Чтобы убедиться, что это работает, выберите **Проверить правила (предварительная версия)**>**+Добавить устройства**>, выберите некоторые облачные компьютеры и устройства, отличные от облачных компьютеров.
8. После завершения проверки выберите **Сохранить**>**Создать**.

Создание динамической группы устройств для всех облачных компьютеров из определенной политики подготовки

В приведенном ниже примере в качестве имени политики подготовки указано "UX Engineering" (Проектирование пользовательского опыта). Заменяйте имя "UX Engineering" именем вашей политики подготовки.

На этих этапах для создания динамической группы устройств используется свойство "Имя профиля регистрации".

1. Войдите в Центр >администрирования Microsoft Intune Группы >**Новая группа**.



2. Выберите **Безопасность** в **поле Тип группы**.
3. Введите следующие сведения.

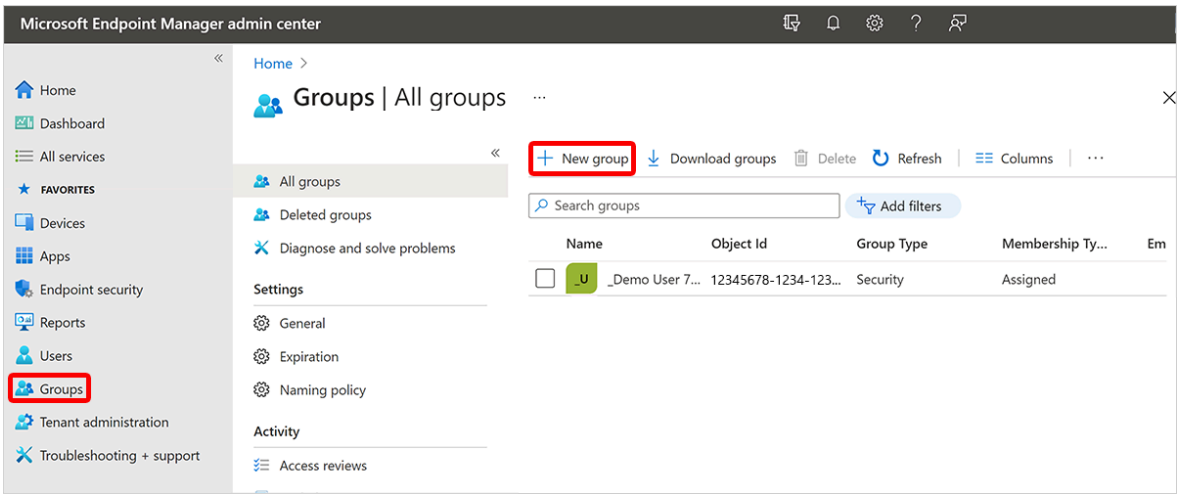
   a. **Имя группы** = "Все Облачные компьютеры UX Engineering"
   b. **Описание группы** = "Динамическая группа устройств, содержащая все Облачные компьютеры UX Engineering".
4. В качестве **типа членства** выберите **Динамическое устройство**.
5. Выберите **Добавить динамический запрос**.
6. На странице **Правила членства в динамической группе** введите следующее:
   a. **Свойство** = "enrollmentProfileName"
   b. **Оператор** = "Equals"
   c. **Значение** = "UX Engineering"
7. Чтобы убедиться, что это работает, выберите **Проверить правила (предварительная версия)**>**Добавить устройства**> . Выберите некоторые облачные компьютеры, которые были подготовлены из политики подготовки "Разработка пользовательского интерфейса", некоторые облачные компьютеры, подготовленные из другой политики подготовки, и некоторые необлачные компьютеры.
8. После завершения проверки выберите **Сохранить**>**Создать**.

Создание динамической группы устройств для всех облачных компьютеров с определенной конфигурацией

В приведенном ниже примере в качестве конфигурации используется 2 виртуальных ЦП и 4 ГБ ОЗУ. Во всех случаях вместо "2 виртуальных ЦП/4 ГБ" укажите требуемые значения. Вы также можете ориентироваться на конкретный размер облачного компьютера, добавив хранилище ОС в составе конфигурации. Вы можете выполнить следующие шаги и создать фильтр для любой из конфигураций, составляющих размеры облачных компьютеров.

На этих этапах для создания динамической группы устройств используется свойство устройства "Модель устройства".

1. Войдите в Центр >администрирования Microsoft Intune Группы >**Новая группа**.



2. Выберите **Безопасность** в **поле Тип группы**.
3. Введите следующие сведения.
   a. **Имя группы** — "Все Облачные компьютеры с 2 виртуальными ЦП и 4 ГБ ОЗУ".
   b. **Описание группы** — "Динамическая группа устройств, содержащая все Облачные компьютеры с 2 виртуальными ЦП и 4 ГБ ОЗУ".
4. В разделе **Тип членства** выберите **Динамическое устройство**.
5. Выберите **Добавить динамический запрос**.
6. На странице **Правила членства в динамической группе** введите следующее:
   a. **Свойство** — deviceModel.
   b. **Оператор** = "Начинается с"
   c. **Значение** — "Cloud PC".
7. Выберите **Добавить выражение** и введите следующее:
   a. **Свойство** — deviceModel.
   b. **Оператор** — Contains.
   c. **Значение** — 2 виртуальных ЦП и 4 ГБ ОЗУ.
8. Чтобы убедиться, что это работает, выберите **Проверить правила (предварительная версия)**>**Добавить устройства**> . Выберите некоторые облачные компьютеры с конфигурацией ОЗУ 2vCPU/4 ГБ, некоторые облачные компьютеры с другой конфигурацией и некоторые устройства, отличные от облачных компьютеров.
9. После завершения проверки выберите **Сохранить**>**Создать**.

Дальнейшие действия

Создание фильтра.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Создание фильтра для облачных компьютеров

Статья • 31.01.2025

Можно создать фильтр, который можно использовать при создании политик и конфигураций Intune. Создаваемый вами фильтр может быть настроен для всех или некоторых облачных компьютеров, в зависимости от настроенных правил. Вы также можете использовать созданный вами фильтр, чтобы исключить облачные компьютеры из существующих политик, предназначенных только для физических устройств. Существуют три различных категории фильтров, которые можно создать для облачных компьютеров:

- Все облачные компьютеры. Этот тип фильтра полезен для применения политик и конфигураций ко всем облачным компьютерам в организации.
- Все облачные компьютеры из определенной политики подготовки. Этот тип фильтра полезен для применения политик и конфигураций к облачным компьютерам на основе одного и того же образа и расположения.
- Все облачные компьютеры с определенной конфигурацией. Этот тип фильтра полезен для применения политик и конфигураций к облачным компьютерам на основе вычислительной мощности (виртуальный ЦП и ОЗУ) или внутренней памяти.

Создание фильтра для всех облачных компьютеров

На этих этапах для создания фильтра используется свойство "Модель устройства".

1. Войдите в центр >администрирования Microsoft Intune администрирования >**клиентаФильтры управляемых**>**устройств**.
2. Выберите **Создать**, а затем введите следующее:
   a. **Имя фильтра** = "Все облачные компьютеры" (или другое имя, указывающее на то, что оно будет содержать все облачные компьютеры)
   b. **Описание** = "Фильтр, содержащий все устройства облачного компьютера"
   c. **Платформа** = "Windows 10 и более поздние версии"
3. На странице **Правила** введите следующее:
   a. **Свойство** = "model (модель)"
   b. **Оператор** = "Contains"
   c. **Value** = "Cloud PC". Чтобы создать фильтр для всех облачных компьютеров GPU, выберите "GPU". Чтобы создать фильтр для облачных компьютеров

frontline, выберите "Облачный компьютер Frontline".

4. Чтобы убедиться, что он работает, выберите **Предварительный просмотр**.
5. На странице **Теги области** выберите нужные теги области для применения, а затем выберите **Далее**.
6. На странице **Проверка и создание** нажмите кнопку **Создать**.

Создание фильтра для всех облачных компьютеров из определенной политики подготовки

В приведенном ниже примере в качестве имени политики подготовки указано "UX Engineering" (Проектирование пользовательского опыта). Заменяйте имя "UX Engineering" именем вашей политики подготовки.

На этих этапах для создания фильтра используется свойство "Имя профиля регистрации" и "Модель устройства".

1. Войдите в Microsoft Intune Центр >**администрирования**> клиентов**Фильтры**.
2. Выберите **Создать**, а затем введите следующее:
   a. **Имя фильтра** = "Все устройства облачного компьютера с проектированием UX"
   b. **Описание** = "Фильтр, содержащий все устройства облачного компьютера с проектированием UX"
   c. **Платформа** = "Windows 10 и более поздние версии"
   d. Нажмите кнопку **Далее**.
3. На странице **Правила** введите следующее:
   a. **Свойство** = "enrollmentProfileName (имя профиля регистрации)"
   b. **Оператор** = "Equals"
   c. **Значение** = "UX Engineering"
4. Чтобы убедиться, что он работает, выберите **Предварительный просмотр**.
5. На странице **Теги области** выберите нужные теги области для применения, а затем выберите **Далее**.
6. На странице **Проверка и создание** нажмите кнопку **Создать**.

Создание фильтра для всех облачных компьютеров с определенной конфигурацией

В приведенном ниже примере в качестве конфигурации используется 2 виртуальных ЦП и 4 ГБ ОЗУ. Во всех случаях вместо "2 виртуальных ЦП/4 ГБ" укажите требуемые значения. Вы также можете ориентироваться на конкретный размер облачного компьютера, добавив хранилище ОС в составе конфигурации. Вы можете выполнить следующие шаги и создать фильтр для любой из конфигураций, составляющих размеры облачных компьютеров.

На этих этапах для создания фильтра используется свойство "Модель устройства".

1. Войдите в Microsoft Intune Центр >**администрирования**> клиентов**Фильтры**.
2. Выберите **Создать**>**управляемые устройства**, а затем введите следующее:
   a. **Имя фильтра** = "Все облачные компьютеры 2 виртуальными ЦП и 4 ГБ ОЗУ."
   b. **Описание** = "Фильтр, содержащий все облачные компьютеры с конфигурацией 2 виртуальных ЦП и 4 ГБ ОЗУ"
   c. **Платформа** = "Windows 10 и более поздние версии"
   d. Нажмите кнопку **Далее**.
3. На странице **Правила** введите следующее:
   a. **Свойство** = "model (модель)"
   b. **Оператор** = "Contains"
   c. **Значение** — "2 виртуальных ЦП и 4 ГБ ОЗУ"
4. Чтобы убедиться, что он работает, выберите **Предварительный просмотр**.
5. На странице **Теги области** выберите нужные теги области для применения, а затем выберите **Далее**.
6. На странице **Проверка и создание** нажмите кнопку **Создать**.

После создания фильтра его можно использовать на странице назначения в поддерживаемых политиках.

Дополнительные сведения об использовании фильтров в Intune см. в следующих руководствах.

- Создание фильтра (руководство по Intune)
- Поддерживаемые свойства фильтра
- Фильтрация и устранение неполадок с созданием отчетов

Дальнейшие действия

Создание профиля конфигурации устройств.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Создание профиля конфигураций устройств

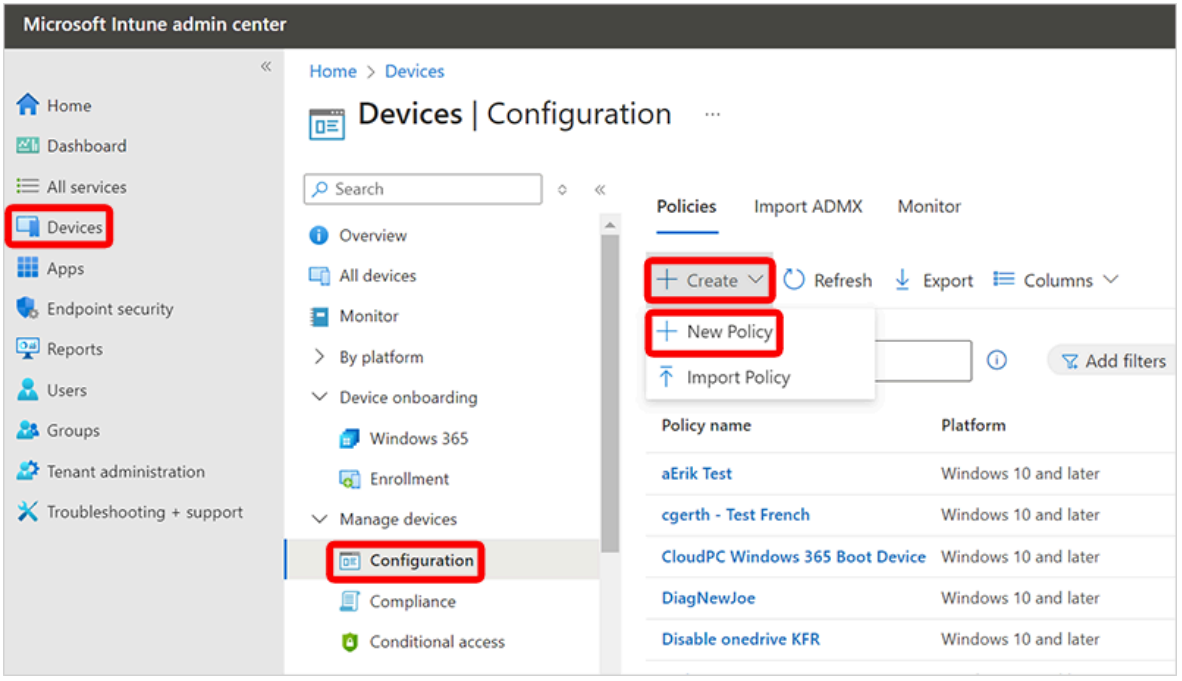
Статья • 31.01.2025

В этом примере мы примем профиль конфигурации устройства**с ограничениями устройств** и применим его ко **всем облачным компьютерам**. Для выполнения этой задачи потребуется динамическая группа устройств или фильтр.

> **Примечание**
>
> Если вы еще этого не сделали, выполните шаги по **созданию динамической группы устройств, содержащей все облачные компьютеры**, или **создайте фильтр для всех облачных компьютеров**, а затем вернитесь сюда, чтобы создать профиль конфигурации устройства.

Теперь, после создания динамической группы устройств или фильтра для всех облачных компьютеров, можно настроить политики для применения ко всем облачным компьютерам в клиенте. Для этого выполните указанные ниже действия.

1. Войдите в**конфигурациюустройств**>центра > администрирования Microsoft Intune (в разделе **Управление устройствами**) >**Создание**>**политики**.



2. В разделе **Создание профиля** выберите **Windows 10 и более поздних версий** для **параметра Платформа**, **Шаблоны** для **типа профиля**, а затем **Ограничения устройств**.

3. Нажмите **Создать**.

4. Введите **Имя** политики, например "Все облачные компьютеры — ограничения устройств", и полезное **Описание**.

5. Нажмите кнопку **Далее**.

6. На странице **Параметры конфигурации** выберите параметры и ограничения, которые необходимо применить к этому профилю.

7. Нажмите кнопку **Далее**.

8. На странице **Теги области** выберите нужные теги области для применения, а затем выберите **Далее**.

9. На странице **Назначения** выберите следующие параметры в зависимости от того, используете ли вы динамическую группу устройств или фильтр:

   а. **Динамическая группа устройств**. Выберите **Добавить группы**> . Найдите и выберите динамическую группу устройств для всех облачных компьютеров >**Выберите**.

   Б. **Фильтр**. Выберите существующую группу пользователей, **изменить фильтр**>**Включить отфильтрованные устройства в поиск назначения**> и выберите фильтр для всех облачных компьютеров.

   с. **Фильтр**. Выберите **Добавить все устройства** или **Добавить всех пользователей**, **Изменить фильтр**>**Включить отфильтрованные устройства в назначение**> и выберите фильтр для всех облачных компьютеров.

10. Выберите **Выбрать**>**Далее**.

11. На странице **Правила применимости** выберите **Далее**.

12. На странице **Проверка и создание** проверьте параметры. Вы увидите все выбранные вами параметры вместе с назначением "Все облачные компьютеры".

13. Выберите **Создать** для развертывания профиля.

Дальнейшие действия

Назначение пользователя в качестве локального администратора.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Конфигурации облачных компьютеров (предварительная версия)

Конфигурации облачных компьютеров включают в себя параметры, влияющие на облачные компьютеры, в частности, для конфигураций, которые можно включить или отключить после первоначальной подготовки. Конфигурации облачных компьютеров поддерживают нацеливание на группы пользователей.

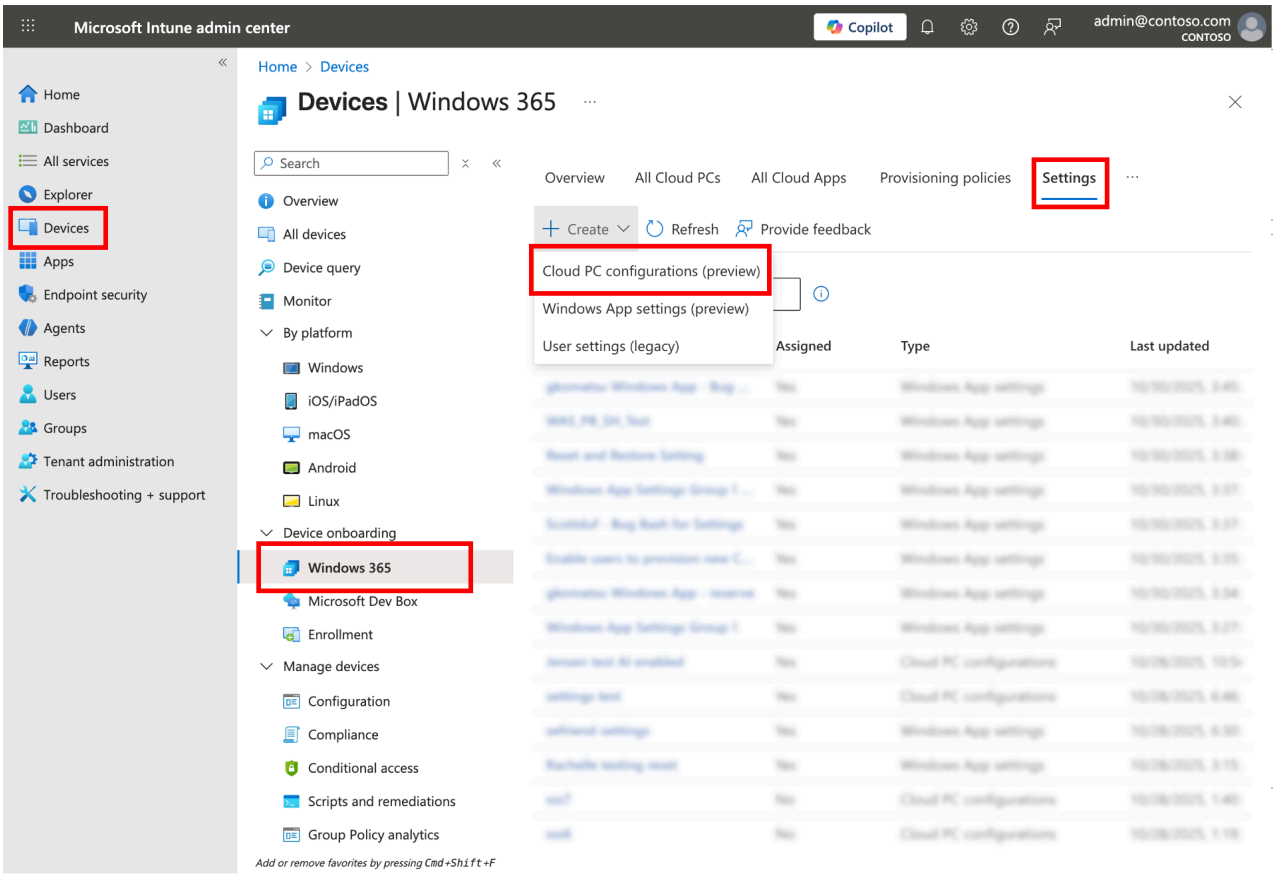
На странице **Конфигурации облачных компьютеров** ИТ-администраторы могут управлять следующими параметрами для пользователя:

- **Функции с поддержкой ИИ:** Будет установлена гибридная платформа вычислений, позволяющая устройству конечного пользователя использовать функции с поддержкой ИИ.

  (Примечание. Применимо только к устройствам со спецификациями 8vCPU/32 ГБ/256 ГБ и выше.)

Добавление нового параметра

1. Войдите в Центр администрирования Microsoft Intune, выберите **Устройства**>**Windows 365** (в разделе **Подключение устройств).**>>**Параметры.**
2. Щелкните **Создать** и выберите **Конфигурации облачных компьютеров** в раскрывающемся списке.
3. Введите **имя** параметра и добавьте **описание** (необязательно).
4. На вкладке **Параметры конфигурации** выберите **Включить** или **Отключить** для любого из параметров, которые вы хотите настроить. "Не настроено" означает, что этот параметр не задан.
5. Добавьте **все теги области,** которые вы хотите настроить. Дополнительные сведения о тегах область см. здесь.
6. В разделе **Назначения** выберите **Добавить группы**.
7. В разделе **Выберите группы для включения** выберите группу пользователей, чтобы получить параметры >**Выбрать**.
8. Нажмите кнопку **Далее**.
9. На странице **Проверка и сохранение** нажмите кнопку **Создать**.



Изменение параметра

1. Войдите в Центр администрирования Microsoft Intune, выберите **Устройства**>**Windows 365** (в разделе **Подключение устройств).**>>**Параметры**. На странице **Параметры** отображаются текущие параметры.

2. Выберите политику **конфигураций облачных компьютеров** , которую вы хотите изменить.

3. Чтобы изменить имя политики или включить или отключить параметры, нажмите кнопку **Изменить** рядом с **элементом Параметры**.

4. В разделе **Параметры** внесите необходимые изменения и нажмите кнопку **Далее**.

5. На странице **Проверка и сохранение** выберите **Обновить**.

6. Чтобы изменить назначения, нажмите **кнопку Изменить** рядом с пунктом **Назначения**>**Добавить группы** , чтобы добавить другую группу. Чтобы удалить существующие группы, выберите многоточие (...) >**Удалить**.

7. Нажмите кнопку **Далее**.

8. На странице **Проверка и сохранение** выберите **Обновить**.

Удаление параметра

1. Войдите в Центр администрирования Microsoft Intune, выберите **Устройства**>**Windows 365** (в разделе **Подключение устройств).**>>**Параметры**.
2. На странице **Параметры** можно просмотреть созданные параметры.
3. Выберите многоточие (**...**) в строке параметра, который требуется удалить >**Удалить**.
4. Нажмите кнопку **Да** во всплывающем окне подтверждения, чтобы навсегда удалить параметр.

Last updated on 19.11.2025

Управление функциями с поддержкой ИИ (Frontier Preview)

Введение

В этой статье объясняется, как настроить, проверить функции с поддержкой ИИ и управлять ими на облачном компьютере. Дополнительные сведения о облачных компьютерах с поддержкой ИИ, включая минимальные требования, которые должны быть выполнены перед выполнением инструкций в этой статье, см. в статье Облачный компьютер с поддержкой ИИ (Frontier Preview) | Microsoft Learn.

Назначение поддержки ИИ облачным компьютерам в Intune

После регистрации пользователей в программе предварительной оценки Windows вы можете назначить включение ИИ облачным компьютерам в Intune, чтобы получить связанные функции.

Чтобы назначить включение ИИ облачным компьютерам, выполните приведенные далее действия.

1. В Intune перейдите на вкладку **Устройства**.
2. В разделе **Подключение устройств** перейдите на страницу Windows 365.
3. Выберите вкладку **Параметры**.
4. Нажмите кнопку **Создать**.
5. Выберите параметр **Конфигурации облачных компьютеров** в раскрывающемся списке.
6. Добавьте **имя** и **описание** (необязательно).
7. На вкладке **Параметры конфигурации** выберите **Включить** для параметра **функций с поддержкой ИИ** .
8. Следуйте инструкциям на экране, пока не перейдете на вкладку **Назначения** .
9. Выбирает целевые группы пользователей. (Помните, что их устройства должны соответствовать всем спецификациям облачных компьютеров.)
10. Перейдите на вкладку **Рецензирование и создание** и нажмите кнопку **Создать**.
11. Подождите до 48 часов, пока процессы включения ИИ завершаются на целевых облачных компьютерах.
12. На облачном компьютере выберите **Проверить наличие обновлений**, установить ожидающие обновления и перезагрузить облачный компьютер. Повторите этот шаг (продолжайте проверку и установку обновлений и при необходимости выполняйте

перезагрузку), пока не будет отложенных обновлений. Может потребоваться повторить этот процесс 3–5 раз.

Инструкции по настройке программы предварительной оценки Windows для облачных компьютеров

После получения прав на включение ИИ облачные компьютеры должны быть зарегистрированы в программе предварительной оценки Windows и получить последнюю сборку канала бета-версии (**сборка ОС 26120.6682 или более поздней версии**), чтобы получить поддерживаемые функции с поддержкой ИИ. Если вы настраиваете отдельный облачный компьютер (вместо нескольких одновременно), перейдите к этому подразделу.

> ⓘ **Внимание**
>
> Необходимо зарегистрировать пользователей в программе предварительной оценки Windows, чтобы обеспечить работу поддерживаемых функций ИИ. Если вам не удается выполнить инструкции в этом разделе, см. **статью Управление предварительными сборками в организации — программа предварительной оценки Windows | Microsoft Learn**.

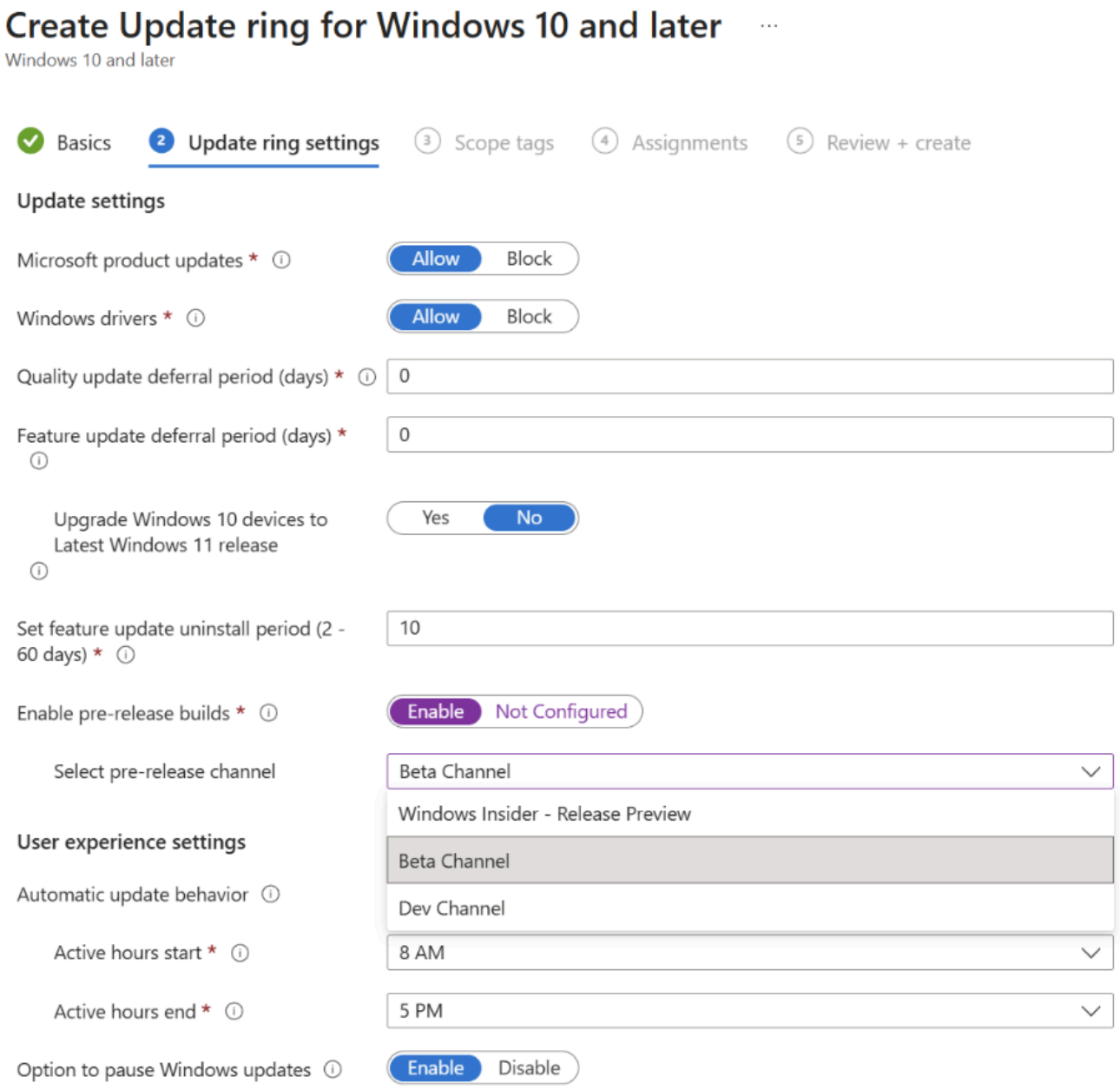
Инструкции по настройке массовой регистрации облачных компьютеров с помощью Intune

Ниже приведены пошаговые инструкции по настройке конечных точек для регистрации конечных точек в программе предварительной оценки Windows в большом масштабе с помощью Intune. Если включены предварительные сборки и выбран канал бета-версии:

1. Войдите в Центр администрирования Microsoft Intune.
2. **Перейдите к:** Устройства > с кругами Центра обновления Windows > для Windows 10 и более поздних версий
3. **Создайте или измените политику круга обновлений**:
   a. Щелкните + **Создать профиль** или выберите существующую политику для изменения.
4. **Настройка сборок программы предварительной оценки**.
   a. Изменение **параметров круга обновления**.
   b. Задайте для **включения предварительных сборок** значение **Включить**.

c. В разделе **Выбор параметра канала предварительной версии выберите Канал бета-версии** в раскрывающемся меню.

5. В разделе **Назначения** выберите группы, содержащие устройства, которые требуется зарегистрировать.



Дополнительные сведения см. в статье Управление предварительными сборками в организации — программа предварительной оценки Windows | Microsoft Learn.

Инструкции по настройке отдельного облачного компьютера (через Windows Обновления)

Если вы хотите настроить отдельное устройство в программе предварительной оценки Windows, вы можете перейти на страницу параметров windows Обновления на облачном компьютере, а не через Intune (описано в разделе Intune). Чтобы выполнить регистрацию

участников программы предварительной оценки Windows на одном устройстве, выполните приведенные далее действия.

1. На облачном компьютере откройте приложение **Параметры** и перейдите на страницу **Windows Обновления**.
2. Выберите раздел **Программа предварительной оценки Windows** и выберите **Начало работы**.
3. Следуйте инструкциям, чтобы войти в учетную запись пользователя, связанную с программой предварительной оценки Windows.
4. Зарегистрируйтесь в **канале бета-версии** , чтобы получить последние возможности облачного компьютера с поддержкой ИИ.
5. Выберите **Проверить наличие обновлений**, установить ожидающие обновления и перезагрузить облачный компьютер. Повторите этот шаг (продолжайте проверять и устанавливать обновления, а также выполнять перезагрузку), пока не будет отложенных обновлений. Может потребоваться повторить этот процесс 3–5 раз. Дополнительные сведения см. в статье Управление предварительными сборками в организации — программа предварительной оценки Windows | Microsoft Learn.

> ⓘ **Внимание**
>
> Если указанные выше параметры программы предварительной оценки Windows **недоступны** , можно задать раздел реестра, чтобы сделать их видимыми. Для этого действия потребуются права администратора.

Инструкции по разделу реестра (требуются права администратора)

1. Откройте приложение **Редактор реестра** .
2. Перейдите к **Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsSelfHost\UI\Visibility**
3. Создайте **DWORD** с именем **HideInsiderPage** и **значением 0**.
4. Перезапустите облачный компьютер, чтобы новый раздел реестра вступил в силу.

Проверка состояния облачного компьютера с поддержкой ИИ в Intune

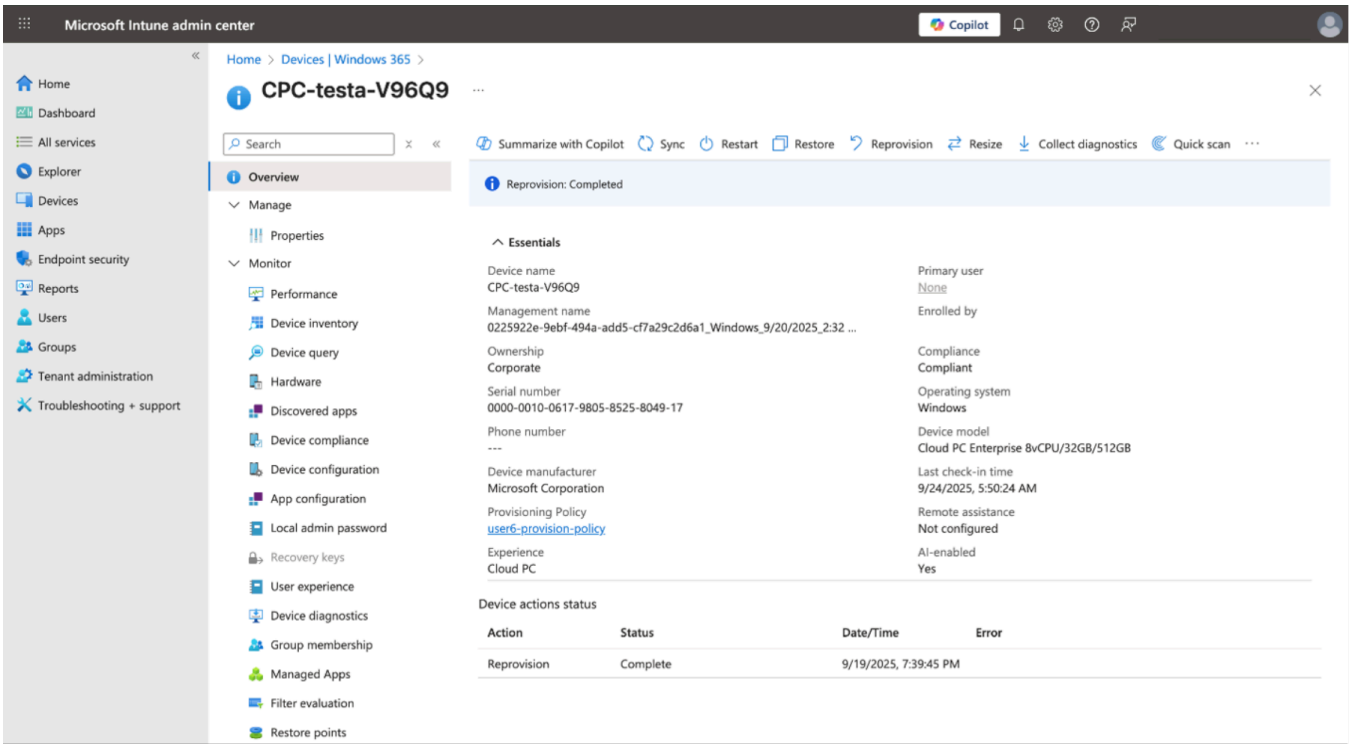
После того как облачным компьютерам будет назначено право с поддержкой ИИ и они зарегистрированы в канале предварительной оценки Windows Beta, для использования

связанных функций может потребоваться до **48 часов** , так как фоновые процессы должны быть полностью настроены, прежде чем будут доступны функции. Через 48 часов **проверка для любых дополнительных Обновления Windows иперезагрузите облачный компьютер (и повторите это, пока не будет ожидающих обновлений).** Скорее всего, вам потребуется повторить проверку и применить обновления 3–5 раз.

После этого ИТ-администраторы могут проверка, поддерживает ли облачный компьютер ИИ, на вкладке Основные компоненты страницы устройства Intune или просмотреть общее состояние клиента на странице Отчеты.

Проверка состояния облачного компьютера с поддержкой ИИ на странице устройства Intune

На вкладке Основные сведения на странице "Обзор" устройства есть поле "С поддержкой ИИ".

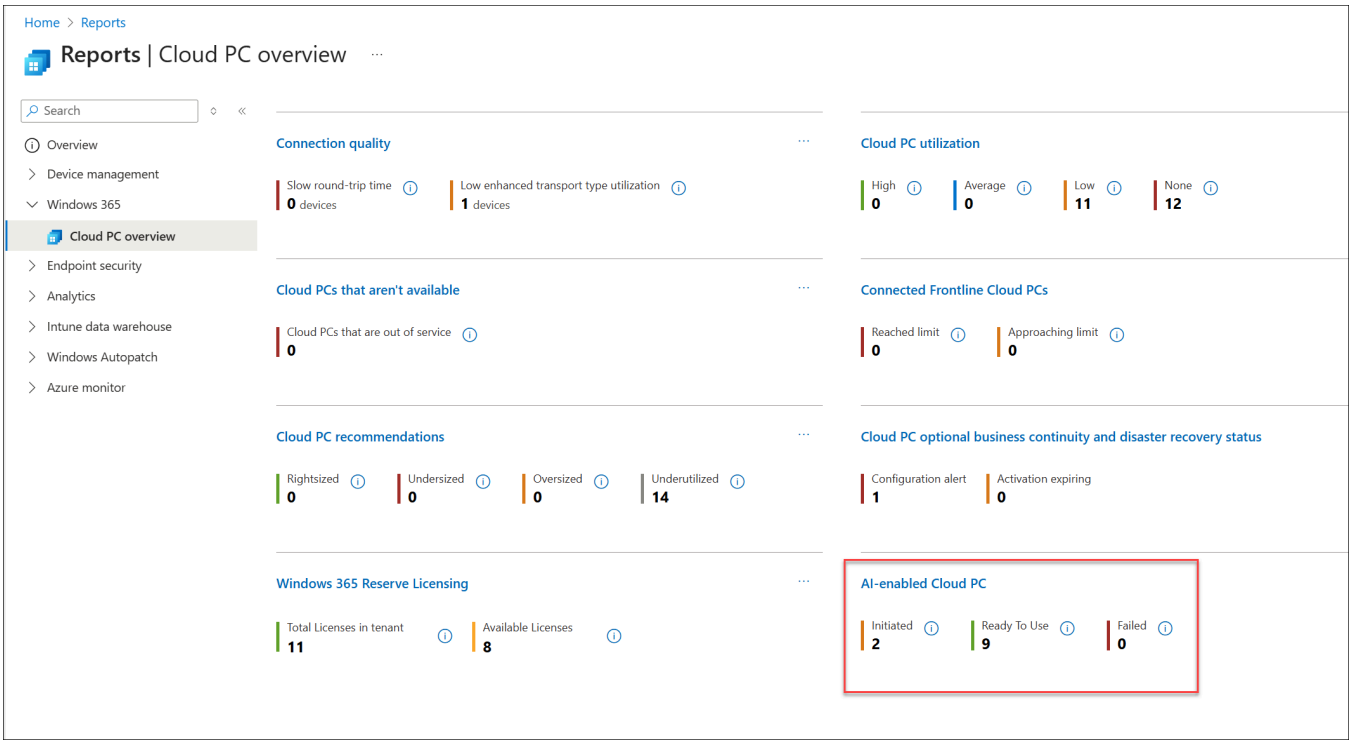


Проверка состояния облачного компьютера с поддержкой ИИ на странице отчетов Intune

На странице обзора Облачный компьютер Windows 365 в разделе Отчеты теперь показано, сколько облачных компьютеров с поддержкой ИИ инициировано, готово к использованию или сбой.

- **Инициировал:** Для этих устройств запущена настройка облачного компьютера с поддержкой ИИ.

- **Готово к использованию:** Настройка облачного компьютера с поддержкой ИИ завершена, и эти функции готовы к использованию.
- **Неудавшийся:** Не удалось завершить настройку облачного компьютера с поддержкой ИИ для этих устройств.



Параметры проверки конечных пользователей

См. статью Облачный компьютер с поддержкой ИИ (Frontier Preview) | Microsoft Learn для того, как конечные пользователи могут проверить, что их облачные компьютеры поддерживают ИИ.

Управление отдельными функциями ИИ в Intune

Если вы хотите сохранить функцию включения ИИ для облачного компьютера и хотите настроить только определенные функции, следуйте указаниям по конкретным функциям:

- Для параметра Click to Do следуйте инструкциям, подробно описанным в разделе Manage Click to Do for Windows clients | Microsoft Learn.
- Улучшенный поиск Windows (поиск в семантических файлах и федеративный поиск) см. в разделе Политики поиска Windows, перечисленные в CSP политики поиска | Microsoft Learn.

Удаление включения ИИ с облачных компьютеров

В Intune существует два способа отключить функцию ИИ для облачного компьютера.

1. Отмена назначения пользователя из включения политики
2. Назначение пользователя для отключения политики

В любом случае будет работать сам по себе (без необходимости выполнять другой параметр). Однако политика Отключения имеет приоритет над политикой Включить во время разрешения конфликтов.

Действия по назначению пользователя для отключения политики

1. В Intune перейдите на вкладку **Устройства**.
2. В разделе **Подключение устройств** перейдите на страницу Windows 365.
3. Выберите вкладку **Параметры**.
4. Нажмите кнопку **Создать**.
5. Выберите параметр **Конфигурации облачных компьютеров** .
6. Добавьте **имя** и **описание** (необязательно).
7. На вкладке **Параметры конфигурации** выберите **Отключить** для параметра **функций с поддержкой ИИ** .
8. Следуйте инструкциям на экране, пока не перейдете на вкладку **Назначения** .
9. Выбирает целевые группы пользователей.
10. Перейдите на вкладку **Рецензирование и создание** и нажмите кнопку **Создать**.
11. Подождите до 48 часов, пока поддержка ИИ не будет отключена на целевых облачных компьютерах.

Last updated on 19.11.2025

параметры Windows App (предварительная версия)

Этот объект параметров позволяет ИТ-администраторам настраивать параметры для пользователей Windows App.

Страница **параметров Windows App** позволяет ИТ-администраторам управлять следующими параметрами для пользователя:

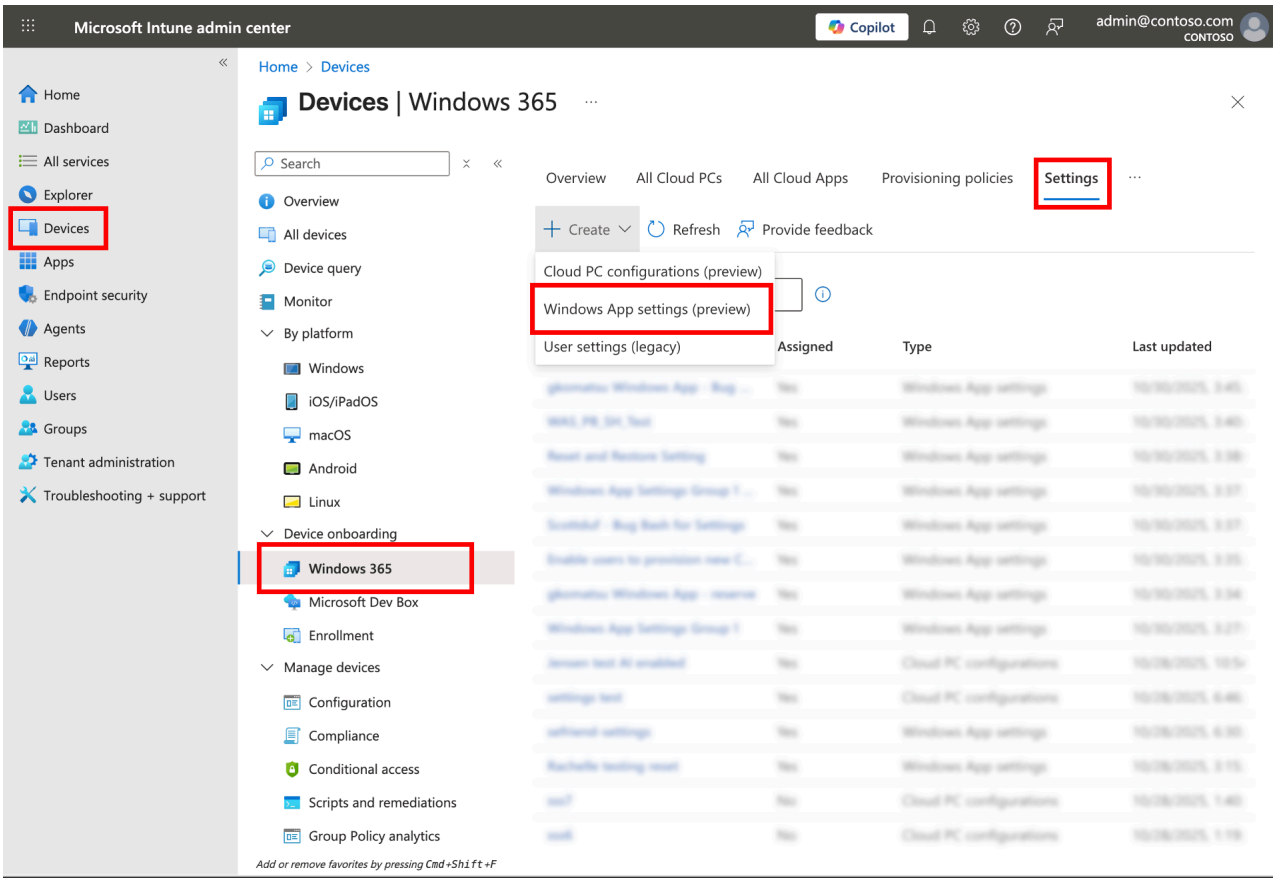
- **Разрешить пользователям сбрасывать свои облачные компьютеры:** Включение этого параметра позволит целевым пользователям повторно создавать облачные компьютеры из приложение Windows 365 и веб-приложения.
  (Примечание. Применимо только к группам пользователей, назначенным политикам подготовки Enterprise, Frontline Dedicated и Reserve.)

- **Разрешить пользователям инициировать восстановление:** Разрешить пользователю инициировать службу восстановления.

  (Примечание. Применимо только к группам пользователей, назначенным политикам подготовки Enterprise и Frontline Dedicated.)

Добавление нового параметра

1. Войдите в Центр администрирования Microsoft Intune, выберите **Устройства**>**Windows 365** (в разделе **Подключение устройств).**>>**Параметры.**
2. Щелкните **Создать** и выберите **Windows App параметры** в раскрывающемся списке.
3. Введите **имя** параметра и добавьте **описание** (необязательно).
4. На вкладке **Параметры конфигурации** выберите **Включить** или **Отключить** для любого из параметров, которые вы хотите настроить.
5. Добавьте **все теги области,** которые вы хотите настроить. Дополнительные сведения о тегах область см. здесь.
6. В разделе **Назначения** выберите **Добавить группы**.
7. В разделе **Выберите группы для включения** выберите группу пользователей, чтобы получить параметры >**Выбрать**.
8. Нажмите кнопку **Далее**.
9. На странице **Проверка и сохранение** нажмите кнопку **Создать**.



> **Примечание.**
>
> Если между **параметрами Windows App** и **пользовательскими параметрами** возникает конфликт, **параметры Windows App** переопределяют **параметры пользователя**.

Изменение параметра

1. Войдите в Центр администрирования Microsoft Intune, выберите **Устройства**>**Windows 365** (в разделе **Подключение устройств).**>>**Параметры**.
2. На странице **Параметры** отображаются текущие параметры.
3. Выберите политику **параметров Windows App**, которую вы хотите изменить.
4. Чтобы изменить имя политики или включить или отключить параметры, нажмите кнопку **Изменить** рядом с **элементом Параметры**.
5. В разделе **Параметры** внесите необходимые изменения и нажмите кнопку **Далее**.
6. На странице **Проверка и сохранение** выберите **Обновить**.
7. Чтобы изменить назначения, нажмите **кнопку Изменить** рядом с пунктом **Назначения**>**Добавить группы** , чтобы добавить другую группу. Чтобы удалить

существующие группы, выберите многоточие (...) >**Удалить**.

8. Нажмите кнопку **Далее**.

9. На странице **Проверка и сохранение** выберите **Обновить**.

Удаление параметра

1. Войдите в Центр администрирования Microsoft Intune, выберите **Устройства**>**Windows 365** (в разделе **Подключение устройств).**>>**Параметры**.

2. На странице **Параметры** можно просмотреть созданные параметры.

3. Выберите многоточие (...) в строке параметра, который требуется удалить >**Удалить**.

4. Нажмите кнопку **Да** во всплывающем окне подтверждения, чтобы навсегда удалить параметр.

Last updated on 19.11.2025

Параметры пользователя

Статья • 24.02.2025

На странице **Параметры пользователя** ИТ-администраторы могут управлять следующими параметрами для пользователя:

- **Включить локального администратора**. Если этот параметр включен, каждый пользователь в назначенных группах получает привилегии до локального администратора каждого из своих облачных компьютеров. Эти разрешения применяются на уровне пользователя.
- **Разрешить пользователям сбрасывать свои облачные компьютеры**. Если этот параметр включен, на Windows App и портале отображается параметр **Сброс** для пользователей в назначенных группах. При сбросе выполняется очистка и повторная подготовка облачного компьютера, удаление всех пользовательских данных и приложений.
- **Разрешить пользователю инициировать службу восстановления**. Если этот параметр включен, каждый пользователь в назначенных группах может восстановить собственные облачные компьютеры до любой доступной версии резервной копии.
- **Конфигурация аварийного восстановления между регионами (необязательно):** позволяет защитить облачные компьютеры во время региональных сбоев. Дополнительные сведения см. в разделе Аварийное восстановление между регионами.

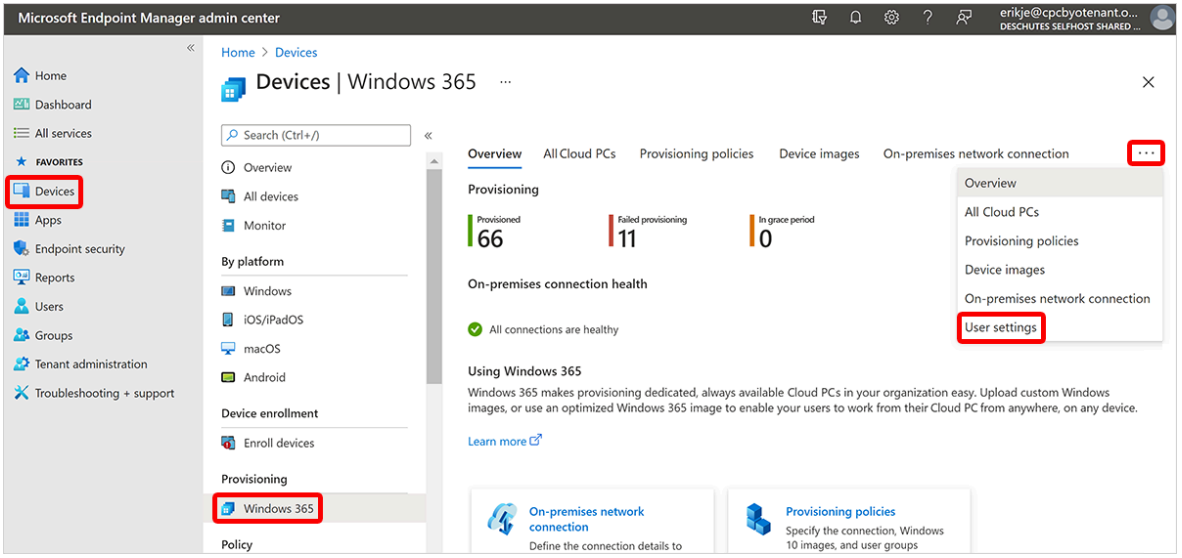
При управлении параметрами помните о следующих моментах:

- Параметры можно применить до или после назначения облачного компьютера.
- Изменения параметров вступают в силу при входе пользователя в систему. Если пользователь в настоящее время вошел в систему, он должен выйти из системы, а затем войти снова, чтобы увидеть изменения.
- Параметры пользователя не применяются к Windows 365 Frontline облачным компьютерам в режиме общего доступа.

Добавление нового параметра

1. Войдите в Центр администрирования Microsoft Intune, выберите **Устройства**>**Windows 365** (в разделе **Подключение**

устройств).>>**Параметры**> пользователя**Добавить**.



2. В разделе **Параметры** введите **имя** параметра.
3. Выберите поля для параметров, которые нужно включить для пользователей.

    - Если выбран **параметр Разрешить пользователю инициировать службу восстановления**, также выберите параметр **Частота службы точки восстановления**.

4. Нажмите кнопку **Далее**.
5. В разделе **Назначения** выберите **Добавить Группы**.
6. В разделе **Выберите группы для включения** выберите группу пользователей, чтобы получить параметры >**Выбрать**.
7. Нажмите кнопку **Далее**.
8. На странице **Проверка и сохранение** нажмите кнопку **Создать**.

Изменение параметра пользователя

1. Войдите в Центр администрирования Microsoft Intune, выберите **Устройства**>**Windows 365** (в разделе **Подготовка**).>>**Параметры пользователя**.
2. На странице **Параметры пользователя** отображаются текущие параметры.
3. Выберите параметр пользователя, который нужно изменить.
4. Чтобы изменить имя политики или включить или отключить параметры, нажмите кнопку **Изменить** рядом с **элементом Параметры**.
5. В разделе **Параметры** внесите необходимые изменения и нажмите кнопку **Далее**.
6. На странице **Проверка и сохранение** выберите **Обновить**.
7. Чтобы изменить назначения, нажмите **кнопку Изменить** рядом с пунктом **Назначения**>**Добавить Группы** добавить другую группу. Чтобы удалить существующие группы, выберите многоточие (...) >**Удалить**.

8. Нажмите кнопку **Далее**.
9. На странице **Проверка и сохранение** выберите **Обновить**.

Удаление параметра пользователя

1. Войдите в Центр администрирования Microsoft Intune, выберите **Устройства**>**Windows 365** (в разделе **Подготовка).**>>**Параметры пользователя**.
2. На странице **Параметры пользователя** можно просмотреть созданные параметры.
3. Выберите многоточие (**...**) в строке параметра, который требуется удалить >**Удалить**.
4. Нажмите кнопку **Да** во всплывающем окне подтверждения, чтобы навсегда удалить параметр.

Разрешение конфликтов для локального администратора

Так как политики параметров пользователей назначаются группам пользователей, существует возможность перекрытия групп или пользователей. Если пользователю назначено несколько политик параметров пользователя, будут использоваться параметры пользователей из последней созданной политики и игнорировать все остальные. Время последнего обновления политики не влияет на этот приоритет. Чтобы убедиться, что параметры пользователя непротиворечивы и понятны, избегайте перекрытий политик.

Дальнейшие действия

Сведения о безопасности в Windows 365.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Рекомендации по безопасности

Статья • 24.02.2025

Чтобы улучшить безопасность облачных компьютеров, необходимо принимать во внимание следующие общие рекомендации.

1. Применяйте политики условного доступа для управления устройствами и приложениями, которые могут подключаться к вашей электронной почте и ресурсам компании. Используйте условный доступ для защиты доступа конечных пользователей к Windows 365. В частности, рассмотрите возможность использования Microsoft Entra многофакторной проверки подлинности для проверки подлинности пользователей. Дополнительные сведения см. в статье Что такое условный доступ в Microsoft Entra ID?

2. Используйте Microsoft Defender для конечной точки, чтобы выявлять угрозы и помечать устройства как несоответствующие. Вы можете легко подключить Microsoft Defender для конечной точки к облачным компьютерам, применить политики соответствия устройств к облачным компьютерам и использовать условный доступ для выявления угроз. Дополнительные сведения см. в статье Обеспечение соответствия требованиям Microsoft Defender для конечной точки с помощью условного доступа в Intune.

3. Используйте политики соответствия Intune с политиками условного доступа для облачных компьютеров. Эти политики помогают определить несоответствующие устройства и пользователей, чтобы они не могли получать доступ к корпоративным ресурсам до снижения уровня риска устройства. Дополнительные сведения см. в статье Параметры соответствия для Windows 10/11 в Microsoft Intune.

   > **Примечание**
   >
   > Облачные компьютеры не поддерживают BitLocker. Рекомендуется исключить этот параметр из политик соответствия требованиям, предназначенных для облачных компьютеров.

4. Одним из наиболее важных элементов безопасности устройств являются обновления ОС. Эти обновления обеспечивают актуальность и безопасность устройств, предоставляя новые возможности и средства защиты от уязвимостей. При работе с облачными компьютерами ИТ-администраторы могут использовать Endpoint Manager для настройки кругов обновления

Windows 10/11 в Intune и политик для Центра обновления Windows для бизнеса. Дополнительные сведения см. в статье Управление обновлениями программного обеспечения Windows 10/11 в Intune.

5. По умолчанию в Windows 365 Корпоративная конечные пользователи не являются администраторами своих облачных компьютеров. Эта политика соответствует рекомендациям руководства по безопасности Windows 10 и 11. Дополнительные сведения об этой рекомендации см. в разделе Локальные учетные записи в документации по Windows.

6. Windows 365 интегрируется с Microsoft Defender для конечных точек. Узнайте, почему Microsoft Defender антивирусная программа и Microsoft Defender для конечной точки лучше работают вместе. Администраторы безопасности и конечных точек могут работать вместе и управлять средой облачных компьютеров точно так же, как они управляют физической конечной точкой. При наличии оформленной подписки облачные компьютеры будут:

   - отправлять данные в Оценку безопасности Microsoft 365.
   - неработоспособные компьютеры будут отображаться в Центре безопасности Microsoft Defender для конечной точки и на панелях мониторинга по анализу угроз;
   - Реагируйте на меры по исправлению так же, как и другие управляемые устройства.
   - Поддержка управления защитой от незаконного изменения с помощью Defender или Intune

7. Windows 365 интегрируется с Microsoft Purview. Подключение к Defender для конечной точки включает защиту от потери данных (DLP) Purview. DLP определяет, когда конфиденциальные элементы используются и совместно используются. Это обеспечивает видимость и контроль, необходимые для правильного использования и защиты данных, а также для предотвращения рискованного поведения, которое может скомпрометировать их. Настройте параметры защиты от потери данных конечной точки , чтобы предотвратить получение данных:

   - Скопировано из буфера обмена или диска облачного компьютера на несанкционированные устройства.
   - Печатается на несанкционированных принтерах.

Дальнейшие действия

Развертывание базовой конфигурации безопасности

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Развертывание базовой конфигурации безопасности

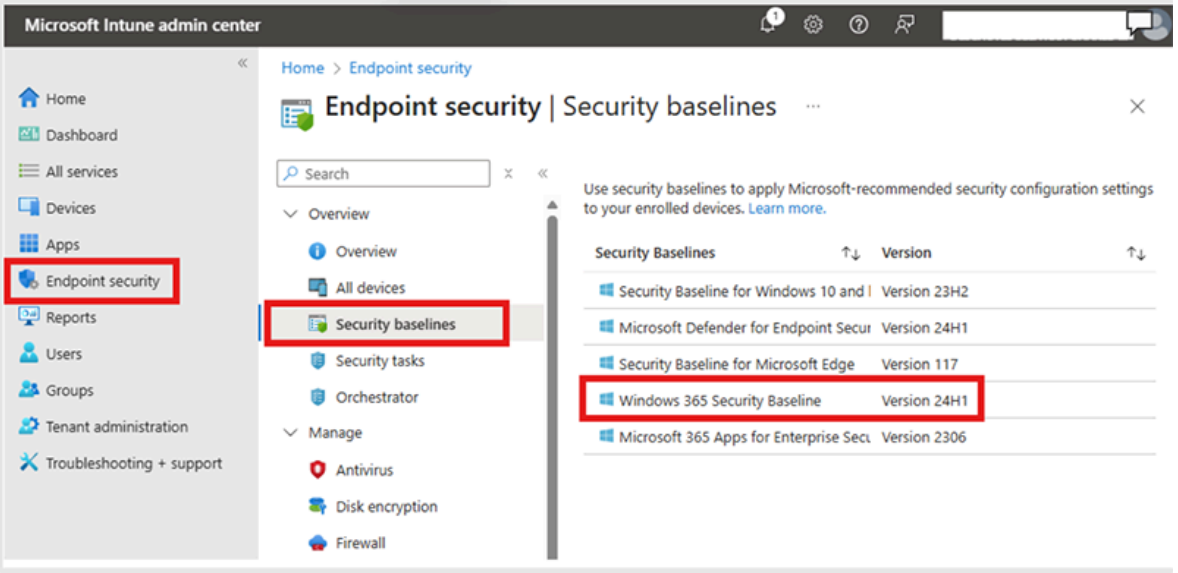
Статья • 31.01.2025

Windows 365 Базовые показатели безопасности версии 24H1 — это набор шаблонов политик, основанных на рекомендациях по обеспечению безопасности и опыте реальных реализаций. С помощью базовых показателей безопасности можно получить рекомендации по безопасности, чтобы снизить риски. Базовые Windows 365 обеспечивают конфигурации безопасности для Windows 11, Windows 10, Microsoft Edge и Microsoft Defender для конечной точки. Они включают в себя функции управления версиями и помогают клиентам выбрать время обновления пользовательских политик до последнего выпуска.

Параметры в Облачный компьютер Windows 365 базовых показателей безопасности версии 24H1 применяются к устройствам Windows, управляемым с помощью Intune. Если это доступно, имя параметра связывается с поставщиком исходной службы конфигурации (CSP), а затем отображает параметры конфигурации по умолчанию в базовом плане.

> **Совет**
>
> Как и любое изменение конфигурации, рекомендуется протестировать базовую конфигурацию безопасности на пилотной группе облачных компьютеров. Сведения о том, как создать план развертывания в Microsoft Intune, см. в **руководстве по планированию Microsoft Intune**. Дополнительные сведения о Microsoft Defender для конечной точки см. в статье **Проверка работы функций Microsoft Defender для конечной точки в режиме аудита**.

1. Войдите в центр администрирования Microsoft Intune выберите**Базовые показатели безопасности**>**конечных точек**.



2. Выберите **Windows 365 базовые показатели безопасности версии 24H1**.

3. На панели **Создание профиля** выберите **Создать профиль**>**Создать**.

4. На странице **Основные сведения** укажите **имя**>**Далее**.

5. На вкладке **Параметры конфигурации** отображаются группы параметров, доступных в выбранной базовой конфигурации. Вы можете развернуть группу, чтобы просмотреть параметры в этой группе, а также значения по умолчанию для этих параметров в базовой конфигурации. Чтобы просмотреть определенные параметры, сделайте следующее:

   - Выберите группу, чтобы развернуть ее и просмотреть доступные параметры.
   - Чтобы отобразить только те группы, которые содержат условия поиска, используйте панель поиска и укажите ключевые слова, которые фильтруют представление.

   Каждый параметр базовой конфигурации имеет значение по умолчанию. Вы можете изменять значения по умолчанию в соответствии со своими требованиями. Отдельные базовые конфигурации могут иметь одинаковые параметры, которым заданы разные значения по умолчанию, определяемые назначением базовой конфигурации.

6. Нажмите кнопку **Далее**.

7. На странице **Области** при необходимости выберите область теги >**Далее**.

8. На вкладке **Назначения** выберите группу устройств с нужными Облачными компьютерами, а затем назначьте базовые показатели одной или нескольким группам с Облачными компьютерами. Используйте **команду Добавить**

группы в разделе **Исключенные группы** , чтобы точно настроить назначение. Нажмите кнопку **Далее**.

9. Подготовив базовую конфигурацию к развертыванию, перейдите на вкладку **Просмотр и создание**, чтобы просмотреть сведения о базовой конфигурации. Щелкните **Создать**, чтобы сохранить и развернуть профиль.

Как только вы создадите профиль, он отправляется в назначенную группу и применяется немедленно.

Дальнейшие действия

Дополнительные сведения см в статье Использование базовых конфигураций безопасности для настройки устройств с Windows в Intune.

Подробный список параметров 24H1 см. в разделе Список параметров для Облачный компьютер Windows 365 базовых показателей безопасности в Intune.

Настройка политик условного доступа.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Управление перенаправлениями устройств RDP для Облачных компьютеров

05.08.2025

Протокол удаленного рабочего стола (RDP) можно использовать для создания перенаправлений, позволяющих пользователям подключаться к периферийным устройствам (например, к камерам, USB-накопителям и принтерам) с удаленных устройств, таких как Облачные компьютеры. По умолчанию буфер обмена, диск, непрозрачные низкоуровневые перенаправления USB и принтеров отключены для облачных компьютеров. Обновите эти перенаправления в соответствии с политиками вашей организации.

Чтобы понять, какие перенаправления поддерживаются в зависимости от платформы, используемой для доступа к облачному компьютеру, см. Сравнение клиентов: перенаправления.

Параметры перенаправления устройств RDP

С помощью соответствующего параметра можно управлять следующими перенаправлениями:

Развернуть таблицу

Перенаправление	Групповая политика
Аудиовход	Разрешить перенаправление записи звука
Аудиовыход	Разрешить перенаправление воспроизведения звука и видео
Камеры	Запретить перенаправление захвата видео
Буфер обмена	Запретить перенаправление буфера обмена
COM-порты	Запретить перенаправление COM-портов
Drives	Запретить перенаправление дисков
Расположение	Не разрешать перенаправление данных расположения
Принтеры	Запретить перенаправление клиентского принтера
Смарт-карты	Запретить перенаправление устройств смарт-карт

Перенаправление	Групповая политика
USB-накопители	Запретить перенаправление поддерживаемых самонастраивающихся устройств

Некоторые параметры могут быть недоступны в каталоге параметров.

Управлять этими перенаправлениями можно двумя способами.

- Каталог параметров. Используйте политику конфигурации устройств в Microsoft Intune. Поддерживает как Microsoft Entra присоединение, так и Microsoft Entra облачные компьютеры с гибридным присоединением.
- Объект групповой политики (GPO): использование объектов групповой политики в Windows Server Active Directory. Поддерживает только облачные компьютеры Microsoft Entra гибридного присоединения.

Следуйте соответствующим указаниям по управлению перенаправлением устройств RDP.

Управление перенаправлением устройств RDP с помощью каталога параметров

Чтобы управлять любыми перенаправлениями с помощью каталога параметров, создайте и назначьте политику конфигурации устройства:

1. Войдите в Центр администрирования Microsoft Intune и выберите **Устройства**>**Профили**> конфигурации**Создать профиль**.

2. Выберите **платформу Windows 10 и более поздних версий**, тип профиля **каталога параметров**, а затем — **Создать**.

3. На странице **Основные сведения** введите значения в поля **Имя** и **Описание** (необязательно) для новой политики.

4. На странице **Параметры конфигурации** выберите **+ Добавить параметры**, чтобы перечислить и выбрать параметры для управления.

    - Чтобы управлять параметрами перенаправления принтеров, выполните поиск по *запросу Перенаправление принтеров*, выберите результирующая категория и выберите параметры, которыми вы хотите управлять.
    - Чтобы управлять другими параметрами перенаправления, найдите "Перенаправление устройства и ресурса", выберите категорию из результатов и выберите параметры, которыми вы хотите управлять.

5. После выбора всех параметров перенаправления, которыми вы хотите управлять, закройте представление **средства выбора параметров** , настройте параметры на странице **Параметры конфигурации** , а затем нажмите кнопку **Далее**.

6. На странице **Теги области** выберите нужные теги области для применения, а затем выберите **Далее**.

7. На странице **Назначения** выберите пользователей или группы, которые вы хотите получить политику перенаправления, а затем нажмите кнопку **Далее**.

8. На странице *Проверка и создание** нажмите кнопку **Создать**.

Дополнительную справку об использовании каталога параметров для создания политики конфигурации устройств см. в статье Использование каталога параметров для настройки параметров на устройствах Windows и macOS.

> ⓘ **Примечание**
>
> Каталог параметров настраивает политики с помощью CSP политики. Чтобы убедиться, что эти параметры имеют приоритет над конфликтующим GPO, можно также настроить ControlPolicyConflict CSP.

Используйте GPO для управления перенаправлением устройств RDP

Для управления любыми перенаправлениями с помощью GPO создайте и назначьте GPO в домене Windows Server Active Directory. Используйте соответствующие политики, как показано в таблице параметров перенаправления устройств RDP. Чтобы узнать больше о политиках, скачайте таблицу-справочник по параметрам групповой политики .

Перенаправления буфера обмена

Перенаправление буфера обмена в Виртуальном рабочем столе Azure и Windows 365 позволяет пользователям копировать и вставлять содержимое (например, текст, изображения и файлы) между устройством пользователя и удаленным сеансом в любом направлении. Дополнительные сведения см. в статье Настройка направления передачи буфера обмена и типов данных, которые можно скопировать в Виртуальном рабочем столе Azure.

Дальнейшие действия

Сведения о приложениях в Windows 365.

Требования соответствия требованиям безопасности устройств для приложений Windows с использованием Microsoft Intune и условного доступа Microsoft Entra

16.04.2025

Вы можете использовать сочетание условного доступа Microsoft Intune и Microsoft Entra, чтобы требовать, чтобы устройства пользователей соответствовали определенным требованиям безопасности, прежде чем они смогут подключиться к виртуальному рабочему столу Azure, Windows 365 и Microsoft Dev Box. Этот подход позволяет применять требования к безопасности для приложения Windows в следующих сценариях:

Развернуть таблицу

Платформа устройства	управление устройствами Intune.
iOS/iPadOS	Управляемый или неуправляемый
Android	Управляемый или неуправляемый
Веб-браузер (только Microsoft Edge в Windows)	Только неуправляемые

1. Не включает поддержку Chrome OS.

Сведения об использовании политик защиты приложений с управляемыми и неуправляемыми устройствами см. в разделе "Целевые политики защиты приложений" на основе состояния управления устройствами.

Некоторые параметры политики, которые можно применить, включают требование ПИН-кода, определенную версию операционной системы, блокировку сторонних клавиатур и ограничение операций вырезания, копирования и вставки между другими приложениями на локальных клиентских устройствах. Полный список доступных параметров см. в разделе "Условный запуск" в параметрах политики защиты приложений iOS и условном запуске в параметрах политики защиты приложений Android.

После установки требований к безопасности вы также можете управлять тем, будут ли локальные ресурсы устройств iOS/iPadOS и Android, такие как камеры, микрофоны, хранилище и буфер обмена, перенаправляться в удаленный сеанс. Требование соответствия безопасности локального устройства является обязательным условием для

управления параметрами перенаправления локальных устройств. Дополнительные сведения об управлении параметрами перенаправления локальных устройств см. в статье "Управление параметрами перенаправления локальных устройств" с помощью Microsoft Intune.

На высоком уровне существует две области, которые необходимо настроить:

- **Политика защиты приложений Intune**: используется для указания требований безопасности, которые должны соответствовать приложению и локальному клиентскому устройству. Фильтры можно использовать для целевых пользователей на основе определенных критериев.
- **Политика условного доступа**: используется для управления доступом к виртуальному рабочему столу Azure и Windows 365 только в том случае, если выполнены критерии, заданные в политиках защиты приложений.

Предпосылки

Прежде чем требовать соответствие безопасности локального клиентского устройства с помощью Intune и условного доступа, вам потребуется:

- Существующий пул узлов с серверами сеансов, или облачными компьютерами.
- По крайней мере, одна группа безопасности Microsoft Entra ID, содержащая пользователей, к которым будут применяться политики.
- Только для управляемых устройств необходимо добавить в Intune каждое из следующих приложений:
  - Для приложения Windows на iOS/iPadOS см. Добавление приложений из магазина iOS в Microsoft Intune.
  - Сведения о Microsoft Edge в Windows см. в статье "Добавление Microsoft Edge для Windows 10/11 в Microsoft Intune".
- Локальное клиентское устройство с одной из следующих версий приложения Windows или с помощью приложения Windows в Microsoft Edge:
  - Приложение Для Windows:
    - iOS/iPadOS: 11.1.1 или более поздней версии.
    - Android 1.0.0.161 или более поздней версии.
  - Microsoft Edge в Windows: 134.0.3124.51 или более поздней версии.
- Кроме того, на локальном клиентском устройстве требуется последняя версия:
  - iOS/iPadOS: приложение Microsoft Authenticator

    - Android: приложение Портал компании, установленное в том же профиле, что и приложение Windows для персональных устройств. Оба приложения должны находиться либо в личном профиле, либо в рабочем профиле, а не одно в каждом профиле.

- Существуют дополнительные предварительные требования Intune для настройки политик защиты приложений и политик условного доступа. Дополнительные сведения можно найти здесь
    - Создание и назначение политик защиты приложений.
    - Используйте политики условного доступа на основе приложений с Intune.

Создание фильтра

Создав фильтр, вы можете применить параметры политики только в том случае, если соответствующие критерии, заданные в фильтре, позволяют сузить область назначения политики. С помощью приложения Windows можно использовать следующие фильтры:

- iOS/iPadOS:
    - Создайте фильтр управляемых приложений для неуправляемых и управляемых устройств.
    - Создайте фильтр для управляемых устройств.

- Андроид:
    - Создайте фильтр управляемых приложений для неуправляемых и управляемых устройств.

- Windows: фильтры не применимы к Microsoft Edge в Windows.

Используйте фильтры, чтобы сузить область назначения политики. Создание фильтра является необязательным; Если фильтр не настроен, те же параметры соответствия безопасности устройства и перенаправления устройств применяются к пользователю независимо от того, находятся ли они на управляемом или неуправляемом устройстве. То, что вы указываете в фильтре, зависит от ваших требований.

Дополнительные сведения о фильтрах и их создании см. в разделе "Использование фильтров" при назначении приложений, политик и профилей в свойствах фильтра приложений Microsoft Intune и управляемых приложений.

Создание политики защиты приложений

Политики защиты приложений позволяют управлять доступом приложений и устройств к данным. Необходимо создать отдельную политику защиты приложений для iOS/iPadOS,

Android и Microsoft Edge в Windows. Не настраивайте как iOS, так и iPadOS и Android в одной политике защиты приложений, так как вы не можете настроить назначение политики на основе управляемых и неуправляемых устройств.

Выберите соответствующую вкладку.

iOS/iPadOS

Чтобы создать и применить политику защиты приложений, выполните действия, описанные в разделе "Создание и назначение политик защиты приложений" и использование следующих параметров:

- Создайте политику защиты приложений для iOS/iPadOS.
- На вкладке "**Приложения**" выберите "**Выбрать общедоступные приложения**", найдите и выберите **приложение Windows**, а затем выберите "**Выбрать**".
- На вкладке "**Защита данных** " применимы только следующие параметры к приложению Windows. Другие параметры не применяются, так как приложение Windows взаимодействует с узлом сеанса, а не с данными в приложении. На мобильных устройствах неутвержденные клавиатуры являются источником ведения журнала нажатия клавиш и кражи.

  Можно настроить следующие параметры.

  Развернуть таблицу

Параметр	Значение и описание
Передача данных	
Отправка данных организации в другие приложения	Установите значение **None** , чтобы включить защиту захвата экрана. Дополнительные сведения о защите захвата экрана в Виртуальном рабочем столе Azure см. в статье "Включение защиты захвата экрана" в виртуальном рабочем столе Azure.
Ограничьте вырезание, копирование и вставку между приложениями	Установите значение "**Заблокировано** ", чтобы отключить перенаправление буфера обмена между приложением Windows и локальным устройством. Использование в сочетании с отключением перенаправления буфера обмена в политике конфигурации приложения.
Клавиатуры сторонних производителей	Установите значение "**Заблокировано** ", чтобы заблокировать сторонние клавиатуры.

- На вкладке условного **запуска** рекомендуется добавить следующие условия:

Развернуть таблицу

Состояние	Тип условия	Ценность	Действие
Минимальная версия приложения	Условие приложения	На основе ваших требований. Введите номер версии для приложения Windows в iOS/iPadOS	Блокировка доступа
Минимальная версия ОС	Состояние устройства	На основе ваших требований.	Блокировка доступа
Основная служба MTD	Состояние устройства	На основе ваших требований. Необходимо настроить соединитель MTD. Для **Microsoft Defender для конечной точки** настройте его в Intune.	Блокировка доступа
Максимальный допустимый уровень угроз для устройства	Состояние устройства	Защищенная	Блокировка доступа

Дополнительные сведения о доступных параметрах см. в разделе "Условный запуск" в параметрах политики защиты приложений iOS.

- На вкладке "**Назначения**" назначьте политику группе безопасности, содержащей пользователей, к которым нужно применить политику. Чтобы политика вступила в силу, необходимо применить политику к группе пользователей. Для каждой группы можно выбрать фильтр, который будет более конкретным в целевой политике конфигурации приложения.

Создание политики условного доступа

Политика условного доступа позволяет управлять доступом к виртуальному рабочему столу Azure, Windows 365 и Microsoft Dev Box на основе определенных критериев подключения пользователя и используемого устройства. Рекомендуется создать несколько политик условного доступа, чтобы обеспечить детализированные сценарии на основе ваших требований. Некоторые примеры политик приведены в следующих разделах.

Важно!

Тщательно рассмотрите диапазон облачных служб, устройств и версий приложения Windows, которые вы хотите, чтобы пользователи могли использовать. В этих примерах политики условного доступа не охватывают все сценарии, и не забудьте непреднамеренно блокировать доступ. Необходимо создать политики и настроить параметры на основе ваших требований.

Чтобы создать и применить политику условного доступа, выполните действия, описанные в разделе "Настройка политик условного доступа на основе приложений с помощью Intune " и использование сведений и параметров в следующих примерах.

Пример 1. Разрешить доступ только в том случае, если политика защиты приложений применяется с приложением Windows

Этот пример разрешает доступ только в том случае, если политика защиты приложений применяется с приложением Windows:

- Для **назначений** в разделе **"Пользователи" или "Удостоверения рабочей нагрузки"** сначала выберите **0 пользователей или удостоверения рабочей нагрузки**, а затем добавьте группу безопасности, содержащую пользователей, к которым будет применена политика. Чтобы политика вступила в силу, необходимо применить политику к группе пользователей.
- Для **целевых ресурсов** выберите, чтобы применить политику к **ресурсам**, затем для **включенных** выберите **Выбрать ресурсы**. Найдите и выберите следующие ресурсы. У вас доступны только эти ресурсы, если вы зарегистрировали соответствующую службу в тенанте.

Развернуть таблицу

Имя ресурса	Идентификатор приложения	Примечания.
Виртуальный рабочий стол Azure	9cdead84-a844-4324-93f2-b2e6bb768d07	Вместо этого его можно назвать **виртуальным рабочим столом Windows** . Проверьте идентификатор приложения.
Windows 365	0af06dc6-e4b5-4f28-818e-e78e62d137a5	Также относится к Microsoft Dev Box.
Вход в Windows Cloud	270efc09-cd0d-444b-a71f-39af4910ec45	Доступно после регистрации одной из других служб.

- Для **условий**:
  - Выберите **платформы устройств**, для **настройки** выберите **"Да"**, а затем в разделе **"Включить"**, выберите " **Выбрать платформы устройств** " и проверьте **iOS** и **Android**.
  - Выберите **клиентские приложения**, для **настройки** выберите **"Да"**, а затем проверьте **браузер** и **мобильные приложения и классические клиенты**.

- Для **элементов управления доступом** в разделе **"Предоставить доступ"** выберите **0 элементов управления**, а затем установите флажок " **Требовать политику защиты приложений** " и установите переключатель для **параметра "Требовать все выбранные элементы управления"**.

- Чтобы **включить политику**, установите для нее значение **"Вкл.**".

Пример 2. Требовать политику защиты приложений для устройств Windows

В этом примере неуправляемые личные устройства Windows ограничиваются использованием Microsoft Edge для доступа к удаленному сеансу, пользуясь приложением Windows только в веб-браузере. Дополнительные сведения об этом сценарии см. в статье "Требовать политику защиты приложений для устройств Windows".

- Для **назначений** в разделе **"Пользователи" или "Удостоверения рабочей нагрузки"** сначала выберите **0 пользователей или удостоверения рабочей нагрузки**, а затем добавьте группу безопасности, содержащую пользователей, к которым будет применена политика. Чтобы политика вступила в силу, необходимо применить политику к группе пользователей.

- Для **целевых ресурсов** выберите, чтобы применить политику к **ресурсам**, затем для **включенных** выберите **Выбрать ресурсы**. Найдите и выберите следующие ресурсы. У вас доступны только эти ресурсы, если вы зарегистрировали соответствующую службу в тенанте.

Развернуть таблицу

Имя ресурса	Идентификатор приложения	Примечания.
Виртуальный рабочий стол Azure	9cdead84-a844-4324-93f2-b2e6bb768d07	Вместо этого его можно назвать **виртуальным рабочим столом Windows** . Проверьте идентификатор приложения.
Windows 365	0af06dc6-e4b5-4f28-	Также относится к Microsoft Dev Box.

Имя ресурса	Идентификатор приложения	Примечания.
	818e-e78e62d137a5	
Вход в Windows Cloud	270efc09-cd0d-444b-a71f-39af4910ec45	Доступно после регистрации одной из других служб.

- Для **условий**:
  - Выберите **платформы устройств**, для **настройки** выберите "**Да**", а затем в разделе "**Включить**", выберите " **Выбрать платформы устройств** " и проверьте **Windows**.
  - Выберите **клиентские приложения**, для **настройки** нажмите **кнопку "Да**", а затем проверьте **браузер**.

- Для **элементов управления доступом** выберите "**Предоставить доступ**", а затем установите флажок " **Требовать политику защиты приложений** " и нажмите переключатель для **параметра "Требовать один из выбранных элементов управления**".

- Чтобы **включить политику**, установите для нее значение "**Вкл**.".

Проверка конфигурации

Теперь, когда вы настроите Intune и условный доступ для обеспечения соответствия безопасности устройств на личных устройствах, вы можете проверить конфигурацию, подключившись к удаленному сеансу. Что необходимо проверить, зависит от того, применяются ли настроенные политики к зарегистрированным или незарегистрированных устройствам, которые платформы и параметры защиты данных заданы. Убедитесь, что вы можете выполнять только те действия, которые можно выполнить в соответствии с ожидаемыми действиями.

Связанный контент

- Управление параметрами перенаправления локальных устройств с помощью Microsoft Intune

Ключ клиента Microsoft Purview для облачных компьютеров Windows 365

Статья • 16.05.2025

Ключ клиента Microsoft Purview — это функция безопасности, которая позволяет добавить дополнительный уровень соответствия вашим данным в службах Microsoft 365.

При использовании ключа клиента с Windows 365 облачными компьютерами:

- Диски, моментальные снимки и образы облачных компьютеров шифруются неактивными ключами, управляемыми клиентом, а не ключами, управляемыми Корпорацией Майкрософт.
- Эти ключи предоставляются вами и управляются с помощью azure Key Vault.
- Корпорация Майкрософт управляет всеми остальными ключами, поддерживая безопасную и управляемую среду.

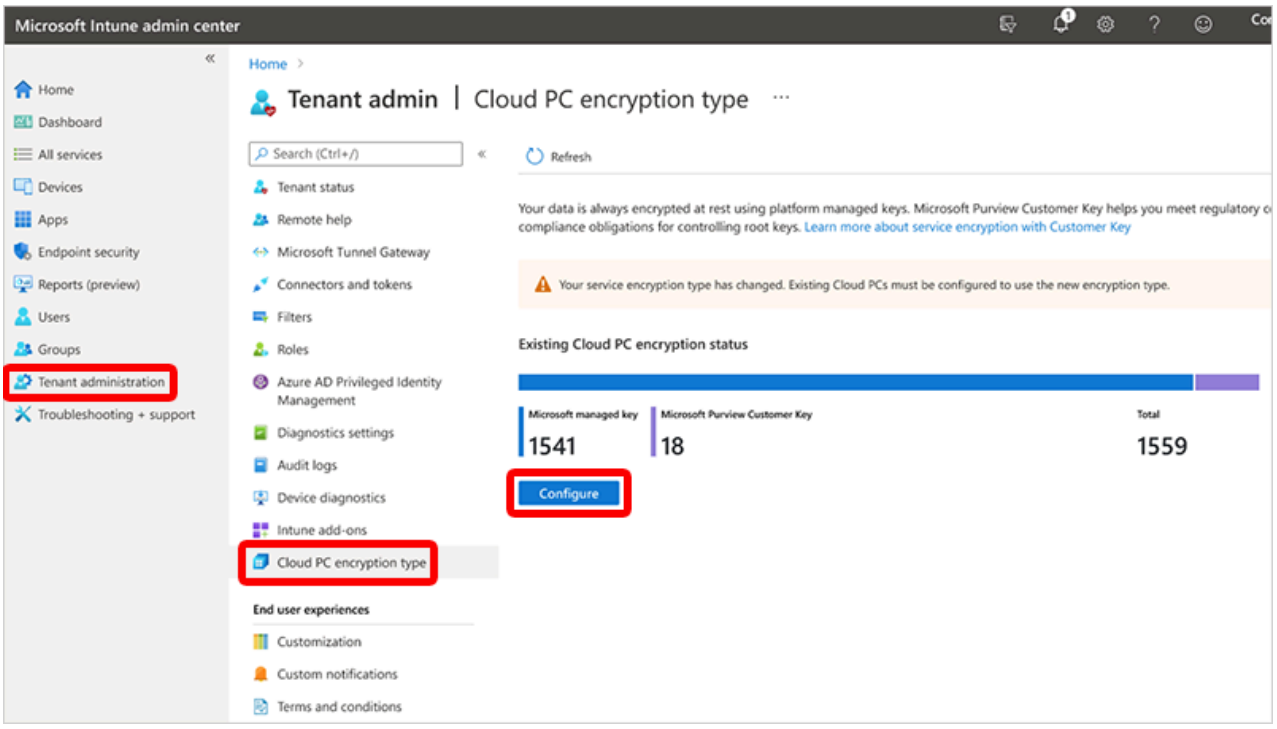
Вы также можете настроить ключ клиента с помощью управляемого модуля HSM.

Настройка ключей клиента для облачных компьютеров Windows 365

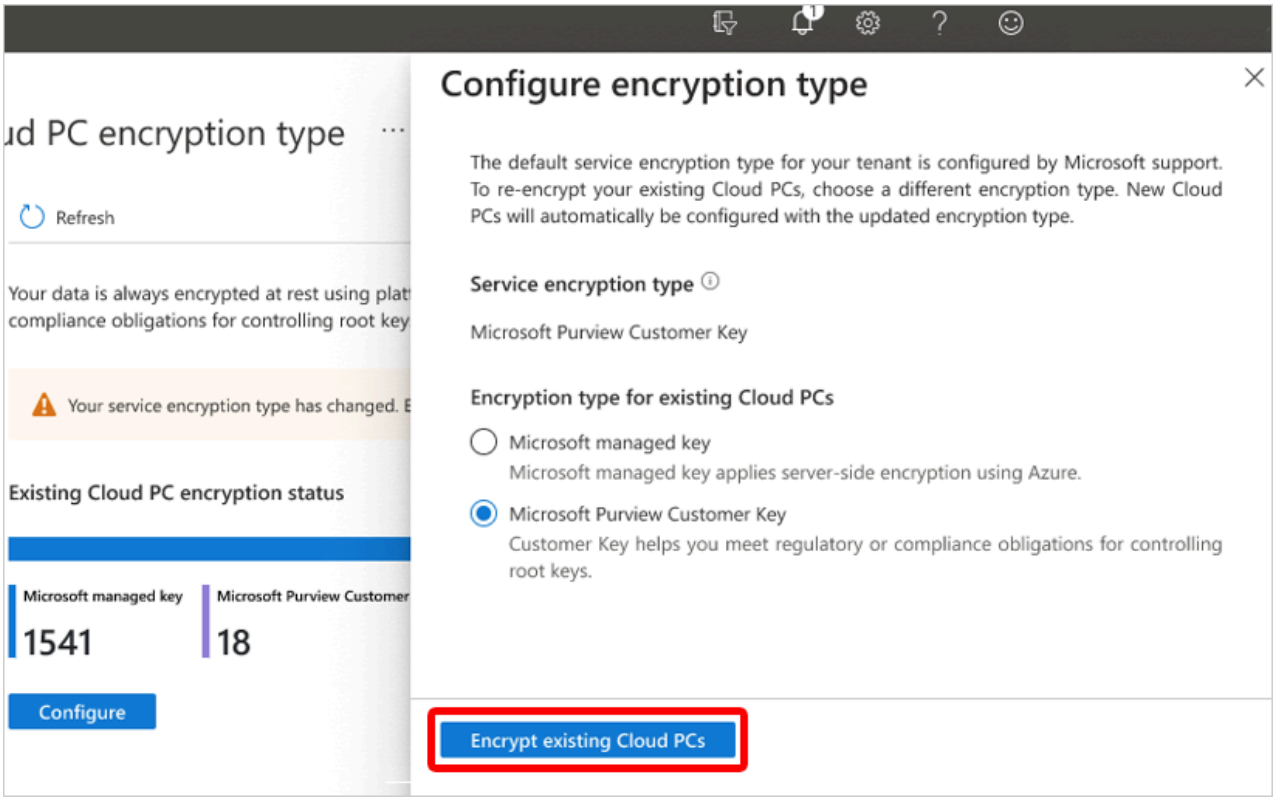
1. Настройка ключа клиента , как описано в документации по ключу клиента Microsoft Purview.

2. Создайте политику шифрования данных для использования с несколькими рабочими нагрузками для всех пользователей клиента. Этот шаг включает назначение политики с несколькими рабочими нагрузками. После завершения этого шага требуется 3–4 часа, чтобы обновить Intune Центре администрирования, чтобы включить кнопку **Настроить**.

3. Войдите в центр >администрирования Microsoft Intune администрирования >**клиентаТип**> шифрования облачного компьютера Настройка.



4. В разделе **Настройка типа шифрования** выберите **Microsoft Purview Customer Key**>**Encrypt (Шифрование существующих облачных компьютеров**).



5. В окне подтверждения выберите **Шифровать**. В уведомлении указано, что шифрование запущено.

Шифрование принудительно перезапускает каждый облачный компьютер.

Шифрование ограничено 20 000 облачных компьютеров одновременно. Эти действия можно повторить, чтобы зашифровать дополнительные облачные компьютеры.

Шифрование может занять много времени в зависимости от количества облачных компьютеров и размера дисков. Страница **Тип шифрования облачного компьютера** обновляется с уведомлением о завершении шифрования.

Дальнейшие действия

Дополнительные сведения о ключе клиента Microsoft Purview см. в статье Общие сведения о шифровании службы с помощью ключа клиента Microsoft Purview.

Windows Cloud IO Protection

> ⓘ **Внимание**
>
> Windows Cloud IO Protection будет доступна в предварительной версии с 25 ноября 2025 г. [Дополнительные условия использования предварительных версий Microsoft Azure](#) см. в статье Юридические условия, применимые к Azure функциям, которые находятся в бета-версии, предварительной версии или еще не выпущены в общедоступную версию.

Обзор. Защита входных данных для Windows 365 облачных компьютеров

Windows 365 облачные компьютеры уже шифруют сеансы и применяют методы проверки подлинности на основе удостоверений, такие как MFA, чтобы предотвратить перехват и атаки "злоумышленник в середине". Тем не менее, угрозы, резидентные конечные точки устройства, нацеленные на облачные сеансы Windows, такие как средства ведения журнала ключей и скребки экрана, которые по-прежнему могут скомпрометировать конфиденциальные данные, что приводит к рискам соответствия требованиям и финансовым потерям.

Защита windows Cloud IO Protection устраняет этот пробел с помощью драйвера уровня ядра и шифрования на уровне системы, которое безопасно направляет нажатия клавиш непосредственно на облачный компьютер, минуя уровни ОС, уязвимые для вредоносных программ. Если эта функция включена на облачном компьютере или узле сеансов Azure Виртуального рабочего стола, она применяет модель строгого доверия:

- **Подключаться могут только физические устройства с защищенной конечной точкой.**
- Для защиты конечных точек должен быть установлен **MSI-файл Windows Cloud IO Protect** .

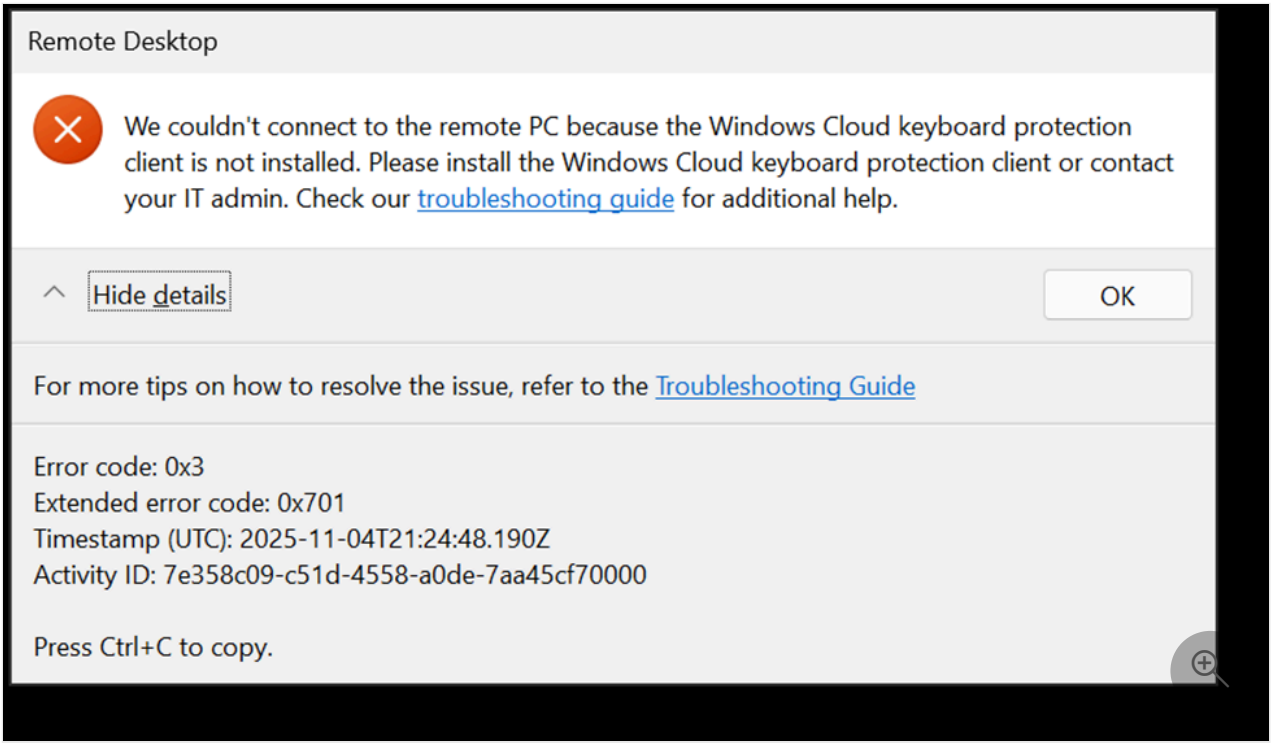
Если MSI отсутствует, подключение блокируется и появляется сообщение об ошибке. Это обеспечивает безопасный канал между приложением Windows и узлом сеансов Облачного компьютера или Azure виртуального рабочего стола, обеспечивая бескомпромиссную защиту входных данных.

Инструкции по установке WINDOWS Cloud Input Protect MSI

Необходимые условия:

- Конечная точка должна быть физическим устройством (виртуальные машины не поддерживаются) с Windows 11. Устройство конечной точки должно использовать TPM 2.0
- Чтобы установить MSI-файл Windows Cloud IO Protect, пользователь должен иметь права **локального Администратор**.

1. Когда пользователь пытается подключиться с физического устройства (без WINDOWS Cloud Input Protect MSI) к узлу сеансов Облачный компьютер Windows 365 или Azure виртуального рабочего стола, появится следующее сообщение об ошибке.

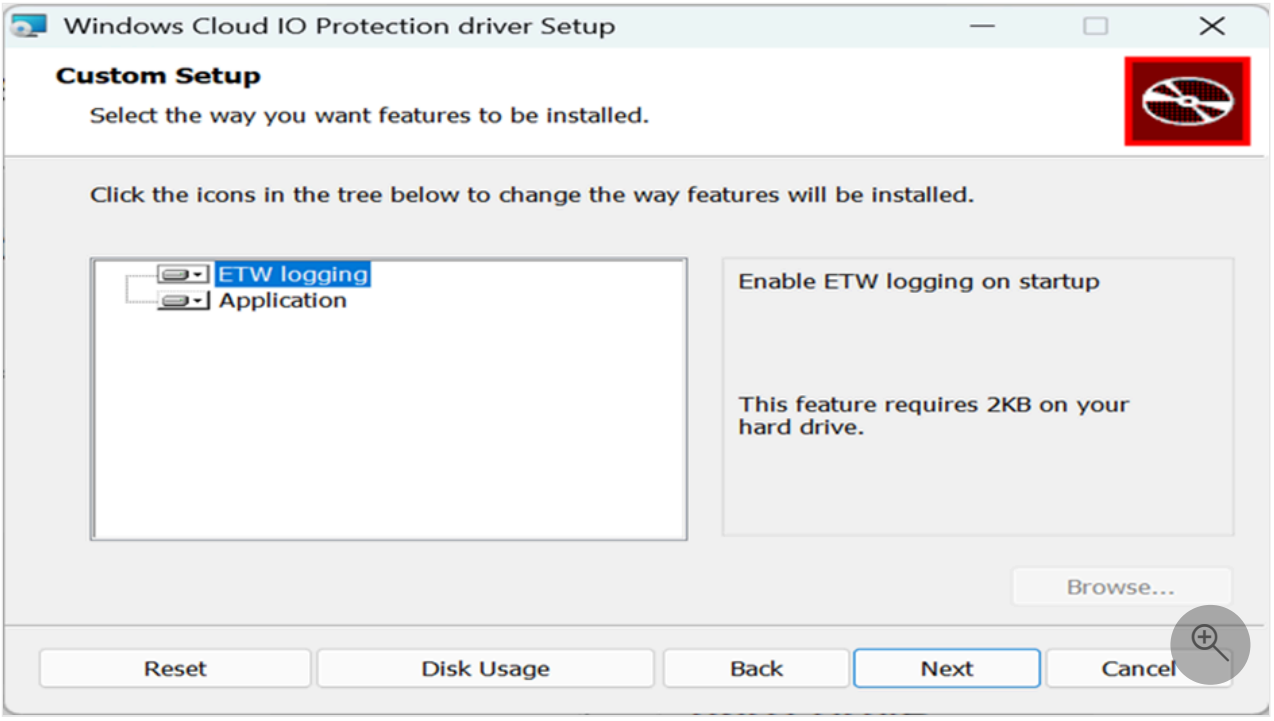


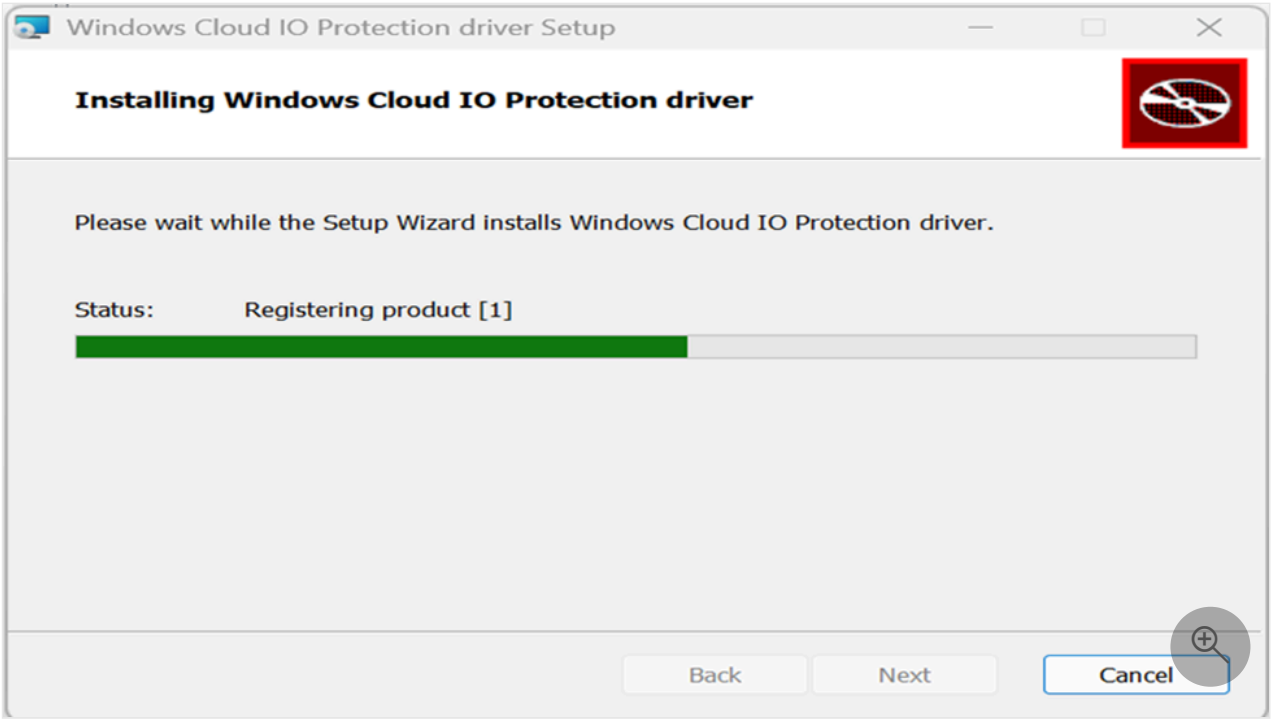
2. Пользователь может выбрать один из двух типов установщика MSI для установки MSI Cloud Input Protect MSI.

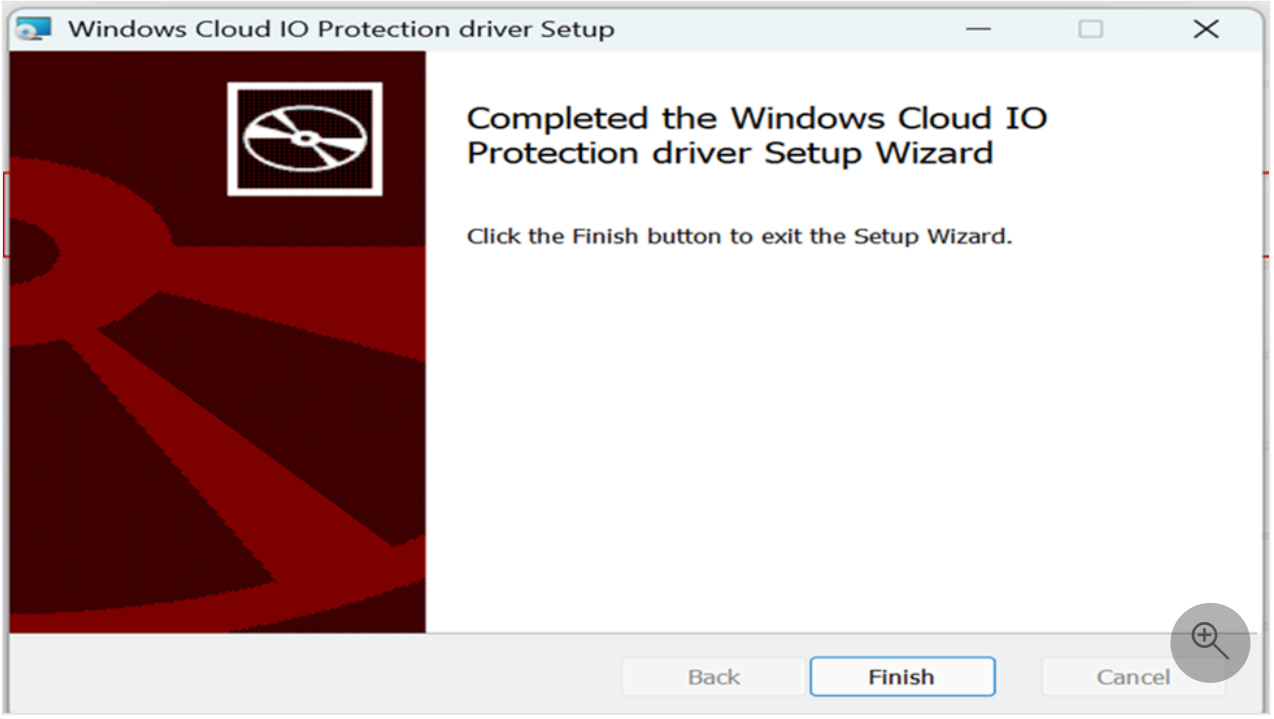
- Windows x64
- Windows AMD 64

3. Выполните действия мастера установки MSI, как показано ниже

Windows Cloud IO Protection driver Setup
Welcome to the Windows Cloud IO Protection driver Setup Wizard
The Setup Wizard will install Windows Cloud IO Protection driver on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

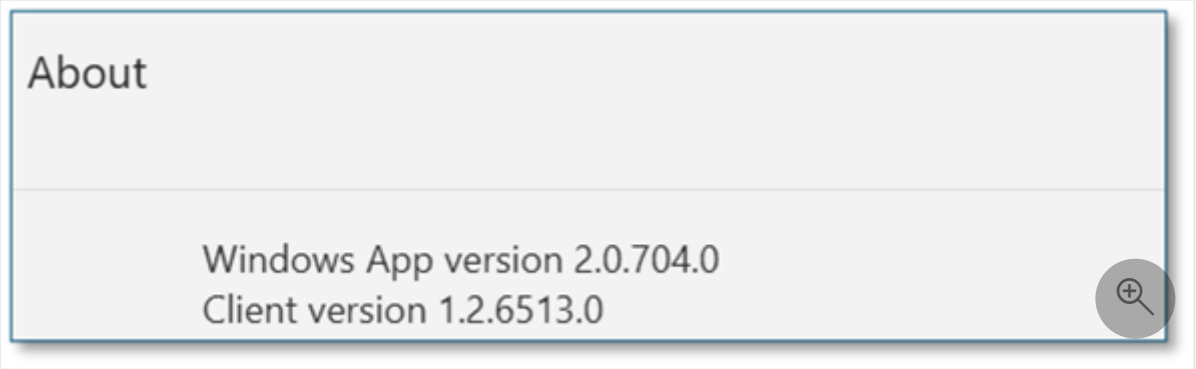

Windows Cloud IO Protection driver Setup
Custom Setup
Select the way you want features to be installed.
Click the icons in the tree below to change the way features will be installed.
ETW logging
Application
Enable ETW logging on startup
This feature requires 2KB on your hard drive.
Browse...
Reset
Disk Usage
Back
Next
Cancel





Предварительные требования Windows App

Эта функция доступна только в последней версии Windows App (версия должна быть 2.0.704.0 или более поздней). Можно обновить до последней версии, доступной в Microsoft Market.



Настройка Windows Cloud Input Protection на облачных компьютерах и узлах сеансов Azure виртуального рабочего стола

В настоящее время эту функцию можно включить только с помощью групповая политика.

> ⓘ **Примечание.**
>
> групповая политика этапы объекта применимы только к гибридным средам. Поддержка для клиентов, присоединившихся к Entra, будет доступна в ближайшее время. Сегодня эту функцию можно включить для пользователей, присоединившихся к Entra, добавив разделы реестра вручную, как показано ниже.
>
> 1. Открытие приложения "Редактор реестра"
> 2. Перейдите к **HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services**
> 3. Создайте **DWORD** с именем **fWCIOKeyboardInputProtection** и **значением 1**.

Действия по настройке защиты от ввода в облаке Windows

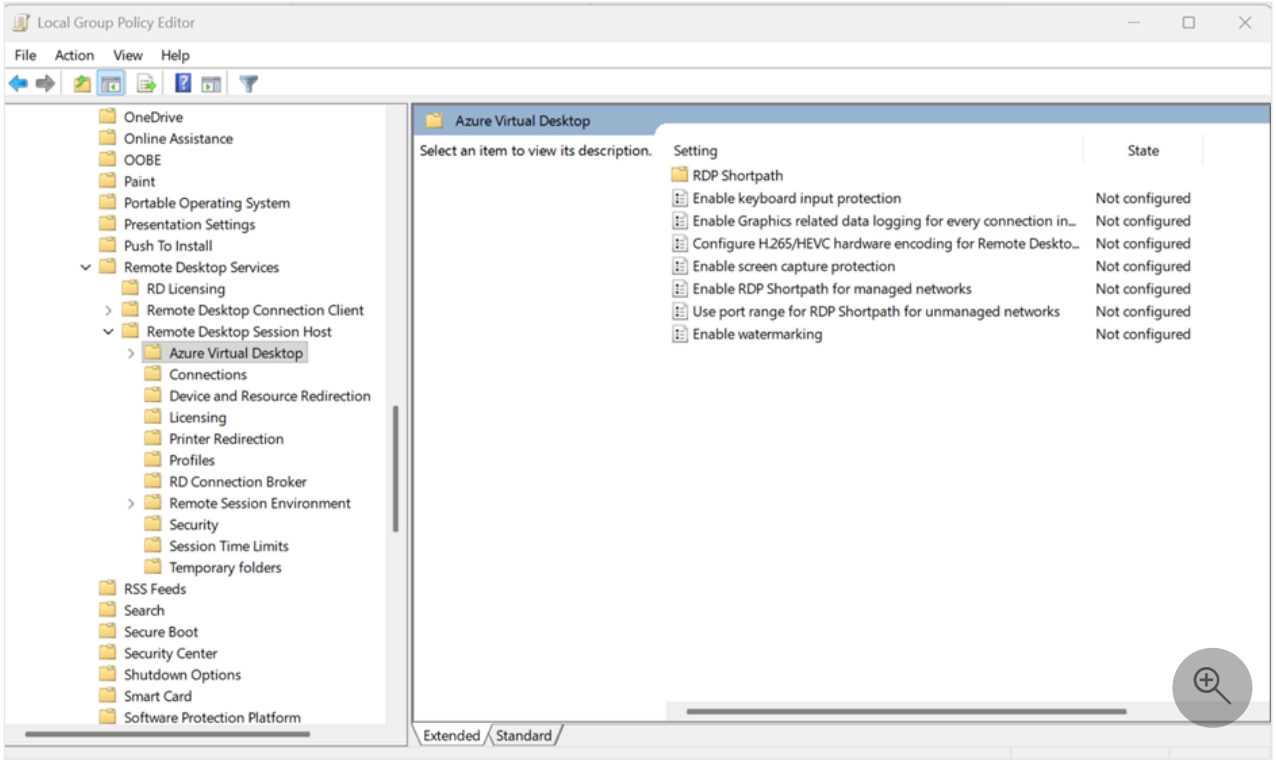
Чтобы включить облачную защиту ввода клавиатуры Windows на узлах сеансов (Azure Виртуальный рабочий стол и Windows 365) с помощью групповая политика в домене Active Directory:

1. Сделайте административный шаблон для виртуального рабочего стола Azure доступным в вашем домене, выполнив действия, описанные в разделе Использование административного шаблона для Azure Виртуального рабочего стола.

2. Откройте консоль **управления групповая политика** на устройстве, используемом для управления доменом Active Directory.

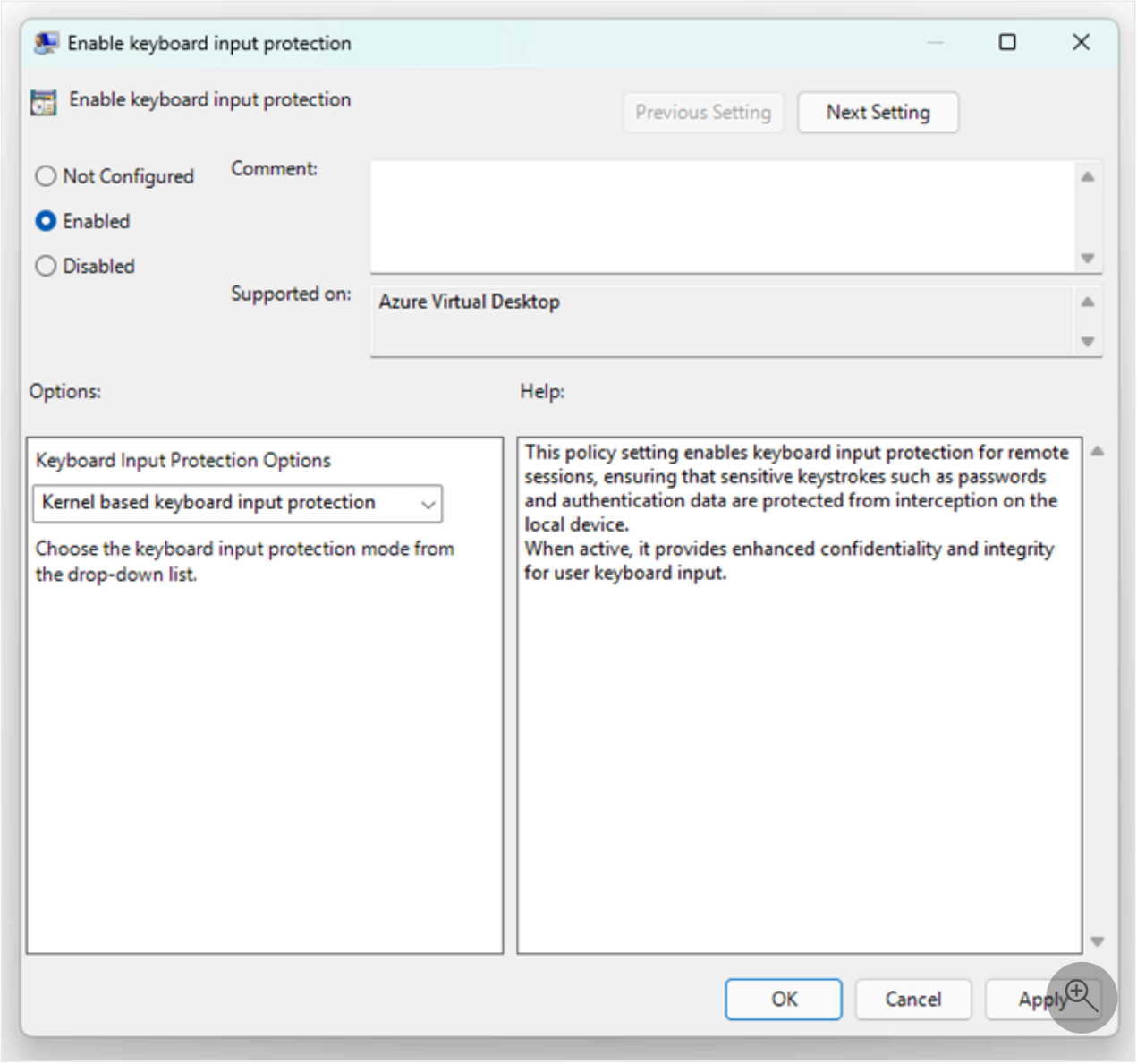
3. Создайте или измените политику, предназначенную для компьютеров, предоставляющих удаленный сеанс, который требуется настроить.

4. Перейдите к**Разделу Политики**>**конфигурации**> компьютера**Административные шаблоны**>**Компоненты**>**Windows Службы удаленных рабочих**>**столов Узел**> сеансов **удаленных рабочих столов Azure Виртуальный рабочий стол**.



5. Дважды щелкните параметр политики **Включить защиту ввода с клавиатуры** , чтобы открыть его.

6. Щелкните **Включено**. После завершения нажмите **кнопку OK**.



7. После применения политики к компьютерам, предоставляющим удаленный сеанс, перезапустите их, чтобы параметры вступили в силу.

> ⓘ **Примечание.**
>
> Эта функция поддерживается для следующих компонентов:
>
> - Windows Cloud PC/Azure узел сеансов виртуального рабочего стола с последними версиями клиентских ОС Windows, поддерживаемыми корпорацией Майкрософт
> - **Поддерживаемые клиенты**. Windows 11 физических устройств под управлением поддерживаемых собственных клиентов, на которых установлен msi Для защиты облачных операций ввода-вывода Windows.

- **Клиенты не поддерживаются.** Виртуальное устройство конечной точки (VM), MAC OS, iOS, Android, Веб-и не windows Cloud IO защищает устройства Windows, включая устройства Windows 365 Link

---

Last updated on 19.11.2025

Включение защиты от захвата экрана в Виртуальном рабочем столе Azure

20.06.2025

Защита от захвата экрана, наряду с водяными знаками, помогает предотвратить захват конфиденциальных данных на клиентских устройствах с помощью определенных функций операционной системы (ОС) и API. При включении защиты снимка экрана удаленное содержимое автоматически блокируется на снимках экранах и совместном использовании экрана.

Если включена защита от захвата экрана, пользователи не могут предоставлять общий доступ к удаленному окну с помощью локального программного обеспечения для совместной работы, например Microsoft Teams. В Teams локальное приложение Teams или с помощью Teams с оптимизацией мультимедиа не может совместно использовать защищенное содержимое.

Совет

- Чтобы повысить безопасность конфиденциальной информации, следует также отключить перенаправление буфера обмена, диска и принтера. Отключение перенаправления помогает запретить пользователям копировать содержимое из удаленного сеанса. Сведения о поддерживаемых значениях перенаправления см. в статье **Перенаправление устройств**.
- Чтобы запретить другие методы захвата экрана, такие как фото экрана с физической камерой, можно включить **подложки**, где администраторы могут использовать QR-код для отслеживания сеанса.

Определение конфигурации

Действия по настройке защиты от захвата экрана зависят от того, где вы ее настраиваете, с каких платформ подключаются пользователи и какой сценарий вы хотите реализовать.

- **Устройства с Windows и macOS**: вы можете запретить захват экрана, настроив узлы сеансов с помощью политики конфигурации устройств Intune или групповая политика. Windows App или клиент удаленного рабочего стола применяет параметры защиты от захвата экрана с узла сеанса без дополнительной настройки.

При настройке защиты от захвата экрана на узлах сеансов можно настроить два дополнительных параметра в соответствии с вашими требованиями:

- **Блокировать захват экрана на клиенте**: запрещает захват экрана с локального устройства приложений, запущенных в удаленном сеансе.
- **Блокировать захват экрана на клиенте и сервере**: запрещает захват экрана с локального устройства приложений, работающих в удаленном сеансе, но также предотвращает захват экрана средствами и службами в узле сеанса.

В этом сценарии ниже приведен результат подключения с каждого типа платформы:

Развернуть таблицу

Платформа	Подключение разрешено	Снимок экрана заблокирован
Windows	✅	✅
macOS	✅	✅
iOS/iPadOS	❌	Н/Д
Android	❌	Н/Д
Web	❌	Н/Д

- **Устройства iOS/iPadOS и Android**: вы можете предотвратить захват экрана, настроив локальные устройства с помощью Microsoft Intune управления мобильными приложениями (MAM). Это не препятствует захвату экрана средствами и службами в узле сеансов. Дополнительные сведения см. в статье Управление параметрами перенаправления локальных устройств с помощью Microsoft Intune.

В этом сценарии ниже приведен результат подключения с каждого типа платформы:

Развернуть таблицу

Платформа	Подключение разрешено	Снимок экрана заблокирован
Windows	✅	❌
macOS	✅	❌
iOS/iPadOS	✅	✅
Android	✅	✅
Web	✅	❌

> ⓘ **Важно!**
>
> Необходимо выбрать, какие локальные устройства следует использовать с защитой от захвата экрана, в зависимости от ваших требований. Не существует сценария, в котором можно включить защиту захвата экрана на всех платформах с одного узла сеансов одновременно. Если они настроены, защита от захвата экрана на узлах сеансов имеет приоритет над использованием политики MAM Intune на локальных устройствах.

Рекомендации по использованию платформы для защиты от захвата экрана в macOS

Хотя в Windows полностью поддерживается, существуют известные ограничения для macOS из-за текущей архитектуры безопасности платформы:

- **Совместимость Microsoft Teams**. В macOS включение защиты от захвата экрана может помешать совместному использованию экрана в Microsoft Teams, что может привести к тому, что общие окна будут отображаться пустыми или не будут отображаться должным образом. Если требуется совместная работа на основе Teams, на устройстве может потребоваться временно отключить защиту от захвата экрана.

- **Принудительное применение на уровне платформы. Из-за** ограничений macOS некоторые собственные приложения могут не полностью соблюдать принудительное применение защиты от захвата экрана. Это ограничение доступных API операционной системы, а не дефект в самой защите от захвата экрана.

Ниже приведены некоторые рекомендации по этим ограничениям.

- Для рабочих процессов macOS с высокой интенсивностью совместной работы рекомендуется настроить параметры защиты от захвата экрана в зависимости от бизнес-потребности и уровня риска.

- Для содержимого с высоким уровнем конфиденциальности рекомендуется использовать конечные точки Windows для полного применения функций защиты экрана.

- Водяные знаки и административные политики можно использовать для дальнейшего противодействия неправильному использованию на платформах с ограниченным применением.

Предварительные условия

Перед настройкой защиты от захвата экрана убедитесь, что выполнены следующие предварительные требования:

- В сценариях, в которых необходимо настроить узлы сеансов, эти узлы сеансов должны работать под управлением Windows 11 версии 22H2 или более поздней или Windows 10 версии 22H2 или более поздней.
- Чтобы использовать защиту от захвата экрана, пользователи должны подключаться к Виртуальному рабочему столу Azure с помощью Windows App или приложения удаленного рабочего стола. В следующей таблице показаны поддерживаемые сценарии.
  - Windows App:

Развернуть таблицу

Платформа	Минимальная версия	Сеанс рабочего стола	Сеанс RemoteApp
Windows App в Windows	Любой	Да	Да. Ос локального устройства должна быть Windows 11 версии 22H2 или более поздней.
Windows App в macOS	Любой	Да	Да
Windows App в iOS/iPadOS	11.0.8	Да	Да
Windows App на Android (предварительная версия)[1]	1.0.145	Да	Да

1. Не включает поддержку Chrome OS, так как Intune MAM не поддерживается в Chrome OS.

  - Клиент удаленного рабочего стола:

Развернуть таблицу

Платформа	Минимальная версия	Сеанс рабочего стола	Сеанс RemoteApp
Windows (классический клиент)	1.2.1672	Да	Да. Ос локального устройства должна быть Windows 11 версии 22H2 или более поздней.
Windows (приложение Магазина виртуальных рабочих столов Azure)	Любой	Да	Да. Ос локального устройства должна быть Windows 11 версии 22H2 или более поздней.
macOS	10.7.0 или более поздней версии	Да	Да

- Чтобы настроить Microsoft Intune, вам потребуется:
  - Microsoft Entra ID учетную запись, которому назначена встроенная роль диспетчера политик и профилей RBAC.
  - Группа, содержащая устройства, которые требуется настроить.
- Чтобы настроить групповая политика, вам потребуется следующее:
  - Учетная запись домена, которая является членом группы безопасности "**Администраторы домена** ".
  - Группа безопасности или подразделение, содержащее устройства, которые нужно настроить.

Включение защиты от захвата экрана на узлах сеансов с помощью политики конфигурации устройства Intune или групповая политика

Выберите соответствующую вкладку для своего сценария.

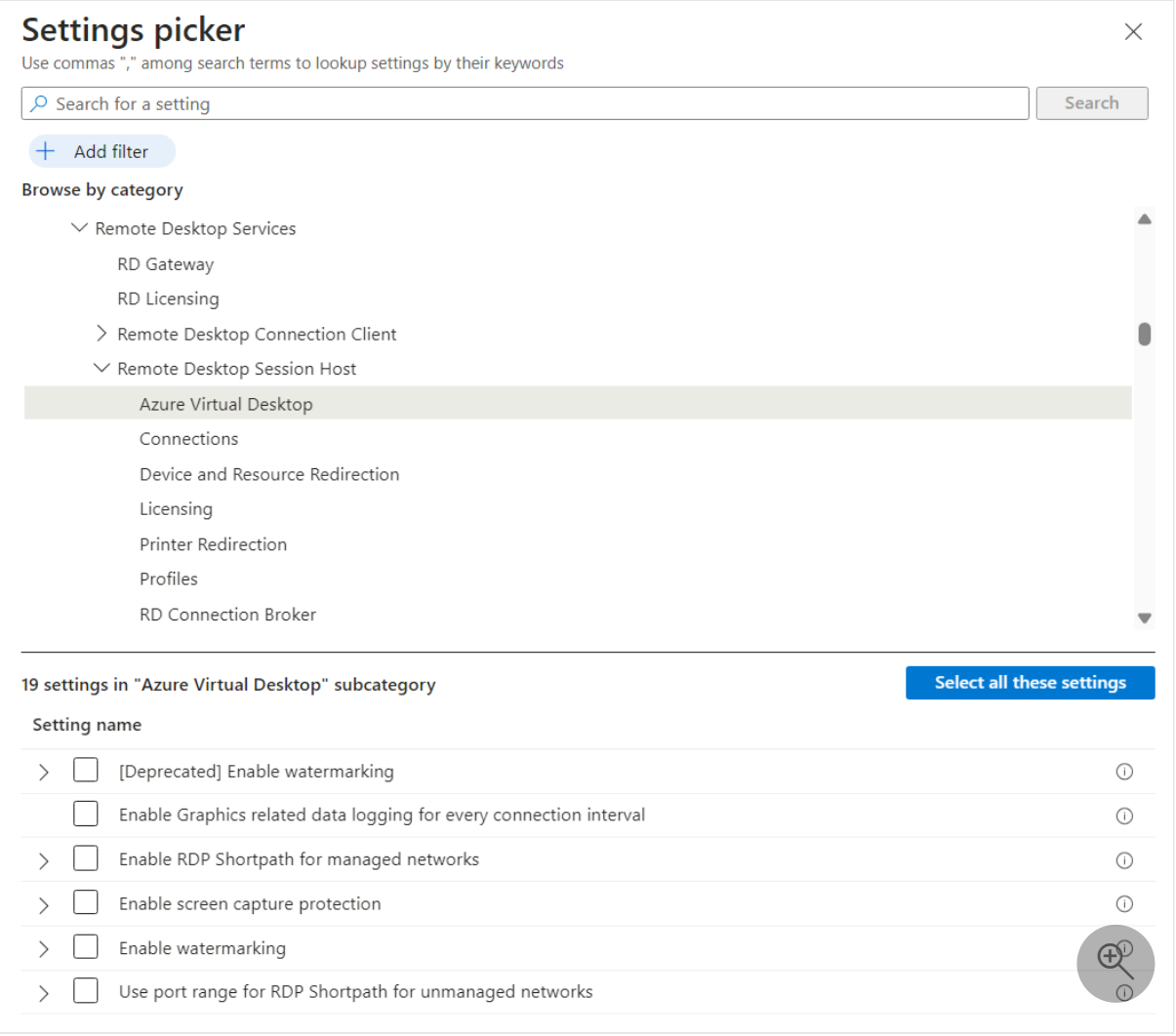
Microsoft Intune

Чтобы настроить защиту снимка экрана на узлах сеансов с помощью Microsoft Intune:

1. Войдите в Центр администрирования Microsoft Intune.

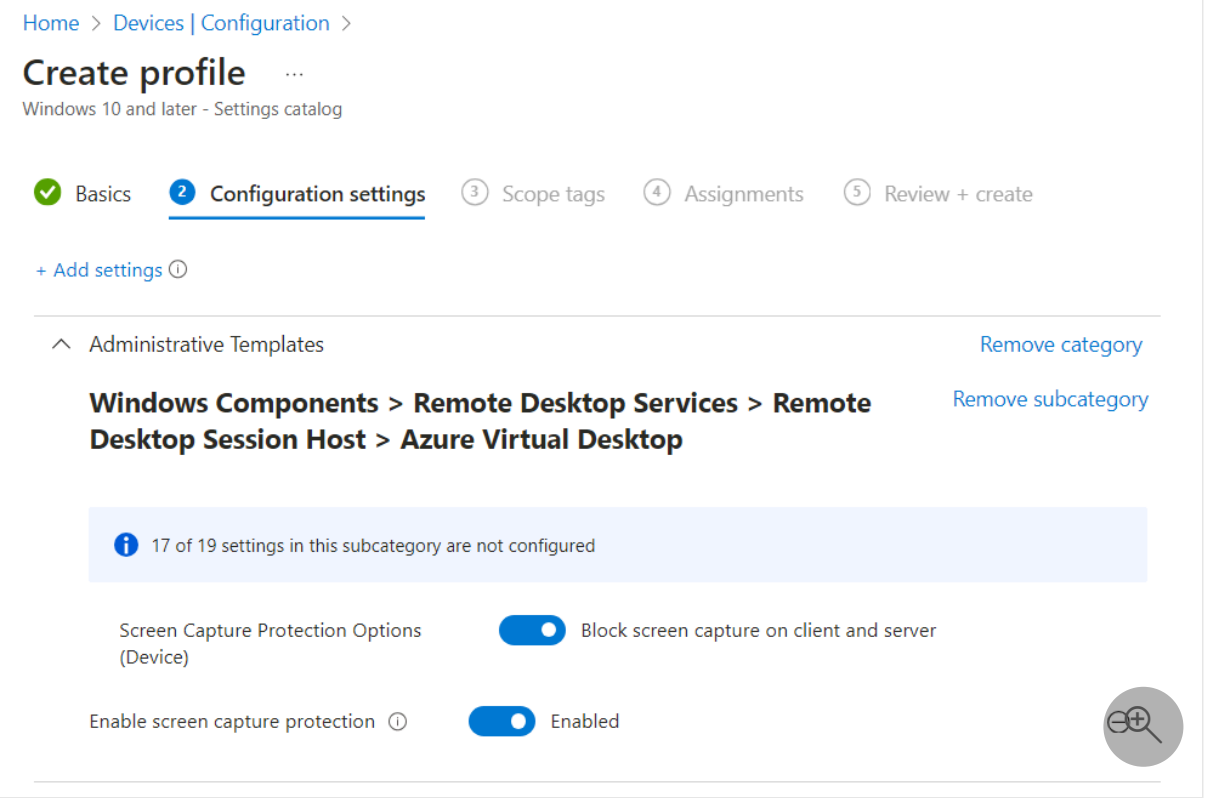
2. Создайте или измените профиль конфигурации для **устройств Windows 10 и более поздних версий** с типом профиля **каталога параметров**.

3. В окне выбора параметров перейдите к **разделу Административные шаблоны**>**Компоненты Windows**Службы**удаленных рабочих**> столов > Узел >**сеансов удаленных рабочих столовAzure Virtual Desktop**.



4. Установите флажок **Включить защиту от захвата экрана**, а затем закройте средство выбора параметров.

5. Разверните категорию **Административные шаблоны** , а затем установите переключатель **Включить защиту снимка экрана** в **положение Включено**.



6. Переключите переключатель параметра **Параметры защиты от захвата экрана (устройство)** в **положение "Отключить "** для **параметра Блокировать захват экрана на клиенте** или **в полеБлокировать захват экрана на клиенте и сервере** в соответствии с вашими требованиями, а затем нажмите **кнопку OK**.

7. Нажмите кнопку **Далее**.

8. *Необязательно*. На вкладке **Теги области** выберите тег область, чтобы отфильтровать профиль. Дополнительные сведения о тегах областей см. в статье Использование управления доступом на основе ролей (RBAC) и тегов области для распределенных ИТ.

9. На вкладке **Назначения** выберите группу, содержащую компьютеры, предоставляющие удаленный сеанс, который требуется настроить, а затем нажмите кнопку **Далее**.

10. На вкладке **Просмотр и создание** просмотрите параметры, а затем выберите **Создать**.

11. После применения политики к компьютерам, предоставляющим удаленный сеанс, перезапустите их, чтобы параметры вступили в силу.

Включение защиты захвата экрана на локальных устройствах с помощью Intune MAM

Чтобы использовать защиту от захвата экрана на устройствах iOS/iPadOS и Android под управлением Windows App, необходимо настроить политику защиты приложений Intune.

Чтобы настроить политику защиты приложений Intune для включения защиты снимка экрана на устройствах iOS/iPadOS и Android:

1. Выполните действия, описанные в статье Требование обеспечения безопасности локального клиентского устройства с помощью Microsoft Intune и условного доступа Microsoft Entra. Соответствие требованиям безопасности локального клиентского устройства обеспечивает основу для настройки защиты от захвата экрана на устройствах iOS/iPadOS и Android под управлением Windows App.

2. При настройке политики защиты приложений на вкладке **Защита данных** настройте следующий параметр в зависимости от платформы:

   a. Для iOS/iPadOS установите для параметра **Отправка данных организации в другие приложения** значение **Нет**.

   b. Для Android установите **для параметра Захват экрана и Google Assistant** значение **Блокировать**.

3. Настройте другие параметры на основе ваших требований и нацелите политику защиты приложений на пользователей и устройства.

Проверка защиты снимка экрана

Чтобы убедиться, что защита от захвата экрана работает, выполните приведенные ниже действия.

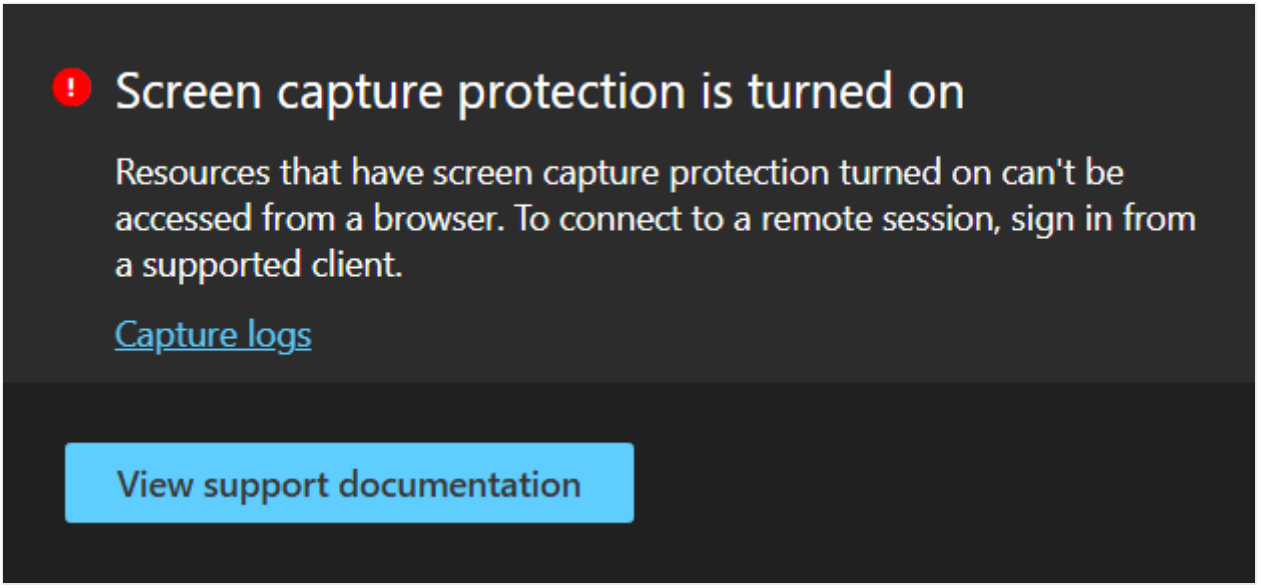
1. Подключитесь к новому удаленному сеансу с помощью поддерживаемого клиента. Не подключайтесь к существующему сеансу. Чтобы изменения вступают в силу, необходимо выйти из существующих сеансов и снова войти в систему.

2. С локального устройства сделайте снимок экрана или поделитесь своим экраном во время звонка или собрания Teams. Содержимое заблокировано или скрыто.

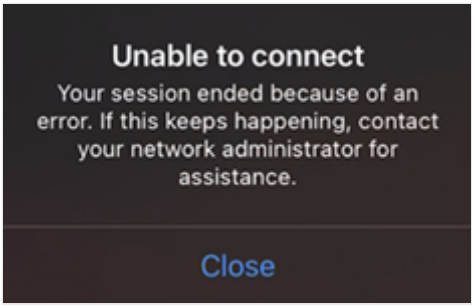
3. Если на устройствах Windows и macOS **включена блокировка записи экрана на клиенте и сервере** на узлах сеансов, попробуйте захватить экран с помощью средства или службы в узле сеансов. Содержимое заблокировано или скрыто.

Если включить защиту снимка экрана на узлах сеансов, необходимо подключиться с поддерживаемого устройства. В противном случае появится сообщение об ошибке, указывающее, что защита от захвата экрана включена. Сообщение об ошибке выглядит примерно так:

- Веб-обозреватель:



- iOS/iPadOS:



Связанные материалы

- Включите подложку, где администраторы могут использовать QR-код для трассировки сеанса.
- Сведения о том, как защитить развертывание Виртуального рабочего стола Azure, см. в статье Рекомендации по обеспечению безопасности.

Подложка в Windows 365

Статья • 31.01.2025

Подложка, наряду с защитой от захвата экрана, препятствует захвату конфиденциальной информации в конечных точках клиента. При включении водяных знаков в составе удаленных рабочих столов отображаются водяные знаки QR-кода. QR-код содержит:

- Идентификатор подключения удаленного сеанса, который администраторы могут использовать для трассировки сеанса.
- Идентификатор устройства облачного компьютера.
- Метка времени.

Подложка настраивается на узлах сеансов и применяется клиентом удаленного рабочего стола.

> ⓘ **Важно!**
>
> - После включения подложки на узле сеанса к узлу сеанса могут подключаться только клиенты, поддерживающие водяные знаки. Если вы попытаетесь подключиться из неподдерживаемого клиента, подключение завершится ошибкой, и вы получите сообщение об ошибке, которое не является конкретным.
> - Подложка применяется только для удаленных рабочих столов и облачных компьютеров. В RemoteApp подложка не применяется, и подключение разрешено.
> - Подложка и захват экрана помогают предотвратить несанкционированную утечку данных, обеспечивая целостность данных. В отличие от функции безопасности или реализации управления цифровыми правами (DRM), нет никакой гарантии, что использование водяных знаков или защиты от захвата экрана будет строго защищать содержимое окон, например когда кто-то делает фотографию экрана.

Требования

Чтобы добавить водяные знаки на облачные компьютеры, вам потребуется:

- Клиент удаленного рабочего стола, поддерживающий подложку. В настоящее время подложки поддерживаются следующими клиентами:
  - Классический клиент Windows версии 1.2.3317 или более поздней версии Windows 10 и более поздних версий.
  - Веб-клиент.

Включение подложки для облачных компьютеров

Чтобы включить подложку для облачных компьютеров, выполните следующие действия.

1. Выполните действия, чтобы сделать шаблон "Административный" для Виртуального рабочего стола Azure доступным.

2. Убедитесь, что административный шаблон доступен.

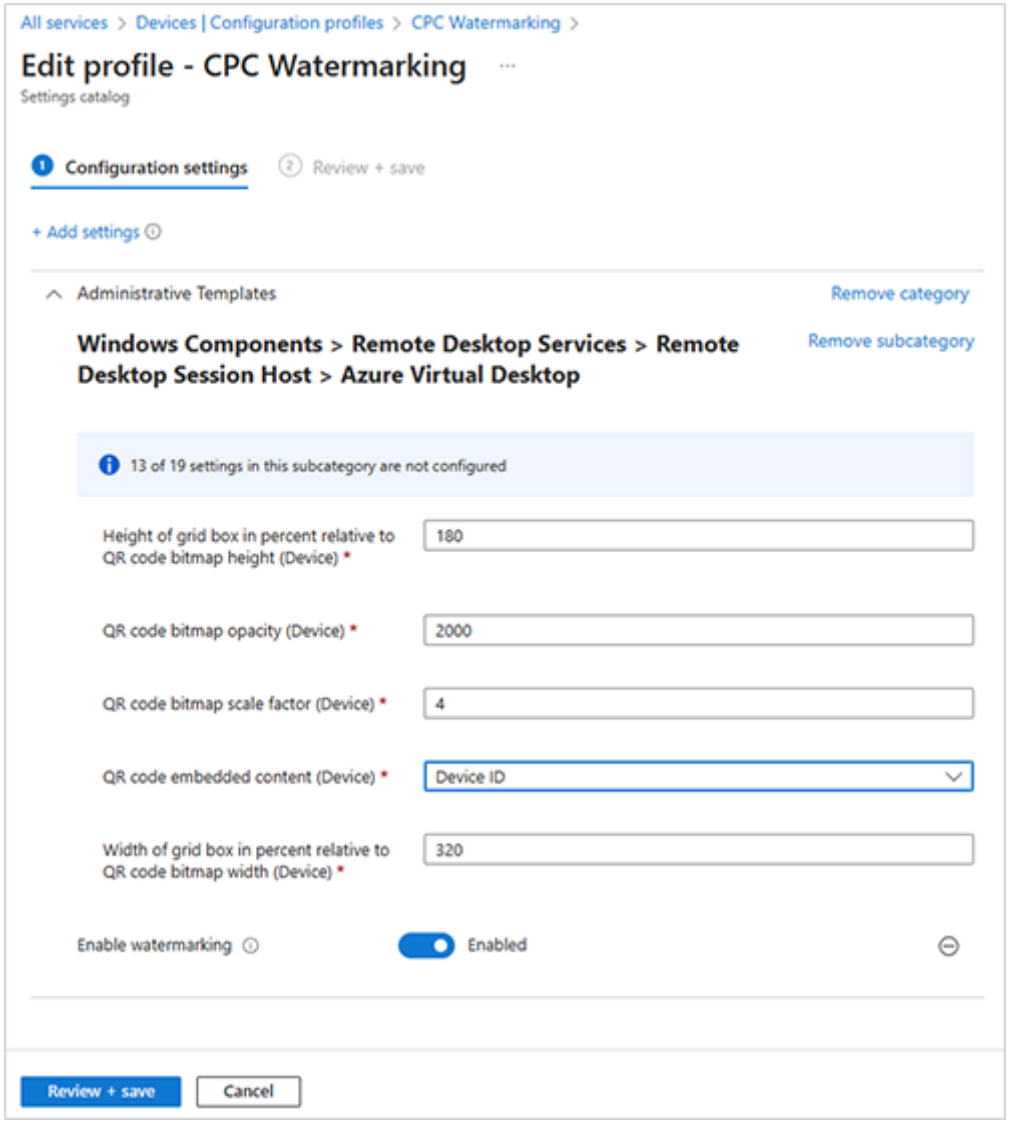
3. Откройте параметр политики **Включить подложку** и установите для него значение **Включено**.

4. Можно настроить следующие параметры:

Развернуть таблицу

Вариант	Значения	Описание
Высота сетки в процентах относительно высоты растрового изображения QR-кода (устройство)	от 100 до 1000 M (default=180)	Расстояние между QR-кодами в процентах. В сочетании с шириной значение 100 приведет к тому, что QR-коды отображаются рядом и заполняют весь экран.
Непрозрачность растрового изображения QR-кода (устройство)	от 100 до 9999 (по умолчанию = 2000)	Прозрачность водяного знака. 100 полностью прозрачный, а более высокие значения становятся все более непрозрачными.
Коэффициент масштабирования растрового изображения QR-кода (устройство)	от 1 до 10 (*по умолчанию = 4*)	Размер каждой точки QR-кода в пикселях. Это значение определяет, сколько квадратов на точку в QR-коде.
Прозрачность растрового изображения QR-кода	От 100 до 9999 (*по умолчанию — 700*)	Насколько прозрачна подложка, где 100 полностью прозрачна.

Вариант	Значения	Описание
Внедренное содержимое QR-кода (устройство)	Идентификатор подключения и идентификатор устройства	Задайте для этого параметра значение Идентификатор устройства при настройке водяных знаков для Windows 365 облачных компьютеров. Параметр Идентификатор устройства действителен только для целевых устройств, которые Microsoft Entra присоединены или Microsoft Entra гибридное присоединение.
Ширина сетки в процентах, соответствующая ширине растрового изображения QR-кода	от 100 до 1000 (*по умолчанию = 320*)	Расстояние между QR-кодами в процентах. В сочетании с высотой значение 100 приведет к тому, что QR-коды отображаются рядом и заполняют весь экран.
Ширина сетки в процентах, соответствующая ширине растрового изображения QR-кода (устройство)	от 100 до 1000 (по умолчанию = 180)	Расстояние между QR-кодами в процентах. В сочетании с шириной значение 100 приведет к тому, что QR-коды отображаются рядом и заполняют весь экран.



> **Совет**
>
> Мы рекомендуем попробовать различные значения непрозрачности, чтобы найти баланс между удобочитаемостью удаленного сеанса и возможностью сканирования QR-кода, но при этом сохранить значения по умолчанию для других параметров.

5. Подключитесь к удаленному сеансу с помощью поддерживаемого клиента, где должны отображаться QR-коды. Все существующие сеансы должны выйти и снова войти, чтобы изменения вступают в силу.

Поиск сведений о сеансе

После включения подложки дополнительные сведения можно найти в сеансе, выполнив следующие действия.

1. Отсканируйте QR-код и запишите GUID идентификатора устройства.

2. Войдите в Центр администрирования Microsoft Intune.
3. Выберите **Устройства** > **Все устройства**.
4. В поле поиска введите GUID идентификатора устройства.

Дальнейшие действия

Узнайте о рекомендациях по безопасности в Windows 365.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Ограничение Office 365 служб облачными компьютерами

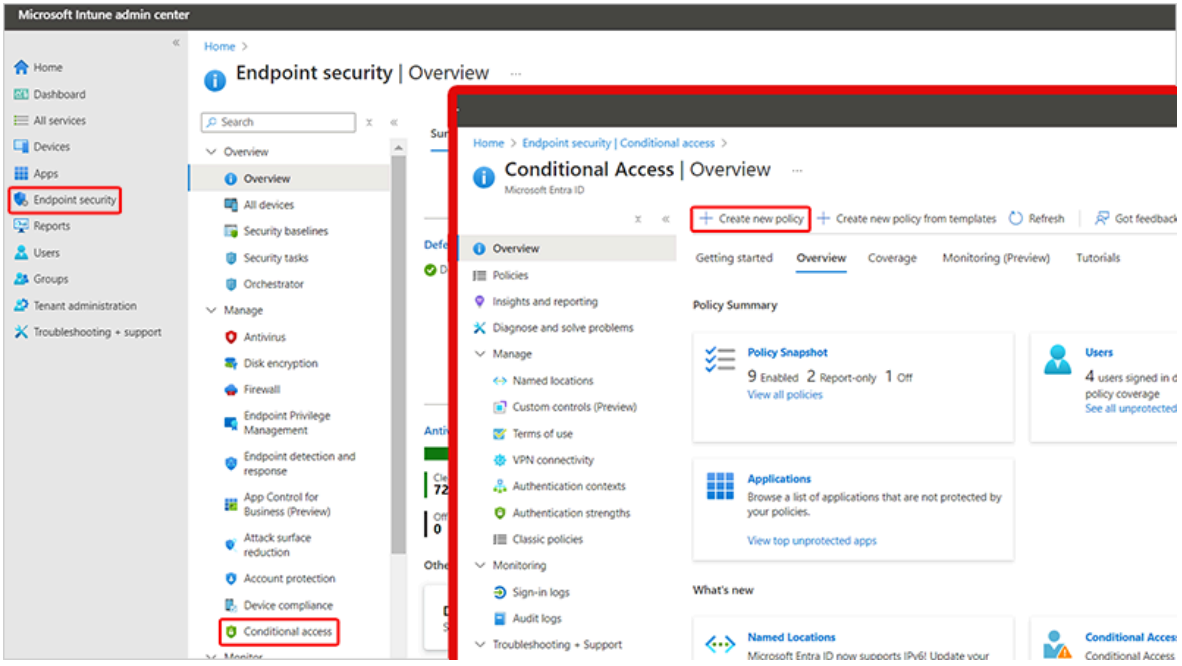
Статья • 31.01.2025

Администраторы могут запретить доступ к службам Office 365 на любом устройстве, кроме облачного компьютера. Для этого можно настроить политики условного доступа Microsoft Entra и фильтры устройств, как описано в этой статье. Выполнив эти действия, вы можете убедиться, что пользователи используют свои облачные компьютеры в качестве основного устройства. Таким образом можно повысить безопасность корпоративных ресурсов и служб.

В этой статье описывается, как ограничить доступ к Office 365 службам. Ту же стратегию можно использовать с любой облачной службой, которая использует Microsoft Entra ID в качестве источника проверки подлинности.

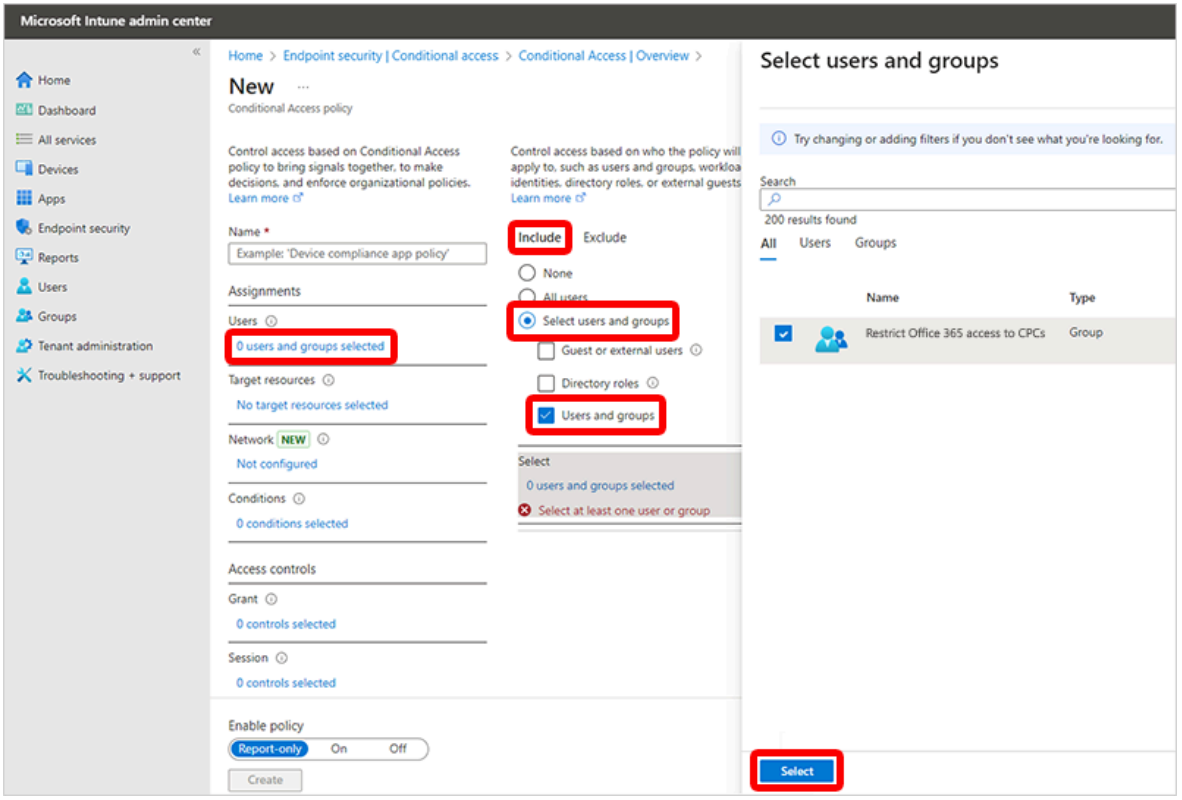
1. Создайте группу безопасности Microsoft Entra для управления пользователями, контролируемыми новой политикой. Добавьте в эту группу всех пользователей облачных компьютеров, которые будут подвергнуты новой политике. Только пользователи в этой группе будут ограничены в использовании облачных компьютеров при доступе к Office 365 службам. Если вы хотите изменить доступ пользователя, его можно просто удалить из этой группы.

2. Войдите в Центр администрирования Microsoft Intune и выберите Пункт Условный**доступ к**>**конечной**>**точке Создать политику**.

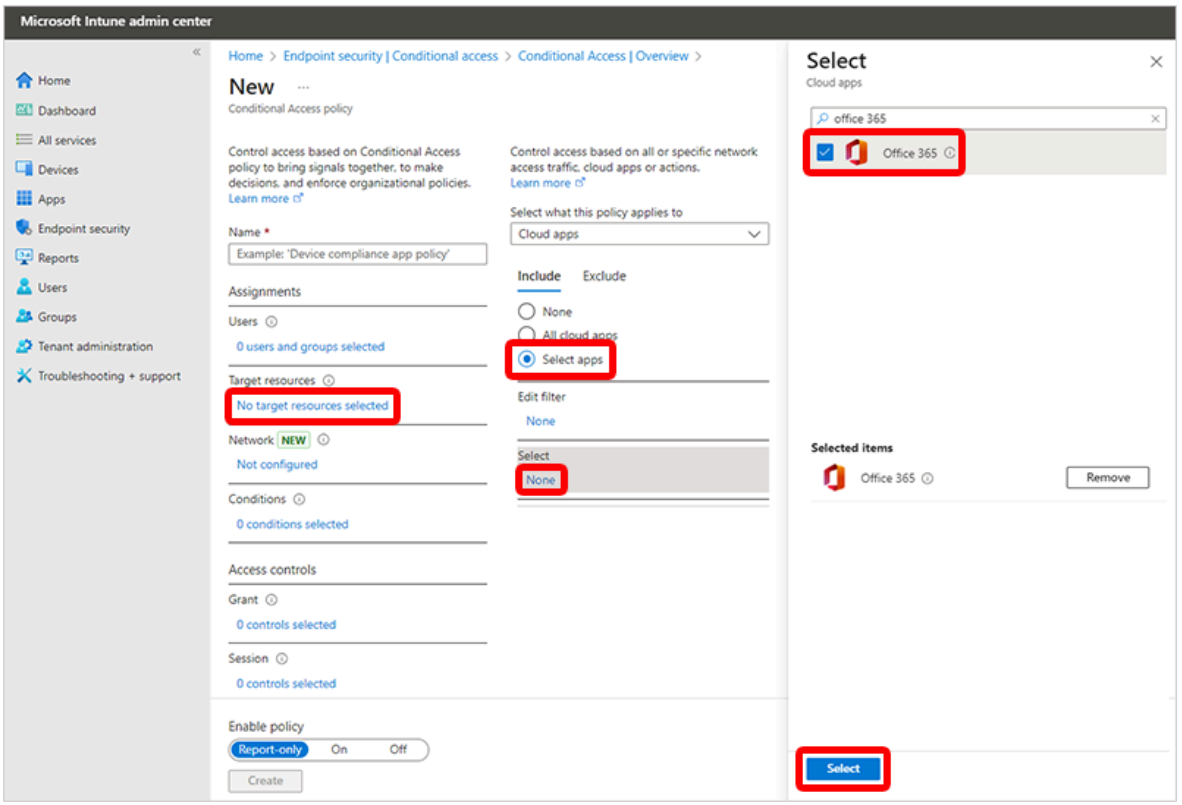


3. Введите **имя** для новой политики условного доступа. Например, "Ограничить доступ Office 365 к ЦП".

4. Выберите **0 пользователей и групп, выбранных**>**Включить**>**Выберите пользователей, а группы**>**Пользователи и группы**>**выберите созданную**> группу безопасности Microsoft Entra.



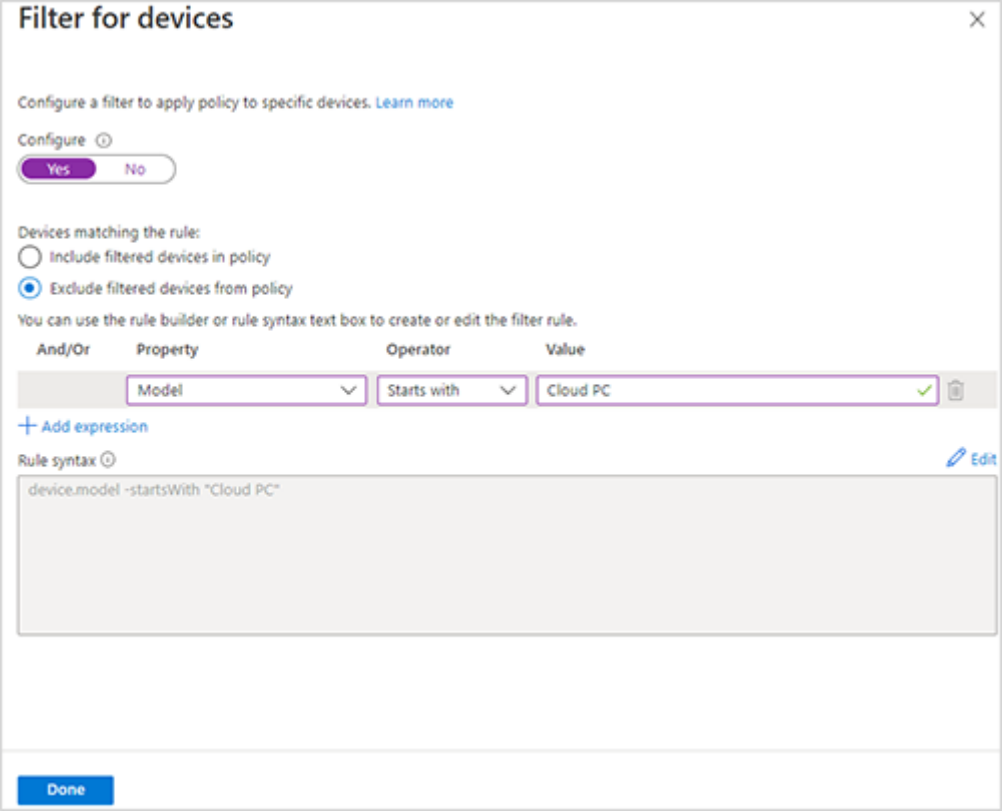
5. Выберите **Пункт Нет целевых ресурсов, выбранный**>**Пункт Включить**>**выбрать приложения**>**Нет** (в разделе **Выбрать**) > найдите и выберите **Office 365**>**Выбрать**.



6. Выберите **Исключить**>**нет** (в разделе **Выбор исключенных облачных приложений**) > найдите и выберите **Виртуальный рабочий стол Azure** и **Windows 365** приложения >**Выбрать**.

7. Выберите **0 выбранных условий** (в разделе **Условия**) >**Не настроено** (в разделе **Фильтр для устройств**).

8. В области **Фильтр для устройств** :
   a. Задайте для **параметра Настройка** значение **Да**.
   b. Выберите **Исключить отфильтрованные устройства из политики**.
   c. Выберите раскрывающийся список в разделе **Модель свойств**>.
   d. Выберите раскрывающийся список **в разделе Оператор**>**начинается с**.
   e. В текстовом поле **в разделе Значение** введите значение **Cloud PC**. Если соглашения об именовании облачных компьютеров изменяются, измените значение фильтра в соответствии с именами устройств.
   f. Нажмите **кнопку Готово** , чтобы задать фильтр.



При необходимости в этой политике можно задать дополнительные параметры, но такие дополнения выходят за рамки область этой статьи.

9. Выберите **0 выбранных элементов управления** (**в разделе Предоставление**) >**Блокировать доступ**>**Выбрать**.

10. Выберите **Включено** (в разделе **Включить политику**). Эта политика ограничивает доступ пользователей к службам Office 365 на устройствах, отличных от облачных компьютеров. Вы можете выбрать **параметр Только отчет,** чтобы отслеживать политику и создавать доверие перед ее применением.

11. Выберите **Создать** , чтобы завершить создание политики.

> ⓘ **Примечание**
>
> Если вы настроили политику подготовки **для использования Microsoft Entra единого входа**, вам также может потребоваться добавить **Удаленный рабочий стол (Майкрософт)** в список исключений на шаге 6, чтобы подключения к единому входу работали должным образом.

Другие устройства

Этот пример политики можно расширить в соответствии с другими вариантами использования, например разрешить доступ к Office 365 службам с мобильных устройств и планшетов пользователей. Для этого внесите в политику следующие изменения:

1. На странице политики выделите текст в разделе **Условия**>**не настроены** (в разделе **Платформы устройств**).
2. Выберите **Да** , чтобы включить параметр конфигурации.
3. Выберите **Включить**>**любое устройство**.
4. Выберите **Исключить**>**Android** и **iOS**.
5. Нажмите **кнопку Готово** , чтобы задать фильтр.
6. Нажмите **Сохранить**.

Дальнейшие действия

Дополнительные сведения об условном доступе.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Настройка судебно-медицинских доказательств Microsoft Purview для Windows 365

Статья • 31.01.2025

Судебно-медицинские доказательства Microsoft Purview помогают получить более подробные сведения о потенциально рискованных действиях пользователей, связанных с безопасностью. Благодаря настраиваемым триггерам событий и встроенным элементам управления защитой конфиденциальности пользователей судебно-медицинские доказательства позволяют настраивать визуальные действия, фиксирующие на разных устройствах. Судебно-медицинские доказательства помогают вашей организации лучше устранять, понимать и реагировать на потенциальные риски данных, такие как несанкционированный кража конфиденциальных данных.

Вы задаете правильные политики для своей организации, например:

- Какие рискованные события являются наивысшим приоритетом для сбора судебно-медицинских доказательств.
- Какие данные являются наиболее конфиденциальными.
- Уведомляются ли пользователи при активации судебной записи.

Запись судебно-медицинских доказательств по умолчанию отключена, а для создания политики требуется двойная авторизация.

Требования

Если указанные ниже требования не выполнены, могут возникнуть проблемы с клиентом Microsoft Purview, а качество судебно-медицинских записей может быть ненадежным.

Чтобы настроить судебно-медицинские доказательства Microsoft Purview, ваша среда должна соответствовать следующим требованиям:

Требования к конфигурации устройства

- Тип изображения коллекции
  - Windows 11 Корпоративная + Приложения Microsoft 365 23H2 или более поздней версии

- Параметры лицензирования
  - Microsoft 365 E5
  - Microsoft 365 E5 (без Teams)
  - Соответствие требованиям Microsoft 365 E5
  - Управление внутренними рисками в Microsoft 365 E5
- Тип соединения и сеть
  - Microsoft Entra присоединено к размещенной сети Майкрософт и сетевым подключениям Azure
  - Microsoft Entra гибридное подключение к сети Azure
- антивирусная программа Microsoft Defender в Windows версии 4.18.2110 или более поздней
- Приложения Microsoft 365 версии 16.0.14701.0 или более поздней
- Устройство должно быть назначено основному пользователю
- Размер облачного компьютера
  - Для оптимальной производительности 8 в ЦП или выше (дополнительные сведения см. в разделе Рекомендации по размеру облачных компьютеров)

Требования к роли

- Учетная запись должна иметь по крайней мере одну из следующих ролей:
  - роль администратора соответствия требованиям Microsoft Entra ID
  - роль глобального администратора Microsoft Entra ID
  - Группа ролей Управления организацией Microsoft Purview
  - Группа ролей администратора соответствия требованиям Microsoft Purview
  - Группа ролей "Управление внутренними рисками"
  - Группа ролей "Администраторы управления внутренними рисками"

> ⓘ **Важно!**
>
> Microsoft рекомендует использовать роли с наименьшим количеством разрешений. Это помогает повысить безопасность вашей организации. Глобальный администратор — это роль с высокими привилегиями, которую следует ограничивать экстренными сценариями, когда вы не можете использовать существующую роль.

Дополнительные сведения о ролях управления внутренними рисками см. в разделе Включение разрешений для управления внутренними рисками.

Включение подключения устройств

1. Откройте портал Microsoft Purview. Выберите **Параметры**>**Подключение устройств**> Подключение**устройств**>.

2. Выберите **метод развертывания** для развертывания пакета конфигурации:

   - Intune. Используйте средства управления мобильными устройствами или Microsoft Intune.
   - Локальный скрипт. Используйте локальный скрипт.

Развертывание пакета конфигурации с помощью Intune

1. Войдите в центр >администрирования Microsoft Intune **Безопасность**> конечных точек Microsoft Defender для конечной точки >**Открыть Центр безопасности в Microsoft Defender**.

2. Установите **для Microsoft Intune подключения** значение *Включено*, а затем **выберите Сохранить параметры**.

3. Вернитесь к **Microsoft Defender для конечной точки** и задайте следующие параметры:

   - **Разрешить Microsoft для конечной точки принудительно применять конфигурации безопасности конечных точек**: *Включено*
   - **Подключение устройств с Windows версии 10.0.15063 и выше к Microsoft Defender для конечной точки**: *Включено*

4. Выберите **Сохранить**.

5. Выберите **Безопасность конечных точек**>**Обнаружение конечных точек и ответ**>**Создать политику**.

6. Выберите следующие параметры:

   - **Платформа**: *Windows 10, Windows 11 и Windows Server*
   - **Тип профиля**: *обнаружение и ответ конечной точки*

7. Нажмите **Создать**.

8. Укажите **имя** и **описание**>**Далее**.

9. На странице **Параметры конфигурации** для **Microsoft Defender для конечной точки тип пакета конфигурации клиента** выберите *Автоматически из соединителя*>**Далее**.

10. На странице **Теги области** выберите **Далее**.

11. На странице **Назначения** выберите группу, в которую входит основной пользователь Облачного компьютера >**Далее**.

12. На странице **Проверка и создание** нажмите кнопку **Создать**.

После создания политики пользователь должен войти на свое устройство, прежде чем она будет применена, и устройство будет подключено к Microsoft Defender для конечной точки.

Развертывание пакета конфигурации с помощью локального скрипта

Следуйте инструкциям в разделе Подключение Windows 10 и Windows 11 устройств с помощью локального скрипта. Этот скрипт может быть полезен при тестировании подмножества облачных компьютеров, прежде чем переходить к подключению всех облачных компьютеров.

Просмотр списка устройств подключения

1. Откройте портал >Microsoft Purview **Параметры устройства**>**подключения**> устройств.

2. Проверьте следующие столбцы:

   - **Состояние конфигурации**. Показывает, правильно ли настроено устройство.
   - **Состояние синхронизации политик**. Показывает, обновлено ли устройство до последней версии политики. Для обновления до последней политики устройства должны быть включено.

Дальнейшие действия

Дополнительные сведения о Microsoft Purview см. в статье Сведения о Microsoft Purview.

Дополнительные сведения о параметрах захвата судебно-медицинских доказательств Microsoft Purview см. в разделе Параметры захвата.

Дополнительные сведения о емкости и выставлении счетов Microsoft Purview см. в разделе Емкость и выставление счетов.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Настройка политик условного доступа

09.09.2025

Условный доступ — это защита регулируемого содержимого в системе путем контроля выполнения определенных условий перед предоставлением доступа к содержимому. Простейшие политики условного доступа — это конструкции типа "если-то". Если пользователь хочет получить доступ к ресурсу, то он должен выполнить какое-то действие. Например, менеджер по заработной плате хочет получить доступ к приложению для расчета заработной платы и должен выполнить многофакторную проверку подлинности (MFA) для этого.

С помощью условного доступа можно достичь двух основных целей:

- Предоставить пользователям возможность работать в любом месте в любое время.
- Защитить активы своей организации.

С помощью политик условного доступа можно применять нужные элементы управления доступом, чтобы в нужных случаях защищать организацию, но не мешать пользователям, когда слишком строгая защита не нужна.

Частота запроса пользователя на повторную проверку подлинности зависит от Microsoft Entra политик адаптивного времени существования сеанса условного доступа. Хотя запоминать учетные данные удобно, это также может сделать развертывания для корпоративных сценариев с использованием личных устройств менее безопасными. Чтобы защитить пользователей, вы можете убедиться, что клиент чаще запрашивает Microsoft Entra учетные данные многофакторной проверки подлинности. Для настройки этого поведения можно использовать частоту входа условного доступа.

Назначение политики условного доступа для Облачных компьютеров

Политики условного доступа не заданы для вашего клиента по умолчанию. Вы можете нацеливать политики ЦС на собственное приложение облачного компьютера, используя одну из следующих платформ:

- Azure. Дополнительные сведения см. в разделе условный доступ Microsoft Entra.
- Microsoft Intune. Этот процесс описан ниже. Дополнительные сведения см. в статье Сведения об условном доступе и Intune.

Какой бы метод вы ни использовали, политики будут применены для портала конечного пользователя Облачного компьютера и подключения к Облачному компьютеру.

1. Войдите в Центр администрирования Microsoft Intune, выберите **Безопасность конечных**> точек**Условный доступ**>**Создать политику**.

2. Укажите **имя** для конкретной политики условного доступа.

3. В разделе **Пользователи** выберите **0 выбранных пользователей и групп**.

4. На вкладке **Включить** выберите **Выбрать пользователей и группы**> проверка **Пользователи и группы**> в разделе **Выбрать**, выберите **0 выбранных пользователей и групп**.

5. На открывающейся новой панели найдите и выберите конкретного пользователя или группу, для которого вы хотите нацелиться с помощью политики ЦС, а затем нажмите **кнопку Выбрать**.

6. В разделе **Целевые ресурсы** выберите **Не выбраны целевые ресурсы**.

7. На вкладке **Включить** выберите **Выберите приложения**> в разделе **Выбрать**, а затем — **Нет**.

8. В области **Выбор** найдите и выберите следующие приложения в зависимости от ресурсов, которые вы пытаетесь защитить:

   - **Windows 365** (идентификатор приложения 0af06dc6-e4b5-4f28-818e-e78e62d137a5). Для некоторых клиентов это приложение может называться **облачным компьютером**. Это приложение используется при получении списка ресурсов для пользователя и при запуске пользователем действий на своем облачном компьютере, таких как перезапуск.
   - **Виртуальный рабочий стол Azure** (идентификатор приложения 9cdead84-a844-4324-93f2-b2e6bb768d07). Это приложение также может отображаться как **Виртуальный рабочий стол Windows**. Это приложение используется для проверки подлинности в шлюзе Виртуальных рабочих столов Azure во время подключения и при отправке клиентом диагностических сведений в службу.
   - **Вход в Облако Windows** (идентификатор приложения 270efc09-cd0d-444b-a71f-39af4910ec45). Это приложение необходимо только при настройке единого входа в политике подготовки. Это приложение используется для проверки подлинности пользователей на облачном компьютере.

   Рекомендуется сопоставлять политики условного доступа между этими приложениями. Сопоставление гарантирует, что политика применяется к порталу конечного пользователя облачного компьютера, подключению к шлюзу и облачному компьютеру для согласованного взаимодействия. Если вы хотите исключить приложения, необходимо также выбрать все эти приложения.

> **Примечание**
>
> Если приложение Windows Cloud Login не отображается при настройке политики условного доступа, выполните следующие действия, чтобы создать приложение. Чтобы внести следующие изменения, необходимо иметь разрешения владельца или участника в подписке:
>
> a. Войдите в **портал Azure**.
>
> b. Выберите **Подписки** в списке Служб Azure.
>
> c. Выберите имя подписки.
>
> d. Выберите **Поставщики ресурсов** , а затем — **Microsoft.DesktopVirtualization**.
>
> e. Выберите **Зарегистрировать** в верхней части окна.
>
> После регистрации поставщика ресурсов приложение Windows Cloud Login отображается в конфигурации политики условного доступа при выборе приложений для применения политики. Если вы не используете Виртуальный рабочий стол Azure, вы можете отменить регистрацию поставщика ресурсов Microsoft.DesktopVirtualization после того, как приложение Windows Cloud Login будет доступно.

9. Если вы хотите настроить политику, в разделе **Предоставление** выберите **0 выбранных элементов управления**.

10. На панели **Предоставление** выберите параметры предоставления или блокировки доступа, которые нужно применить ко всем объектам, назначенным этой политике >**Выберите**.

11. Если вы хотите сначала протестировать политику, в разделе **Включить политику** выберите **Только отчет**. Если задать для него значение **Включено**, политика будет применена сразу после ее создания.

12. Выберите **Создать**, чтобы создать политику.

Список активных и неактивных политик можно просмотреть в представлении **Политики** в пользовательском интерфейсе условного доступа.

Настройка частоты входа

Политики частоты входа позволяют настроить частоту входа пользователей при доступе к ресурсам на основе Microsoft Entra. Эта конфигурация может помочь защитить среду и особенно важна для личных устройств, где локальная ОС может не требовать MFA или не может автоматически блокироваться после бездействия. Пользователям предлагается

пройти проверку подлинности только при запросе нового маркера доступа у Microsoft Entra ID при доступе к ресурсу.

Политики частоты входа приводят к по-разному в зависимости от выбранного Microsoft Entra приложения:

Развернуть таблицу

Название приложения	ИД приложения;	Поведение
Windows 365	0af06dc6-e4b5-4f28-818e-e78e62d137a5	Обеспечивает повторную проверку подлинности, когда пользователь получает свой список облачных компьютеров и когда пользователи инициируют действия на своем облачном компьютере, такие как перезапуск.
Виртуальный рабочий стол Azure	9cdead84-a844-4324-93f2-b2e6bb768d07	Принудительно выполняет повторную проверку подлинности, когда пользователь проходит проверку подлинности в Шлюзе Виртуальных рабочих столов Azure во время подключения.
Вход в Windows Cloud	270efc09-cd0d-444b-a71f-39af4910ec45	Принудительно выполняет повторную проверку подлинности при входе пользователя в облачный компьютер при включенном едином входе .

Чтобы настроить период времени, по истечении которого пользователю будет предложено повторно выполнить вход, выполните следующие действия:

1. Откройте политику, созданную ранее.
2. В разделе **Сеанс** выберите **0 выбранных элементов управления**.
3. В области **Сеанс** выберите **Частота входа**.
4. Выберите **Периодическая повторная проверку подлинности** или **Каждый раз**.

    - Если выбран параметр **Периодическая повторная проверка подлинности**, задайте значение для периода времени, по истечении которого пользователю будет предложено выполнить вход еще раз при выполнении действия, требующего нового маркера доступа, а затем нажмите кнопку **Выбрать**. Например, если установить значение **1** , а единице — **Часы**, требуется многофакторная проверка подлинности, если подключение запускается более чем через час после последней проверки подлинности пользователя.
    - Параметр Каждый раз поддерживается только при применении к приложению **Windows Cloud Login** , если для облачных компьютеров включен единый вход. При выборе **параметра Каждый раз** пользователям будет предложено

выполнить повторную проверку подлинности при запуске нового подключения через период от 5 до 10 минут с момента последней проверки подлинности.

5. В нижней части страницы нажмите кнопку **Сохранить**.

> ⓘ **Примечание**
>
> - Повторная проверка подлинности происходит только в том случае, если пользователь должен пройти проверку подлинности в ресурсе и требуется новый маркер доступа. После установки подключения пользователям не будет предложено, даже если подключение длится дольше, чем настроенная частота входа.
> - Пользователи должны пройти повторную проверку подлинности, если сеть перебоев в работе, в результате чего сеанс будет восстановлен после настройки частоты входа. Такая повторная проверка подлинности может привести к более частым запросам проверки подлинности в нестабильных сетях.

Дальнейшие действия

Управление перенаправлениями устройств RDP

Настройка единого входа для Windows 365 с помощью проверки подлинности Microsoft Entra

02.10.2025

В этой статье описывается процесс настройки единого входа (SSO) для Windows 365 с помощью Microsoft Entra проверки подлинности. При включении единого входа для входа на облачный компьютер можно использовать проверку подлинности без пароля и сторонние поставщики удостоверений, федеративные с идентификатором Microsoft Entra. Если эта функция включена, она обеспечивает единый вход как при проверке подлинности на облачном компьютере, так и в сеансе при доступе к приложениям и веб-сайтам на основе идентификаторов Microsoft Entra.

Сведения об использовании проверки подлинности без пароля в сеансе см. в разделе Проверка подлинности без пароля в сеансе.

Чтобы приступить к работе, выполните действия по настройке единого входа для Виртуального рабочего стола Azure со следующими предупреждениями:

- Если объект Kerberos Server отсутствует для Microsoft Entra политик подготовки с гибридным присоединением, в проверка работоспособности сетевого подключения Azure (ANC) для единого входа появится новая ошибка.
- Если у вас есть политики условного доступа, которые применяются при доступе к Windows 365, ознакомьтесь с рекомендациями по настройке политик условного доступа для Windows 365, чтобы убедиться, что пользователи имеют ожидаемые возможности.
- Единый вход можно включить для любых политик подготовки. Параметр **Использовать единый вход Microsoft Entra** можно найти в **разделе Тип присоединения** на странице **Общие**. Это можно сделать при создании новой политики подготовки или при изменении существующей политики подготовки с возможностью применения единого входа к существующим облачным компьютерам.
- При подготовке компьютеров Frontline Cloud в режиме общего доступа скройте запрос согласия , чтобы пользователи не видели его на каждом общем устройстве. Для область этой конфигурации можно использовать динамическую группу устройств на основе имени политики подготовки.
- При подготовке облачных компьютеров для внешних удостоверений требуется единый вход. Если единый вход не настроен, пользователи не смогут завершить вход на облачный компьютер.

Дальнейшие действия

- Сведения о включении проверки подлинности без пароля см. в разделе Проверка подлинности без пароля в сеансе .

Подготовка облачных компьютеров для внешних удостоверений (предварительная версия)

В этой статье описывается процесс предоставления облачных компьютеров внешним удостоверениям.

Этот компонент находится в состоянии общедоступной предварительной версии.

Предварительные требования

Перед подготовкой облачных компьютеров ознакомьтесь с требованиями и ограничениями для внешних удостоверений.

Подготовка облачных компьютеров для внешних удостоверений

Подготовка облачных компьютеров для внешних удостоверений

1. Выполните действия, описанные в разделе Настройка единого входа для Windows 365 с помощью проверки подлинности Microsoft Entra, чтобы:
   a. Убедитесь, что в клиенте включен единый вход.
   b. (Необязательно) Скрыть запрос на согласие.
2. Выполните действия, описанные в разделе Создание политик подготовки со следующими конфигурациями:
   a. На странице Общие выберите **тип соединения Microsoft Entra Присоединиться**.
   b. На странице Общие проверка поле **Использовать единый вход Microsoft Entra**.
   c. На странице Образ выберите образ под управлением поддерживаемой ОС (определенные в требованиях и ограничениях для внешних удостоверений).
   d. На странице Назначения выберите Microsoft Entra группу пользователей, содержащую внешние удостоверения.

Подключение к облачным компьютерам с помощью внешнего удостоверения

Выполните действия, описанные в разделе Управление учетными записями пользователей в Windows App, чтобы войти в поддерживаемый клиент Windows App с внешним удостоверением и подключиться к облачному компьютеру.

Дальнейшие действия

- Сведения о настройке политик условного доступа для внешних удостоверений см. в статье Настройка политик условного доступа.

Last updated on 07.11.2025

Приложения в Windows 365

Статья • 31.01.2025

ИТ-администратор может легко начать работу с Windows 365 путем создания облачных компьютеров с помощью стандартных образов Windows 10/11 Корпоративная из коллекции. После подготовки вы можете настроить взаимодействие с пользователем, используя Microsoft Intune для отправки приложений на облачные компьютеры пользователей. Эти образы могут включать существующие клиентские приложения Windows, которые уже находятся в Microsoft Intune среде. Так как эти облачные компьютеры зарегистрированы в Intune, вы можете обрабатывать их как любое другое устройство Windows в вашей среде.

Следующие приложения доступны без дополнительной отправки:

- Приложения Microsoft 365 для предприятий (ранее Office 365 Pro Plus)
- Microsoft Teams
- Microsoft OneDrive
- Microsoft Edge

Поддерживаемые форматы приложений в Windows 365

.IntuneWin

Формат IntuneWin — это способ предварительной обработки классических приложений Windows (Win32). Это средство преобразует файлы установки приложения в формат intunewin.

После использования этого средства в папке установщика приложений вы можете создать конфигурацию регистрации приложений для расширенных возможностей развертывания. Например, зависимости версий ОС и методы удаления, когда необходимо удалить приложения удаленно.

Если выбрать наиболее распространенный формат приложения (Win32), необходимо инкапсулировать EXE- или MSI-файл в файл IntuneWin. Эта инкапсуляция необходима для Windows 365 в рамках набора конфигурации приложения.

MSI

Параметры бизнес-приложений и приложений для Windows (win32) в Intune поддерживают установщики формата MSI. Последний вариант лучше адаптирован для зависимостей приложений.

MSIX

MSIX — это новый формат пакетов приложений для Windows от Майкрософт для упаковки всех приложений для Windows современным способом. Формат пакета MSIX сохраняет функциональные возможности существующих пакетов приложений и устанавливает файлы. Он также обеспечивает новые современные функции упаковки и развертывания для приложений Win32, WPF и Windows Forms.

MSIX сочетает лучшие функции MSI, AppX и App-V.

AppX

Также известны как современные приложения (UWP). Файлы с расширением AppX готовы к распространению и установке.

В магазине Windows в составе Windows 10/11 Корпоративная приложения автоматически распространяются в формате AppX – UWP.

AppX упрощает распространение приложений, поддерживаемых для нескольких устройств, включая ПК, планшеты и смартфоны, работающие на Windows.

Office

Облачные компьютеры Windows 365 поддерживают Office только в версии Приложений Microsoft 365. Дополнительные сведения о различиях между Приложениями Microsoft 365 и другими версиями Office см. в статье О Приложениях Microsoft 365 на предприятии.

Универсальная печать

Универсальная печать — это современное решение печати, которое упрощает организациям работу с инфраструктурой печати через облачные службы от Майкрософт. Универсальную печать можно использовать с Windows 365 Корпоративная нативно или через одного из партнеров Универсальной печати.

Устаревшие среды серверов печати также можно использовать вместе с Windows 365.

Сведения о требованиях Универсальной печати см. в статье о средстве подготовки принтера Универсальной печати.

Сведения о настройке универсальной печати с Windows 365 Корпоративная конфигурацией гибридной Microsoft Entra см. в статье Включение гибридной среды AD и среды Azure AD для универсальной печати.

Дальнейшие действия

Назначение приложений для облачных компьютеров

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

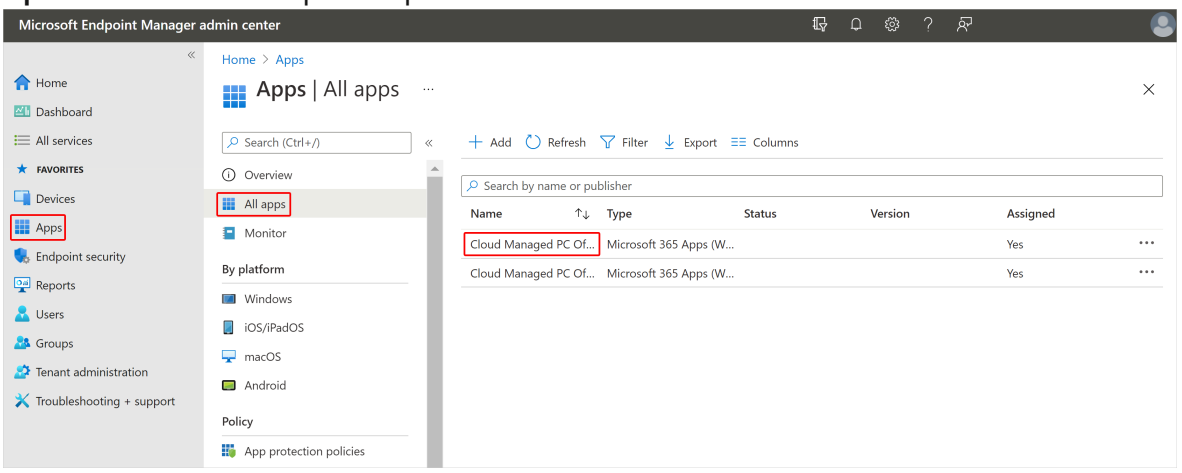
Отзыв о продукте

Назначение приложений облачным компьютерам

Статья • 31.01.2025

Выполните следующие действия, чтобы развернуть приложения Windows 10 Intune на облачных компьютерах.

1. Войдите вцентр >администрирования Microsoft Intune Приложения >**Все приложения**> выбирают приложение.



2. На странице приложения выберите **Свойства**>**Изменить** (рядом с разделом **Назначения**).
3. На странице **Назначения** выберите **Добавить группу** (в разделе **Обязательный**).
4. В области **Выбор групп** выберите группы, которым требуется назначить это приложение>, **выберите**>**Просмотр и сохранение**.
5. На странице **Проверка и сохранение** нажмите кнопку **Сохранить**.

Дальнейшие действия

Узнайте об управлении устройствами для облачных компьютеров.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

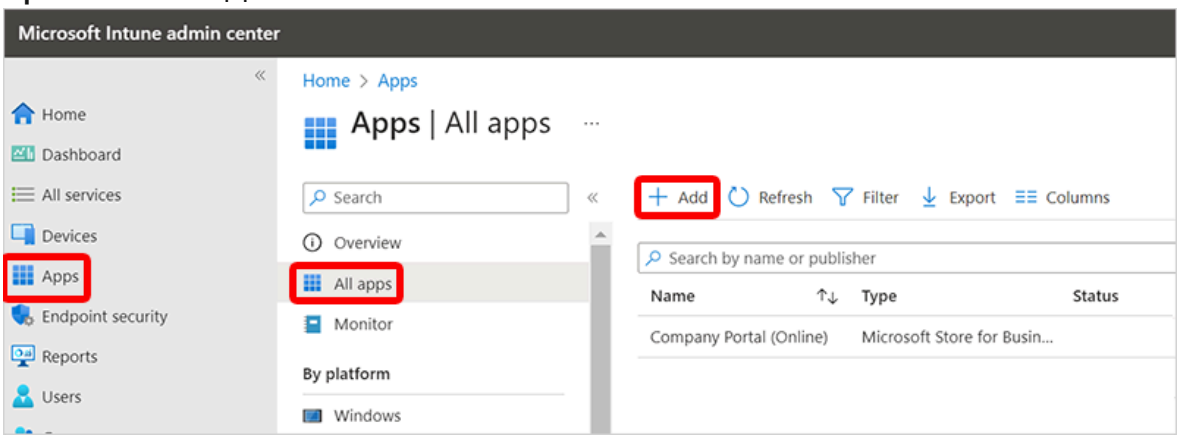
Отзыв о продукте

Использование Intune, установка Windows App на физических устройствах

Статья • 31.01.2025

У некоторых пользователей могут быть физические устройства, у которых нет доступа к Microsoft Store для установки приложения Для Windows. В таких случаях приложение Windows можно установить на свои устройства с помощью Intune процесса назначения приложений. Назначив приложение группам устройств, вы можете автоматически установить Windows App на их устройствах.

1. Войдите в центр >администрирования Microsoft Intune Приложения >**Все приложения**> Добавить.



2. В области **Выбор типа приложения** в поле **Тип приложения** выберите **Приложение Microsoft Store (новое)**>**Выбрать**.
3. На странице **Добавление приложения** выберите **Поиск в приложении Microsoft Store (новое),** найдите **приложение Windows** и нажмите > кнопку **Выбрать**.
4. На странице **Сведения о приложении** можно оставить все параметры без изменений или изменить их >**Далее**. Дополнительные сведения об этих параметрах см. в статье Добавление приложений Microsoft Store в Microsoft Intune.
5. (Необязательно) На странице **Теги области** можно использовать теги область, чтобы обеспечить правильный доступ и видимость для Intune объектов соответствующим администраторам. Дополнительные сведения о тегах областей см. в статье Использование управления доступом на основе ролей (RBAC) и тегов области для распределенных ИТ. Нажмите кнопку **Далее**.
6. На странице **Назначения** добавьте группы устройств и (или) пользователей, содержащие облачные компьютеры, на которых необходимо автоматически установить Windows App. Если вы нацелены на группу пользователей, перед

установкой приложения пользователи должны сначала войти на свой облачный компьютер. Если вы нацелены на группу устройств, приложение устанавливается до входа пользователя.

   a. В разделе **Обязательно** выберите **Добавить группу** и добавьте группы, содержащие физические устройства, на которых вы хотите автоматически установить Windows App.
   b. В разделе **Доступно для зарегистрированных устройств** выберите **Добавить группу** и добавьте группы пользователей. Windows App отображается в приложении и веб-сайте Корпоративный портал для установки пользователей при необходимости.
   c. Выбрав все группы, нажмите кнопку **Далее**.
7. На странице **Проверка и создание** нажмите кнопку **Создать**.

Блокировка доступа к Microsoft Store

Если вы хотите запретить пользователям доступ к Microsoft Store, создайте политику профиля конфигурации каталога параметров. В **окне выбора параметров** найдите **Microsoft App Store** и выберите **Требовать только частный магазин**.

Дополнительные сведения об использовании каталога параметров для создания политики профиля конфигурации см. в статье Использование каталога параметров для настройки параметров на устройствах Windows и macOS.

Дальнейшие действия

Узнайте больше о добавлении приложений на устройства с помощью Intune.

Узнайте об управлении устройствами для облачных компьютеров.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Microsoft Teams на обласном компьютере

Статья • 31.01.2025

Microsoft Teams является одним из основных приложений Microsoft 365, используемых в Windows 365. Образы Microsoft 10/11, оптимизированные для приложений Windows 365, доступны в коллекции образов Windows 365 и поддерживают оптимизации чата, присутствия, звонков и собраний Teams. Образы из коллекции используют новую версию Microsoft Teams.

Использование Microsoft Teams на облачном компьютере отличается от использования Teams на физическом ПК. Для оптимальной работы Teams на облачных компьютерах выполните следующие действия.

- Ознакомьтесь с требованиями и ограничениями для использования Microsoft Teams в виртуализированных средах.
- Подготовьте сеть к Microsoft Teams.
- Убедитесь, что установлены необходимые компоненты для оптимизаций Microsoft Teams.
- Проверьте соответствие требованиям к определению размера облачных компьютеров для Microsoft Teams.
- Проверьте соответствие требованиям к оборудованию конечных пользователей для Microsoft Teams.

Оптимизации Teams

Образы Windows 10/11 в коллекции предварительно настроены с помощью необходимых компонентов оптимизации. При установке и использовании новой microsoft Teams на облачном компьютере вы получаете оптимизированный интерфейс. Эти компоненты оптимизации позволяют совершать одноранговые аудио- и видеозвонки от физической конечной точки до конечной точки другого человека. При этом взаимодействие происходит так же, как на физической конечной точке, где запущена служба Microsoft Teams.

Ниже перечислены некоторые основные преимущества оптимизаций.

- Высокопроизводительная одноранговая потоковая передача, поддерживаемая WebRTC и напрямую отображаемая конечной точкой.
- Устройства перенаправляются как одно и то же устройство, что обеспечивает лучшую поддержку аппаратного перенаправления.

- Конечные точки Windows 10/11 и macOS получают все преимущества современного стека мультимедиа, включая аппаратное декодирование видео.
- Оптимизация Teams VDI 2.0 в настоящее время не поддерживается для macOS.

Поддерживаемые конечные точки

Оптимизация мультимедиа для Microsoft Teams доступна только для конечных точек Windows и macOS. Для оптимизации мультимедиа требуется:

- Windows App для Windows через Microsoft Store (в идеале — последняя версия).
- Клиент удаленного рабочего стола для Windows версии 1.2.1026.0 или более поздней (в идеале — последняя версия).
- Клиент удаленного рабочего стола для macOS версии 10.7.7 или более поздней (бета-версия клиента). При обновлении с версий, предшествующих 10.7.7, необходимо также перейти в раздел **Настройки удаленного рабочего стола (Майкрософт)**>**Общие** и включить оптимизацию Teams. Если клиент используется впервые и у вас уже установлена версия 10.7.7 или более поздняя, вам не потребуется ее включать. В этом случае оптимизация Teams включена по умолчанию.

> **Примечание**
>
> Microsoft Teams устанавливается во время первого входа на облачный компьютер. Установка может занять несколько минут. Чтобы активировать оптимизацию AV, перенаправляющую аудио и видео, обязательно перезапустите Teams. Также можно выйти из системы облачного компьютера и снова войти в нее.

Сбор журналов Teams для службы поддержки Майкрософт

При возникновении проблем с классическим приложением Teams в среде Windows 365 соберите журналы клиентов на Облачном компьютере в

```
%appdata%\Microsoft\Teams\logs.txt
```

При возникновении проблем со звонками и собраниями соберите журналы веб-клиента Teams с помощью сочетания клавиш CTRL + ALT + SHIFT + 1. Журналы будут записаны на Облачном компьютере в

```
%userprofile%\Downloads\MSTeams Diagnostics Log DATE_TIME.txt
```

Обращение в службу поддержки Microsoft Teams

Сведения о том, как связаться со службой поддержки Microsoft Teams, см. в статье о центре администрирования Microsoft 365.

Дальнейшие действия

Назначение приложений облачному компьютеру.

Сведения об известных проблемах, ограничениях и способах регистрации проблем см. в статье Устранение неполадок Teams на Виртуальном рабочем столе Azure.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Создание пользовательского образа облачного компьютера с поддержкой Microsoft Teams

Статья • 06.05.2025

Во время первоначальной настройки клиента рекомендуется подготавливать облачные компьютеры с помощью образов Windows 10/11 Корпоративная и Microsoft 365, доступных в коллекции образов. Эти образы предоставляют преимущество оптимизации и предварительной установки всех приложений Office без необходимости в дополнительном уровне конфигурации.

Если вы хотите создать пользовательские образы, не включающие оптимизации для Microsoft Teams, необходимо выполнить в пользовательском образе следующие действия. Эти действия гарантируют правильность параметров и политик реестра образа для поддержки Teams.

Следующие действия необходимы только в том случае, если не используются образы из коллекции Windows 365 с предварительной установкой Microsoft 365. Для создания пользовательского образа вы также можете использовать образ из коллекции. В этом случае вам не потребуется выполнять действия ниже.

1. Создайте следующий раздел реестра, необходимый для пользовательских образов, в HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Teams:

   - Имя: IsWVDEnvironment
   - Тип: DWORD
   - Значение: 1

2. Установите последнюю версию среды выполнения Visual C++. Эта среда выполнения необходима для работы перенаправления протокола WebRTC Teams.
3. Установите подключаемый модуль перенаправителя WebRTC (websocket). Инструкции по установке см. в разделе Установка службы WebSocket Teams. Подключаемый модуль необходим для правильной работы Teams в среде облачного компьютера с оптимизацией.

> **Примечание**
>
> Не устанавливайте приложение Microsoft Teams для компьютера. Если вы хотите использовать Microsoft Teams на облачном компьютере, установите Приложения Microsoft 365 и Teams с помощью Microsoft Intune.

Убедитесь в успешной загрузке оптимизаций Teams.

Если необходимо проверить работу оптимизаций Teams на облачном компьютере (например, для пользователя), сообщите пользователю облачного компьютера о необходимости выполнить следующие действия.

1. В Microsoft Teams выберите многоточие (**...**) в строке > меню **О**>**версии**.
2. Убедитесь в том, что рядом с версией отображается фраза **WVD Media Optimized** (Оптимизировано для мультимедиа WVD). Если это так, можно приступать к тестированию улучшенного интерфейса.

Если оптимизации мультимедиа загружены, то доступные локально звуковые устройства и камеры будут указаны в меню устройства. Если в меню отображается **Удаленный звук**, выполните следующие действия.

1. Закройте приложение Teams и повторите попытку.
2. Если устройства по-прежнему не отображаются в меню, проверьте **параметры конфиденциальности** на локальном компьютере. Убедитесь, что для параметра **Разрешить приложениям доступ к микрофону** (в разделе **Параметры**>**Конфиденциальность**>**Разрешения приложения — микрофон**) установлено значение **Вкл.**.
3. Отключение от удаленного сеанса
4. Отсоедините видео- и звуковое устройства и повторите проверку.

Чтобы присоединяться к звонкам и собраниям с видео, необходимо также предоставить приложениям разрешение на доступ к камере.

Дальнейшие действия

Назначение приложений для облачных компьютеров

Настройка поддержки рабочих нагрузок на основе виртуализации

Статья • 31.01.2025

Рабочие нагрузки на основе виртуализации дают клиентам возможность использовать следующие системы на облачных компьютерах Windows 365 Корпоративная:

- Подсистема Windows для Linux (WSL)
- Подсистема Windows для Android
- Песочница
- Hyper-V

Требования

Для использования рабочих нагрузок на основе виртуализации, облачный компьютер должен соответствовать следующим требованиям:

- Облачный компьютер с 4-м ЦП или более поздней (уменьшение размера до 2-х виртуальных ЦП приведет к отключению вложенной виртуализации).
- Подготовка в одном из поддерживаемых регионов для Windows 365. (В настоящее время в северной части Южной Африки вложенная виртуализация не поддерживается.
- Некоторые пользователи могут столкнуться с снижением производительности облачных компьютеров с 4vCPU при использовании вложенной виртуализации. Дополнительные сведения об устранении таких проблем с производительностью см. в разделе Устранение неполадок.

Облачные компьютеры GPU не поддерживают вложенную виртуализацию.

Настройка рабочих нагрузок на основе виртуализации

Сведения о настройке системы рабочих нагрузок на основе виртуализации см. в следующих статьях:

- Настройка среды разработки WSL.
- Подсистема Windows для Android™ .
- Установка Hyper-V в Windows 10.

Дальнейшие действия

Дополнительные сведения о рабочих нагрузках на основе виртуализации см. в статье Запуск Hyper-V на виртуальной машине с вложенной виртуализацией.

Если при вложенной виртуализации возникают проблемы с производительностью, см. статью Устранение неполадок.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

App Assure помогает решать проблемы с приложениями на Облачных компьютерах

Статья • 31.01.2025

App Assure — это служба, которая помогает клиентам решать проблемы с приложениями на Облачных компьютерах. Если у вас возникли проблемы с приложениями, Майкрософт поможет вам устранить их бесплатно.

Приложение Assure доступно для соответствующих клиентов без дополнительной платы. Дополнительные сведения о критериях бесплатного предоставления см. в разделе Критерии.

Посетите страницу App Assure и войдите, чтобы отправить запрос на помощь выделенного менеджера App Assure. Если при отправке запроса возникают проблемы, свяжитесь с ACHELP@microsoft.com вами, и члены нашей команды свяжутся с вами.

App Assure входит в состав преимущества FastTrack в Microsoft 365.

Дальнейшие действия

Назначение приложений для облачных компьютеров

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Оптимизация Cisco Webex для Облачного компьютера Windows 365

Статья • 31.01.2025

Cisco Webex — это стороннее приложение, предоставляющее возможности проведения виртуальных собраний, в том числе в виртуализированных средах, таких как Облачные компьютеры Windows 365. Инструкции в этой статье помогут вам оптимизировать трафик для собраний Cisco Webex при использовании клиента Удаленного рабочего стола (Майкрософт) на компьютере с Windows, используемого для доступа к Облачному компьютеру.

Чтобы оптимизировать Cisco Webex, необходимо:

- Установить клиент VDI Cisco Webex на Облачный компьютер.
- Установить подключаемый модуль VDI Webex App на локальный компьютер с Windows, который будет использоваться для доступа к Облачному компьютеру.

> **Примечание**
>
> В случае возникновения проблем с Cisco Webex для VDI на Облачном компьютере обратитесь в службу поддержки Cisco.

Требования

Эти инструкции не поддерживают подключения через веб-браузер.

- **Windows App**
- **Клиент удаленного рабочего стола Windows**
- **Операционная система**: Windows

Установка клиента HVD Cisco Webex на Облачном компьютере

1. Войдите на Облачный компьютер как локальный администратор и в браузере перейдите на страницу загрузки Webex VDI.
2. В столбце **Дата выпуска** таблицы перейдите к самой последней дате (например, 14.12.2021).

3. Выберите соответствующую ссылку для вашей системы Windows (32-разрядная или 64-разрядная), чтобы скачать MSI.
4. Для установки компонентов VDI необходимо установить необходимые переключатели. Итак, чтобы запустить MSI-файл, откройте командную строку с повышенными правами и выполните следующую команду установки. Замените путь и имя MSI-файла на путь и имя файла, который вы скачали.
   `msiexec /i %path%\Webex.msi ALLUSERS=1 ENABLEVDI=1 AUTOUPGRADEENABLED=0`
5. Чтобы завершить установку MSI, следуйте соответствующим инструкциям.

Кроме того, развернуть клиент VDI Cisco Webex может администратор. Дополнительные сведения о развертывании приложений см. в руководстве по управлению приложениями Win32.

Установка плагина на локальном компьютере Windows

1. Войдите в компьютер с Windows, который будет использоваться для доступа к Облачному компьютеру.
2. В браузере перейдите на страницу загрузки Webex VDI.
3. В таблице найдите строку с тем же выпуском, который был установлен на облачном компьютере. Выберите соответствующую ссылку на подключаемый модуль **, 32-разрядную** или **64-разрядную версию Windows**.
4. Запустите MSI и следуйте инструкциям по установке.

Дополнительные инструкции по установке см. в руководстве Cisco по развертыванию Webex App для инфраструктуры виртуальных рабочих столов.

Использование оптимизированного клиента Cisco Webex

Чтобы воспользоваться преимуществами оптимизации, пользователи должны войти на свой Облачный компьютер с компьютера с Windows. После этого пользователь может открыть Cisco Webex на Облачном компьютере и использовать клиент WebEx, оптимизированный для Облачного компьютера Windows 365.

Подтверждение, что клиент Cisco Webex использует настройки оптимизации

1. Войдите в Облачный компьютер с помощью клиента Windows.
2. Откройте клиент Cisco Webex и войдите в систему, используя соответствующие учетные данные.
3. Выберите значок > профиля пользователя **Справка**>**по проверке работоспособности**.
4. В разделе VDI **Проверки работоспособности** отображается состояние параметров оптимизации.

Дальнейшие действия

Дополнительные сведения о развертывании приложений см. в руководстве по управлению приложениями Win32.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Оптимизация Zoom на Облачном компьютере Windows 365

Статья • 31.01.2025

Zoom — это стороннее приложение для проведения онлайн-собраний, включая поддержку виртуализированных сред, таких как Облачные компьютеры Windows 365. Инструкции в этой статье помогут вам оптимизировать трафик для собраний Zoom при использовании клиента Удаленного рабочего стола (Майкрософт) на компьютере с Windows для доступа к Облачному компьютеру.

Чтобы оптимизировать Zoom, необходимо установить клиент Zoom VDI на Облачном компьютере и плагин Виртуального рабочего стола Azure для Zoom на локальном компьютере с Windows, с помощью которого пользователь будет работать с Облачным компьютером.

> ⓘ **Примечание**
>
> Если на облачном компьютере у вас возникают проблемы с Zoom для VDI, свяжитесь со службой поддержки Zoom.

Требования

- **Клиент удаленного рабочего стола Windows***
- **Windows App**
- **Операционная система**: Windows

* Они не поддерживают подключения через веб-браузер.

Установка клиента Zoom VDI на Облачном компьютере

1. Попросите пользователя войти в Облачный компьютер в качестве локального администратора и в браузере перейдите на страницу загрузок Zoom VDI и обратной совместимости.
2. Найдите и скачайте последнюю версию клиента VDI.
3. Запустите MSI и следуйте инструкциям по установке.

Также клиент VDI Zoom может развернуть администратор. Дополнительные сведения о развертывании приложений см. в руководстве по управлению приложениями Win32.

Установка плагина на локальном компьютере Windows

1. Войдите в компьютер с Windows, который будет использоваться для доступа к Облачному компьютеру.
2. В браузере перейдите на страницу версий выпуска VDI, соответствующую странице, которую вы использовали для установки клиента VDI. Например, VDI release версии 5.16.6.
3. В таблице **Совместимые подключаемые модули** найдите установленный клиент VDI и выберите соответствующую запись для **Виртуального рабочего стола Azure**. Например, **Windows x86 или x64 (телефон и собрания): 5.8.4.21112**. Для этих оптимизаций поддерживаются только клиенты Windows.
4. Запустите MSI и следуйте инструкциям по установке.

> **Примечание**
>
> Zoom рекомендует использовать одинаковые номера версий как для клиента VDI, так и для плагина. Zoom не поддерживает запуск плагина, версия которого выше версии клиента VDI.

Дополнительные сведения об этих шагах установки см. в статье Zoom Начало работы с VDI.

Использование оптимизированного клиента Zoom

Чтобы воспользоваться преимуществами оптимизации, пользователи должны войти на свой Облачный компьютер с компьютера с Windows. После этого пользователи смогут открыть Zoom с Облачного компьютера.

Дальнейшие действия

Дополнительные сведения о развертывании приложений см. в руководстве по управлению приложениями Win32.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Copilot в Intune для Windows 365

18.09.2025

Microsoft Copilot в Intune поддерживает Windows 365, что позволяет получать аналитические сведения для облачных компьютеров, включая сетевое подключение, использование лицензий и рекомендуемые улучшения производительности.

- **Copilot в Intune для Windows 365** доступен через Центр администрирования Microsoft Intune. Запросы Copilot и их выходные данные находятся в контексте Windows 365 и ваших Windows 365 данных. Этот функционал ориентирован на ИТ-администраторов или ИТ-специалистов.
- **Microsoft Security Copilot** — это автономное средство, предоставляемое на портале Microsoft Security Copilot. Этот параметр предоставляет аналитические сведения в различных службах, таких как Windows 365, Intune, Microsoft Defender, идентификатор Microsoft Entra и Microsoft Purview. Это средство в основном предназначено для использования Центра управления безопасностью (SOC), но также может быть доступно ИТ-администраторам. Дополнительные сведения см. в статье Доступ к данным Microsoft Intune в Security Copilot.

В этой статье объясняется, как получить доступ к Windows 365 интеграции с Copilot в чате Intune.

Подготовка к работе

Включение Copilot в Microsoft Intune

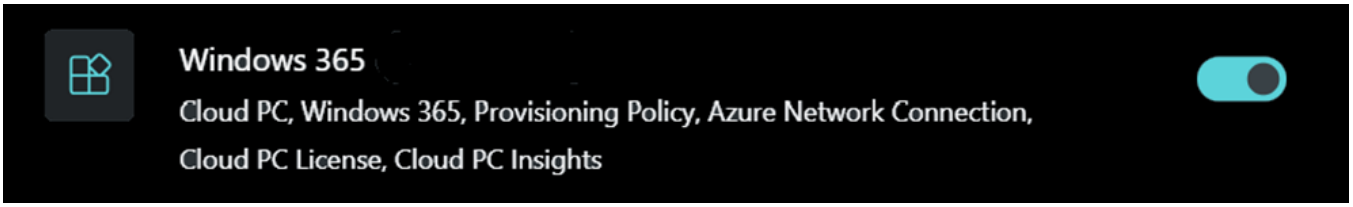
Чтобы получить доступ к Copilot в Intune для Windows 365 функций, убедитесь, что включено приложение Copilot в Microsoft Intune. Чтобы приступить к работе, ознакомьтесь с обзором Microsoft Copilot в Intune.

Подключаемый модуль Windows 365

Чтобы использовать Copilot в Microsoft Intune, требуется подключаемый модуль Windows 365, включенный в Security Copilot. Этот подключаемый модуль позволяет получать доступ к данным Windows 365 и использовать Copilot в Intune для Windows 365 возможностей в Центре администрирования Intune.

Перейдите на портал Security Copilot и выберите **Источники** (строка запроса > в правом углу).

В **разделе Управление источниками** включите Windows 365.



> **Совет**
>
> Некоторые роли могут включать или отключать подключаемые модули. Дополнительные сведения см. в статье Управление подключаемыми модулями в Microsoft Security Copilot.

- **Данные Windows 365**. Copilot использует данные Windows 365. Когда администратор Windows 365 отправляет запрос, Copilot может получить доступ только к данным, на которые у него есть разрешения, включая роли RBAC и область теги, назначенные ему.

> **Совет**
>
> Некоторые распространенные вопросы, задаваемые о Copilot в Intune, см. в статье часто задаваемые вопросы Microsoft Copilot в Intune.

Возможности

Copilot в Intune для Windows 365 объединяет рекомендации по использованию ИИ и Майкрософт по управлению облачными компьютерами, чтобы получить аналитические сведения о подключении, производительности облачных компьютеров и управлении лицензиями.

Вы можете использовать естественный язык с Copilot в чате Intune, чтобы определять запросы, которые обращаются к этим аналитическим сведениям, помогая вам решать задачи управления из любого места на портале Intune.

Начните использовать Copilot в Intune для управления Windows 365

Вы можете получить доступ к интеграции Windows 365 с Copilot в Intune через Центр администрирования Intune.

Варианты использования

интеграция Windows 365 с Copilot в Intune поможет ИТ-администраторам, работающим с облачными компьютерами, лучше понять производительность, возможности экономии средств и использование их инвестиций в Windows в облаке.

Основные предполагаемые варианты использования:

- **Оптимизация производительности облачных компьютеров**. Copilot помогает определить потенциальные области повышения производительности, предоставляя рекомендации по размеру облачного компьютера для оптимизации взаимодействия с пользователем. Он также предоставляет подробный анализ и практические рекомендации по оптимизации использования ресурсов облачных компьютеров.

- **Улучшения взаимодействия с пользователем**. Copilot обобщает проблемы с подключением (например, высокую задержку или дрожание) и предоставляет аналитические сведения о том, является ли они системными или изолированными для набора облачных компьютеров или регионов. Он предоставляет аналитические сведения о задержке (время кругового пути), удаленных подключениях, пропускной способности и использовании UDP на региональном уровне. Гибкие параметры отчетности позволяют сосредоточиться на сводной информации, шаблонах тенденций или состоянии. Вы можете определить, улучшаются ли метрики, ухудшаются ли они или остаются статическими, что позволяет упреждающий мониторинг тенденций качества подключения и решение региональных проблем с производительностью.

- **Оптимизация лицензий:** Copilot определяет неиспользуемые устройства, чтобы оптимизировать лицензии и сократить затраты на Windows 365. Copilot предоставляет комплексный анализ шаблонов использования облачных компьютеров и использования лицензий в организации. Copilot помогает анализировать метрики использования, журнал подключений и сведения о дате создания для выявления недостаточно используемых ресурсов. Он предлагает подробные отчеты на уровне устройства и сводки по всей организации, которые помогут вам выявить недостаточно загруженные ресурсы. Copilot предоставляет фиксированные запросы, которые обобщают тип устройства, категории

использования и возраст развертывания. Возможности перераспределения лицензий выводятся на основе метрик использования. Copilot анализирует использование на уровне устройства (например, отсутствие использования, низкое использование) и помечает лицензии, привязанные к неактивным или недостаточно используемым облачным компьютерам. Это помогает определить кандидатов для перераспределения.

- **Помощь по управлению облачными компьютерами**. Copilot определяет проблемы с политикой подготовки и лицензиями, включая причины для использования льготных периодов для облачных компьютеров. Copilot предоставляет подробные диагностика и рекомендации по разрешению для облачных компьютеров, которые находятся в льготном периоде или еще не подготовлены. Он выполняет автоматизированные диагностика на основе системных кодов ошибок и метаданных подготовки. Для устранения неполадок с льготным периодом он включает в себя критически важную информацию о датах окончания льготного периода и потенциальной потере данных. Он также поддерживает как массовый анализ (до 10 устройств одновременно), так и целевое устранение неполадок для отдельных облачных компьютеров или конкретных пользователей. Результаты включают подробные объяснения и прямые ссылки на ресурсы по исправлению, чтобы эффективно устранить выявленные проблемы.

Примеры запросов :

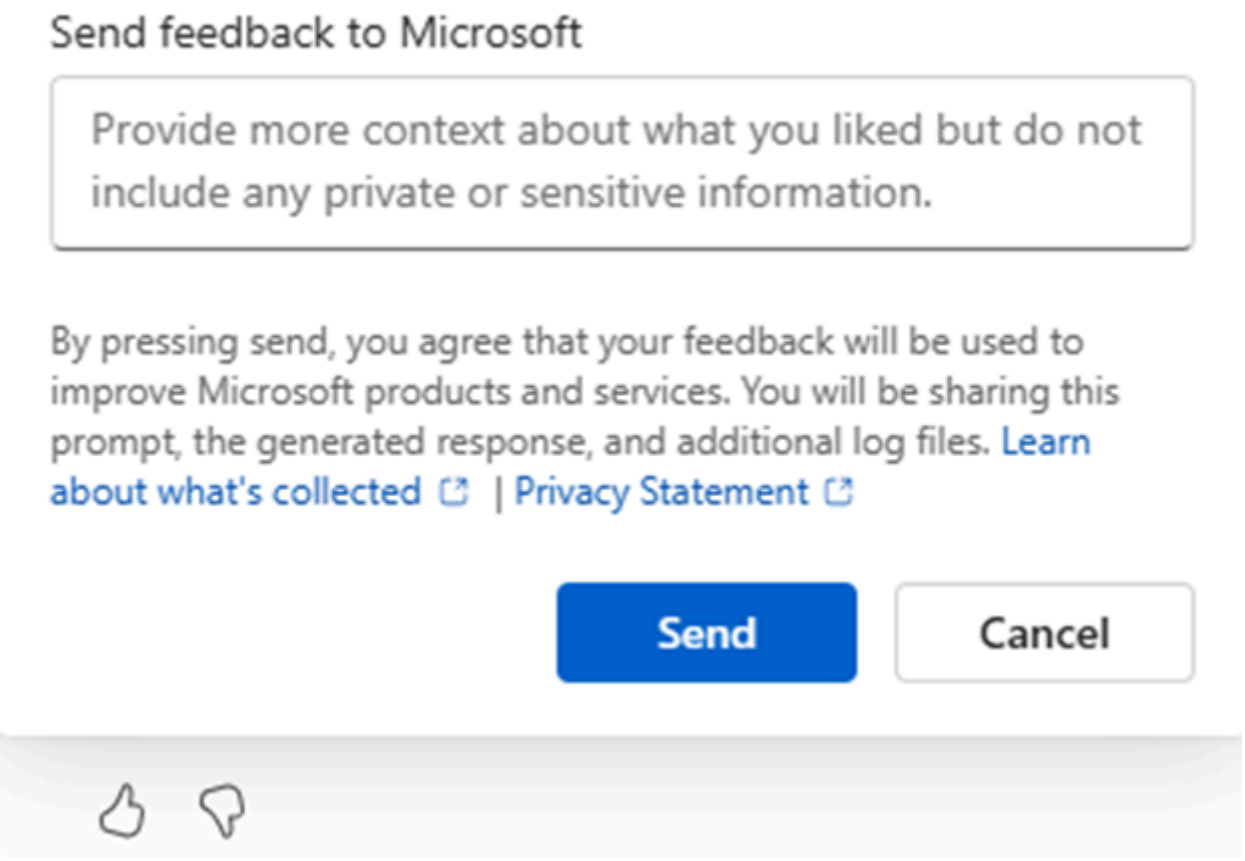
Развернуть таблицу

функциональность.	**Пример Запросы**
Доступность облачных компьютеров	*"Анализ недоступных облачных компьютеров""Сводка облачных компьютеров, которые не могут подключиться""Сводка облачных компьютеров, которые не могут подключиться по регионам"*
Качество подключения	*"Показать регионы с увеличением задержки облачных компьютеров""Показать облачные компьютеры с низкой пропускной способностью""Показать облачные компьютеры с низким потреблением UDP"*
Сведения о лицензировании	*"Сводные данные об инвентаризации лицензий облачных компьютеров""Показать мне лицензии корпоративных облачных компьютеров""Показать мне мои лицензии на облачные компьютеры frontline"*
Сводка по состоянию регионального облачного компьютера	*"Сводка по сбоям подготовки облачных компьютеров""Сводка по регионам моих облачных компьютеров"*

функциональность.	Пример Запросы
Использование облачных компьютеров	*"Суммирование недостаточно используемых облачных компьютеров""Сводные данные по облачным компьютерам, которые никогда не использовались""Суммировать частоту использования облачных компьютеров"*
Производительность облачного компьютера	*"Суммирование производительности моих облачных компьютеров""Показать облачные компьютеры, которые являются кандидатами на понижение уровня""Показать облачные компьютеры с недостаточной производительностью"*
Сводки по состоянию действий	*"Суммирование облачных компьютеров, которые были изменены за последние 28 дней""Сводка облачных компьютеров, которые были перемещены за последние 28 дней""Сводка облачных компьютеров, которые были повторно подготовлены за последние 28 дней"*

Свяжитесь с нами

Обратную связь можно предоставить, щелкнув большие пальцы вверх/большие пальцы вниз в боковом автомобиле Copilot, как показано ниже.



Связанные статьи

- Что такое Microsoft Security Copilot?
- Конфиденциальность и безопасность данных в Microsoft Security Copilot
- Использование Microsoft Copilot в Intune

Обзор управления устройствами для Облачных компьютеров

Статья • 06.02.2025

Для управления облачными компьютерами вы будете использовать Центр администрирования Microsoft Intune. Intune — это облачный поставщик услуг для управления мобильными устройствами (MDM) и мобильными приложениями (MAM) для ваших приложений и устройств (включая Облачные компьютеры). Чтобы войти в Intune, перейдите в Центр администрирования Microsoft Intune.

Страница обзора Облачных компьютеров

Вкладка "Обзор" — это целевая страница для управления вашими Облачными компьютерами. Чтобы просмотреть его, войдите вцентр >администрирования Microsoft Intune **Windows 365**> (в разделе Подготовка).

Здесь вы увидите некоторые сведения, которые помогут вам быстро оценить состояние своих Облачных компьютеров:

- Состояние **подготовки**. Сводка по состоянию Облачного компьютера в организации.
- **Работоспособность сетевого подключения Azure**. Сводка о работоспособности сетевого подключения Azure в вашей организации.

Если у вас больше компьютеров Frontline Cloud, чем доступных лицензий, на этой странице появится предупреждение. Кроме того, вы не сможете подготовить новые облачные компьютеры, пока не отмените подготовку облачных компьютеров в соответствии с допустимым числом.

Страница "Все Облачные компьютеры"

На странице **Все Облачные компьютеры** отображается сводка и представление списка с подробными сведениями о состоянии каждого Облачного компьютера в организации.

Представление списка поддерживает функции поиска, фильтрации и сортировки. Оно автоматически обновляется каждые пять минут.

Если пользователю назначено несколько SKU Windows 365, он получает несколько облачных компьютеров. В результате такой ситуации для одного пользователя в

списке **Все облачные компьютеры** будет отображаться несколько строк.

Сведения о столбце

Имя устройства: имя компьютера Windows, которое также используется в Intune и Microsoft Entra ID.

Политика подготовки. Политика, используемая для создания устройства.

Образ. Образ, используемый во время подготовки. Этот образ может не использовать текущую версию Облачного компьютера. Например, администратор может обновить Windows с помощью Центра обновления Windows для бизнеса, и это обновление не будет отражено в этом представлении списка.

Размер облачного компьютера: номер SKU Windows 365, назначенный пользователю. Пользователю может быть назначено больше одной лицензии или номера SKU. В этом представлении списка у них больше облачных компьютеров.

Тип устройства: тип устройства (Enterprise, Frontline, Dev Box, Power Automate).

Состояние. Текущее состояние подготовки Облачного компьютера. Возможные состояния:

- **Подготовлено** — подготовка Облачного компьютера прошла успешно, назначенный пользователь может войти в систему.
- **Подготовка** — подготовка выполняется в данный момент.
- **Подготовлено с предупреждениями** — если некритический этап в процессе подготовки завершается сбоем, доступ пользователей не блокируется, но выдается предупреждение.
- **Не подготовлено** — пользователю была назначена лицензия Windows 365, но не политика подготовки. Чтобы подготовить Облачный компьютер, назначьте этого пользователя политике подготовки.

  Когда пользователю назначается лицензия Windows 365, в списке **Все облачные компьютеры** автоматически создается новая строка. Если пользователю также назначена политика подготовки, Облачный компьютер подготавливается автоматически.

  Если политика подготовки не назначена, Облачный компьютер не создается. Для этой ситуации будет указано состояние **Не подготовлено**. В этом нет ничего плохого. Это просто информация. Рекомендуем назначить политику

подготовки, чтобы максимально эффективно использовать вложения в Windows 365.

- **Отзыв**. Это кратковременное состояние указывает на то, что семидневный льготный период закончился и облачный компьютер в настоящее время активно отзывается. Когда отмена подготовки завершится, облачный компьютер невозможно будет восстановить, а для затронутых пользователей потребуется подготовить новый облачный компьютер.

- **Сбой** — сбой процесса подготовки для этого облачного компьютера. Щелкните ссылку, чтобы узнать подробную причину сбоя, устранить неполадки и повторить подготовку.

- **Период отсрочки** — если для пользователя с текущим облачным компьютером происходит изменение лицензии или назначения, объект облачного компьютера переходит в состояние **Период отсрочки**. Период отсрочки позволяет администраторам избежать ошибок лицензирования и назначения, которые могут привести к потере доступа пользователей к Облачным компьютерам.

  Благодаря характеру динамических групп Microsoft Entra пользователи могут быть не назначены политике подготовки или Windows 365 лицензии. Так как для работы облачного компьютера требуются политики лицензий и подготовки, удаление любого из них приводит к потере доступа к облачному компьютеру.

  Когда облачный компьютер вступает в льготный период, активируется оповещение. Оповещение отображается в Центре администрирования Microsoft Intune как всплывающее уведомление. Дополнительные сведения о настройке оповещений, включая настройку уведомлений по электронной почте, см. в разделе Оповещения в Windows 365.

  Если Облачный компьютер находится в периоде отсрочки, пользователь может продолжать использовать Облачный компьютер в течение семи дней. По истечении семидневного льготного периода пользователь выйдет из облачного компьютера, и он потеряет доступ.

  Если период отсрочки был активирован по ошибке, можно устранить это критическое изменение в течение 7 дней, чтобы вернуть облачный компьютер в состояние **Подготовлено**.

  Также можно вручную завершить период отсрочки с помощью команды Окончание периода отсрочки.

- **Ожидание**. Если в клиенте недостаточно доступных лицензий для обработки запроса на подготовку, новые облачные компьютеры помечаются состоянием **Ожидание**.

  В клиенте Windows 365 может содержаться лишь столько активных облачных компьютеров, сколько позволяют выделенные лицензии. Активный облачный компьютер может находиться в состоянии **Подготовлено** или **Период отсрочки**.

  Чтобы начать подготовку на ожидающих облачных компьютерах, освободите некоторые лицензии Windows 365 или завершите период отсрочки на облачных компьютерах в состоянии периода отсрочки.

Пользователь. Это пользователь, назначенный облачному компьютеру.

Дата изменения. Метка времени последнего изменения состояния Облачного компьютера.

Сторонний соединитель. Если сторонний соединитель установлен и используется на облачном компьютере, поставщик соединителя отображается вместе с состоянием соединителя. По умолчанию этот столбец скрыт и должен быть выбран из списка отображаемых столбцов.

Сетевое подключение Azure: сетевое подключение Azure, если оно есть.

Состояние шифрования

Сторонний соединитель

Дальнейшие действия

Удаленно управляемые Облачные компьютеры.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Оповещения в Windows 365

Статья • 24.02.2025

Система оповещений Windows 365 уведомляет вас о сбоях в среде облачного компьютера, таких как сбои подключения, подготовки или отправки изображений. Существуют также оповещения, которые уведомляют вас о достижении или превышении максимального порогового значения параллелизма для Windows 365 Frontline облачных компьютеров. По умолчанию оповещения отображаются в Центре администрирования Microsoft Intune как всплывающие уведомления (вы также можете включить Уведомления по электронной почте). Вы можете настроить встроенные правила генерации оповещений:

- Задайте условия и пороговые значения для активации оповещений.
- Определите серьезность оповещений.
- Включите или отключите каждое правило генерации оповещений.
- Настройте каждое оповещение для уведомления в консоли и (или) по электронной почте.

Если сообщения электронной почты включены, при срабатывании правила генерации оповещений на указанный адрес отправляется одно сообщение электронной почты. Если оповещение будет разрешено снова, на указанный адрес отправляется другое сообщение электронной почты.

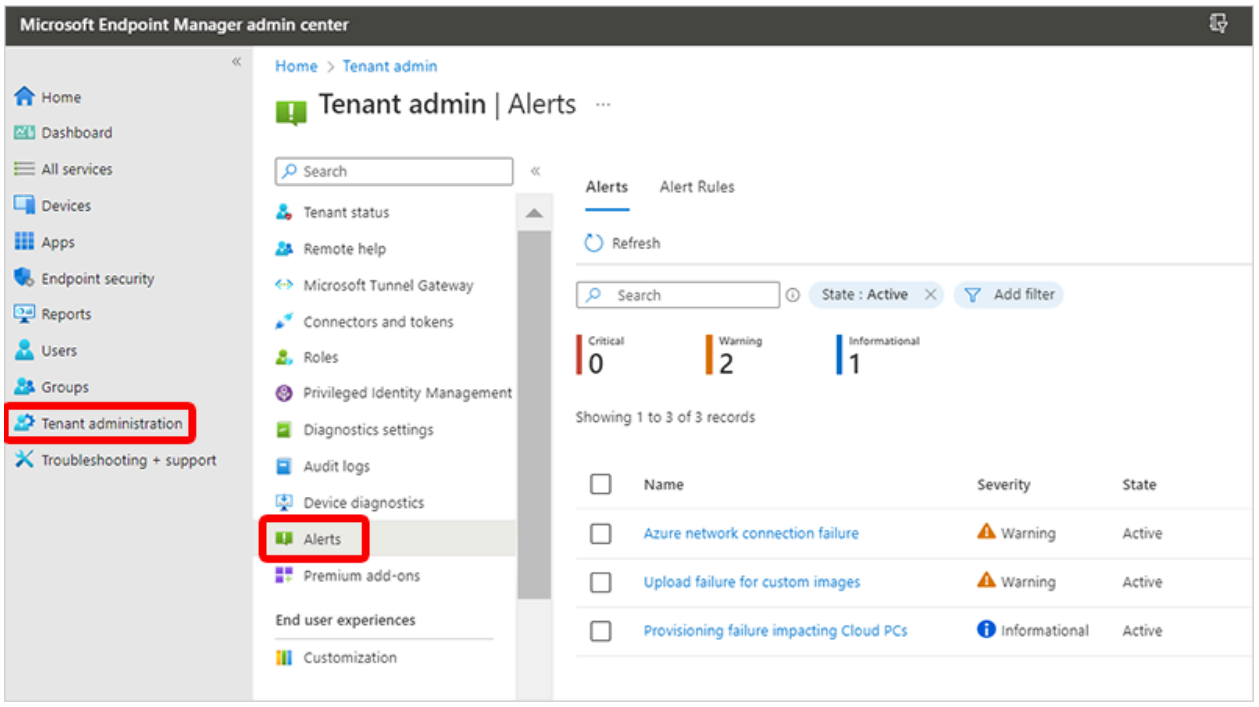
Требования

Для просмотра оповещений учетная запись должна соответствовать следующим требованиям:

- Windows 365 Корпоративная
- Одна из следующих ролей:
  - Администратор Intune
  - Администратор Windows 365

Просмотр оповещений

Чтобы просмотреть список последних оповещений, войдите в центр администрирования > Microsoft Intune**Оповещенияадминистрирования**> клиента.



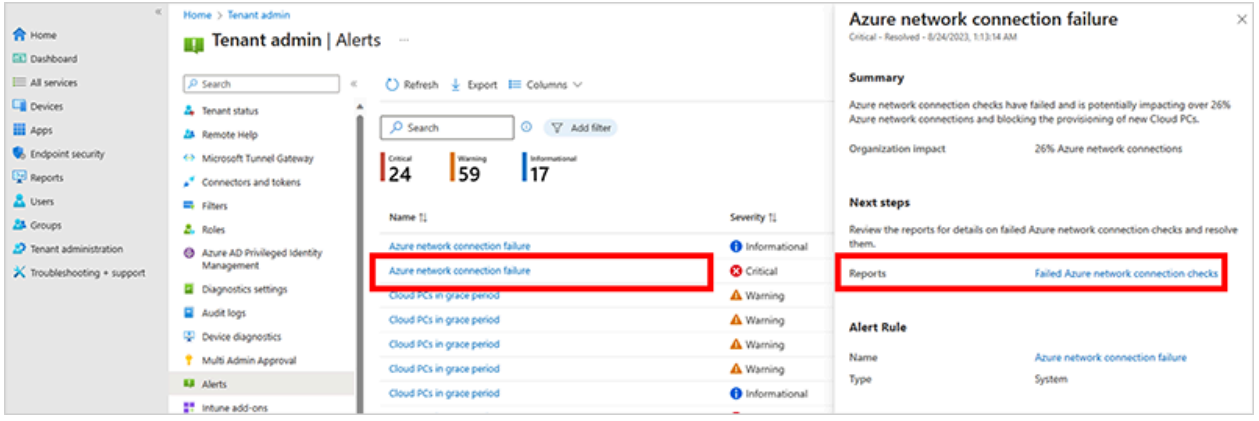
Фильтры

По умолчанию отображаются только активные оповещения. Параметр **Добавить фильтр** можно использовать для фильтрации по следующим параметрам:

- Severity
  - Информационный
  - Предупреждение
  - Critical
- Состояние
  - Активное
  - Устранено

Сводка оповещений

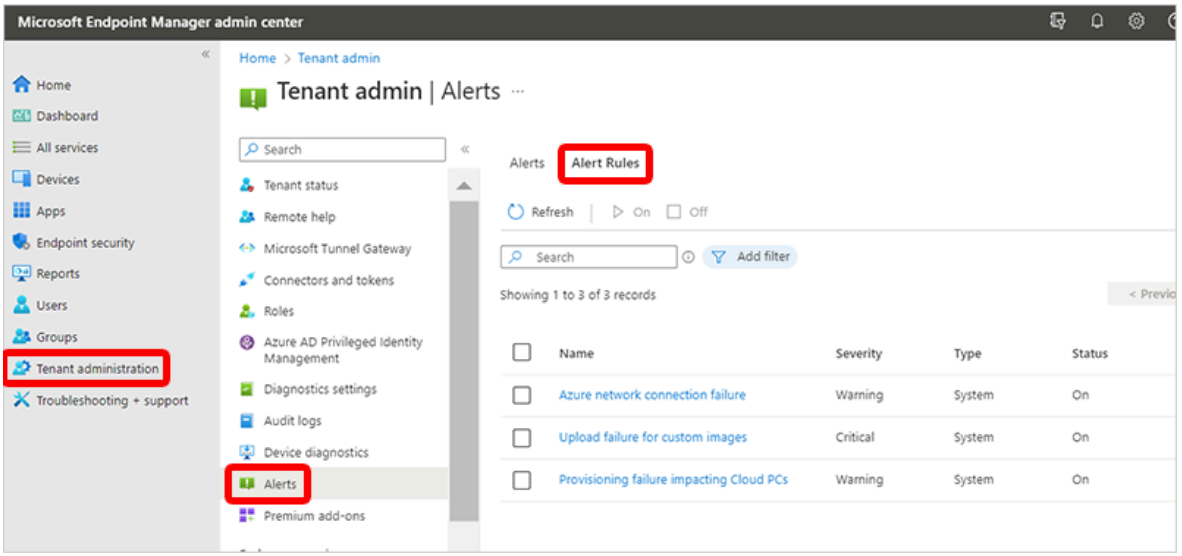
Вы можете выбрать оповещение в списке, чтобы просмотреть сводку по его оповещению.



Щелкните ссылку рядом с **пунктом Отчеты** , чтобы просмотреть дополнительные сведения.

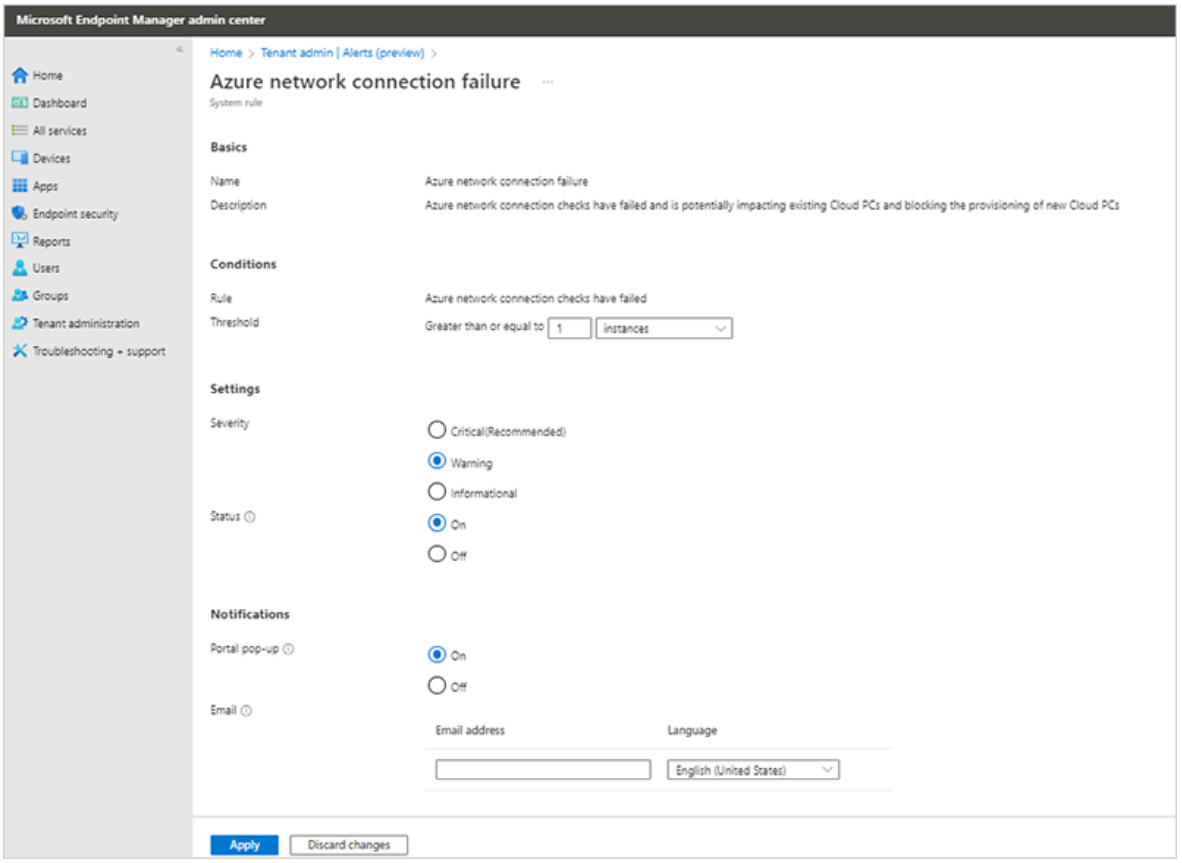
Настройка правила генерации оповещений

1. Войдите в правила**оповещений оповещений**>центра администрирования клиента Microsoft Intune >**администрирования**> клиента.



2. Выберите правило из списка.

3. На странице **Системное правило** внесите необходимые изменения в **разделах Условия**, **Параметры** и **Уведомления** .



4. Нажмите **кнопку Применить** , чтобы сохранить изменения в правиле.

Дальнейшие действия

Дополнительные сведения об устранении неполадок см. в разделе Устранение неполадок.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Дистанционное управление устройствами с Windows 365

Статья • 31.01.2025

Вы можете удаленно управлять Облачными компьютерами в Intune так же, как любым другим управляемым устройством. Дополнительные сведения см. в статье Использование удаленных действий для управления устройствами с помощью Intune.

Облачные компьютеры поддерживают следующие действия по удаленному управлению:

Развернуть таблицу

Удаленное действие	Поддержка массовых действий?
Сбор диагностики	Да
Создание точки восстановления cloud PC вручную	Да
Полная проверка	Нет
Переместите облачный компьютер под проверку	Да
Выключение питания (Windows 365 Frontline) (предварительная версия)	Да
Power On (Windows 365 Frontline) (предварительная версия)	Да
Быстрая проверка	Нет
Удаление облачных компьютеров из проверки	Да
Переименовать	Нет
Повторная подготовка	Да
Resize	Да
Перезапуск	Да
Восстановление	Да
Совместное использование точки восстановления облачного компьютера в хранилище	Да

Удаленное действие	Поддержка массовых действий?
Синхронизация	Да
Устранение неполадок	Да
Обновление Защитника Windows	Нет

Вы можете выполнять удаленные действия для до 5000 облачных компьютеров одновременно. Дополнительные сведения о массовых действиях см. в разделе Использование массовых действий устройства.

На портале Intune можно перейти на вкладку Массовые действия, выбрав **Устройства**>**Все устройства**>**Массовые действия устройств**.

облачные компьютеры Windows 365 Frontline

Облачные компьютеры с интерфейсом поддерживают удаленные действия, такие как корпоративные облачные компьютеры.

Состояние питания конечного пользователя

Одно из различий заключается в том, что состояние питания frontline Cloud PC определяется конечным пользователем. Когда компьютер Frontline Cloud включен, удаленные действия запускаются немедленно. Если компьютер Frontline Cloud отключен, удаленные действия начинаются сразу после включения облачного компьютера. Когда облачный компьютер включен, он использует лицензию, которую другие пользователи не могут использовать. При отключении облачного компьютера лицензия освобождается, чтобы другие пользователи могли ее использовать.

Состояние питания для компьютеров Frontline Cloud можно просмотреть на портале Intune на странице **Свойства** устройств.

Вы можете удаленно включить и выключить облачный компьютер Frontline. При включении компьютера Frontline Cloud лицензия используется автоматически. При выключении компьютера Frontline Cloud:

- Любой пользователь, вошедшего в систему, вошел в систему.
- Несохраненные данные на облачном компьютере теряются.

Вы также можете включить и отключить облачные компьютеры Frontline в пакетном режиме, чтобы помочь в:

- Запустите обновление.
- Применение приложения на всех облачных компьютерах.
- Убедитесь, что облачные компьютеры включены для входящей смены.
- Управление ограничениями параллелизма.

Массовая повторная подготовка облачных компьютеров Frontline в общем режиме

Для облачных компьютеров frontline в общем режиме можно выполнить массовую повторную подготовку всех облачных компьютеров в политике подготовки. Администраторы также могут выбрать процент облачных компьютеров, доступных для подключения пользователей, без влияния процесса повторной подготовки.

Дальнейшие действия

Повторная подготовка Облачного компьютера.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Изменение значения chroma по умолчанию для облачных компьютеров Windows 365

Статья • 31.01.2025

Значение chroma определяет цветовое пространство, используемое для кодирования. По умолчанию значение chroma установлено в 4:2:0 для Windows 365 облачных компьютеров. Это значение обеспечивает хороший баланс между качеством изображения и пропускной способностью сети. Чтобы улучшить качество изображения, можно увеличить значение хрома по умолчанию до 4:4:4. Вам не нужно использовать ускорение GPU для изменения значения chroma по умолчанию.

Требования

- Microsoft Entra ID учетную запись, которому назначена встроенная роль диспетчера политик и профилей RBAC.
- Группа, содержащая устройства, которые требуется настроить.

Увеличьте значение chroma по умолчанию до 4:4:4

1. Войдите в центр администрирования Microsoft Intune .
2. Создайте или измените профиль конфигурации для **устройств Windows 10 и более поздних версий** с типом профиля **каталога параметров**.
3. В окне выбора параметров перейдите к **разделу Административные шаблоны**>**КомпонентыWindows Удаленные рабочие столы**> Службы**удаленных рабочих**> столов Узел >**сеансов удаленных рабочих столов Среда удаленного сеанса**.
4. Установите флажок для следующих параметров, а затем закройте средство выбора параметров:
    - **Определение приоритета режима графики H.264/AVC 444 для подключений к удаленному рабочему столу**
    - **Настройка качества изображения для адаптивной графики RemoteFX**

5. Разверните категорию **Административные шаблоны** , а затем задайте каждый параметр следующим образом:

    - Установите переключатель для **параметра Приоритет режима графики H.264/AVC 444 для подключений к удаленному рабочему столу** значение **Включено**.

    - Установите переключатель **Настройка качества изображения для RemoteFX Adaptive Graphicsзначение Включено**, а затем для **параметра Качество изображения (устройство)** выберите **Высокий**.

6. Нажмите кнопку **Далее**.

7. *Необязательно*. На вкладке **Теги области** выберите тег область, чтобы отфильтровать профиль. Дополнительные сведения о тегах областей см. в статье Использование управления доступом на основе ролей (RBAC) и тегов области для распределенных ИТ.

8. На вкладке **Назначения** выберите группу, содержащую компьютеры, предоставляющие удаленный сеанс, который требуется настроить, а затем нажмите кнопку **Далее**.

9. На вкладке **Просмотр и создание** просмотрите параметры, а затем выберите **Создать**.

10. После применения политики к компьютерам, предоставляющим удаленный сеанс, перезапустите их, чтобы параметры вступили в силу.

Дальнейшие действия

Управление облачными компьютерами Windows 365

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Окончание периода отсрочки для Облачных компьютеров

Статья • 31.01.2025

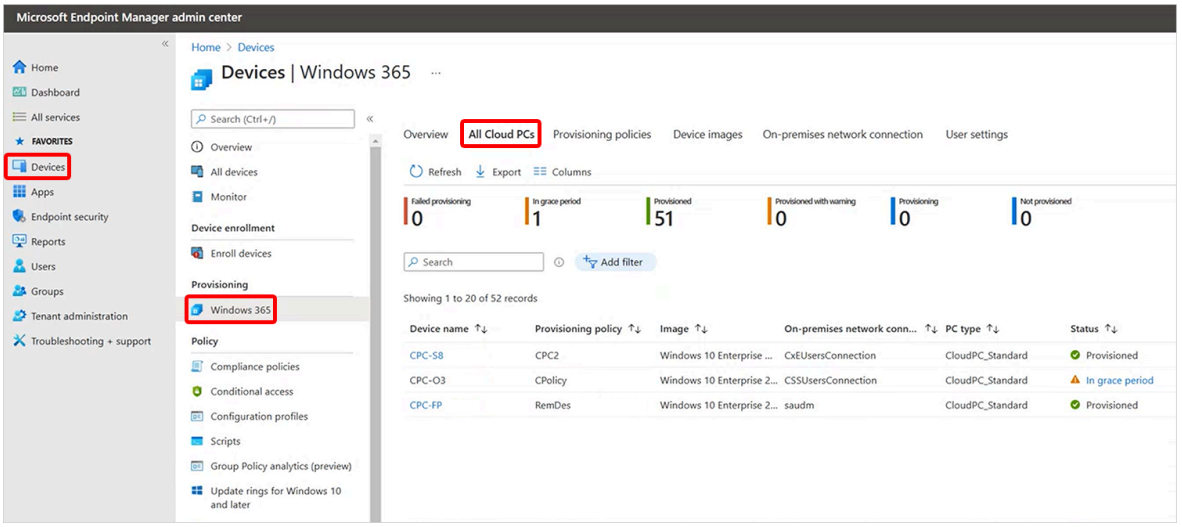
Если Облачный компьютер находится в периоде отсрочки, пользователь может продолжать использовать Облачный компьютер в течение семи дней. По истечении семидневного периода отсрочки пользователь выйдет из Облачного компьютера. Пользователь потеряет доступ, и Облачный компьютер будет удален.

Могут возникнуть ситуации, когда ждать окончания периода отсрочки не требуется. В этом случае для немедленного окончания периода отсрочки можно использовать параметр **Окончание периода отсрочки**.

Окончание льготного периода

1. Окончание периода отсрочки является необратимым действием. Прежде чем закончить период отсрочки, уведомите пользователей и убедитесь, что они полностью осведомлены о последствиях.

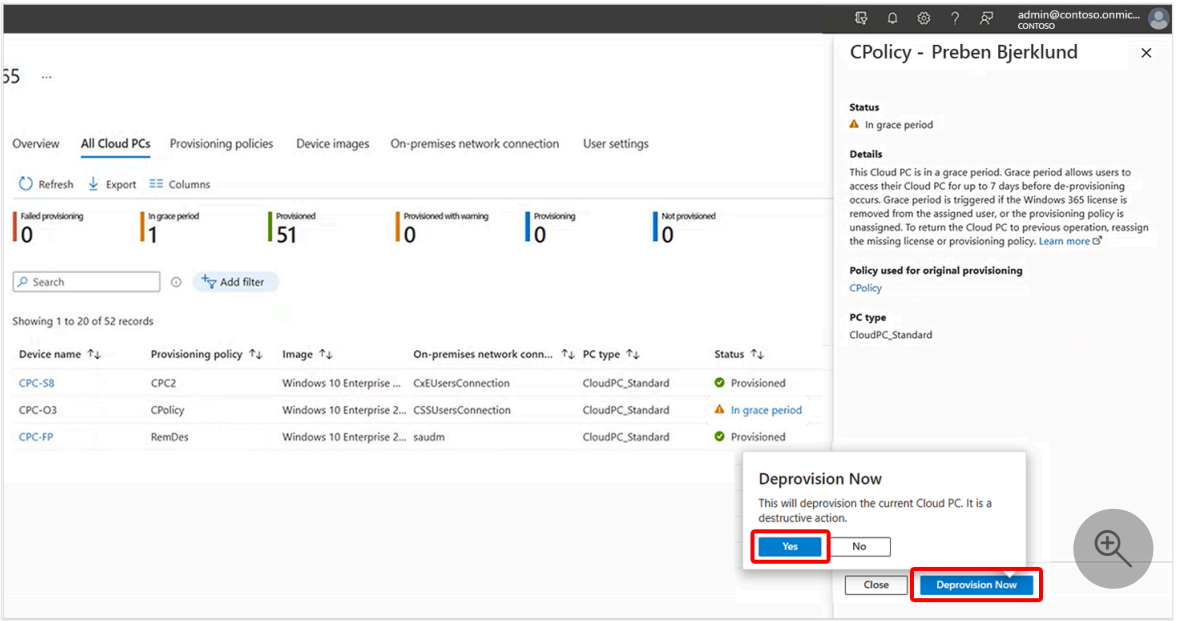
2. Войдите в Центр администрирования Microsoft Intune, выберите **Устройства**>**Windows 365** (в разделе **Подготовка**) >**Все облачные компьютеры**.



3. В столбце **Состояние** списка выберите **В льготный период**>**Отменить подготовку сейчас**>**Да**.

> ⓘ **Важно!**

Это действие необратимо. Оно удаляет операционную систему и данные. Облачный компьютер больше не будет доступен.



После нажатия **Да** автоматически произойдет следующее:

a. Начнется удаление Облачного компьютера.
b. Пользователь потеряет доступ к Облачному компьютеру.
c. Операционная система и данные будут удалены с Облачного компьютера. Облачный компьютер больше не будет доступен.
d. Если первоначальная политика подготовки была заменена другой политикой, Облачный компьютер будет повторно подготовлен с настройками новой политики.

Дальнейшие действия

Дополнительные сведения о периодах отсрочки см. в статье Общие сведения об управлении устройствами для Облачных компьютеров.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Окна обслуживания облачных компьютеров (предварительная версия)

Статья • 13.05.2025

Администраторы могут использовать периоды обслуживания облачных компьютеров, чтобы запланировать определенное время для выполнения массовых действий изменения размера на облачных компьютерах. Для максимальной гибкости можно запланировать следующие окна:

- Ежедневно.
- Еженедельно.
- Выходные.
- Определенные часы в течение дня (локальное время облачного компьютера).
- С двумя или более часами на окно.
- Для определенных групп Microsoft Entra.
- С уведомлениями для пользователей о предстоящем окне.
- Только для действий массового изменения размера.

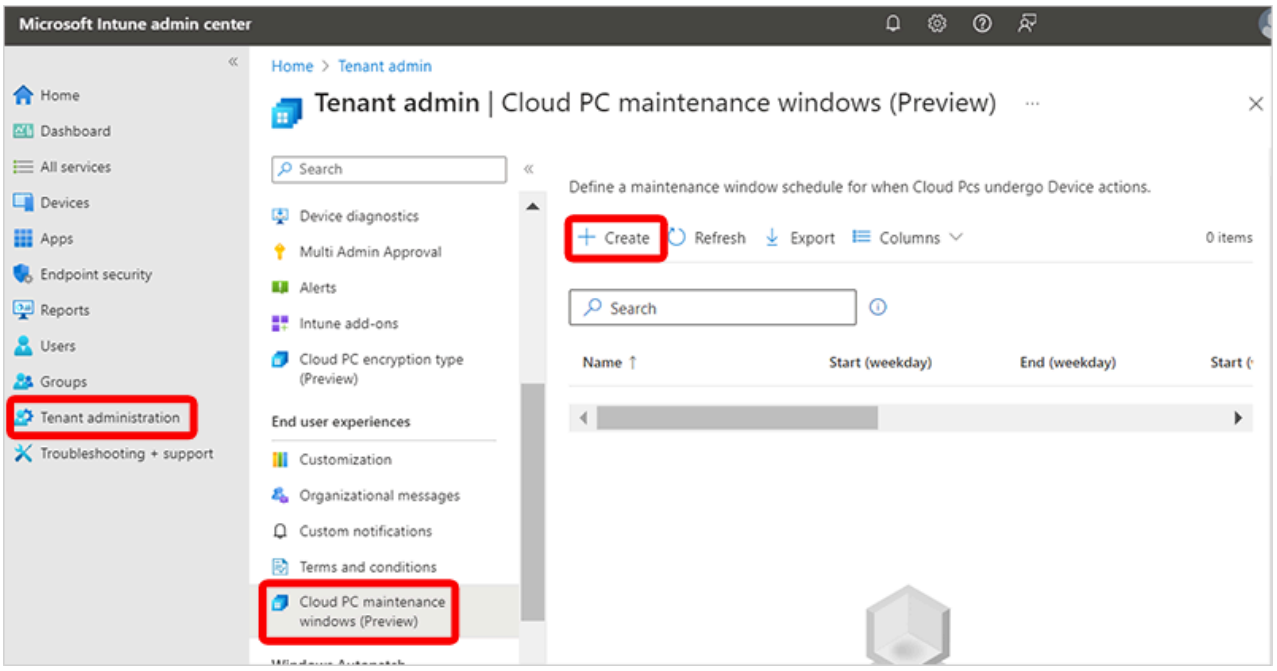
Эти окна помогают эффективно планировать и администрировать действия по обслуживанию облачных компьютеров, сокращать нагрузку на производительность пользователей и соблюдать политики организации.

Создание периода обслуживания

Чтобы создать период обслуживания, выполните следующие действия.

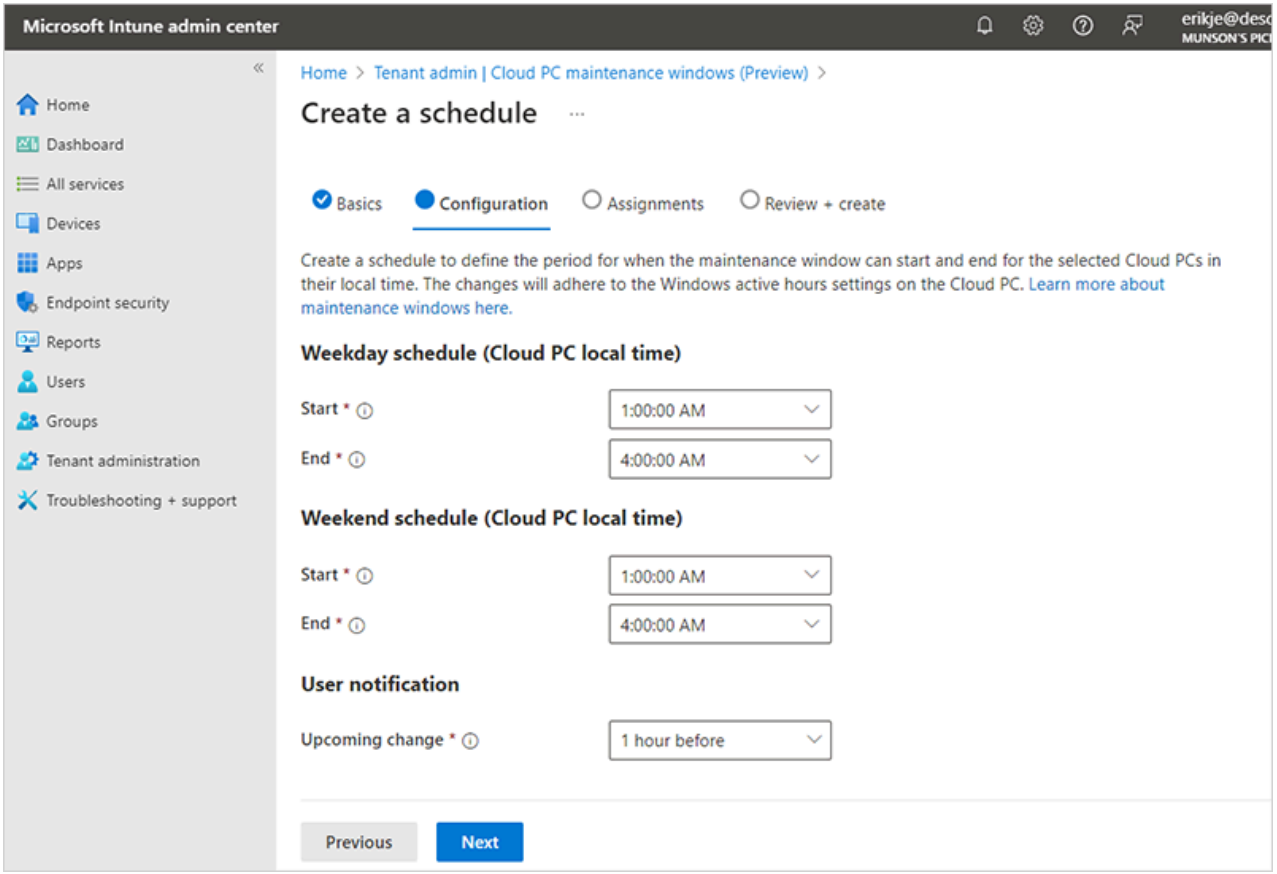
1. Войдите в Центр администрирования Microsoft Intune.

2. Выберите **Администрирование**> клиента**Окна обслуживания облачных компьютеров (предварительная версия)**>**Создать**.



3. На странице **Основные сведения** введите **имя** и **описание**.

4. На странице **Конфигурация** в разделе **Расписание рабочих дней** и (или) **Расписание выходных дней** выберите время **начала** и **окончания** по местному времени Облачного компьютера. Продолжительность каждого окна должна составлять не менее двух часов.



5. В разделе **Уведомление пользователей** в поле **Предстоящие изменения** выберите время, в течение срока действия, необходимое для уведомления пользователя о

предстоящем перебое. Пользователь получает уведомление в сеансе и не может переопределить или отложить период обслуживания.

6. Нажмите кнопку **Далее**.
7. На странице **Назначения** выберите **Добавить группы**.
8. В области **Выберите группы для включения** выберите группы, которые нужно включить в этот период > обслуживания **Выберите**.
9. Нажмите **Далее**.
10. На странице **Проверка + создание** нажмите кнопку **Создать**.
11. Выполните действия, описанные в статье Массовое изменение размера облачных компьютеров и убедитесь, что на странице Основные сведения установите флажок **Использовать окна обслуживания облачных компьютеров**.

Срочные или критические изменения для облачных компьютеров

Если необходимо устранить проблему немедленно и не дожидаться периода обслуживания, не выбирайте параметр **Использовать периоды обслуживания облачных компьютеров** . Если этот параметр не выбран, удаленное действие запускается немедленно.

Ограничения

Периоды обслуживания не отвечают за успешное или неудачное выполнение удаленных действий. Они не охватывают обслуживание служб, обновления Windows, полезные данные Intune, обновления ОС и другие действия.

Дальнейшие действия

Удаленное управление облачным компьютером.

Перемещение облачного компьютера

Статья • 22.04.2025

Изменив политику подготовки, вы можете переместить некоторые или все существующие облачные компьютеры в политике из:

- Один регион к другому.
- Одно сетевое подключение Azure (ANC) к другому ANC.
- Сеть, размещенная корпорацией Майкрософт в ANC, и наоборот.

Перемещение облачных компьютеров не приводит к повторной подготовке.

После перемещения облачного компьютера в новый регион или ANC его точки восстановления в старом регионе или ANC удаляются и становятся недоступными.

Поддерживаемые сценарии перемещения облачных компьютеров

Развернуть таблицу

Тип соединения	В/из	В/из	Поддержка
Microsoft Entra присоединение <—> Microsoft Entra присоединение	Регион сети или группа регионов, размещенных в майкрософт	Другой регион сети или группа регионов, размещенных майкрософт	Да
Microsoft Entra присоединение <—> Microsoft Entra присоединение	АНК	Другой ANC	Да
Microsoft Entra присоединение <—> Microsoft Entra присоединение	Регион сети или группа регионов, размещенных в майкрософт	АНК	Да
Microsoft Entra гибридное соединение <—> Microsoft Entra гибридное соединение	АНК	Другой ANC	Да
Microsoft Entra гибридное соединение <—> Microsoft Entra соединение	ANC (Microsoft Entra гибридное соединение)	Регион сети или группа регионов, размещенных в майкрософт	Нет

Тип соединения	В/из	В/из	Поддержка
Microsoft Entra гибридное соединение <—> Microsoft Entra соединение	ANC (Microsoft Entra гибридное соединение)	Другой ANC (Microsoft Entra присоединение)	Нет

Массовое перемещение всех облачных компьютеров в политике

1. Войдите в Центр администрирования Microsoft Intune, выберите **Устройства**>**Windows 365** (в разделе **Подготовка**) > Политики >**подготовки** выберите политику.

2. В разделе **Общие** выберите **Изменить**.

3. В разделе **Сведения о типе соединения** внесите изменения в зависимости от исходного типа:

   - Для **гибридного Microsoft Entra присоединения** измените ANC*.

   - Для **Microsoft Entra присоединения:**
     - Вы можете изменить тип **сети** с ANC на размещенную сеть Майкрософт или наоборот.
     - Если **используется размещенная сеть Майкрософт** , измените **географию** и (или) **регион**.
     - Если используется **сетевое подключение Azure** , измените ANC*.

4. Выберите **Next**Update (Далее >**обновление**).

5. Когда все будет готово для перемещения существующих облачных компьютеров, выберите **Применить эту конфигурацию**.

6. В поле **Применить эту конфигурацию к существующим облачным компьютерам** выберите **Регион или Сетевые подключения Azure для всех устройств**>**Применить**.

* Домен, определенный в новом ANC, должен соответствовать домену облачных компьютеров, которые требуется переместить. Домен, используемый в исходном ANC, должен быть доступен из нового ANC.

Все новые облачные компьютеры, подготовленные после обновления конфигурации политики, соответствуют обновленной конфигурации политики и создаются в новом регионе или ANC.

Перемещение подмножества облачных компьютеров

1. Войдите в Центр администрирования Microsoft Intune, выберите **Устройства**>**Windows 365** (в разделе **Подготовка**) > Политики >**подготовки** выберите политику.

2. В разделе **Общие** выберите **Изменить**.

3. В разделе **Сведения о типе соединения** внесите изменения в зависимости от исходного типа:

   - Для **гибридного Microsoft Entra присоединения** измените ANC*.

   - Для **Microsoft Entra присоединения:**
     - Вы можете изменить тип **сети** с ANC на размещенную сеть Майкрософт или наоборот.
     - Если **используется размещенная сеть Майкрософт** , измените **географию** и (или) **регион**.
     - Если используется **сетевое подключение Azure** , измените ANC*.

4. Выберите **Next**Update (Далее >**обновление**).

5. Когда все будет готово для перемещения существующих облачных компьютеров, выберите **Применить эту конфигурацию**.

6. В поле **Применить эту конфигурацию к существующим облачным компьютерам** выберите **Регион или Сетевые подключения Azure для нескольких устройств**>**Применить**.
7. В разделе **Выбор устройств** выберите устройства, которые нужно переместить. Одновременно можно перемещать до 100 устройств.
8. Нажмите **кнопку "Продолжить**>".

Лучшие методики

Лучшее время для выполнения перемещений — в выходные дни, чтобы убедиться, что влияние на пользователей сведено к минимуму. Облачные компьютеры отключены и недоступны в течение нескольких часов в процессе перемещения. Перед перемещением необходимо уведомить пользователей, чтобы они могли сохранить свою работу и выйти из нее.

При перемещении большого количества устройств в новый регион начните с нескольких некритических облачных компьютеров и проверка для успешного перемещения

критически важных облачных компьютеров.

Вы можете отслеживать состояние перемещения облачных компьютеров с помощью отчета о действиях облачного компьютера.

Новые облачные компьютеры, созданные измененной политикой подготовки, назначаются новому региону или ANC.

Другие операции перемещения

Облачные компьютеры нельзя перемещать из одной политики подготовки в другую.

Вы не можете переместить некоторые облачные компьютеры в один регион, а другие облачные компьютеры в другой регион в той же операции изменения политики.

Вы не можете перемещать облачные компьютеры из одной виртуальной сети или подсети в другую с помощью метода политики редактирования подготовки. Чтобы внести изменения в виртуальную сеть или подсеть, создайте новый ANC с обновленной виртуальной сетью или подсетью, а затем переместите облачные компьютеры в новый ANC.

Дальнейшие действия

Управление облачными компьютерами.

Повторная подготовка облачного ПК

Статья • 31.01.2025

Удаленное действие **повторной подготовки** удаляет текущий облачный компьютер пользователя и создает новый облачный компьютер для этого же пользователя.

При запуске удаленного действия **повторной подготовки** пользователь выходит из системы. Исходный облачный компьютер удаляется, включая все пользовательские данные, приложения, настройки и т. д.

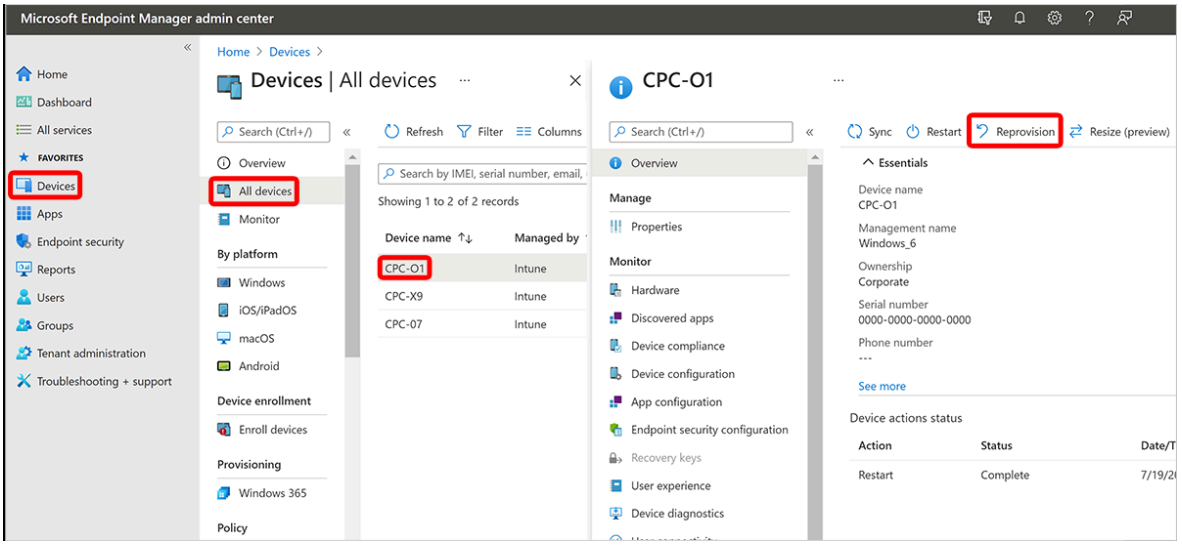
Чтобы **повторно подготовить** облачный компьютер, нужно обеспечить, чтобы он находился в состоянии **Ошибка** или **Подготовлен** в узле подготовки Windows 365.

Сведения о том, когда следует использовать действие **повторной подготовки**, см. в статье Повторная подготовка.

Для облачных компьютеров frontline в общем режиме можно выполнить массовую повторную подготовку всех облачных компьютеров в политике подготовки. Администраторы также могут выбрать процент облачных компьютеров, доступных для подключения пользователей, без влияния процесса повторной подготовки.

Повторная подготовка облачного ПК

1. Войдите в Центр администрирования Microsoft Intune, выберите **Устройства**>**Все устройства**> Выберите **повторное создание** устройства > облачного компьютера.



2. В поле **Повторная подготовка** выберите **Да**. Начнется процесс повторной подготовки.
3. После создания нового облачного компьютера Windows 365 отправляет сведения о доступе новому пользователю.

Дальнейшие действия

Дополнительные сведения см. в статье Подготовка.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Массовая повторная подготовка Windows 365 Frontline облачных компьютеров в общем режиме

Статья • 11.02.2025

Windows 365 Frontline облачные компьютеры, созданные в режиме общего доступа, можно выполнить массовую повторную подготовку. Все данные, сохраненные на отдельных облачных компьютерах, удаляются.

Использование массовых действий для повторной подготовки нескольких облачных компьютеров за раз может помочь вам:

- Примените новые конфигурации. Например, примените новый образ.
- Возврат к известной конфигурации всех облачных компьютеров Frontline в общем режиме. Это действие поможет свести к минимуму расхождения в конфигурации, которые могут возникнуть в пуле доступных общих облачных компьютеров. Такие несоответствия могут возникать со временем, когда к отдельным системам применяются различные политики или обновления.

Массовая повторная подготовка облачных компьютеров Frontline в общем режиме

1. Войдите в Центр администрирования Microsoft Intune, выберите **Устройства**>**Windows 365** (в разделе **Подключение устройств**) >**Политики подготовки**.

2. Выберите политику подготовки для облачных компьютеров Frontline.

3. Выберите **Повторная подготовка**.

4. В **поле**> Продолжить**сохранение процента доступных устройств** введите процент устройств, которые вы хотите сохранить доступными во время действия повторной подготовки. Если задать значение более 0 %, повторная подготовка развертывается на всех облачных компьютерах и всегда сохраняет эту процентную долю облачных компьютеров, доступных для использования.

   При выборе процента учитывайте следующие сведения:

   - Заданный процент — это количество облачных компьютеров, которые остаются доступными, пока остальные облачные компьютеры будут

повторно подготовлены. После повторной подготовки (и доступности для использования) нескольких облачных компьютеров, равных проценту, ранее отведенных в сторону облачных компьютеров начнется повторная подготовка.

- Облачные компьютеры не выполняют повторную подготовку, пока пользователи по-прежнему вошли в систему. Чтобы принудительно отключить пользователей, запустите повторную подготовку, введите 0 %, а затем используйте удаленное действие **Перезапустить** на каждом облачном компьютере.
- Минимальное количество устройств, которые будут повторно подготовлены, — одно. Например, если у вас есть один облачный компьютер и вы указали 99 %, то одно устройство по-прежнему будет повторно подготовлено, даже если ближайшим целым числом будет один облачный компьютер, который будет доступен.
- Система округляется до ближайшего целого числа. Например, если общее количество облачных компьютеров составляет 150 и вы сохраняете 27 % доступности, результатом будет 40,5 облачных компьютеров. Это число округляется, чтобы одновременно было доступно 40 облачных компьютеров.

Планирование массовой повторной подготовки облачных компьютеров Frontline в общем режиме

1. Войдите в Центр администрирования Microsoft Intune, выберите **Устройства**>**Windows 365** (в разделе **Подключение устройств**) >**Политики подготовки**.
2. Выберите политику подготовки для облачных компьютеров Frontline.
3. Выберите **Reprovision**>**Schedule reprovision reprovision** (Повторная подготовка расписания).
4. Выберите время и дату (в формате UTC) для первого события повторной подготовки.
5. В разделе **Повторять каждый** выберите *Один раз*, *Еженедельно* или *Ежемесячно*. Параметры Weekly и Monthly можно использовать для периодической повторной подготовки всей коллекции устройств Frontline Shared.

Дальнейшие действия

Удаленное управление Windows 365 облачных компьютеров.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Общие сведения об изменении размера облачного компьютера

23.07.2025

Удаленное действие "**Изменить размер** ", которое сохраняет данные пользователя и диска, позволяет:

- Обновите объем ОЗУ, ЦП и хранилища облачного компьютера.
- Понижение уровня ОЗУ и ЦП облачного компьютера. Изменение размера не приводит к уменьшению дискового пространства.
- Изменение размера одного облачного компьютера.
- Массовое изменение размера нескольких облачных компьютеров.

Эти операции не требуют повторной подготовки облачного компьютера.

Вы можете рассмотреть возможность изменения размера облачного компьютера, когда пользователю нужно:

- Больше ядер ОЗУ и виртуальных ЦП для запуска приложений с интенсивным использованием ЦП.
- Больше места на диске для хранения файлов.
- Меньше ядер ОЗУ и виртуальных ЦП для выполнения текущих приложений рабочей нагрузки.

Изменение размера поддерживает:

- Прямые и групповые лицензии.
- Платные, предварительные и пробные лицензии.
- Массовые операции и операции с одним устройством.

Изменение размера не поддерживает:

- Облачные компьютеры GPU. Облачные компьютеры GPU могут отображаться в потоке изменения размера, но попытка изменить размер облачного компьютера GPU приводит к ошибке.

Изменение размера автоматически отключает пользователя от сеанса, и все несохраненные работы могут быть потеряны. Поэтому перед началом рекомендуется согласовать изменения размера с пользователями. Обратитесь к конечным пользователям и попросите их сохранить свою работу и выйти из нее, прежде чем вы начнете изменять размер.

Уменьшение размера может повлиять на поддержку вложенной виртуализации. Дополнительные сведения см. в статье Настройка поддержки рабочих нагрузок на основе виртуализации.

Изменение размера сведений

> ⓘ **Важно!**
>
> Перед активацией изменения размера для Windows 365 Корпоративная облачных компьютеров убедитесь, что вы выполняете рекомендации по назначению лицензий. Изменение размера облачных компьютеров проще при использовании дискретных групп Entra для лицензирования, которые отличаются от групп Entra, используемых для таргетинга политик подготовки. Дополнительные сведения см. **в разделе Подготовка в Windows 365 | Microsoft Learn**.

Для Windows 365 Корпоративная размер облачного компьютера привязан к лицензии, назначенной пользователю. При изменении размера облачных компьютеров, подготовленных с прямыми назначенными лицензиями, служба Windows 365 выполнит переназначение лицензии от имени администратора. При изменении размера облачных компьютеров, подготовленных с помощью лицензий на основе групп (назначенных через членство в группе Entra), облачный компьютер перейдет в состояние **Ожидание изменения размера лицензии**. После этого администратор должен назначить соответствующую целевую лицензию для активации изменения размера.

Состояние **ожидающей изменения размера лицензии** :

- Имеет продолжительность 48 часов. Если исходная лицензия удаляется, но новая лицензия не назначается в течение 48 часов, устройство переходит в льготный период.
- Если выбрана неправильная целевая лицензия, облачный компьютер подготавливается в соответствии с конфигурацией этой неправильной лицензии.
- Если исходная лицензия не удаляется первым, а новая лицензия назначается пользователю, новая лицензия используется для изменения размера текущего облачного компьютера. Кроме того, исходная лицензия используется для подготовки другого, нового облачного компьютера для пользователя.
- Если исходная лицензия не удалена, а целевая лицензия не назначена в течение 48 часов, устройство возвращается в состояние **Подготовлено** .

Если у вас есть сочетание платных и пробных лицензий, функция изменения размера сначала использует платные лицензии. После того как эти лицензии иссякнет, операция изменения размера использует пробные лицензии.

При запуске изменения размера пользователь автоматически отключается от своего облачного компьютера, и все несохраненные работы могут быть потеряны.

Изменение размера может занять от 15 до 20 минут, прежде чем пользователь снова сможет получить доступ к своему облачному компьютеру. Состояние можно отслеживать в колонке подготовки Windows 365. Пользователи могут просмотреть состояние своего облачного компьютера по адресу https://windows365.microsoft.com .

Если в инвентаризации нет лицензий, изменение размера завершается ошибкой. Чтобы запросить дополнительные лицензии, обратитесь к администратору закупок. После приобретения лицензии и добавления в инвентаризацию в Центр администрирования Microsoft 365 можно повторить операцию изменения размера. Лицензии можно приобрести по различным каналам: EA, CSP, MCA и Web Direct.

Размеры устройств с состоянием **Resize не поддерживаются** . Сообщение о состоянии и сведения помогут вам определить проблему. Вы по-прежнему можете продолжить массовое изменение размера, даже если в списке есть устройства, которые помечены как **Изменение размера не поддерживается**.

Изменение размера с помощью лицензий step-up

Windows 365 лицензии на расширение — это лицензии на состояние потенциальных пользователей, доступные для администраторов enterprise с прямым Соглашение Enterprise. Более высокий номер SKU упрощает для администраторов перенос пользователей с лицензии с более низкой конфигурацией на лицензию с более высокой конфигурацией без полной стоимости лицензирования двух отдельных подписок продукта. Для Windows 365 доступны дополнительные шаги для вычислений (ОЗУ/ЦП) и хранилища и ограничены обновлениями, а не более ранними версиями лицензий.

Если вы преобразовали подписку на лицензию Windows 365 Корпоративная путем приобретения лицензий Microsoft Step-up License, вы можете перенести пользователей на новую лицензию и сохранить все данные пользователей, выполнив массовое изменение размера для этих пользователей.

Например, предположим, что вы использовали покупку step-up для преобразования лицензий из подписки Windows 365 Корпоративная 2vCPU/4 ГБ/128 ГБ в подписку Windows 365 Корпоративная 4vCPU/16 ГБ/128 ГБ. В этом случае выполните действия, описанные в разделе Массовое изменение размера облачных компьютеров, изначально подготовленных с помощью лицензий на основе групп. Windows 365 2vCPU, 4 ГБ, 128 ГБ является вашей базовой лицензией, а Windows 365 4vCPU/16 ГБ/128 ГБ является вашей целевой лицензией.

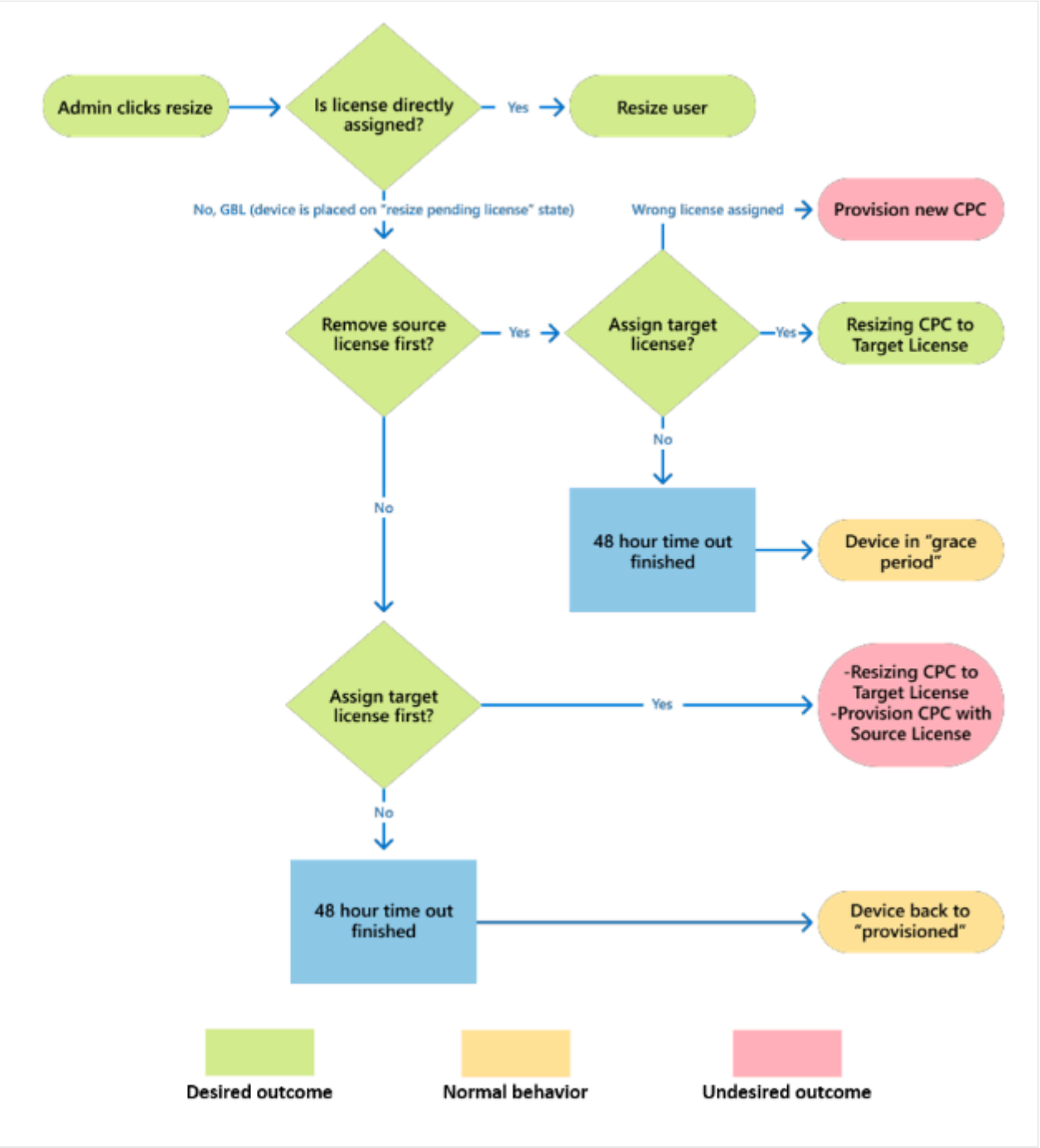
При переходе на шаг вверх в инвентаре отображаются дополнительные лицензии, равные количеству старых лицензий, которые вы решили преобразовать. Если выполнить шаг 10 лицензий Windows 365 Корпоративная 2 vCPU/4GB/128 ГБ до 4vCPU/16 ГБ/128 ГБ, вы итоге удостоверяете еще 10 лицензий 4vCPU/16 ГБ/128 ГБ и 10 лицензий 2 vCPU/4GB/128 ГБ. Эти изменения отображаются на странице **Ваши продукты** в Центре администрирования Майкрософт.

При активации подписки на лицензию необходимо убедиться, что вы готовы перенести или изменить размер пользователей в новую подписку на лицензию, до которую выполняете шаг. При активации всех лицензий в рамках подписки у вас есть 90 дней, чтобы перенести пользователей на новые лицензии, прежде чем они потеряют доступ к облачному компьютеру, подготовленному с исходной лицензией. Однако если в подписке выполняется только расширение подмножества лицензий, необходимо немедленно перенести пользователей, чтобы избежать прерывания работы службы. Чтобы обеспечить непрерывный доступ для пользователей, планируйте миграцию пользователей сразу после приобретения лицензий на расширение.

Изменение размера после обновления лицензий, приобретенных через Клиентское соглашение Майкрософт

Если у вас есть Клиентское соглашение Майкрософт (MCA), вы можете обновить лицензию, как описано в разделе Обновление или переход на другой план Microsoft 365 для бизнеса. После обновления можно изменить размер облачных компьютеров, как описано в этой статье.

Изменение размера схемы потока облачного компьютера



Дальнейшие действия

Изменение размера одного облачного компьютера.

Массовое изменение размера нескольких облачных компьютеров.

Дополнительные сведения о размерах облачных компьютеров см. в этой статье.

Изменение размера одного облачного компьютера

Статья • 30.04.2025

Удаленное действие **Изменить размер** можно использовать для изменения размера одного облачного компьютера, который был подготовлен с прямой назначенной лицензией или лицензией на основе группы.

Дополнительные сведения о массовом изменении размера облачных компьютеров см. в статье Изменение размера облачных компьютеров в пакетном режиме.

Дополнительные сведения об изменении размера см. в статье Общие сведения об изменении размера облачного компьютера.

Требования

Требования к роли

Чтобы изменить размер облачного компьютера, администратор должен иметь определенные встроенные Microsoft Entra роли.

- Для облачного компьютера, подготовленного с прямой назначаемой лицензией, по крайней мере одна из следующих ролей
  - Администратор службы Intune
  - Intune читатель + роли Администратор облачного компьютера
  - читатель Intune и администратор Windows 365
- Для облачного компьютера, подготовленного с лицензией на основе группы, по крайней мере одна из следующих ролей
  - Администратор службы Intune
  - читатель Intune и администратор Windows 365
  - Помимо одной из трех предыдущих ролей, роль с Microsoft Entra разрешениями на чтение и запись в группах, а также разрешениями на лицензирование, например роль Windows 365 Администратор.

Кроме того, можно назначить пользовательскую роль, которая включает разрешения этих встроенных ролей.

Требования к IP-адресу

При изменении размера Microsoft Entra гибридного соединения с облачным компьютером с помощью собственной сети в подсети должен быть доступен второй IP-адрес для изменения размера облачного компьютера.

Во время операции изменения размера при переходе к новому размеру используется второй IP-адрес. Эта мера предосторожности гарантирует, что облачный компьютер может быть откатлен до исходного компьютера в случае возникновения проблемы.

Чтобы учесть эту меру предосторожности, вы можете:

- Убедитесь, что в виртуальной сети доступны соответствующие IP-адреса для всех облачных компьютеров, которые будут изменены, или
- Измените размер операций, чтобы убедиться, что адрес область поддерживается.

Если доступны неадекватные адреса, могут возникнуть ошибки изменения размера.

Другие требования

Чтобы использовать **Изменение размера** , в инвентаризации должны быть доступные лицензии для измененной конфигурации облачного компьютера.

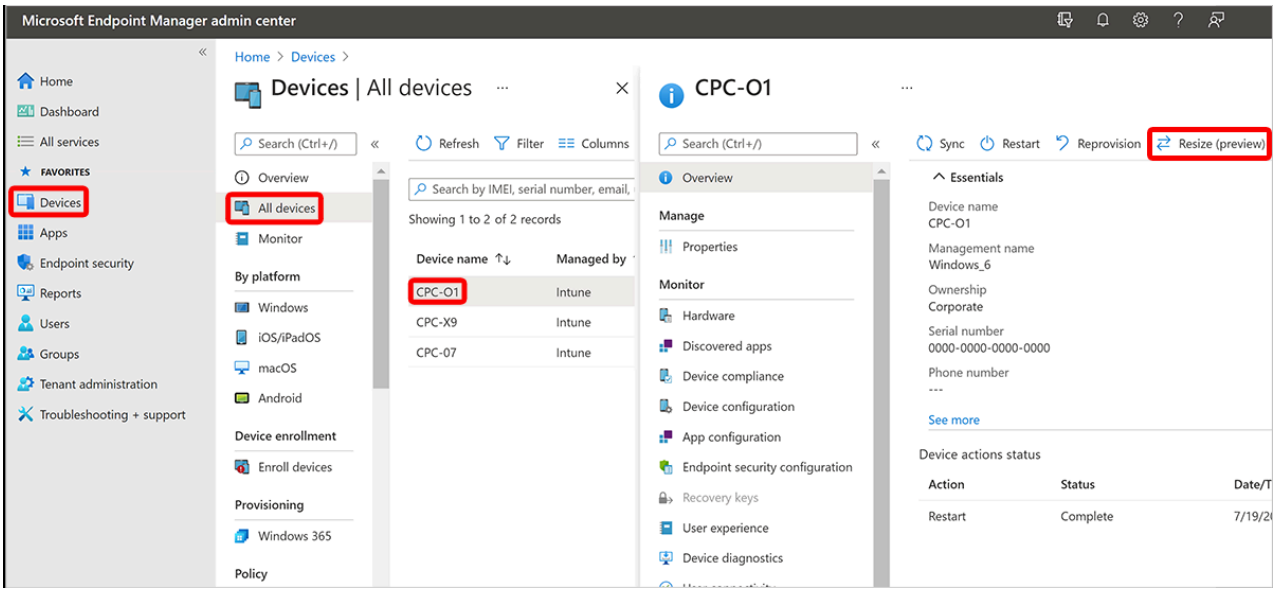
Чтобы **изменить размер** облачного компьютера, он должен иметь состояние **Подготовлено** в узле подготовки Windows 365.

Изменение размера одного облачного компьютера, подготовленного с помощью прямой назначаемой лицензии

При изменении размера облачных компьютеров, подготовленных с помощью прямых назначенных лицензий, служба Windows 365 автоматически выполняет следующие действия:

- Отмена назначения исходной лицензии.
- Назначение новой лицензии от имени администратора.

1. Войдите в Центр администрирования Microsoft Intune, выберите **Устройства**>**Все устройства**> выберите **изменение размера** устройства>.



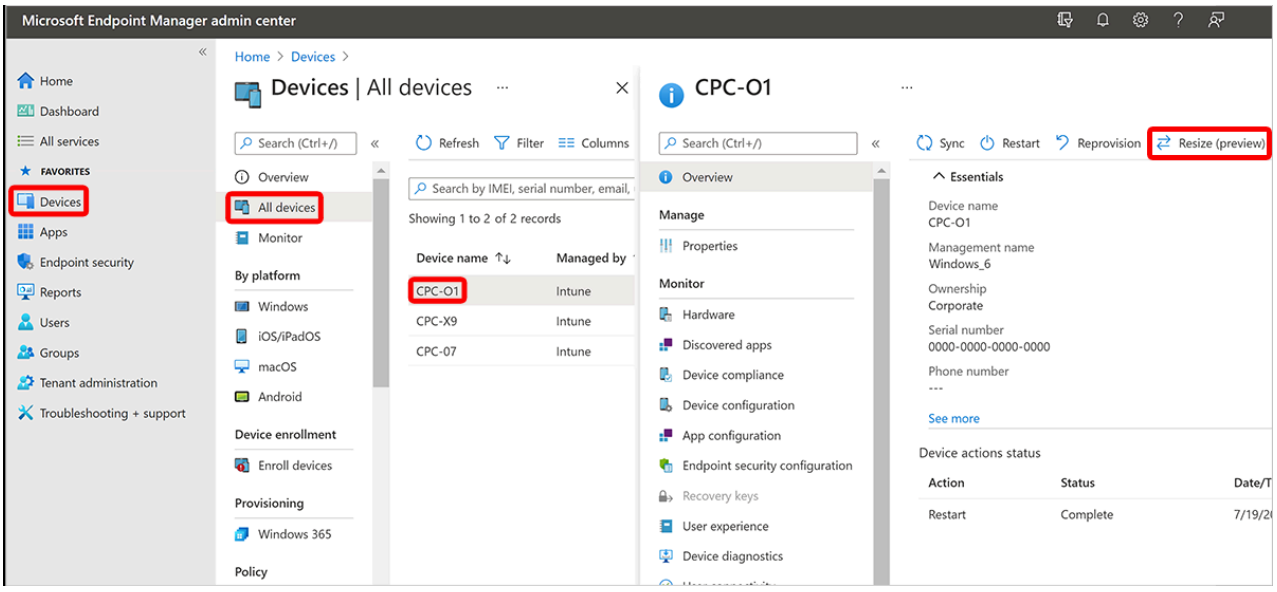
2. В разделе **Изменить размер** содержится список размеров, которые можно обновить или уменьшить на основе лицензий, доступных в инвентаре. Вы можете обновить или перейти на более раннюю версию ОЗУ и виртуальный ЦП облачного компьютера. Вы можете обновить только хранилище дисков ОС. При понижении уровня облачного компьютера пользователя параметры с меньшим объемом хранилища будут неактивны. Выберите один из доступных вариантов.
3. Выберите **Изменить размер**.

При наличии доступных лицензий начинается изменение размера.

Изменение размера одного облачного компьютера, подготовленного с помощью групповой лицензии

1. Создайте целевую группу Microsoft Entra. Добавьте пользователей из исходной Microsoft Entra группы, размер которой требуется изменить. Кроме того, можно использовать существующие Microsoft Entra группы, если вы сопоставляете группы с отдельными типами лицензий Windows 365.
2. Назначьте существующую политику подготовки, предназначенную для исходной группы Microsoft Entra источника, новой целевой группе Microsoft Entra. Это необходимо сделать, только если у вас нет дискретной группы Microsoft Entra для назначения политики подготовки. Если у вас есть дискретные Microsoft Entra группы для управления назначениями политик подготовки, этот шаг можно опустить.
3. Войдите в Центр администрирования Microsoft Intune, выберите **Устройства**>**Все устройства**> выберите устройство, которое вы хотите добавить в целевую группу >

Microsoft Entra **изменить размер**.



4. Отобразится список со всеми возможными номерами SKU, которые можно обновить или уменьшить в зависимости от лицензий, доступных в вашем инвентаре. Вы можете обновить или перейти на более раннюю версию ОЗУ и виртуальный ЦП облачного компьютера. Вы можете обновить только хранилище дисков ОС. При уменьшении объема облачного компьютера пользователя параметры с меньшим объемом хранилища будут неактивны. Выберите один из доступных вариантов.
5. Выберите **Изменить размер**.
6. Облачный компьютер пользователя помещается в состояние "**Изменение размера ожидающей лицензии**", как показано в колонке Windows 365 подготовки.
7. Выберите **Пользователи**> найдите имя пользователя, назначенное облачному компьютеру, и выберите его >**Группы**.
8. Чтобы получить старую лицензию, удалите пользователей из исходного источника Microsoft Entra группы. Если вы не выполните этот шаг, новый облачный компьютер будет подготовлен с исходной исходной лицензией после назначения целевой лицензии.

    - При использовании Microsoft Entra ID гибридной среды после удаления пользователя из исходной группы необходимо подождать, пока Microsoft Entra Connect не синхронизирует локальная служба Active Directory с вашим Microsoft Entra ID. Такая синхронизация может занять до 30 минут. Затем можно добавить пользователя в новую группу.

9. Назначьте целевую лицензию новой целевой группе Microsoft Entra. Теперь начинается процесс изменения размера.

Дальнейшие действия

Дополнительные сведения о размерах облачных компьютеров см. в этой статье.

Массовое изменение размера облачных компьютеров

Статья • 30.04.2025

Размер облачных компьютеров можно изменить в массовом режиме с помощью Microsoft Intune.

Массовое изменение размера может оказать большое влияние на масштаб. Перед изменением размера большой группы облачных компьютеров попробуйте изменить размер небольшой группы. Этот шаг поможет вам ознакомиться с процессом.

Одновременно можно изменить размер до 5000 облачных компьютеров.

Дополнительные сведения об изменении размера одного облачного компьютера см. в статье Изменение размера одного облачного компьютера.

Дополнительные сведения об изменении размера см. в статье Общие сведения об изменении размера облачного компьютера.

Требования

Требования к роли

Чтобы изменить размер облачного компьютера, администратор должен иметь определенные встроенные Microsoft Entra роли.

- Для облачного компьютера, подготовленного с прямой назначаемой лицензией, по крайней мере одна из следующих ролей
  - Администратор службы Intune
  - Intune читатель + роли Администратор облачного компьютера
  - читатель Intune и администратор Windows 365
- Для облачного компьютера, подготовленного с лицензией на основе группы, по крайней мере одна из следующих ролей
  - Администратор службы Intune
  - читатель Intune и администратор Windows 365
  - Помимо одной из трех предыдущих ролей, роль с Microsoft Entra разрешениями на чтение и запись в группах, а также разрешениями на лицензирование, например роль Windows 365 Администратор.

Кроме того, можно назначить пользовательскую роль, которая включает разрешения этих встроенных ролей.

Требования к IP-адресу

При изменении размера Microsoft Entra гибридного соединения с облачным компьютером с помощью собственной сети в подсети должен быть доступен второй IP-адрес для изменения размера облачного компьютера.

Во время операции изменения размера при переходе к новому размеру используется второй IP-адрес. Эта мера предосторожности гарантирует, что облачный компьютер может быть откатлен до исходного компьютера в случае возникновения проблемы.

Чтобы учесть эту меру предосторожности, вы можете:

- Убедитесь, что в виртуальной сети доступны соответствующие IP-адреса для всех облачных компьютеров, которые будут изменены, или
- Измените размер операций, чтобы убедиться, что адрес область поддерживается.

Если доступны неадекватные адреса, могут возникнуть ошибки изменения размера.

Другие требования

Чтобы использовать **Изменение размера** , в инвентаризации должны быть доступные лицензии для измененной конфигурации облачного компьютера.

Чтобы **изменить размер** облачного компьютера, он должен иметь состояние **Подготовлено** в узле подготовки Windows 365.

Массовое изменение размера облачных компьютеров, изначально подготовленных с помощью напрямую назначенных лицензий

1. Войдите в Центр администрирования Microsoft Intune, выберите **Устройства**>**Все устройства**>**Массовые действия**> устройств**ОС (Windows)**>**Выберите тип устройства (облачные компьютеры)**>**Действие устройства (изменение размера).**
2. На странице **Основные** сведения выберите **размер источника** для изменяемого размера облачных компьютеров.
3. Выберите **целевой размер** для измененных облачных компьютеров >**Далее**.
4. На странице **Устройства** выберите **Выбрать отдельные устройства в вашей среде**>**Далее**.
5. В разделе **Выберите устройства** выберите устройства, размер которого требуется изменить >**далее**.
6. На странице **Проверка и создание** нажмите кнопку **Создать**.

Массовое изменение размера облачных компьютеров, изначально подготовленных с помощью групповых лицензий

1. Войдите в Центр администрирования Microsoft Intune, выберите **Устройства**>**Все устройства**>**Массовые действия**> устройств**ОС (Windows)**>**Выберите тип устройства (облачные компьютеры)**>**Действие устройства (изменение размера).**
2. На странице **Основные** сведения выберите **размер источника** для изменяемого размера облачных компьютеров.
3. Выберите **целевой размер** для измененных облачных компьютеров >**Далее**.
4. На странице **Устройства** выберите **Применить это действие к устройствам, зарегистрированным для участников**> группы**Далее**.
5. В разделе **Выберите группы для включения** выберите группы, содержащие пользователей, владеющих устройствами, размер которых требуется изменить >**далее**.
6. На странице **Проверка и создание** нажмите кнопку **Создать**. Облачный компьютер пользователя помещается в состояние "**Изменение размера ожидающей лицензии**", как показано в колонке Windows 365 подготовки.
7. Выберите **Группы**> выберите группу, в которую **измененные**> лицензии > выберите старую лицензию >**Удалить лицензию**>**Да**>**Сохранить**. Повторите этот шаг для каждой группы, которую вы хотите изменить.
8. Выберите **Назначения,**> выберите лицензию, которую вы хотите изменить для облачных компьютеров, чтобы >**сохранить**. Облачный компьютер пользователя начинает изменять размер, который можно проверка в колонке подготовки Windows 365.

Массовое изменение подмножества облачных компьютеров, изначально подготовленных с помощью лицензий на основе групп

1. Создайте целевую группу Microsoft Entra. Добавьте пользователей из исходной Microsoft Entra группы, размер которой требуется изменить. Кроме того, можно использовать существующие Microsoft Entra группы, если вы сопоставляете группы с отдельными типами лицензий Windows 365.
2. Назначьте существующую политику подготовки, предназначенную для исходной группы Microsoft Entra источника, новой целевой группе Microsoft Entra. Это необходимо сделать, только если у вас нет дискретной группы Microsoft Entra для

назначения политики подготовки. Если у вас есть дискретные Microsoft Entra группы для управления назначениями политик подготовки, этот шаг можно опустить.

3. Войдите в Центр администрирования Microsoft Intune, выберите **Устройства**>**Все устройства**>**Массовые действия**> устройств**ОС (Windows)**>**Выберите тип устройства (облачные компьютеры)**>**Действие устройства (изменение размера).**
4. На странице **Основные** сведения выберите **размер источника** для изменяемого размера облачных компьютеров.
5. Выберите **целевой размер** для измененных облачных компьютеров >**Далее**.
6. На странице **Устройства** выберите **Применить это действие к устройствам, зарегистрированным для участников**> группы**Далее**.
7. В разделе **Выберите группы для включения** выберите группы, содержащие пользователей, владеющих устройствами, размер которых требуется изменить >**далее**.
8. На странице **Проверка и создание** нажмите кнопку **Создать**. Облачный компьютер пользователя помещается в состояние "**Изменение размера ожидающей лицензии**", как показано в колонке Windows 365 подготовки.
9. Чтобы получить старую лицензию, удалите пользователей из исходного источника Microsoft Entra группы. Если вы не выполните этот шаг, после назначения целевой лицензии будет подготовлен новый облачный компьютер с исходной лицензией.

    - При использовании Microsoft Entra ID гибридной среды после удаления пользователя из исходной группы необходимо подождать, пока Microsoft Entra Connect не синхронизирует локальная служба Active Directory с вашим Microsoft Entra ID. Эта синхронизация может занять до 30 минут. Затем можно добавить пользователя в новую группу.

10. Назначьте целевую лицензию новой целевой группе Microsoft Entra. Теперь начинается процесс изменения размера.

Дальнейшие действия

Дополнительные сведения о размерах облачных компьютеров см. в этой статье.

Изменение размера Windows 365 Frontline облачных компьютеров в выделенном режиме (предварительная версия)

Статья • 01.05.2025

Политику подготовки можно использовать для изменения размера Windows 365 Frontline облачных компьютеров в выделенном режиме.

размер Windows 365 Frontline облачных компьютеров в режиме общего доступа изменить нельзя.

Изменение размера Windows 365 Frontline облачных компьютеров в выделенном режиме доступно в общедоступной предварительной версии.

Дополнительные сведения об изменении размера см. в статье Общие сведения об изменении размера облачного компьютера.

Требования

Требования к роли

Чтобы изменить размер облачного компьютера, администратор должен иметь определенные встроенные Microsoft Entra роли.

- Для облачного компьютера, подготовленного с прямой назначаемой лицензией, по крайней мере одна из следующих ролей
  - Администратор службы Intune
  - Intune читатель + роли Администратор облачного компьютера
  - читатель Intune и администратор Windows 365
- Для облачного компьютера, подготовленного с лицензией на основе группы, по крайней мере одна из следующих ролей
  - Администратор службы Intune
  - читатель Intune и администратор Windows 365
  - Помимо одной из трех предыдущих ролей, роль с Microsoft Entra разрешениями на чтение и запись в группах, а также разрешениями на лицензирование, например роль Windows 365 Администратор.

Кроме того, можно назначить пользовательскую роль, которая включает разрешения этих встроенных ролей.

Требования к IP-адресу

При изменении размера Microsoft Entra гибридного соединения с облачным компьютером с помощью собственной сети в подсети должен быть доступен второй IP-адрес для изменения размера облачного компьютера.

Во время операции изменения размера при переходе к новому размеру используется второй IP-адрес. Эта мера предосторожности гарантирует, что облачный компьютер может быть откатлен до исходного компьютера в случае возникновения проблемы.

Чтобы учесть эту меру предосторожности, вы можете:

- Убедитесь, что в виртуальной сети доступны соответствующие IP-адреса для всех облачных компьютеров, которые будут изменены, или
- Измените размер операций, чтобы убедиться, что адрес область поддерживается.

Если доступны неадекватные адреса, могут возникнуть ошибки изменения размера.

Другие требования

Чтобы использовать **Изменение размера** , в инвентаризации должны быть доступные лицензии для измененной конфигурации облачного компьютера.

Чтобы **изменить размер** облачного компьютера, он должен иметь состояние **Подготовлено** в узле подготовки Windows 365.

Использование политики подготовки для изменения размера Windows 365 Frontline облачных компьютеров в выделенном режиме

1. Войдите в Центр администрирования Microsoft Intune, выберите **Устройства**>**Windows 365**>**Политики подготовки**.
2. Выберите политику подготовки, которая включает назначение с Windows 365 Frontline облачных компьютеров в выделенном режиме, размер которого требуется изменить.
3. На странице политики выберите **Изменить** рядом с **пунктом Назначения**.
4. На вкладке **Назначения** в столбце **Размер облачного компьютера** выберите запись Переднюю линию облачного компьютера, размер которой требуется изменить.

Размер всех облачных компьютеров в назначении будет изменен.

5. В области **Выбор размера облачного компьютера** в разделе **Доступные размеры** выберите новый размер > облачного компьютера **Далее**.
6. На странице **Назначения** нажмите кнопку **Далее**.
7. На вкладке **Просмотр и сохранение** выберите **Обновить** , чтобы инициировать изменение размера.

Ход изменения размера можно отслеживать на странице **Все облачные компьютеры** и отчете **о действиях облачного компьютера**.

Дальнейшие действия

Дополнительные сведения о размерах облачных компьютеров см. в этой статье.

Установка ограничений на время сеанса для облачных компьютеров Windows 365 Frontline

Статья • 03.04.2025

Ограничения по времени сеанса определяют, как долго пользователи неактивны в вашей организации до выхода из сеанса Windows 365 Frontline облачного компьютера. Существует два типа ограничений по времени:

- Ограничения по времени для сеанса активных, но неактивных удаленных рабочих столов.
- Ограничения времени для отключенных сеансов.

Ограничения по времени помогают защитить конфиденциальные данные компании и добавить еще один уровень безопасности для конечных пользователей, работающих на общих устройствах.

Windows 365 Frontline облачных компьютеров в выделенном режиме

Windows 365 Frontline облачных компьютерах в выделенном режиме поддерживайте сеанс пользователя активным до следующих действий:

- Облачный компьютер бездействует в течение 30 минут (значение по умолчанию). За две минуты до ограничения времени простоя пользователь получает уведомление с помощью диалогового окна.
- Пользователь выходит из облачного компьютера с помощью меню "Пуск".
- Браузер или Windows App закрыты (в результате чего облачный компьютер будет отключен).

Windows 365 Frontline облачные компьютеры в выделенном режиме остаются включено в течение двух часов после того, как сеанс пользователя становится неактивным. В течение этого неактивного времени параллелизм сеанса не используется.

Windows 365 Frontline облачных компьютеров в режиме общего доступа

Windows 365 Frontline облачных компьютерах в режиме общего доступа поддерживайте сеанс пользователя активным до следующих действий:

- Облачный компьютер бездействует в течение 15 минут (значение по умолчанию).
- Пользователь выходит из облачного компьютера с помощью меню "Пуск".
- Сеанс пользователя остается отключенным более 30 минут (значение по умолчанию).

Если пользователь забыл отключиться или выйти из нее, это может помешать другим пользователям подключаться к компьютерам Frontline Cloud, так как достигнуто максимальное количество активных сеансов. Чтобы избежать этой проблемы, можно создать профиль конфигурации для применения ограничений времени сеанса простоя и отключения ограничений времени на всех облачных компьютерах Frontline.

Изменение ограничений времени сеанса простоя

Ограничения времени сеанса простоя определяют время автоматического отключения пользователя от Windows 365 Frontline облачного компьютера.

1. Войдите в Центр администрирования Microsoft Intune, выберите **Конфигурация устройств**> (в разделе **Управление устройствами**) >**Создать**>**новую политику**.

2. В **разделе Создание профиля** выберите следующие параметры:

   - **Платформа**: Windows 10 и более поздних версий
   - **Тип профиля**: каталог параметров

3. Нажмите **Создать**.

4. На странице **Основные сведения** укажите имя и необязательное описание >**Далее**.

5. В разделе **Параметры конфигурации** нажмите **Добавить параметры**.

6. В разделе **Средство выбора параметров** найдите "Ограничения времени сеанса".

7. В разделе **Обзор по категории** выберите **Административные шаблоны\Компоненты Windows\Службы удаленных рабочих столов\Узел**

сеансов удаленных рабочих столов\Ограничения времени сеанса.

8. Установите флажок **Задать ограничение времени для активного, но простоя сеанса служб удаленных рабочих столов**.

9. В разделе **Создание профиля** разверните узел **Административные шаблоны**> включить **установить ограничение времени для активных, но неактивных сеансов служб удаленных рабочих столов**.

10. В поле **Ограничение сеанса простоя (устройство)** выберите ограничение времени, соответствующее требованиям вашей компании. Когда облачный компьютер frontline простаит в течение этого периода времени, облачный компьютер автоматически отключается.

11. Нажмите кнопку **Далее**.

12. На странице **Теги области** выберите теги область, которые требуется >**далее**.

13. На странице **Назначения** добавьте группы, которые вы хотите предоставить облачные компьютеры > Frontline **Далее**.

14. На странице **Проверка и создание** нажмите кнопку **Создать**.

Изменение ограничений времени сеанса отключения

Ограничение времени сеанса отключения — это время, пока пользователь не выйдет из компьютера Frontline Cloud автоматически.

1. Войдите в Центр администрирования Microsoft Intune, выберите **Конфигурация устройств**> (в разделе **Управление устройствами**) >**Создать**>**новую политику**.

2. В **разделе Создание профиля** выберите следующие параметры:

   - **Платформа**: Windows 10 и более поздних версий
   - **Тип профиля**: каталог параметров

3. Нажмите **Создать**.

4. На странице **Основные сведения** укажите имя и необязательное описание >**Далее**.

5. В разделе **Параметры конфигурации** нажмите **Добавить параметры**.

6. В разделе **Средство выбора параметров** найдите "Ограничения времени сеанса".

7. В разделе **Обзор по категории** выберите **Административные шаблоны\Компоненты Windows\Службы удаленных рабочих столов\Узел сеансов удаленных рабочих столов\Ограничения времени сеанса**.

8. Установите флажок **Задать ограничение времени для отключенных сеансов**.

9. В разделе **Создание профиля** разверните узел **Административные шаблоны**> включить **параметр Задать ограничение времени для отключенных сеансов**.

10. В разделе **Завершение отключенного сеанса (устройство)** выберите ограничение времени, соответствующее требованиям вашей компании. Если компьютер Frontline Cloud отключен в течение этого периода времени, пользователь автоматически выходит из облачного компьютера.

11. Нажмите кнопку **Далее**.

12. На странице **Теги области** выберите теги область, которые требуется >**далее**.

13. На странице **Назначения** добавьте группы, которые вы хотите предоставить облачные компьютеры > Frontline **Далее**.

14. На странице **Проверка и создание** нажмите кнопку **Создать**.

Дальнейшие действия

Управление облачными компьютерами.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Восстановление на определенный момент времени для Windows 365 Корпоративная

15.08.2025

Функция восстановления до состояния на определенный момент времени дает возможность администратору восстановить облачный компьютер до точного состояния, в котором этот компьютер ранее находился в определенный момент времени. Вы можете создать новые или изменить параметры , чтобы автоматически создавать точки восстановления через регулярные интервалы для групп облачных компьютеров. Вы также можете создавать точки восстановления по запросу для определенного времени. Администраторы также могут предоставить пользователям разрешение восстанавливать их собственные облачные компьютеры.

Параметры точек восстановления

Существует три разных способа задания точек восстановления:

- Краткосрочные точки восстановления
- Точки долгосрочного восстановления
- Точки восстановления по запросу вручную

Каждый тип точки восстановления можно восстановить одинаковым образом.

Краткосрочные точки восстановления

Вы можете задать краткосрочные точки восстановления каждые 4, 6, 12, 16 или 24 часа. Каждый облачный компьютер в назначенных группах имеет 10 точек краткосрочного восстановления, сохраненных с интервалами, определенными в параметре пользователя. Например, если выбран четырехчасовой интервал, каждый назначенный облачный компьютер имеет 10 точек восстановления, распределенных каждые четыре часа за последние 40 часов.

Точки долгосрочного восстановления

В дополнение к настраиваемым краткосрочным точкам восстановления существуют также четыре точки долгосрочного восстановления, которые не настраиваются. Долгосрочные точки восстановления сохраняются через каждые семь дней.

Точка восстановления по запросу вручную

Точки восстановления вручную позволяют администраторам при необходимости создавать точку восстановления как для одного облачного компьютера, так и для групп облачных компьютеров (с помощью массовых действий).

Среди прочего, полезны точки ручного восстановления по запросу:

- Для создания резервной копии перед выполнением действий по управлению.
- Во время отключения сотрудников с общим доступом к точке восстановления.

Только администраторы могут создать точку восстановления вручную, и каждый облачный компьютер может иметь только одну точку восстановления вручную за раз.

Срок действия точек восстановления

Для краткосрочных и долгосрочных точек восстановления по мере того как время проходит и добавляется новая точка восстановления, самая старая точка восстановления удаляется.

Каждый облачный компьютер может иметь одну точку восстановления вручную. При создании другой точки восстановления вручную для облачного компьютера, на который уже есть точка восстановления вручную, существующая точка восстановления перезаписывается новой точкой восстановления. Если точка восстановления не перезаписывается, срок действия точки восстановления вручную истекает примерно через 28 дней. Точки восстановления вручную имеют дату окончания срока действия, показывающую время их создания.

Восстановление облачных компьютеров, отмененных из-за истечения срока действия лицензии

Для Windows 365 Корпоративная облачных компьютеров, которые были отменены из-за истечения срока действия лицензии на Windows 365 Корпоративная, сохраняется snapshot хранения. Если следовать предварительным требованиям, вы можете восстановить облачный компьютер до момента его отзыва.

Чтобы следовать предварительным требованиям для восстановления облачных компьютеров, выполните следующие действия:

- Убедитесь, что истек срок действия лицензий Windows 365 продлен. Они должны иметь один номер SKU.

- Убедитесь, что политика подготовки отзываемого облачного компьютера по-прежнему существует.
- Убедитесь, что назначения с нужными пользователями назначены политике подготовки.
- Убедитесь, что конечные пользователи по-прежнему существуют, по-прежнему назначаются тем же Entra ID группам, что и раньше, или группам, включенным в назначения политики.

При соблюдении указанных выше предварительных требований после продления лицензии необходимо подготовить новый облачный компьютер для всех конечных пользователей, потерявших облачные компьютеры. После успешной подготовки облачных компьютеров вы можете по отдельности восстановить облачные компьютеры с помощью моментальных снимков хранения, эффективно восстанавливая потерянный облачный компьютер. Срок snapshot хранения истекает через 28 дней, и этот обратный отсчет отслеживается рядом с snapshot хранения в списке точек восстановления.

Риски и результаты восстановления облачного компьютера

С облачными компьютерами связаны те же риски, что и со всеми компьютерами Windows при выполнении полного восстановления диска. К этим рискам и результатам относятся:

- Все изменения, внесенные в облачный компьютер между сохраненной точкой восстановления и началом восстановления, будут потеряны. Эти потерянные сведения включают все данные, документы, установленные приложения, конфигурации, загрузки и другие изменения. Внешние данные, хранящиеся в облачных службах, например OneDrive, не будут потеряны.
- В различных приложениях, агентах и средствах также используются развертываемые пароли, секреты, сертификаты и ключи. Если какие-либо из этих учетных данных обновлены между текущим моментом и точкой восстановления, это повлияет на связанную службу или приложение.
- Вероятность потери данных и автоматического обновления пароля учетной записи компьютера повышается с увеличением промежутков времени между выбранной точкой восстановления и текущим моментом.

Рекомендации

- Чтобы свести к минимуму потерю данных и риск конфликта развертываемого пароля, выберите точку восстановления, наиболее близкую к текущему моменту.
- После завершения восстановления пользователь должен немедленно войти в свой облачный компьютер, чтобы убедиться в возможности подключения. Если пользователь не может подключиться или наблюдается неожиданное поведение, попробуйте второе восстановление до другой (более свежей) точки восстановления. В редких случаях может потребоваться повторная подготовка или сброс облачного компьютера, если все точки восстановления имеют устаревшие развертываемые учетные данные.

Неработоспособная точка восстановления

При просмотре списка точек восстановления для облачного компьютера Windows 365 отмечает все неработоспособные моментальные снимки значком символа треугольника (⚠). Неработоспособные snapshot имеют низкую вероятность успешного восстановления облачного компьютера. Это состояние рекомендаций не блокирует использование snapshot для любых действий (таких как экспорт, восстановление, общий доступ).

Аварийное восстановление

При запуске восстановления виртуальная инфраструктура, используемая для облачного компьютера, остается неизменной. Если инфраструктура недоступна, но соответствующая альтернативная инфраструктура доступна в том же регионе Azure, облачный компьютер автоматически помещается в доступную инфраструктуру. Эта автоматизация гарантирует, что для сценария аварийного восстановления в зоне Azure облачный компьютер устойчив к восстановлению в другой зоне в регионе. Восстановление в альтернативной инфраструктуре выполняется автоматически. Администратору или пользователю не требуется ничего, кроме как начать восстановление.

Дальнейшие действия

- Чтобы приступить к работе с краткосрочными и долгосрочными точками восстановления, необходимо сначала настроить параметры восстановления на определенный момент времени. После этого администраторы смогут выполнять следующие действия:
  - Восстановление одного облачного компьютера (пользователи с необходимыми разрешениями также могут восстановить собственный облачный компьютер).
  - Массовое восстановление нескольких облачных компьютеров .

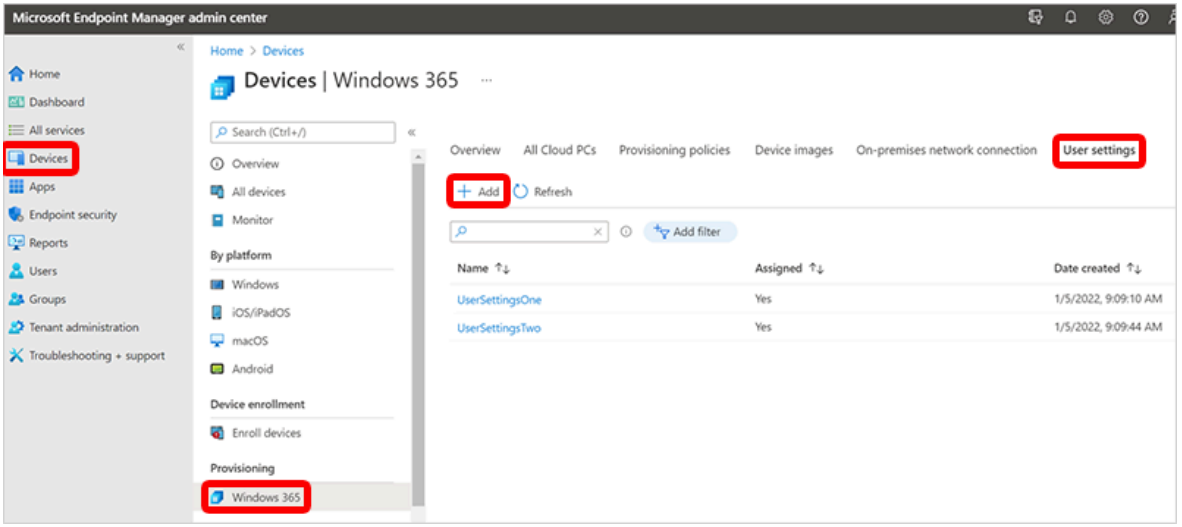
- Создание точек восстановления по запросу вручную.
- Ознакомьтесь с разделом Известные проблемы с восстановлением облачного компьютера.

Настройка параметров восстановления на момент времени

Статья • 31.01.2025

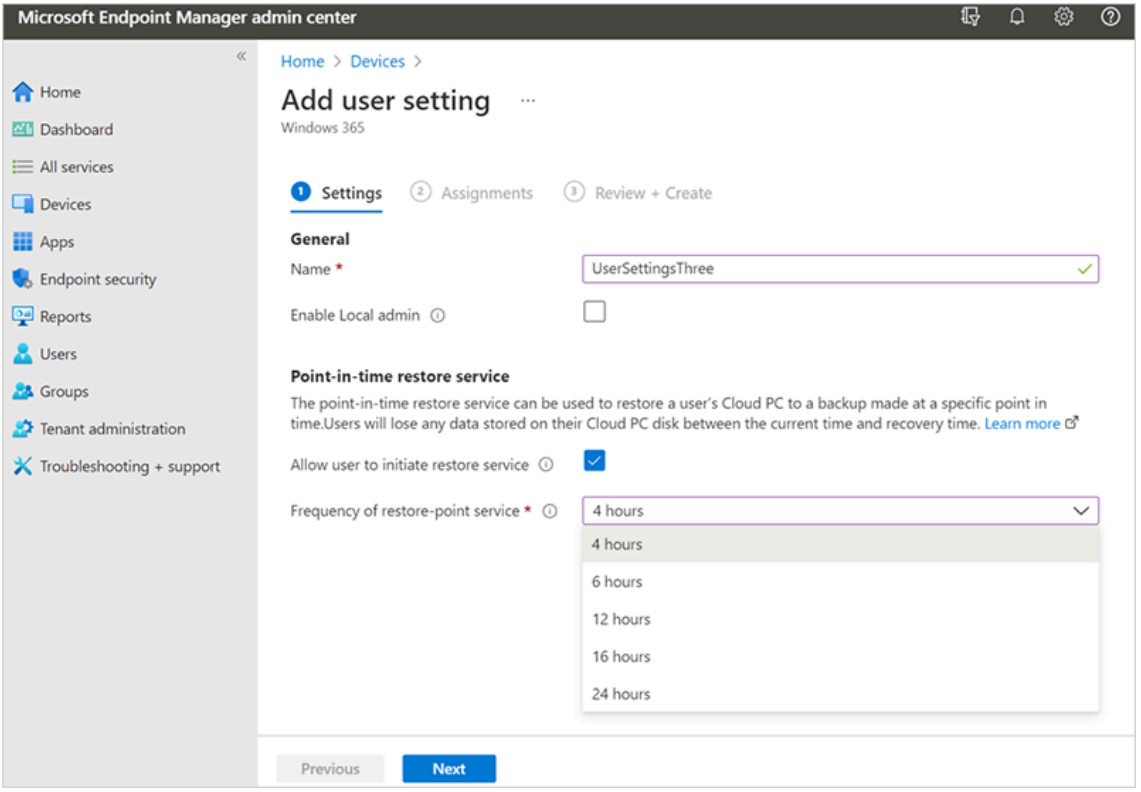
Восстановление до точки во времени можно настроить в новом или существующем параметре пользователя. Все пользователи в группах, которые назначены параметру пользователя, имеют разрешение на использование функции восстановления до точки во времени. Вы можете настроить восстановление до точки во времени, чтобы корпоративные пользователи могли начать восстановление на облачном компьютере. Кроме того, в системе можно настроить другую частоту для краткосрочных точек восстановления.

1. Войдите в центр > администрирования Microsoft Intune**Устройства**> Windows 365 >**Параметры**>**пользователя Добавить**. (Кроме того, можно изменить существующий параметр пользователя.)



2. На странице **Добавление параметра пользователя**:
   a. Введите **имя**.
   b. Если вы хотите, чтобы у пользователей этого параметра были локальные права администратора, выберите **Разрешить права локального администратора**.
   c. Если вы хотите, чтобы у конечных пользователей были разрешения на восстановление собственных облачных компьютеров, выберите **Разрешить пользователю инициировать службу восстановления**.
   d. Для **частоты создания точек восстановления** выберите интервал для частоты создания точек восстановления. Существует ограничение в 10 точек восстановления. Таким образом, более короткая частота приводит к меньшему общему объему истории точек восстановления.

e. Нажмите кнопку **Далее**.



3. На странице **Назначения** выберите группы, для которых требуется установить этот параметр >**Далее**.
4. На странице **Проверка и создание** убедитесь, что выбран вариант >**Готово**.

Пользователи в группах, которые назначены этому параметру пользователя, теперь смогут использовать функцию восстановления на момент времени, как описано ниже.

Дальнейшие действия

- Восстановление одного облачного компьютера
- Массовое восстановление нескольких облачных компьютеров

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Создание точек восстановления по запросу вручную для облачных компьютеров

Статья • 31.01.2025

Точки восстановления облачного компьютера можно создавать вручную как по отдельности, так и в массовом режиме.

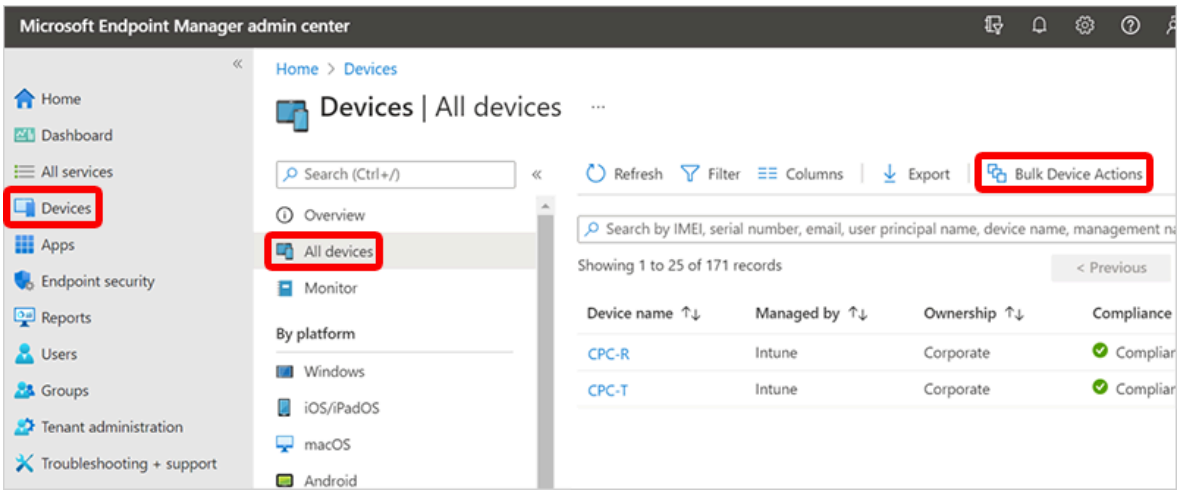
Создание одной точки восстановления вручную

1. Войдите вцентр >администрирования Microsoft IntuneУстройства >**Все устройства**> выберите **устройство**> Точки > восстановления**Создать точки восстановления**.
2. (Optiona) Если вы хотите предоставить точку восстановления учетной записи хранения, выберите **Создать новую точку восстановления для общего доступа**. В этом случае необходимо также выбрать **подписку**, **учетную запись хранения** и **уровень доступа**.
3. Выберите **Создать точки**> восстановления**Да**.

Будет создана новая точка восстановления. Чтобы новая точка восстановления появилась в списке точек восстановления, может потребоваться до часа. Если точка восстановления уже существует для этого облачного компьютера, она будет перезаписана новой точкой восстановления.

Массовое создание нескольких точек восстановления вручную

1. Войдитев центр >администрирования Microsoft IntuneУстройства >**Все устройства**>**Массовые действия устройств**.



2. На странице **Базовые** выберите следующие параметры:

   - **ОС**: Windows
   - **Тип устройства**: облачные компьютеры
   - **Действие устройства**: создание точек восстановления

3. (Необязательно) Если вы хотите предоставить точку восстановления учетной записи хранения, выберите **Создать новую точку восстановления для общего доступа**. Затем выберите следующие параметры:

   - **Подписка**: одна из ваших подписок Azure.
   - **Учетная запись хранения**
   - **Уровень доступа**

4. Нажмите кнопку **Далее**.
5. На странице **Устройства** выберите **Выбрать устройства для включения**.
6. В разделе **Выбор устройств** выберите облачные компьютеры, на которые нужно создать точки восстановления вручную, для >**параметра Нажмите кнопку**>**Далее**.
7. На странице **Просмотр и создание** убедитесь, что выбран вариант >**Создать**.

Будут созданы новые точки восстановления. Для появления новых точек восстановления в списке точек восстановления может потребоваться до часа или более. Если на любом из выбранных облачных компьютеров уже есть точка восстановления, существующие точки восстановления будут перезаписаны.

Можно создавать точки массового восстановления на 5000 облачных компьютерах одновременно.

Дальнейшие действия

- Восстановление одного облачного компьютера
- Массовое восстановление нескольких облачных компьютеров

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

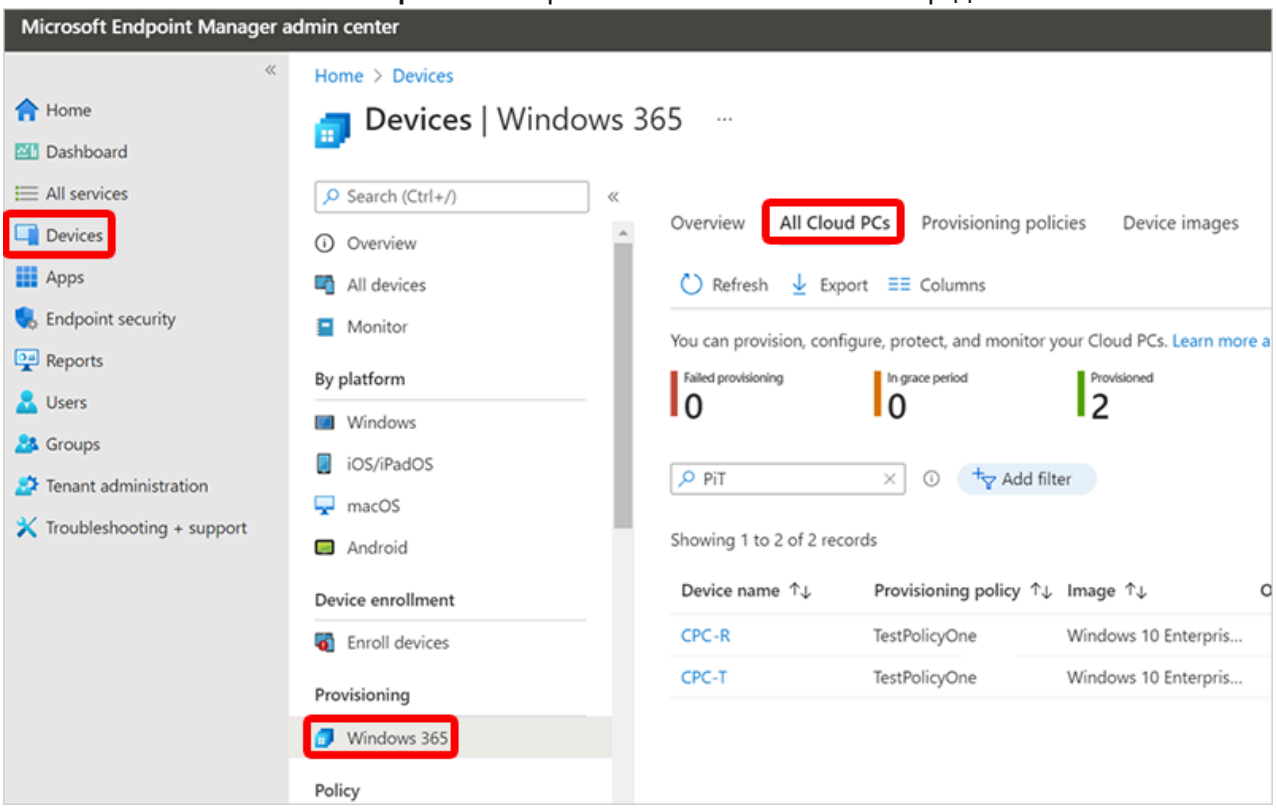
Отзыв о продукте

Восстановление одного облачного компьютера до предыдущего состояния

Статья • 30.04.2025

Вы можете использовать центр администрирования Microsoft Intune для восстановления облачного компьютера до предыдущего состояния.

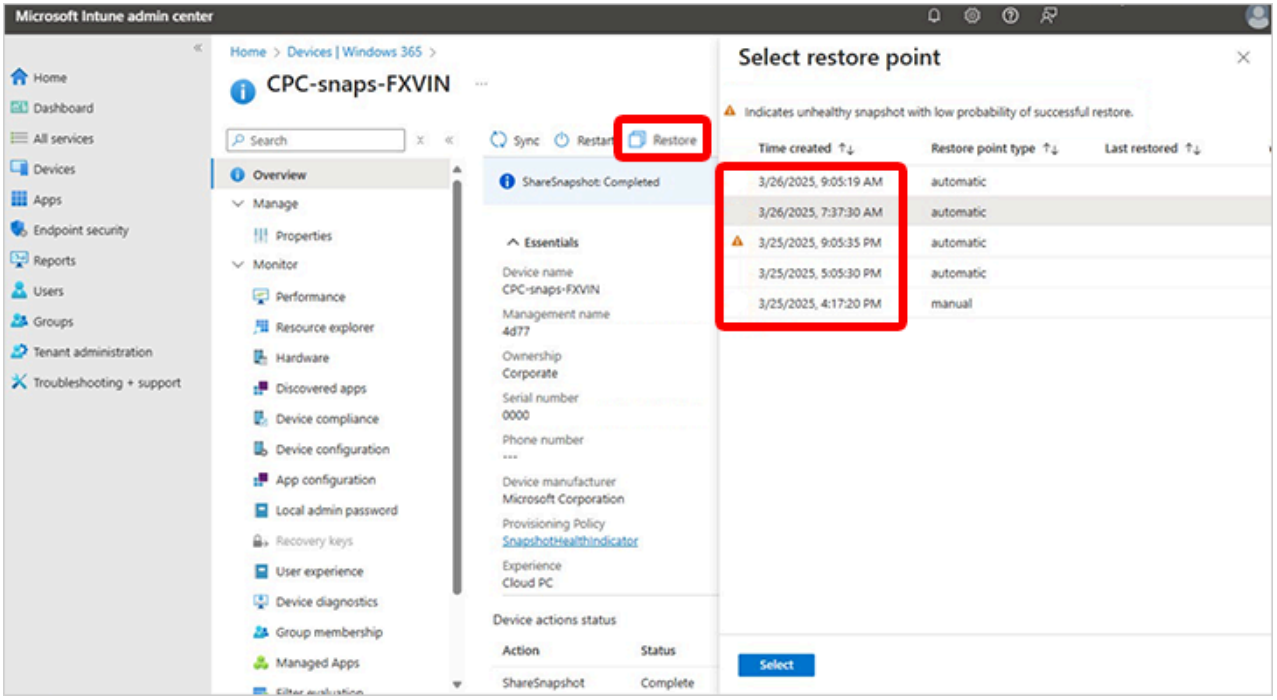
1. Войдите вцентр > администрирования Microsoft Intune**Устройства**> Windows 365 >**Все облачные компьютеры**> выберите облачный компьютер для восстановления.



2. Выберите **Восстановить**> в разделе **Выберите точку восстановления** и выберите точку, для которой нужно восстановить облачный компьютер, чтобы **выбрать**>.

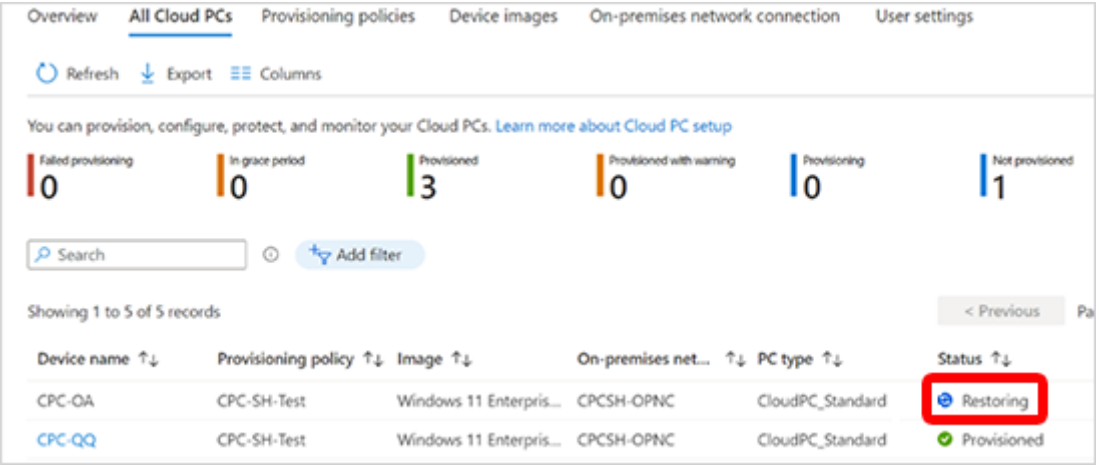
   Неработоспособные моментальные снимки отображаются в значке ⚠ ". Неработоспособные моментальные снимки можно использовать для

восстановления, но с меньшей вероятностью успешного восстановления.

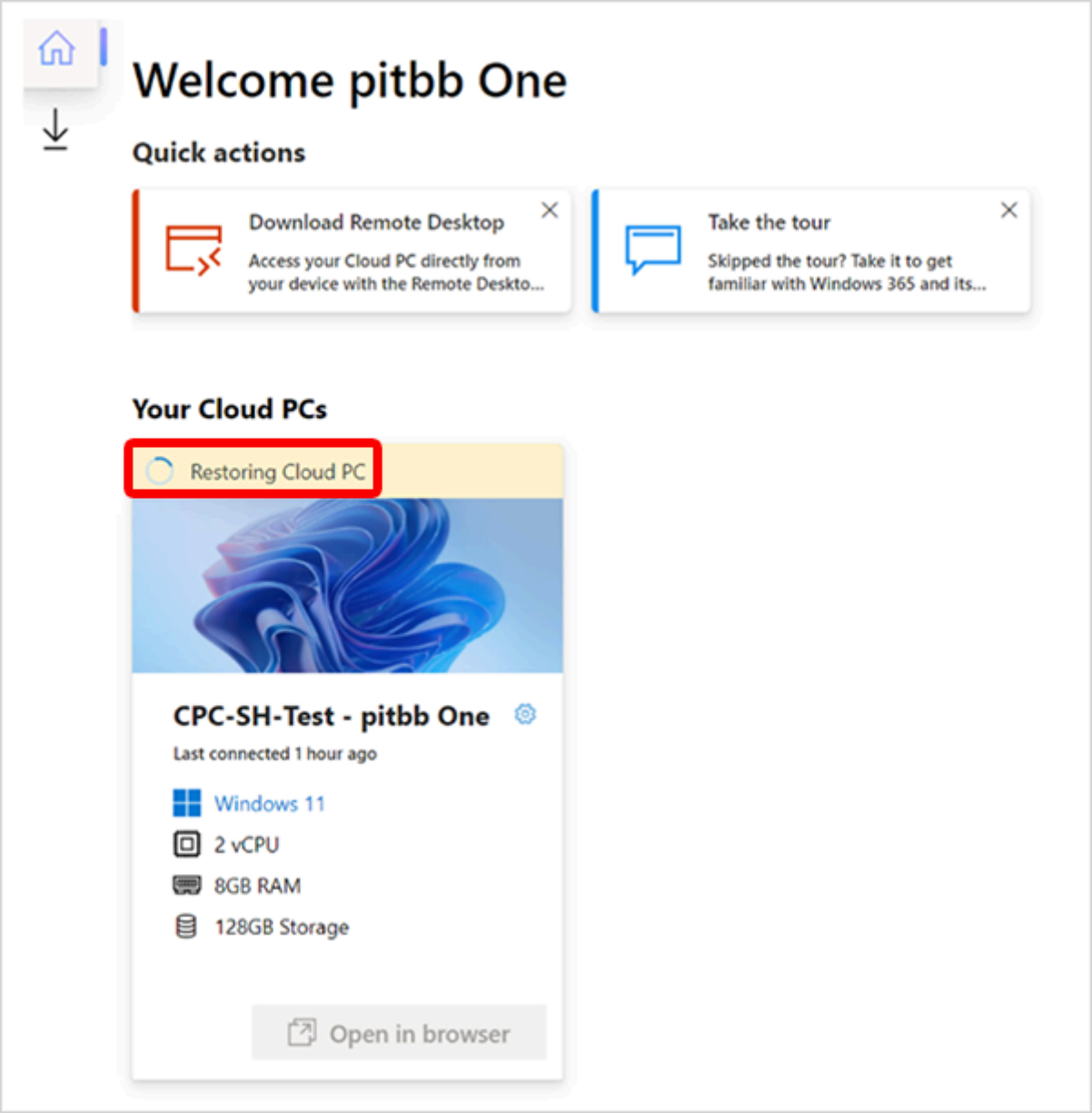


3. В диалоговом окне подтверждения выберите **Восстановить**.

На странице **Все облачные компьютеры** состояние устройства будет отображаться как **Идет восстановление** до завершения восстановления.



На странице пользователя windows365.microsoft.com состояние облачного компьютера будет отображаться как "Идет восстановление" до завершения восстановления.



Дальнейшие действия

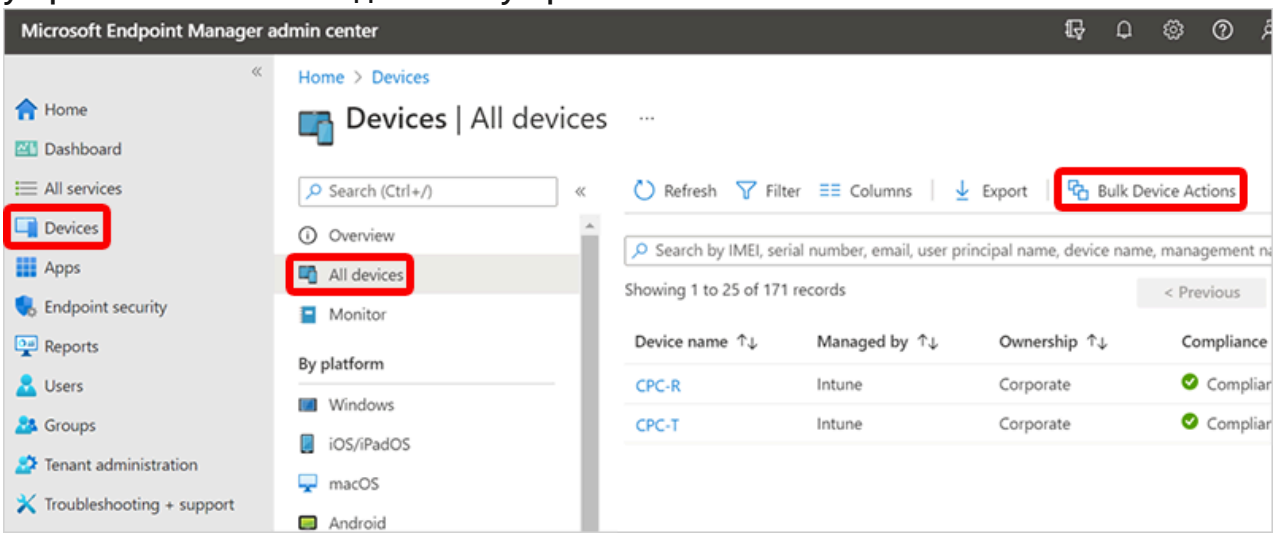
- Массовое восстановление нескольких облачных компьютеров

Восстановление нескольких облачных компьютеров одновременно

Статья • 19.04.2025

Центр администрирования Microsoft Intune можно использовать для массового восстановления нескольких облачных компьютеров.

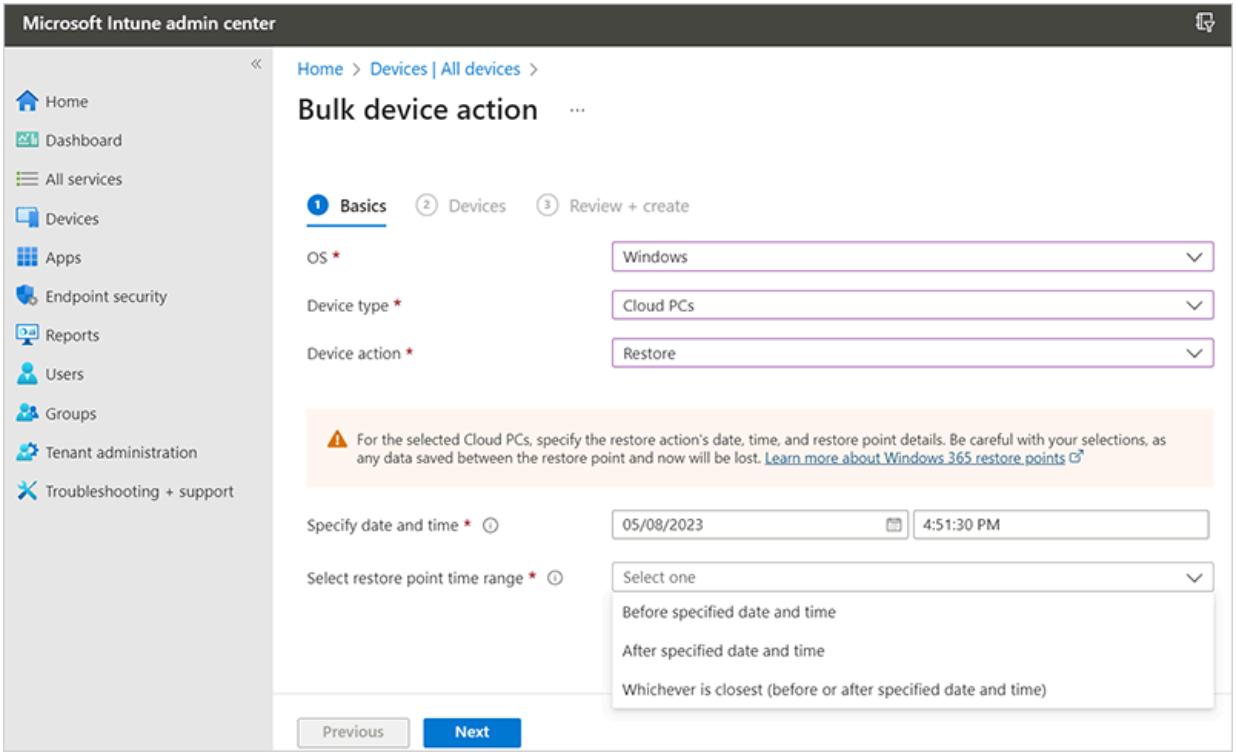
1. Войдитев центр >администрирования Microsoft Intune Устройства >**Все устройства**>**Массовые действия устройств**.



2. На странице **Базовые** выберите следующие параметры:
   a. **ОС**: Windows
   b. **Тип устройства**: облачные компьютеры
   c. **Действие устройства**: восстановление
   d. **Укажите дату и время**: выберите дату и время. Этот параметр определяет момент времени, до которого следует восстановить облачные компьютеры. Следующие параметры помогут точно определить, какая точка восстановления будет использоваться.
   e. **Выберите диапазон времени для точки восстановления**: выберите один из следующих вариантов:

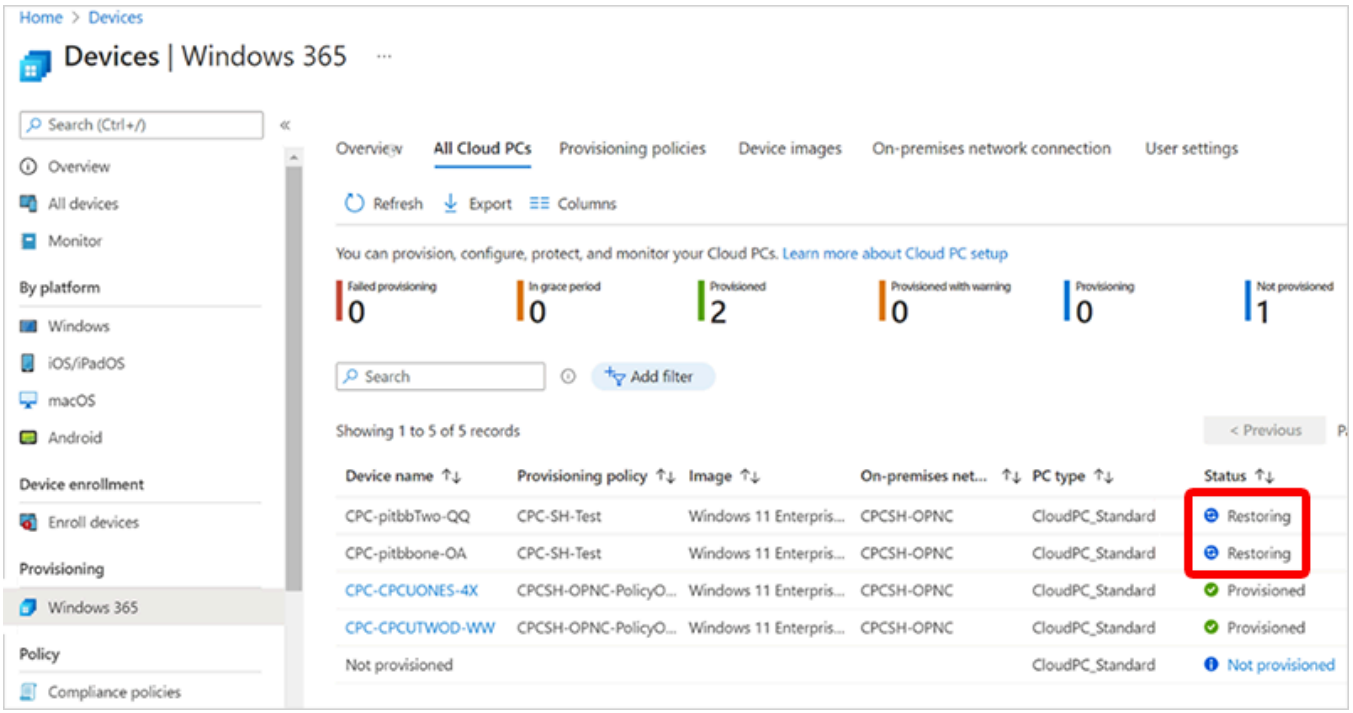
      - **До указанной даты и времени**: если выбрать этот параметр, облачные компьютеры будут восстановлены до ближайшей точки восстановления до указанной вами даты и времени.
      - **После указанной даты и времени**: если выбрать этот параметр, облачные компьютеры будут восстановлены до ближайшей точки восстановления после указанной вами даты и времени.
      - **Ближайшая точка восстановления (до или после указанной даты и времени)**: если выбрать этот вариант, облачный компьютер будет восстановлен с использованием точки восстановления, ближайшей к указанной даты и времени.

f. Если вы не хотите использовать неработоспособные моментальные снимки для процесса восстановления, выберите **Пропустить неработоспособные моментальные снимки, если все моментальные снимки неработоспособны для выбранного диапазона времени**. При выборе этого параметра при восстановлении используются только работоспособные моментальные снимки (если в выбранном диапазоне времени есть хотя бы один работоспособный snapshot). Если все моментальные снимки неработоспособны, для попытки восстановления используется тот, который соответствует другим критериям.



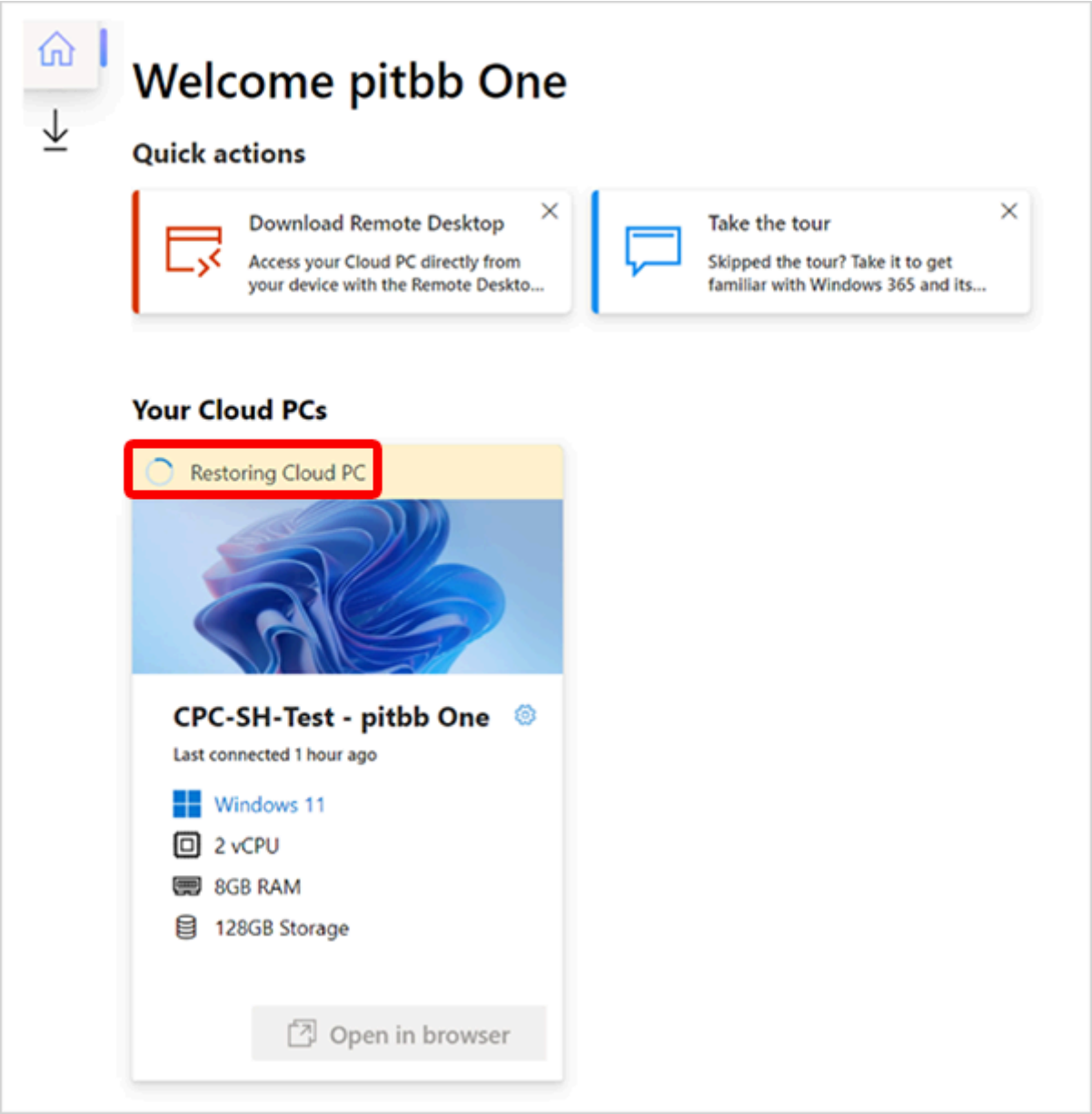
3. Нажмите кнопку **Далее**.
4. На странице **Устройства** выберите облачные компьютеры, которые требуется восстановить >**Далее**.
5. На странице **Просмотр и создание** убедитесь, что выбран вариант >**Создать**.

На странице **Все облачные компьютеры** состояние каждого устройства изменится на **Восстановление**, пока не будет завершено восстановление каждого устройства.



На странице windows365.microsoft.com каждого пользователя будет отображаться состояние облачного компьютера "восстановление", пока не будет завершено

восстановление.



Дальнейшие действия

- Восстановление одного облачного компьютера

Совместное использование точек восстановления облачного компьютера с учетной записью хранения Azure

Статья • 31.01.2025

Точки восстановления облачных компьютеров можно совместно использовать в учетной записи хранения как для отдельных облачных компьютеров, так и для массовых операций.

Может потребоваться предоставить общий доступ (переместить или скопировать) облачный компьютер и его содержимое в:

- Создайте географически распределенную копию облачного компьютера.
- Создайте копию облачного компьютера во время процесса отключения.
- Получение исторического представления облачного компьютера (или текущего) для обнаружения электронных данных.
- Создайте виртуальный жесткий диск, который можно подключить к физическому устройству.

Совместное использование одной точки восстановления

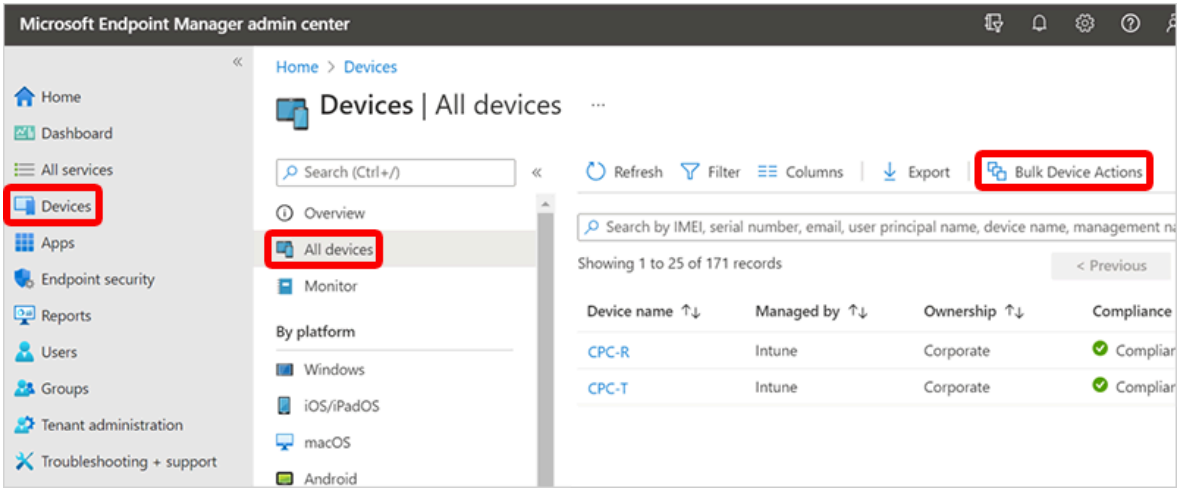
1. Войдите в центр > администрирования Microsoft Intune**Устройства**> Windows 365 >**Все облачные компьютеры**>, выберите **точки**> восстановления устройства>. Для точки восстановления выберите многоточие (**...**) >**Общий доступ**.
2. В области **Общая точка восстановления** выберите **подписку**, **учетную запись хранения** и **уровень доступа**.
3. Нажмите **Поделиться**.

В учетной записи хранения создается папка. Имя папки идентично имени облачного компьютера. Папка содержит VHD-копию диска устройства облачного компьютера.

Чтобы избежать проблем с истечением времени ожидания, одновременно предоставляйте до 3000 точек восстановления учетной записи хранения Azure.

Массовый общий доступ к нескольким точкам восстановления

1. Войдитев центр >администрирования Microsoft Intune Устройства >**Все устройства**>**Массовые действия устройств**.



2. На странице **Базовые** выберите следующие параметры:
   a. **ОС**: Windows
   b. **Действие устройства**: совместное использование точки восстановления облачного компьютера в хранилище
   c. **Укажите дату и время**: выберите дату и время. Этот параметр определяет точку восстановления облачного компьютера, к которому вы хотите предоставить общий доступ. Следующие параметры помогают точно определить, какая точка восстановления используется для каждого выбранного облачного компьютера.
   d. **Выберите диапазон времени для точки восстановления**: выберите один из следующих вариантов:

      - **До указанной даты и времени**. Предоставьте доступ к ближайшей точке восстановления облачного компьютера до указанной даты и времени.
      - **После указанной даты и времени**. Предоставление общего доступа к ближайшей точке восстановления облачного компьютера после указанной даты и времени.
      - **Какой бы ни был ближайший (до или после указанной даты и времени)**: предоставьте общий доступ к точке восстановления облачного компьютера, ближайшей к указанной дате и времени.

3. Выберите **Подписка**, **Учетная запись хранения** и **Уровень**> доступа**Далее**.
4. На странице **Устройства** выберите **Выбрать устройства для включения**.
5. В разделе **Выбор устройств** выберите облачные компьютеры, к которым вы хотите предоставить общий доступ к точкам восстановления, в поле >**Далее**>.

6. На странице **Просмотр и создание** убедитесь, что выбран вариант >**Создать**.

Для каждой общей точки восстановления облачного компьютера в учетной записи хранения создается папка. Имя папки идентично имени облачного компьютера. Папка содержит VHD-копию диска устройства облачного компьютера.

Дальнейшие действия

- Восстановление одного облачного компьютера
- Массовое восстановление нескольких облачных компьютеров
- Настройте учетную запись хранения Azure.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Использование RDP Multipath с Windows 365

Обзор

Протокол удаленного рабочего стола (RDP) Multipath повышает надежность и производительность подключения к Windows 365 облачным компьютерам за счет интеллектуального управления несколькими сетевыми путями. Эта функция обеспечивает беспроблемный пользовательский интерфейс даже в средах с переменными условиями сети.

RDP Multipath расширяет RDP Shortpath и использует интерактивное подключение (ICE) для динамического определения и выбора наиболее надежного транспортного пути в режиме реального времени.

> ⓘ **Внимание**
>
> **RDP Multipath теперь общедоступна и полностью развернута!** Все подходящие подключения пользуются повышенной надежностью и производительностью.

Преимущества RDP MultiPath

- **Простая интеграция**. Изменения конфигурации не требуются, кроме того, что ваша среда поддерживает RDP Shortpath.
- **Интеллектуальное управление путями**. ICE обнаруживает и оценивает несколько маршрутов Shortpath протокола удаленного рабочего стола (RDP) с помощью протокола UDP по протоколу STUN (простой обход под NAT) и TURN (обход с использованием ретрансляторов вокруг NAT).
- **Повышенная надежность**: пути резервного копирования остаются в режиме ожидания. Если активный путь становится нестабильным или завершается сбоем, RDP Multipath автоматически переключается на следующий оптимальный путь, уменьшая количество прерываний и прерываний сеанса.

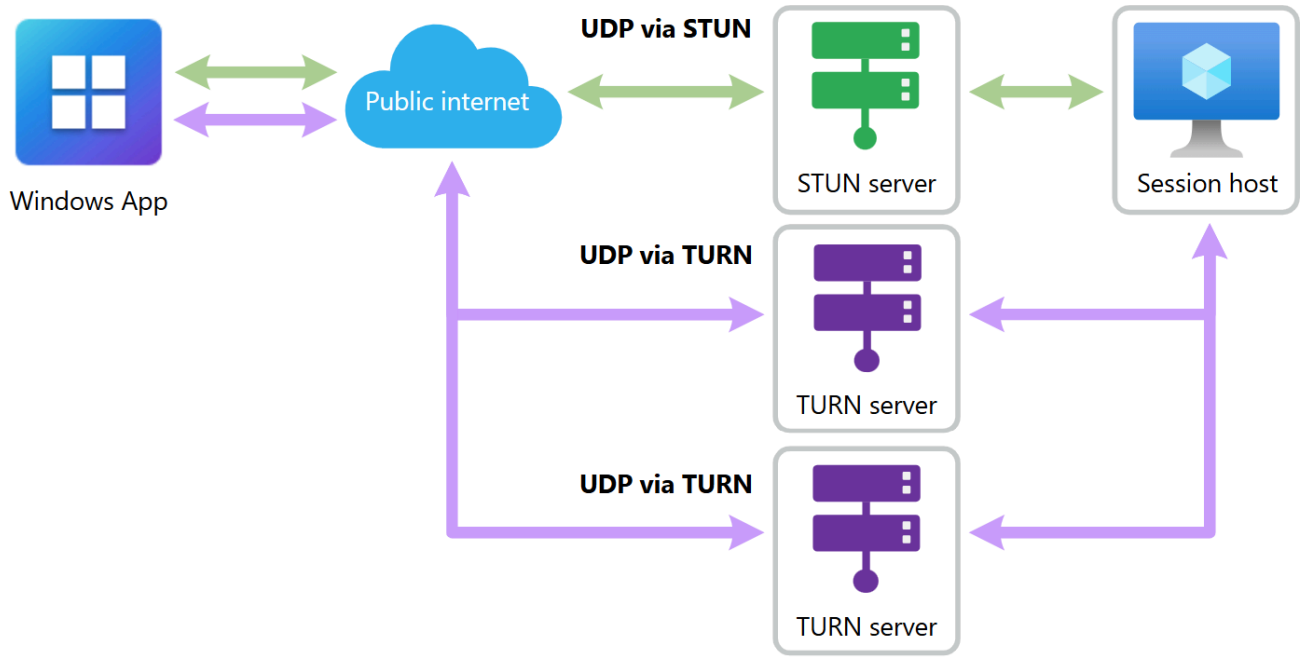
> ⓘ **Внимание**
>
> Если все пути завершаются ошибкой из-за сбоя локальной сети, система пытается повторно подключиться после восстановления подключения.

Как это работает?

RDP Multipath использует несколько сетевых путей, обнаруженных с помощью интерактивного подключения (ICE), для повышения надежности подключения. Эти пути могут включать такие сочетания, как UDP через STUN или UDP через ретранслятор. Если основное подключение завершается сбоем, система автоматически переключается на путь резервного копирования. Если все пути потеряны(например, во время сбоя сети), система пытается повторно подключиться после того, как сеть снова становится доступной.

> ⓘ **Примечание.**
>
> Эта версия Multipath не поддерживает пользователей, которые подключаются исключительно через WebSocket (на основе TCP).

Ниже приведен пример установки, которая может использовать UDP через STUN в качестве основного пути с двумя резервными UDP-подключениями через сервер TURN.

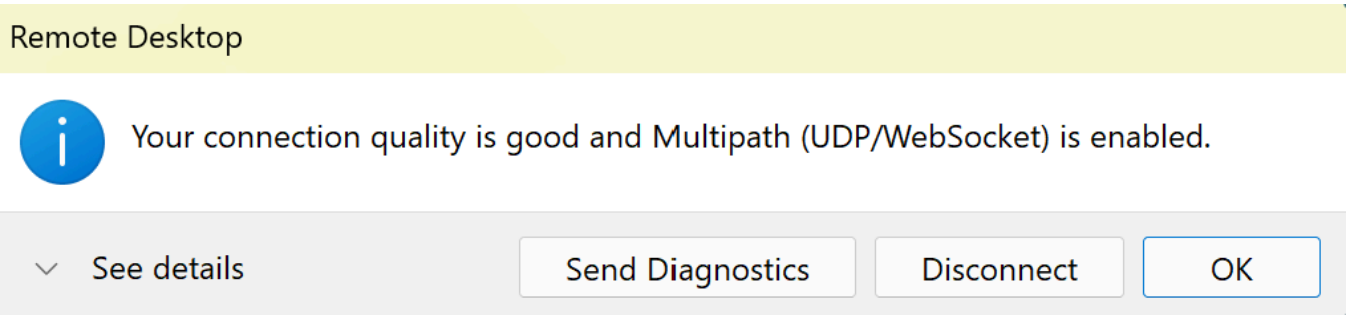


Требования

- **Включите RDP Shortpath для общедоступных сетей:** Чтобы включить RDP Shortpath для общедоступных сетей, перейдите на следующую страницу и следуйте инструкциям: Включение RDP Shortpath для общедоступных сетей.
- **Версия клиента**. Требуется последняя версия клиента удаленного рабочего стола с минимальными версиями: **MSRDC 1.2.6353 или более поздней** версии и **Windows App 2.0.559.0 или более поздней версии**.

Проверка подключения по протоколу RDP Multipath

Пользователи могут проверка состояние подключения удаленного сеанса с панели подключения, на которой показано, что RDP Multipath включен, как показано на следующем снимке экрана:



Управление доступностью RDP Multipath

RDP Multipath развертывается поэтапно.
Если у вас возникли проблемы и вы хотите временно отключить его или попробовать его на ранних этапах, вы можете вручную включить или отключить его на узлах сеансов с помощью следующего раздела реестра:

Включение RDP Multipath на ранних этапах (согласие):

Чтобы включить RDP Multipath вручную, выполните следующую команду в командной строке с повышенными привилегиями, чтобы задать для раздела реестра значение 100:

Bash

```bash
reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\RdpCloudStackSettings" /v SmilesV3ActivationThreshold /t REG_DWORD /d 100 /f
```

Отключение RDP Multipath на ранних этапах (отказ):

Чтобы отключить RDP Multipath вручную, выполните следующую команду в командной строке с повышенными привилегиями, чтобы задать для раздела реестра значение 0:

Bash

```bash
reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\RdpCloudStackSettings" /v SmilesV3ActivationThreshold /t REG_DWORD /d 0 /f
```

Примечание.

После обновления раздела реестра пользователи должны отключиться и повторно подключиться к узлу сеансов, чтобы их Облачный компьютер Windows 365, чтобы изменения вошли в силу.

Last updated on 11.11.2025

Использование RDP Shortpath для общедоступных сетей с Windows 365

Статья • 31.01.2025

Теперь вы можете использовать Shortpath RDP (протокол удаленного рабочего стола) для общедоступных сетей с облачными компьютерами с Windows 365. RDP Shortpath для общедоступных сетей может предоставить альтернативный путь подключения для лучшего подключения к облачному компьютеру, особенно при неоптимальных сетевых условиях.

Требования

Чтобы использовать RDP Shortpath для общедоступных сетей с Windows 365, необходимо выполнить следующие требования:

- Узел сеансов (облачный компьютер)
  - Исходящий UDP во все общедоступное IP-пространство (поскольку в большинстве случаев невозможно узнать исходный IP-адрес подключающегося компьютера).
  - Диапазоны IP-адресов STUN-сервера на UDP-порте 3478.
- Компьютерная сеть клиента
  - Исходящий UDP:
    - Общедоступные IP-адреса, назначенные шлюзу преобразования сетевых адресов (NAT) или Брандмауэр Azure в сценарии размещенной сети Azure.
    - Для сценария сети, размещенной на сервере Майкрософт, все пространства общедоступных IP-адресов.

Включение RDP Shortpath для общедоступных сетей

Чтобы включить RDP Shortpath для общедоступных сетей, перейдите на следующую страницу документации по Виртуальному рабочему столу Azure и следуйте инструкциям:

Включите RDP Shortpath для общедоступных сетей.

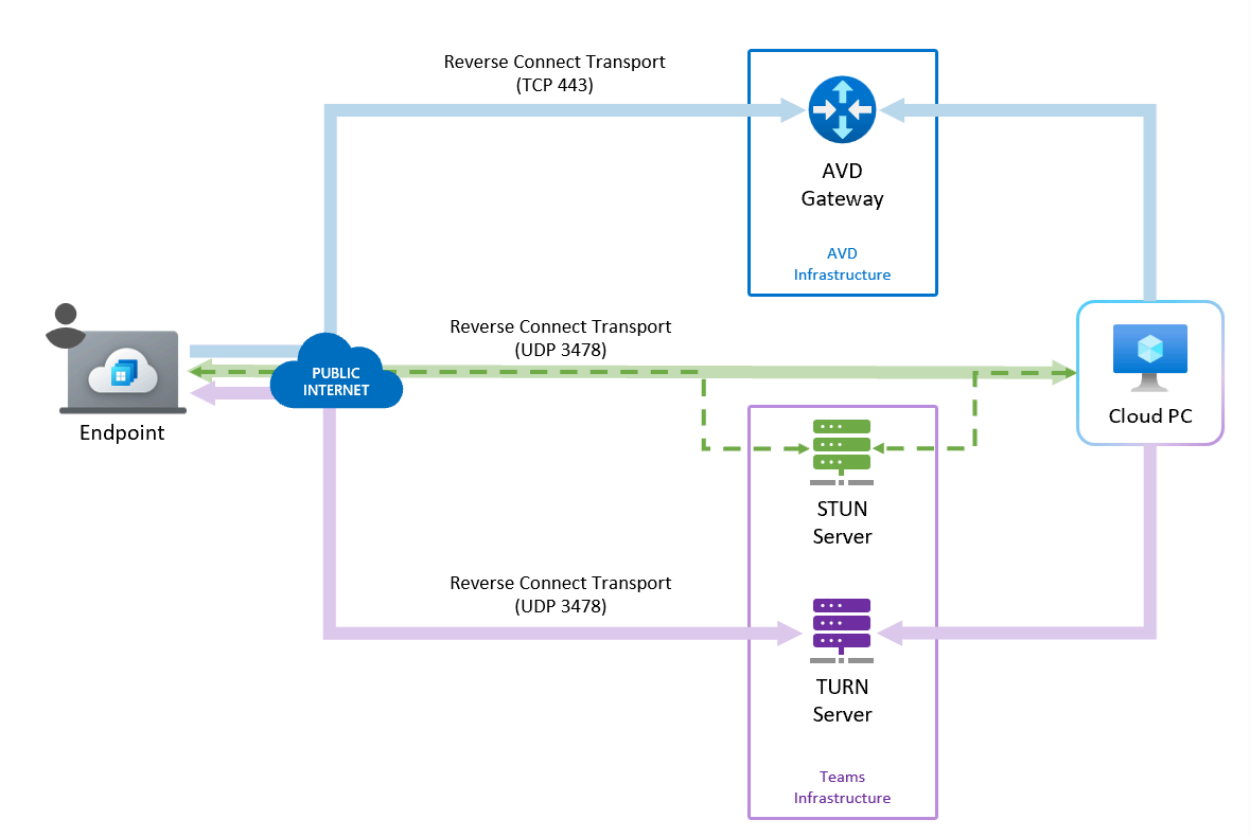
Проверка UDP-подключения

Соединение UDP можно проверить в разделе "Сведения о соединении" удаленного сеанса. Дополнительные сведения см. в разделе Проверка работы RDP Shortpath.

Преимущества RDP Shortpath

По умолчанию подключение к облачному компьютеру с Windows 365 осуществляется через TCP-подключение, которое проходит через шлюз с использованием транспорта обратного подключения. Обратный транспорт означает, что нет необходимости во входящем подключении к узлу сеанса (облачному компьютеру) для подключения трафика RDP.

RDP Shortpath улучшает TCP-подключение, предоставляя дополнительное прямое или ретрансляторное подключение между клиентом удаленного рабочего стола и Облачный компьютер Windows 365 с помощью UDP. Это повышает надежность подключения, сокращает задержки и увеличивает доступную пропускную способность.



Дополнительные сведения о преимуществах RDP Shortpath см. в разделе Ключевые преимущества.

Процесс подключения RDP Shortpath

При использовании RDP Shortpath соединение с облачным компьютером происходит следующим образом.

1. Соединение RDP устанавливает соединение на основе TCP с использованием транспорта обратного соединения через шлюз (аналогично соединению без RDP Shortpath).
2. Если на узле сеанса (облачном компьютере) включен короткий путь RDP, служба создает сокет UDP на всех жизнеспособных сетевых интерфейсах.
3. Чтобы проверить подключение, служба пытается подключиться к STUN-серверу Windows 365 в общедоступном Интернете через UDP-порт 3478. На этом шаге также устанавливается внешний IP-адрес маршрутизатора NAT.
4. В таблице кандидатов узла сеанса перечислены общедоступные IP-адреса и порт прослушивания, к которым он имеет доступное подключение. Эти сведения предоставляются подключаемому клиенту через установленный сеанс TCP.
5. Клиент отправляет свой список доступных общедоступных IP-адресов или портов на узел сеанса.
6. Обе стороны пытаются установить соединение одновременно. Поскольку оба создают исходящие соединения, это часто позволяет установить соединение через брандмауэры, поскольку входящее соединение не происходит. Если это подключение не установлено, предпринята попытка непрямого UDP-подключения с помощью ретранслятора.
7. Если подключение установлено успешно, служба оценивает, является ли подключение самым быстрым путем. Если это так, все динамические виртуальные каналы (такие как графика, ввод, перенаправление устройств и т. д.) переключаются на новый транспортный поток.

Непрямое UDP-подключение с помощью TURN

По умолчанию непрямые UDP-подключения с помощью TURN для всех включено. Вы можете отключить UDP-подключения для общедоступного (и частного) RDP Shortpath, как описано в разделе POlicy CSP — ADMX_TerminalServer , и задать **для ADMX_TerminalServer/TS_SELECT_TRANSPORTзначение Использовать только TCP**.

Известные проблемы

RDP Shortpath для общедоступных сетей может не работать с облачными компьютерами, где:

- Существует двойной NAT. Например, если трафик направляется через защищенный веб-шлюз (SWG) или прокси-сервер, где подключение использует NAT дважды (во-первых, на выходе из Azure и, во-вторых, из конечной точки VPN/SWG).)
- Подключение маршрутизируется через интернет-прокси или другое устройство проверки.
- Любая сеть, которая ограничивает доступ по протоколу UDP или ограничивает доступ к определенным портам или диапазонам IP-адресов.
- Используется NAT класса носителя (CGN). Если сеть использует общий IP-адрес с другими сетями.

Дополнительные технические сведения об этих сценариях см. в статье Принцип работы RDP Shortpath.

Дальнейшие действия

Полные сведения см. в статье Azure Virtual Desktop RDP Shortpath для общедоступных сетей.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Использование RDP Shortpath для частных сетей с Windows 365

Статья • 31.01.2025

Вы можете использовать Shortpath по протоколу удаленного рабочего стола (RDP) для частных сетей с Windows 365 облачных компьютеров.

Требования

Чтобы использовать RDP Shortpath для частных сетей с Windows 365, необходимо выполнить следующие требования:

- Облачные компьютеры, подготовленные в частной сети клиента. Частные сети поддерживаются с сетевыми подключениями Azure. Размещенные в Майкрософт сети не поддерживаются.
- Узел сеансов (облачный компьютер)
  - Включите прослушиватель UDP на порту UDP 3390.
- Прямое подключение между клиентом и узлом сеансов. Это означает, что клиент может подключаться непосредственно к узлу сеансов через порт 3390 (по умолчанию):
  - Без блокировки брандмауэрами (включая брандмауэр Windows) или группой безопасности сети.
  - Использование управляемой сети, например:
    - Частный пиринг ExpressRoute.
    - VPN типа "сеть — сеть" или "точка — сеть" (IPsec), например Azure VPN-шлюз.

Если вы используете другие типы VPN для подключения к Azure, VPN на основе UDP обеспечивает более высокую производительность. Хотя большинство VPN-решений на основе TCP поддерживают вложенные UDP, они добавляют наследуемые издержки управления перегрузкой TCP, что снижает производительность RDP.

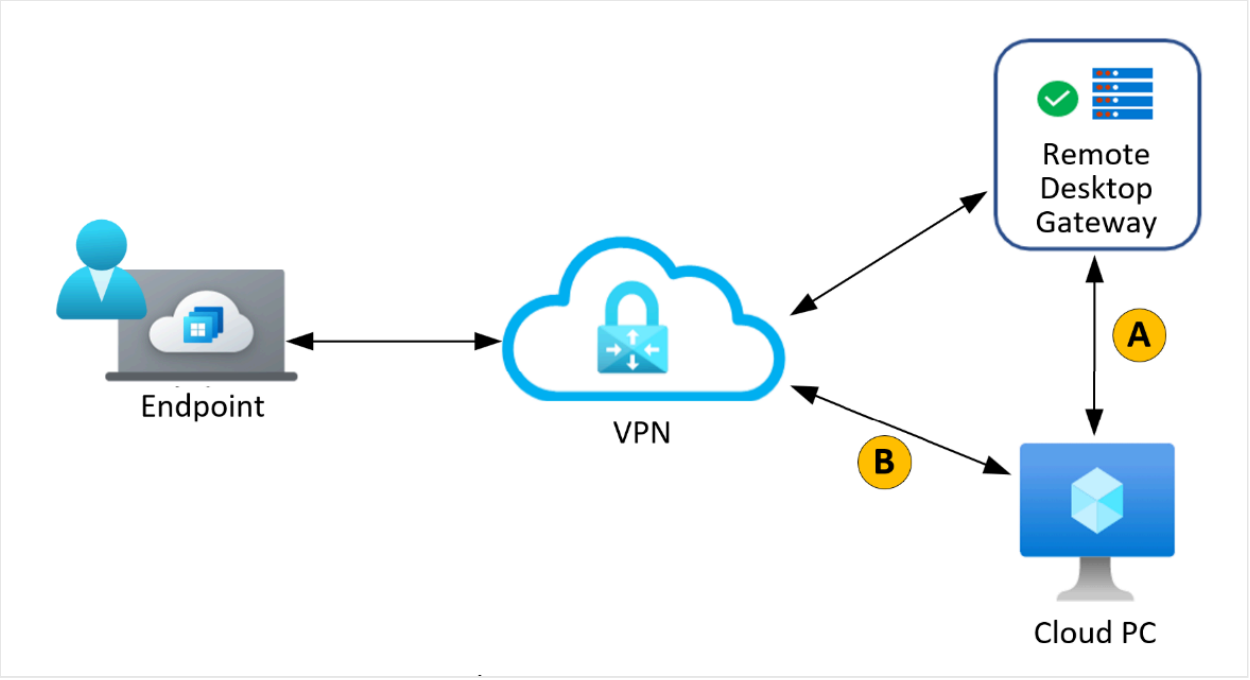
Включение RDP Shortpath для частных сетей

Чтобы настроить и включить RDP Shortpath для частных сетей, перейдите на страницу документации по Виртуальному рабочему столу Azure и следуйте инструкциям.

Преимущества RDP Shortpath

По умолчанию подключение к облачному компьютеру с Windows 365 осуществляется через TCP-подключение, которое проходит через шлюз с использованием транспорта обратного подключения. Обратный транспорт означает, что нет необходимости во входящем подключении к узлу сеанса (облачному компьютеру) для подключения трафика RDP.

RDP Shortpath использует TCP-подключение и по возможности обеспечивает другое прямое подключение между клиентом удаленного рабочего стола и облачным компьютером с Windows 365. Это подключение использует UDP в качестве базового транспортного протокола. Это UDP-подключение является прямым подключением по сети, управляемой клиентом.



О. После проверки подлинности через порт 443 устанавливается обратное подключение WebSocket по протоколу TCP.

Б. UDP через частную сеть с помощью порта 3390. Если UDP-подключение установлено успешно, сеанс RDP переключается на этот путь.

Дополнительные сведения о преимуществах RDP Shortpath см. в разделе Ключевые преимущества.

Процесс подключения RDP Shortpath

При использовании RDP Shortpath соединение с облачным компьютером происходит следующим образом.

1. Соединение RDP устанавливает соединение на основе TCP с использованием транспорта обратного соединения через шлюз (аналогично соединению без RDP Shortpath).
2. Узел сеанса отправляет клиенту список своих IPv4- и IPv6-адресов.
3. Клиент запускает фоновый поток для установки параллельного транспорта на основе UDP непосредственно к одному из IP-адресов узла сеансов.
4. Пока клиент проверит предоставленные IP-адреса, он продолжает устанавливать начальное подключение через транспорт обратного подключения, чтобы обеспечить отсутствие задержки в подключении пользователя.
5. Если клиент имеет прямое подключение к узлу сеансов, клиент устанавливает безопасное подключение с помощью TLS через надежный UDP.
6. После установки транспорта RDP Shortpath все динамические виртуальные каналы (DVCs), включая удаленную графику, ввод и перенаправление устройств, перемещаются в новый транспорт. Однако если брандмауэр или топология сети не позволяет клиенту установить прямое UDP-подключение, RDP продолжает использовать транспорт с обратным подключением.

Дальнейшие действия

Полные сведения см. в статье RDP Shortpath для Виртуального рабочего стола Azure.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Аварийное восстановление между регионами в Windows 365

18.06.2025

Windows 365 аварийное восстановление между регионами — это дополнительная служба для Windows 365 Корпоративная, которая защищает облачные компьютеры и данные от региональных сбоев. При правильной лицензировании и активации он создает географически удаленные временные копии облачных компьютеров, к которым можно получить доступ в выбранном регионе резервного копирования. Эти копии помогают повысить доступность и сохранить производительность.

Администраторы должны вручную активировать и отключить аварийное восстановление между регионами.

Возможность восстановления в альтернативном регионе зависит от доступной емкости в этом регионе на момент сбоя. Независимо от того, может ли устройство восстановиться в любой момент времени, точки восстановления устойчивы в альтернативном регионе.

Windows 365 аварийное восстановление между регионами доступно в качестве дополнительной службы для Windows 365 Frontline выделенном режиме (в общедоступной предварительной версии).

Лицензирование

Для каждого пользователя, добавленного в службу, требуется лицензия на надстройку Windows 365 Корпоративная:

- Windows 365 аварийное восстановление между регионами

Временный облачный компьютер

При активации аварийное восстановление между регионами временно создает копию облачных компьютеров пользователей в альтернативном регионе. Он использует последнюю точку восстановления для каждого облачного компьютера и включает все установленные приложения, параметры пользователей и данные.

Когда администратор отключает аварийное восстановление между регионами после сбоя, временный облачный компьютер удаляется. Приложения, параметры, данные и другие сведения не сохраняются на временном облачном компьютере.

Цель точки восстановления (RPO) и целевое время восстановления (RTO)

В случае сбоя служба имеет следующие целевые цели для аварийного восстановления между регионами:

- RTO — < 4 часа для клиентов с менее чем 50 000 облачных компьютеров.
- RPO <4 часа.

Устройства восстанавливаются как можно быстрее. Вы можете использовать определенные устройства для восстановления раньше, чем другие. Скорость и масштаб процесса восстановления — для каждого региона и клиента. Таким образом, при выполнении нескольких действий по активации аварийного восстановления между регионами можно определить приоритеты для определенных устройств, которые будут восстановлены в предыдущих действиях. Эта стратегия определяет приоритеты определенных устройств, но не изменяет общую RTO для всей среды.

Сбои в нескольких регионах

Аварийное восстановление между регионами защищает от потери данных в случае регионального сбоя или полного сбоя данных в основном регионе. Если регион резервного копирования не имеет доступной емкости или не работает во время аварийного восстановления, облачный компьютер резервного копирования не подготавливается. Однако данные по-прежнему сохраняются и остаются доступными в регионе резервного копирования.

Взаимодействие с пользователем

При активации аварийного восстановления между регионами затронутые пользователи получают предупреждение при следующем входе на облачный компьютер.

После завершения активации аварийного восстановления в разных регионах, когда пользователь входит на свой облачный компьютер, он получает временный облачный компьютер. С помощью этого устройства они получают полный контекст пользователя, в том числе:

- Конфигурация
- Данные, хранящиеся на локальном диске
- Приложения, установленные пользователем, вплоть до RPO для устройства.

При отключении аварийного восстановления между регионами временное устройство удаляется. Пользователь возвращается на основное устройство, как это было до события аварийного восстановления. Приложения, параметры, данные или другие сведения, сохраненные на локальном диске ОС (диск C), не сохраняются. Данные, хранящиеся в облачном хранилище, облачных приложениях и т. д., не затрагиваются событием аварийного восстановления облачного компьютера.

Дальнейшие действия

Сведения о настройке, активации и отключении и мониторинге аварийного восстановления в разных регионах.

Настройка аварийного восстановления между регионами

Статья • 31.01.2025

Аварийное восстановление между регионами настроено, как описано в следующих шагах. Дополнительные сведения о параметрах пользователей см. в разделе Параметры пользователя.

> ⓘ **Важно!**
>
> При использовании аварийного восстановления между регионами очень важно настроить и протестировать весь поток между регионами в рамках повторяющегося **планирования непрерывности бизнес-процессов и аварийного восстановления**. Перед выпуском во всей среде необходимо активировать и отключить несколько тестовых устройств, чтобы убедиться, что они работают должным образом. Вы также должны периодически работать и правильно настраивать среду с помощью **отчета о состоянии аварийного восстановления между регионами облачных компьютеров**.

1. Войдите вцентр > администрирования Microsoft Intune**Windows 365**>(в разделе **Подключение устройств**)>**Параметры пользователей**.
2. Выберите **Добавить** (кроме того, можно внести следующие изменения в существующий параметр пользователя).
3. На странице **Параметры** введите имя в поле **Имя** .
4. Задайте значения в разделе **Служба восстановления на определенный момент времени в** соответствии с вашими требованиями. Эти значения также применяются к аварийному восстановлению между регионами.
5. Выберите **Конфигурация аварийного восстановления между регионами (необязательно),** а затем:
   - Для **параметра Включить аварийное восстановление между регионами** выберите *Да*.
   - Для **параметра Тип сети** выберите параметр:
     - **Сеть, размещенная в Майкрософт**. Выберите **географию** и **регион** , где создаются резервные копии облачных компьютеров для аварийного восстановления между регионами.

- **Сетевое подключение Azure** (ANC). Выбранный объект ANC определяет, где создаются резервные копии облачных компьютеров для аварийного восстановления между регионами. Необходимо настроить ANC для региона резервного копирования для поддержки восстановленных облачных компьютеров.

При настройке расположения резервного копирования учитывайте такие аспекты, как независимость данных и географическое расстояние между пользователем и расположением резервного копирования облачного компьютера. Большее расстояние между облачным компьютером резервного копирования и расположением подключения пользователя увеличивает задержку в сети и влияет на производительность. Полные копии облачных компьютеров хранятся в расположении резервной копии, включая все данные, хранящиеся на диске облачного компьютера.

6. Нажмите кнопку **Далее**.

7. На странице **Назначения** добавьте группы, содержащие пользователей, к которым нужно применить этот параметр пользователя. Все облачные компьютеры, связанные с пользователем, будут использовать одни и те же параметры аварийного восстановления между регионами.

8. На странице **Проверка и создание** нажмите кнопку **Создать**.

После завершения настройки первая резервная копия облачного компьютера может занять несколько дней. Чтобы просмотреть текущее состояние резервных копий, проверка отчет об аварийном восстановлении между регионами. После первого резервного копирования целевая точка восстановления (RPO) будет такой же, как для восстановления на определенный момент времени, а также несколько минут для репликации между регионами.

Дальнейшие действия

Узнайте, как активировать и деактивировать аварийное восстановление, а также отслеживать аварийное восстановление между регионами .

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Активация или отмена аварийного восстановления между регионами в Windows 365

Статья • 23.04.2025

В случае регионального сбоя необходимо определить, следует ли активировать аварийное восстановление между регионами. Перед этим необходимо настроить аварийное восстановление между регионами.

С помощью массовых действий можно активировать или отключить аварийное восстановление между регионами для отдельных устройств или устройств для всех пользователей в группе.

Активация аварийного восстановления между регионами перемещает пользователей на новый облачный компьютер во временном регионе. Пользователи не смогут получить доступ к своим облачным компьютерам до завершения перемещения. Пока аварийное восстановление между регионами не будет деактивировано, пользователи работают с облачного компьютера в этом регионе.

1. Войдите в Центр администрирования Microsoft Intune.
2. Проверьте отчет о состоянии аварийного восстановления между регионами облачных компьютеров . Если есть ошибки, поработайте над их исправлением, прежде чем продолжить.
3. Выберите **Устройства**>**Все устройства**>**Массовые действия устройств**.
4. На странице **Базовые** выберите следующие параметры:
   - **ОС**: Windows
   - **Тип устройства**: облачные компьютеры
   - **Действие устройства**: необязательное аварийное восстановление
5. В поле **Тип действия** выберите один из следующих параметров:
   - **Активация аварийного восстановления между регионами**
   - **Отключите аварийное восстановление между регионами**. Передача обратно на основной облачный компьютер может занять до одного часа. В течение этого времени пользователь может продолжать использовать свой временный резервный облачный компьютер. После завершения передачи пользователь снова войти на свое основное устройство в течение нескольких минут.
6. Нажмите кнопку **Далее**.

7. На странице **Устройства** выберите отдельные облачные компьютеры или группу облачных компьютеров. При выборе устройств в списке отображаются только соответствующие устройства. Если вы хотите отключить все устройства, которые сейчас активированы, можно выбрать поле для выбора всех устройств.

8. Нажмите **Далее**.

9. На странице **Проверка и создание** нажмите кнопку **Создать**.

Дальнейшие действия

Узнайте, как настроить и отслеживать аварийное восстановление между регионами .

Аварийное восстановление Windows 365

12.08.2025

Аварийное восстановление Windows 365 — это дополнительная служба для Windows 365 Корпоративная, которая помогает улучшить аварийное восстановление и устойчивость данных для облачных компьютеров. Аварийное восстановление плюс:

- Создает три копии диска ОС Cloud PC в другой регион или регион.
- Выделяет и резервирует емкость для облачного компьютера в альтернативном регионе.

Если существует событие регионального уровня Azure, которое ограничивает доступ к облачным компьютерам в основном регионе, копии дисков можно использовать для восстановления устройства на выделенном облачном компьютере в альтернативном регионе.

При настройке Аварийное восстановление Windows 365 для пользователя Windows 365 создает копию диска ОС для всех облачных компьютеров пользователя в указанный регион или другой регион. Начальная полная копия диска может занять до трех дней, но последующие добавочные копии занимают всего минуты.

По сравнению с восстановлением на определенный момент времени и аварийным восстановлением между регионами

Чтобы успешно восстановить облачный компьютер во время сбоя, восстановление на определенный момент времени в альтернативной зоне и аварийное восстановление между регионами зависит от емкости целевого региона или зоны.

Аварийное восстановление Windows 365 выделяет ресурсы при настройке, заблаговременно резервируя их. Такое упреждающее выделение значительно повышает вероятность успешного восстановления.

Если восстановление на определенный момент времени завершается сбоем из-за ограничений емкости, Windows 365 аварийное восстановление плюс предоставляет вторичную возможность восстановления облачного компьютера до зарезервированной емкости альтернативного региона.

Цель точки восстановления и целевое время восстановления

Если произошел сбой, служба имеет следующие целевые цели для аварийного восстановления, а также:

- Цель точки восстановления (RPO) < в 61 минуту.
- Целевое время восстановления (RTO) в < 31 минуту.

Устройства восстанавливаются как можно быстрее.

Временный облачный компьютер

При активации аварийное восстановление и временно создает копию облачных компьютеров пользователей в альтернативном регионе. Он использует последнюю точку восстановления для каждого облачного компьютера и включает все установленные приложения, параметры пользователей и данные.

При использовании временного устройства Windows 365 аварийного восстановления плюс отображается предупреждающее сообщение.

При отключении аварийного восстановления и после сбоя временный облачный компьютер удаляется. Приложения, параметры, данные и другие сведения не сохраняются на временном облачном компьютере. Все, что вы сохраняете на временном облачном компьютере, не будет скопировано обратно на основное устройство. Однако при хранении файлов в OneDrive они автоматически синхронизируются с основным устройством.

Дальнейшие действия

Настройка аварийного восстановления плюс.

Настройка аварийного восстановления плюс

Статья • 22.04.2025

Чтобы настроить функцию аварийного восстановления плюс, выполните следующие действия. Дополнительные сведения о параметрах пользователей см. в разделе Параметры пользователя.

> ⓘ **Важно!**
>
> При использовании функции аварийного восстановления плюс важно настроить и протестировать весь поток между регионами в рамках **повторяющегося планирования непрерывности бизнес-процессов и аварийного восстановления**. Перед выпуском во всей среде необходимо активировать и отключить несколько тестовых устройств, чтобы убедиться, что они работают должным образом. Следует также периодически проверка, что среда работоспособна и правильно настроена с помощью **отчета о состоянии непрерывности бизнес-процессов и аварийного восстановления облачного компьютера**.

1. Войдите вцентр > администрирования Microsoft Intune**Windows 365**>(в разделе **Подключение устройств**)>**Параметры пользователей**.
2. Выберите **Создать** (кроме того, можно внести следующие изменения в существующий параметр пользователя).
3. На странице **Параметры** введите имя в поле **Имя** .
4. Задайте значения в разделе **Служба восстановления на определенный момент времени в** соответствии с вашими требованиями. Эти значения также применяются к аварийному восстановлению плюс.
5. Выберите **Необязательные параметры непрерывности бизнес-процессов и аварийного восстановления**.
6. Для **параметра Включить дополнительное аварийное восстановление для этого параметра пользователя** выберите **Аварийное восстановление плюс**.
7. Для **параметра Тип сети** выберите параметр:
    - **Сеть, размещенная в Майкрософт**. Выберите **географию** и **регион** , в которых создаются резервные копии облачного компьютера.

- **Сетевое подключение Azure** (ANC). Выбранный параметр ANC определяет, где создаются резервные копии облачного компьютера для аварийного восстановления. Необходимо настроить ANC для региона резервного копирования для поддержки восстановленных облачных компьютеров.

При настройке расположения резервного копирования учитывайте такие аспекты, как независимость данных и географическое расстояние между пользователем и расположением резервного копирования облачного компьютера. Большее расстояние между облачным компьютером резервного копирования и расположением подключения пользователя увеличивает задержку в сети и влияет на производительность. Полные копии облачных компьютеров хранятся в расположении резервной копии, включая все данные, хранящиеся на диске облачного компьютера.

8. Укажите, разрешено ли пользователям самостоятельно активировать и деактивировать DR Plus. В настоящее время пользователи могут активировать или деактивировать только на пользовательском портале Облачного компьютера.

9. Нажмите кнопку **Далее**.

10. На странице **Назначения** добавьте группы, содержащие пользователей, к которым нужно применить этот параметр пользователя. Все облачные компьютеры, связанные с пользователем, используют одни и те же параметры аварийного восстановления.

11. На странице **Проверка и создание** нажмите кнопку **Создать**.

После завершения этой настройки первая резервная копия облачного компьютера может занять до трех дней. Последующие добавочные копии занимают всего несколько минут. Чтобы просмотреть текущее состояние резервных копий, проверка отчет о состоянии непрерывности бизнес-процессов и аварийного восстановления на облачном компьютере.

Дальнейшие действия

Узнайте, как активировать и деактивировать, а также отслеживать аварийное восстановление плюс.

Активация или отключение аварийного восстановления в Windows 365

Статья • 22.04.2025

Во время простоя или тестирования можно активировать или деактивировать Аварийное восстановление Windows 365 для перемещения пользователей на их временные облачные компьютеры и обратно. Функция "Аварийное восстановление плюс" предназначена для использования во время крупномасштабных событий, при этом временные облачные компьютеры активируются и деактивируются в центре администрирования Intune.

С помощью массовых действий можно активировать или отключить аварийное восстановление между регионами для отдельных устройств или устройств для всех пользователей в группе.

Активация аварийного восстановления и перемещение пользователей на новый временный облачный компьютер во временном регионе. Пользователи не смогут получить доступ к новым облачным компьютерам до завершения перемещения. Пока не будет отключена функция аварийного восстановления и не будет отключена, пользователи будут работать с временным облачным компьютером в альтернативном регионе.

1. Войдитев центр >администрирования Microsoft Intune Устройства >**Все устройства**>**Параметры пользователей Массовые**>**действия устройств**.
2. На странице **Базовые** выберите следующие параметры:

    - **ОС**: **Windows**
    - **Тип устройства**: **облачные компьютеры**
    - **Действие устройства**: **необязательное аварийное восстановление**
    - **Необязательное аварийное восстановление**: **активация аварийного восстановления плюс** или **деактивация аварийного восстановления плюс**

3. Нажмите кнопку **Далее**.
4. На странице **Устройства** выберите по крайней мере одно устройство >**Далее**.
5. На странице **Проверка и создание** нажмите кнопку **Создать**.

Дальнейшие действия

Узнайте, как настроить аварийное восстановление плюс.

Цифровая экспертиза и облачные компьютеры с Windows 365 Корпоративная

Статья • 31.01.2025

Как и физические устройства, облачные компьютеры Windows 365 Корпоративная можно развертывать, защищать и управлять ими с помощью Microsoft Intune. В рамках владения компьютером вам может потребоваться передать облачные компьютеры внутренним или третьим лицам для проведения цифровой экспертизы. Цифровая экспертиза — это наука, которая занимается восстановлением и исследованием цифровых данных для поддержки уголовных расследований или гражданского судопроизводства.

Для поддержки такой экспертизы Windows 365 предлагает возможность помещения облачного компьютера на проверку. Это действие безопасно сохранит моментальный снимок облачного компьютера в учетной записи хранения Azure клиента. После переноса на эту учетную запись клиент полностью владеет моментальным снимком. Чтобы snapshot было очевидно, клиент должен создать хэш файла snapshot сразу после сохранения snapshot в учетной записи хранения Azure.

Следователи могут прикреплять дисковые копии моментального снимка Cloud PC и передавать его в защищенную учетную запись хранения, предназначенную для экспертного анализа. Этот процесс можно выполнить без повторного создания, включения или доступа к исходному облачному компьютеру.

Сценарии

Вам может потребоваться поместить облачный компьютер на проверку для любого из следующих сценариев:

1. Запрос от команды внутреннего центра управления безопасностью (SOC).
2. Ответ на запрос внутреннего или внешнего аудитора третьей стороны.
3. В ответ на начатое или продолжающееся судебное расследование.

Рекомендация цифровой экспертизы

В ответ на юридические запросы на данные, хранящиеся на облачном компьютере, администраторы должны подтвердить, что предоставляемые ими цифровые

доказательства демонстрируют действительную цепочку хранения (CoC) на протяжении всего процесса сбора, сохранения и доступа к доказательствам. По этой причине администраторы должны обеспечить адекватную поддержку:

- Управление доступом. Дополнительные сведения об управлении JIT-доступом см. в разделах Рекомендации по Azure RBAC и Начало использования управление привилегированными пользователями.
- Защита и целостность данных. Только виртуальная сеть в выделенной подписке, содержащая snapshot, имеет доступ к учетной записи хранения и хранилищу ключей, которое архивирует доказательства. Дополнительные сведения см. в статье Ключ клиента Microsoft Purview для Windows 365 облачных компьютеров.
- Мониторинг и оповещение. Дополнительные сведения см. в статье Оповещение о назначении привилегированных ролей Azure.
- Ведение журнала и аудит, разделение обязанностей. Только небольшой список администраторов с доступом к учетной записи хранения может предоставить следователям временный доступ (который был записан и утвержден) к доказательствам.

Дальнейшие действия

Поместить облачный компьютер на проверку.

Дополнительные сведения о поддержке цифровых расследований корпорацией Майкрософт см. в статье Цепочка хранения компьютерной криминалистики в Azure.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Поместить облачный компьютер с Windows 365 Корпоративная на рассмотрение

27.06.2025

В рамках запроса цифровой экспертизы вас могут попросить предоставить снимок облачного компьютера внутренним или внешним следователям. Помещение облачного компьютера на проверку сохраняет моментальный снимок облачного компьютера в вашей учетной записи хранилища Azure. Оттуда вы можете предоставить снимок следователю.

> **Примечание**
>
> Одновременно можно поместить на проверку до 10 облачных компьютеров. Если одновременно проверяется более 10, запросы помещаются в очередь для обработки, но вероятность превышения времени ожидания увеличивается, если запросы остаются в очереди слишком долго. Если время ожидания истекло, рекомендуется шататься, чтобы предоставить достаточно времени для выполнения предыдущих запросов первым.

Требования

Чтобы поместить облачный компьютер на рассмотрение, необходимо соответствие следующим требованиям:

- Лицензия на Windows 365 Корпоративная.
- Учетная запись хранения Azure в том же клиенте, настроенная в соответствии с требованиями, приведенными в следующем разделе.

Настройка учетной записи хранения Azure

Чтобы поместить облачный компьютер на проверку, необходимо наличие учетной записи хранения Azure в том же клиенте, что и облачный компьютер. Дополнительные сведения, необходимые для выбора типа учетной записи, соответствующей своим потребностям, можно найти в разделе Обзор учетной записи хранения. Рекомендуется создать и поддерживать специальную учетную запись хранения с выделенными элементами управления доступом для аудита облачных компьютеров. В рамках процесса проверки облачных компьютеров Windows 365 требуются роли **Участник учетной записи**

хранения и **Участник данных BLOB-объектов хранилища** для учетной записи хранения Azure.

1. Создайте учетную запись хранения в выбранной подписке Azure. Чтобы создать учетную запись, можно использовать PowerShell, Azure CLI, шаблон Azure Resource Manager или портал Azure.

2. Настройте учетную запись хранения со следующими параметрами: — **Сведения об экземпляре** - **Регион**: тот же регион, что и облачный компьютер, предлагаемый для повышения производительности. В каком регионе нет ограничений. - **Производительность**: **premium** (поддерживает горячий уровень доступа) или **Standard** (поддерживает все уровни доступа). - **Тип учетной записи premium**: **страничные BLOB-объекты** - **Безопасность** — минимальная версия TLS: **версия 1.2**. — Убедитесь, что **параметр Разрешить анонимный доступ к BLOB-объектам** отключен (значение по умолчанию). — Отключить **включение доступа к ключу учетной записи хранения**. - **Сети** - **Сетевой доступ**: **включение общедоступного доступа из всех сетей**

   НЕОБЯЗАТЕЛЬНО. Если вы хотите скопировать учетную запись хранения, скопированную в неизменяемое хранилище, задайте следующие поля:

   - Выберите **Включить управление версиями для BLOB-объектов**.
     - Выберите **Включить поддержку неизменяемости на уровне версии**.
     - Если выбран параметр **Производительность уровня "Премиум"**, необходимо также выбрать **хранилище, избыточное между зонами (ZRS).** Локально избыточное хранилище (LRS) не является поддерживаемым вариантом неизменяемого хранилища.

   После создания учетной записи хранения необходимо применить политику блокировки. Дополнительные сведения о настройке Хранилище BLOB-объектов Azure для неизменяемости и соблюдения правил, таких как правило 17a-4 SEC, см. в отчете Azure — Cohasset Assessment — WORM Storage (2024).

   НЕ ПОДДЕРЖИВАЕТСЯ. Настройка область разрешений для операций копирования. Он должен иметь значение (NULL), значение по умолчанию, чтобы разрешить копирование из любой учетной записи хранения в целевую учетную запись.

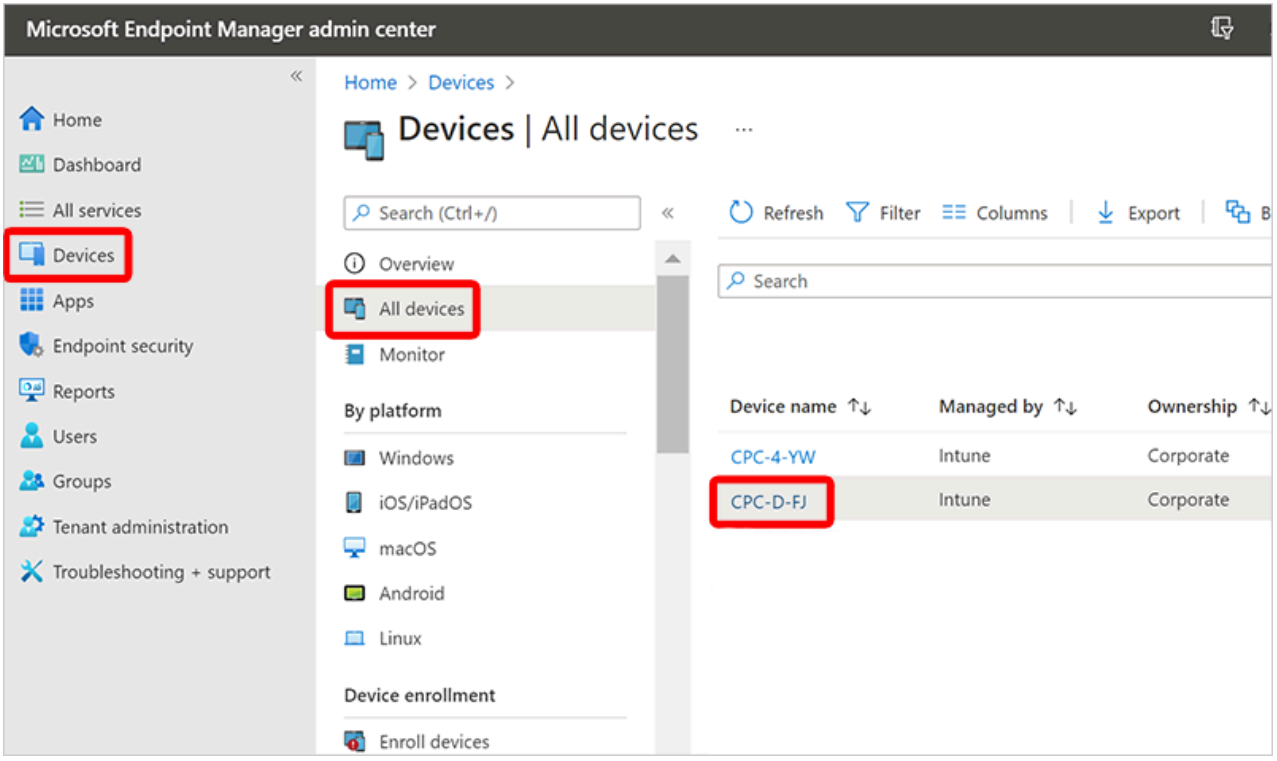
3. Назначьте роль Azure для доступа к данным больших двоичных объектов.. Минимальные разрешения, необходимые службе Windows 365 для размещения облачного компьютера под проверкой: **участник учетной записи хранения** и **участник данных BLOB-объектов хранилища**. В зависимости от того, когда был подготовлен клиент, удостоверение для службы Windows 365 для RBAC будет

отображаться *как Windows 365* в то время как для старых клиентов может отображаться *облачный компьютер*.

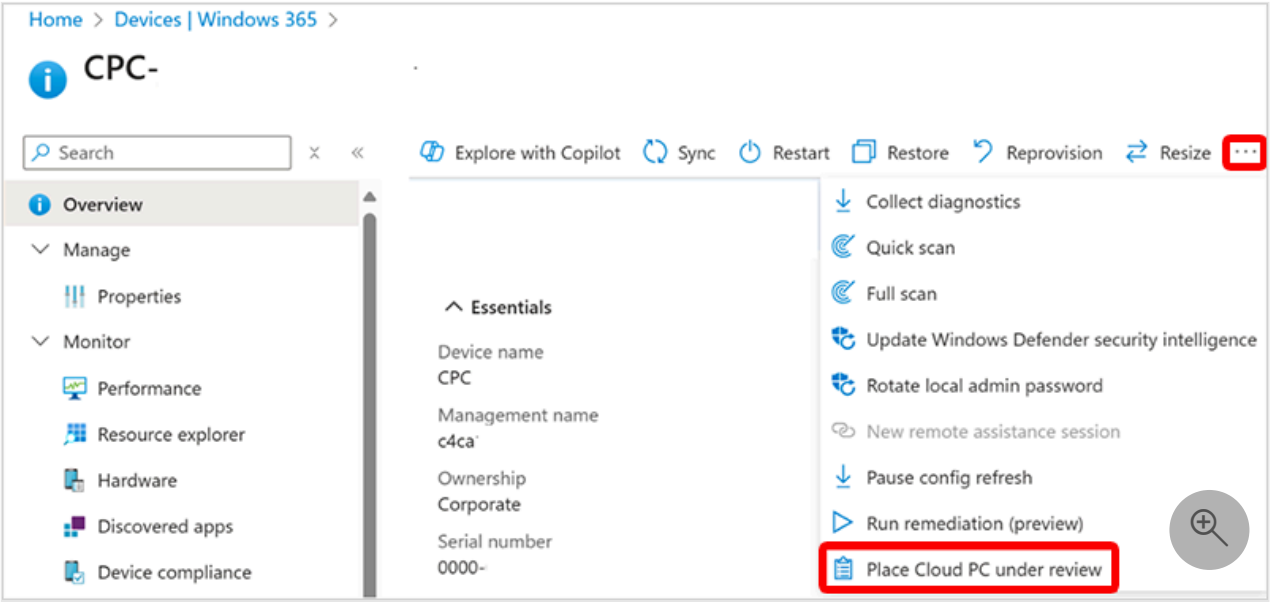
Помещение облачного компьютера на проверку

После настройки учетной записи хранения Azure с разрешениями, как описано в предыдущем разделе, вы можете поместить облачный компьютер под проверку, выполнив следующие действия.

1. Войдите в Центр администрирования Microsoft Intune и выберите **Устройства**>**Все устройства**> выберите устройство.



2. Выберите многоточие (...) >**Переместите облачный компьютер под проверку**.



3. Выберите уровень **подписки**, **учетной записи хранения** и **уровня доступа** (самые горячие затраты, а архивные — минимальные), для которых службе Windows 365 были предоставлены разрешения **участник учетной записи хранения** и **участник данных BLOB-объектов хранилища**.

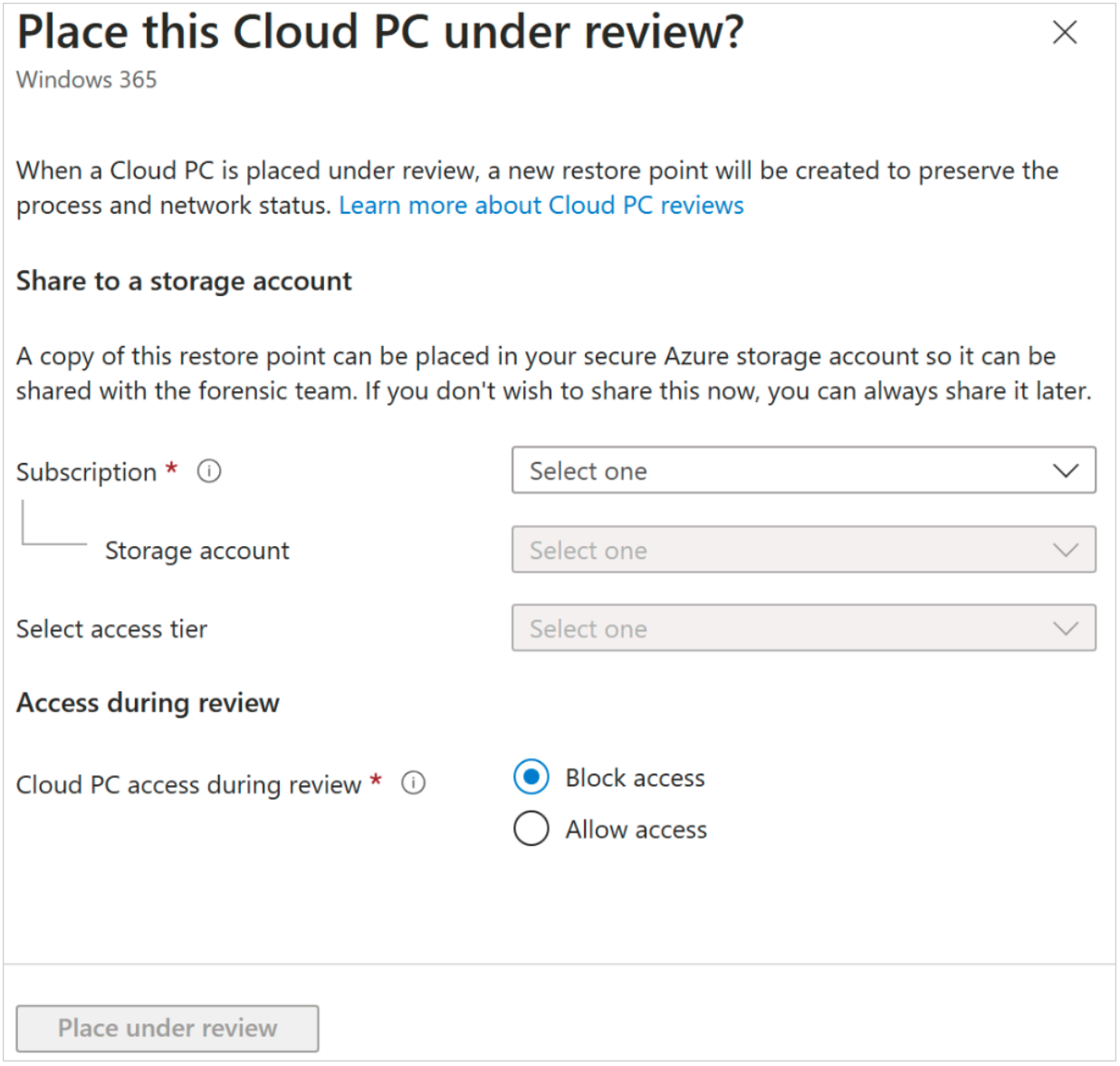
   На виртуальной машине могут быть подключены только страничные BLOB-объекты горячего уровня. Все остальные уровни — это блочные BLOB-объекты, которые необходимо преобразовать в страничный BLOB-объект, если требуется подключить диск к виртуальной машине. Архивный уровень является автономным, поэтому перед преобразованием в страничный BLOB-объект необходимо выполнить восстановление на сетевой уровень.

   Standard уровни учетных записей хранения производительности. Для учетной записи хранения производительности Standard уровень для большого двоичного объекта, копируемого из Windows 365 в учетную запись хранения, может быть другим. При настройке учетной записи хранения горячего уровня другие объекты будут по умолчанию горячими. Тем не менее вы можете настроить образ облачного компьютера, на который выполняется проверка, как холодный, холодный или архивный.

   Уровни учетных записей хранения производительности уровня "Премиум". Производительность "Премиум" всегда является учетной записью хранения горячего уровня. Раскрывающееся меню уровня доступа игнорируется для учетных записей хранения производительности уровня "Премиум".

4. Если выбрано, в разделе **Доступ во время проверки**

- **Блокировать доступ**. Облачный компьютер будет немедленно выключен, чтобы пользователь не смог получить доступ к облачному компьютеру, а затем будет создан snapshot. Этот параметр полезен в тех случаях, когда может потребоваться сдержать угрозу безопасности путем отключения облачного компьютера и последующего анализа snapshot в изолированной среде.
  - **Разрешить доступ**. Пользователь облачного компьютера может продолжать использовать облачный компьютер даже при создании snapshot в учетной записи хранения.



5. Выберите **Поместить на проверку**. В зависимости от размера диска облачного компьютера и региона назначения учетной записи хранения он может находиться в диапазоне от нескольких минут до нескольких часов для каждого snapshot, сохраняемого в учетной записи хранения. Например, для учетной записи хранения в том же регионе Azure может потребоваться до одного часа или более на 128 ГБ дисковых данных.

Чтобы snapshot было очевидно, следует создать хэш файла snapshot после его сохранения в учетной записи хранения. Одним из способов создания хэша файла является использование командлета Get-FileHash . Для обеспечения максимальной производительности командлет Get-FileHash должен выполняться в одном из следующих командлетов:

- копию скачаемого файла;
- snapshot в учетной записи хранения Azure из ресурса, расположенного в том же регионе Azure;

Удаление облачного компьютера из проверки

Войдите в Центр администрирования Microsoft Intune и выберите **Устройства**>**Все устройства**> выберите устройство >**...**>**Удалить из проверки**.

Массовые операции

Вы также можете использовать массовые операции с устройствами Intune для одновременной проверки нескольких облачных компьютеров. Дополнительные сведения см. в статье Использование массовых операций устройств.

> **Примечание**
>
> Одновременно можно поместить на проверку до 10 облачных компьютеров. Если на проверку одновременно помещается более 10, запросы помещаются в очередь, а время ожидания может увеличиться, если запрос остается в очереди слишком долго. Если время ожидания истекло, рекомендуется шататься, чтобы предоставить достаточно времени для выполнения предыдущих запросов первым. Время завершения зависит от размера диска облачного компьютера, расположения и типа учетной записи хранения Azure.

Управление с помощью API

Вы можете использовать API Graph для размещения или удаления облачного компьютера из проверки. Дополнительные сведения см. в статье managedDevice: setCloudPcReviewStatus.

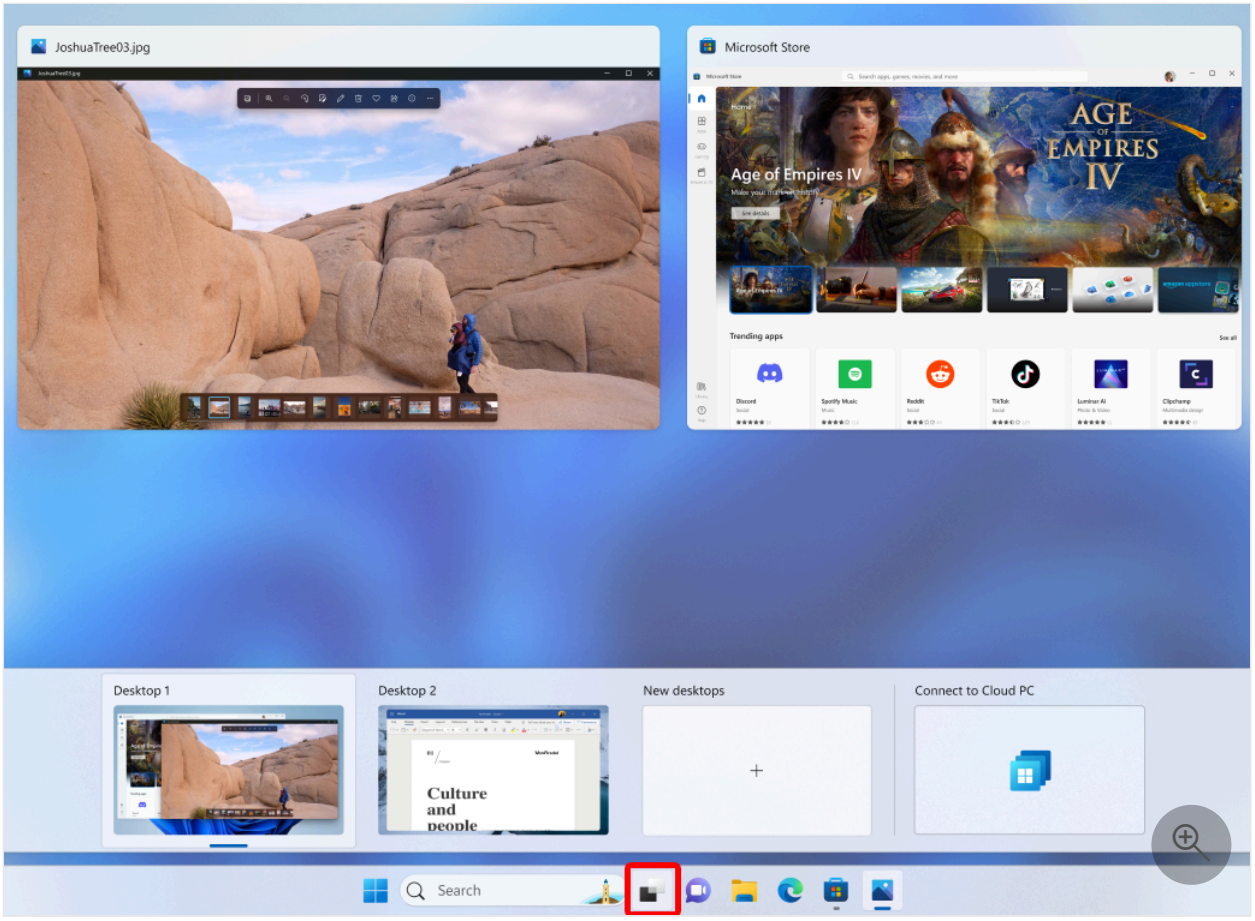
Дальнейшие действия

Подробнее о цифровой экспертизе и облачных компьютерах..

Что такое Windows 365 Switch?

Статья • 24.02.2025

Windows 365 переключение позволяет пользователям перемещаться между локальным устройством и одним из облачных компьютеров с помощью нескольких рабочих столов в представлении задачи Windows 11.



Пользователи также могут запускать облачный компьютер и подключаться к нему непосредственно из представления задач без необходимости использования https://windows365.microsoft.com или приложение Windows 365.

Требования

Чтобы использовать Windows 365 Switch, физическое устройство и облачный компьютер должны соответствовать следующим требованиям:

- Windows 11 Корпоративная или Профессиональная версии 22H2 сборка 22621.3235 или 23H2, сборка 22631.3235 или более поздняя.
- Облачный компьютер Windows 365 лицензия. Дополнительные сведения см. в разделе Назначение лицензий.

Сведения об установке Windows 365 Switch на устройстве пользователя см. в статье справки Windows 365 переключение конечного пользователя.

Дальнейшие действия

статья справки Windows 365 переключение пользователя

Windows 365 переключение известных проблем

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Миграция в Windows 365

22.10.2025

API миграции

API миграции — это интерфейс на основе REST, который позволяет организациям автоматизировать и оптимизировать миграцию пользовательских сред, приложений и данных на Windows 365 облачные компьютеры. Он предоставляет безопасный и масштабируемый способ интеграции рабочих процессов миграции с существующими инструментами и процессами, сокращая усилия вручную и сводя к минимуму время простоя. Применяя API, ИТ-отделы могут оркестрировать массовую миграцию, отслеживать ход выполнения и обеспечивать согласованность взаимодействия для конечных пользователей, сохраняя при этом стандарты соответствия требованиям и безопасности.

В этом документе содержатся технические требования и пошаговые инструкции для партнеров и клиентов Майкрософт, которые переносятся на виртуальные машины на основе Azure на Windows 365 облачные компьютеры с помощью API Graph Майкрософт. Он предназначен для команд инженеров и ИТ-администраторов, ответственных за планирование и выполнение миграции в Windows 365.

Вы найдете подробные спецификации для подготовки виртуального жесткого диска (VHD), параметров API, шагов проверки и схемы процесса, чтобы обеспечить беспроблемную и безопасную миграцию. В этом документе также описываются поддерживаемые сценарии, текущие ограничения и рекомендации по подготовке на основе snapshot. Следуя этим рекомендациям, партнеры и клиенты могут ускорить подключение, свести к минимуму ошибки миграции и обеспечить согласованное взаимодействие с облачными компьютерами для корпоративных клиентов.

1. Поддерживаемые сценарии миграции

- Миграция с виртуальных машин на основе Azure (присоединенных к Entra и Entra hybrid joined) на Windows 365 облачные компьютеры.
- Поддерживается только подготовка виртуальных жестких дисков snapshot. Импорт на основе образов недоступен.

2. Требования к формату виртуального жесткого диска и хранилищу

Формат VHD

Развернуть таблицу

Требование	Сведения
Формат	Только виртуальный жесткий диск фиксированного формата (без виртуального жесткого диска версии 2 (VHDX) или динамических дисков)
Generation	Только виртуальные машины 2-го поколения
Диск ОС	Windows 10 или более поздней версии; диски данных отсутствуют
Состояние виртуальной машины	Виртуальная машина должна быть остановлена (освобождена) перед snapshot
Агент виртуальной машины	Требуется работоспособный агент виртуальной машины Azure
Сторонние агенты	Необходимо удалить перед созданием snapshot

Хранилища

- Сохраните snapshot виртуальной машины в качестве страничного BLOB-объекта в учетной записи хранения Azure, принадлежащей клиенту.
- Доступ через URI SAS (рекомендуется) или назначение необходимых разрешений службе Windows 365 с помощью управляемого удостоверения.
- Межтенантный доступ не поддерживается.

3. Параметры API и поток подготовки

Обязательные параметры API

Развернуть таблицу

Параметр	Описание
userId	Entra ID целевого пользователя
snapshotLocation	Сведения о URI SAS или учетной записи хранения
policyId (необязательно)	Используется для определения политики подготовки

- Убедитесь, что пользователь Entra ID присоединен и у него еще нет той же версии Облачного компьютера.
- Назначьте пользователю соответствующую лицензию после отправки snapshot для активации подготовки.

4. Требования к проверке (контрольный список)

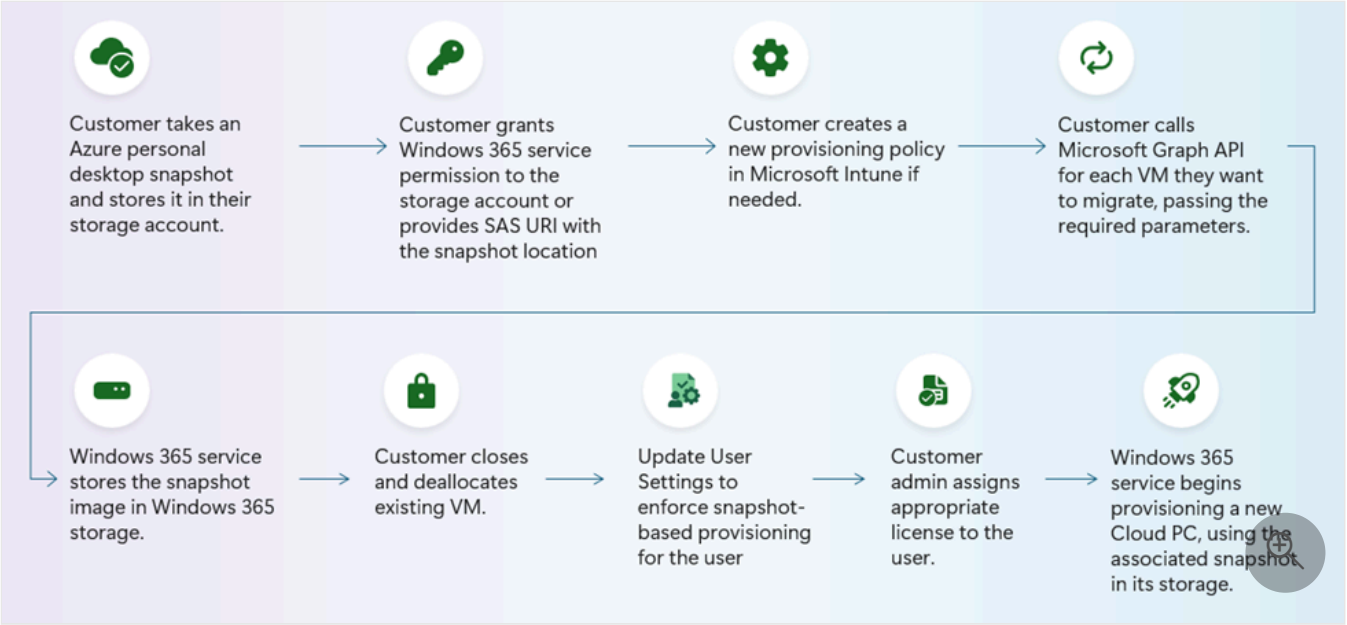
Перед началом миграции убедитесь, что выполнены следующие проверки:

Развернуть таблицу

#	Проверка проверки	Назначение
1	Возможность загрузки на виртуальном жестком диске	Проверка загрузки виртуальной машины и работоспособности агента виртуальной машины Azure
2	Формат 2-го поколения	Поддерживаются только виртуальные машины 2-го поколения
3	Совместимость версий ОС	Должен поддерживаться Windows 365
4	Нет сторонних агентов	Сторонние агенты не поддерживаются
5	Нет диска данных	Поддерживается только диск ОС
6	Работоспособности агента виртуальной машины Azure	Должен быть работоспособным и реагировать
7	Совместимость размера диска	Должен соответствовать назначенной лицензии
8	Готовность CSE	Обеспечение совместимости сети
9	Совпадение пользователя с моментальным снимком	Предотвращение межпользовательской подготовки
10	Целостность файлов	Убедитесь, что нет повреждений
11	Формат файла	Только виртуальный жесткий диск фиксированного формата (без виртуального жесткого диска версии 2 (VHDX) или динамических дисков).
12	ОС Windows	Должно быть Windows 10+

Отслеживайте состояние подготовки и сообщения об ошибках с помощью API Graph.

5. Схема потока миграции



6. Подготовка Snapshot-Based

- Применяется только через API Graph (не Intune).
- Администраторы должны помечать пользователей для подготовки на основе snapshot с помощью параметров пользователей; партнеры должны реализовать эту функцию.
- После подготовки пользователи могут быть удалены из группы snapshot, чтобы разрешить повторную подготовку на основе изображений.

7. Ограничения

- Поддерживаются только корпоративные облачные компьютеры.
- Изначально поддерживается только коммерческое облако; Облако Gov и GPU могут быть включены на будущих этапах.
- Нет повторного использования моментальных снимков в нескольких положениях.
- Один пользователь может одновременно иметь только один импортированный виртуальный жесткий диск в Windows 365. Новый виртуальный жесткий диск можно импортировать только после использования или удаления текущего.
- Поддержка пользовательского интерфейса Intune отсутствует— партнеры должны создавать собственные инструменты.
- Поддержка сторонних агентов не поддерживается— необходимо удалить до создания snapshot.

Отчет о действиях облачного компьютера (предварительная версия)

Статья • 31.01.2025

В этом отчете показано состояние и ход выполнения действий, которые администраторы выполнили на облачных компьютерах:

- Отдельные действия на вкладке **Устройства** .
- Несколько устройств, использующих **массовые действия устройств** на вкладке **Массовые пакеты** .

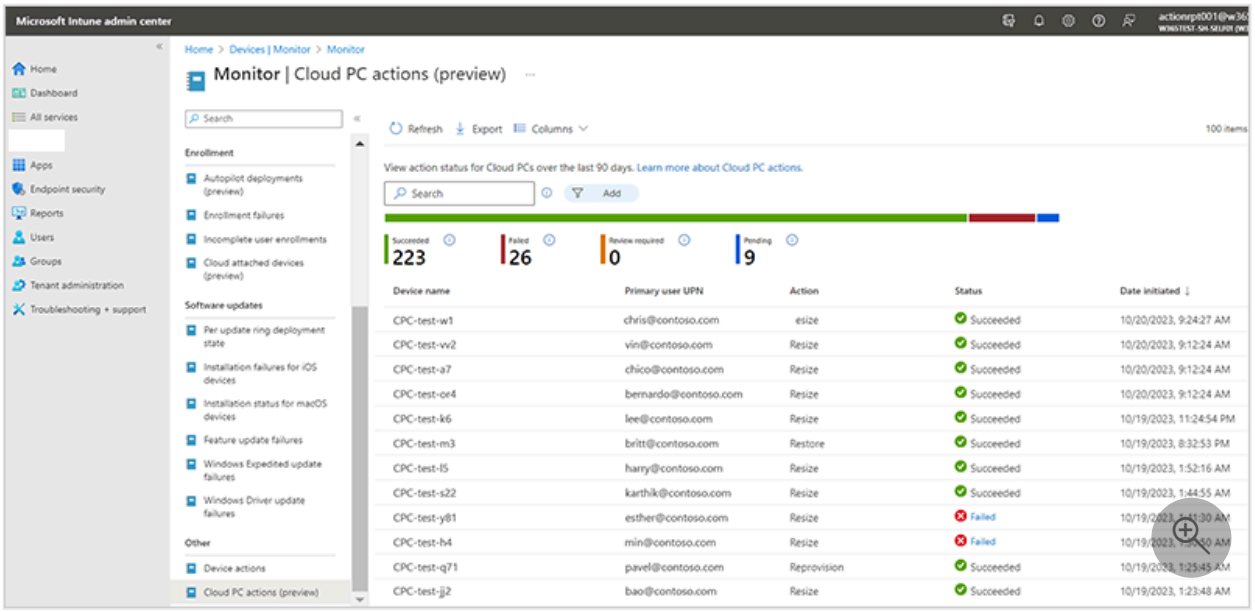
В отчете отображаются состояния действий за последние 90 дней.

Отчет о действиях облачного компьютера находится в общедоступной предварительной версии.

Использование отчета о действиях облачного компьютера

Чтобы открыть отчет о **действиях облачного компьютера**, войдите в центр администрирования Microsoft Intune и выберите **Устройства**>**Мониторинг**>**действий облачного компьютера (предварительная версия).**

Вкладка "Устройства"



На вкладке отображаются следующие столбцы:

- **Имя устройства**
- **Имя участника-пользователя основного пользователя**
- **Действие**: в отчет включаются следующие действия:
  - Создание моментального снимка
  - Переместить регион
  - Место под проверкой
  - Включение и выключение питания (только для W365 frontline)
  - Повторная подготовка
  - Resize
  - Перезапуск
  - Восстановление
  - Устранение неполадок
- **Состояние**. Существует четыре возможных состояния для действия:
  - **Успешно:** действие успешно завершено.
  - **Сбой**: действие не завершено. Если это доступно, нажмите **кнопку Повторить** , чтобы повторить попытку.
  - **Ожидание**. Действие выполняется. Не вносите изменения в облачный компьютер (например, удаление лицензии).
  - **Проверка требуется**. Администратор должен выполнить действие, чтобы завершить действие. Например, назначение целевой лицензии устройству в состоянии "**Изменение размера ожидающей лицензии**" для действия "**Изменить размер** ".
- **Дата инициирована**

Вкладка "Массовые пакеты"

Когда администратор одновременно выполняет действие на нескольких облачных компьютерах с помощью **массовых действий устройства**, эти действия объединяются в пакет.

На вкладке отображаются следующие столбцы:

- **Имя пакетной службы** — автоматически созданное имя для пакета устройств, проходящих удаленное действие.
- **Действие** — то же, что и вкладка "**Устройства** ".
- **Завершение** — ход выполнения действия на пакете устройств.
- **Дата инициирована**

Дальнейшие действия

Отчет о качестве подключения к облачному компьютеру

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

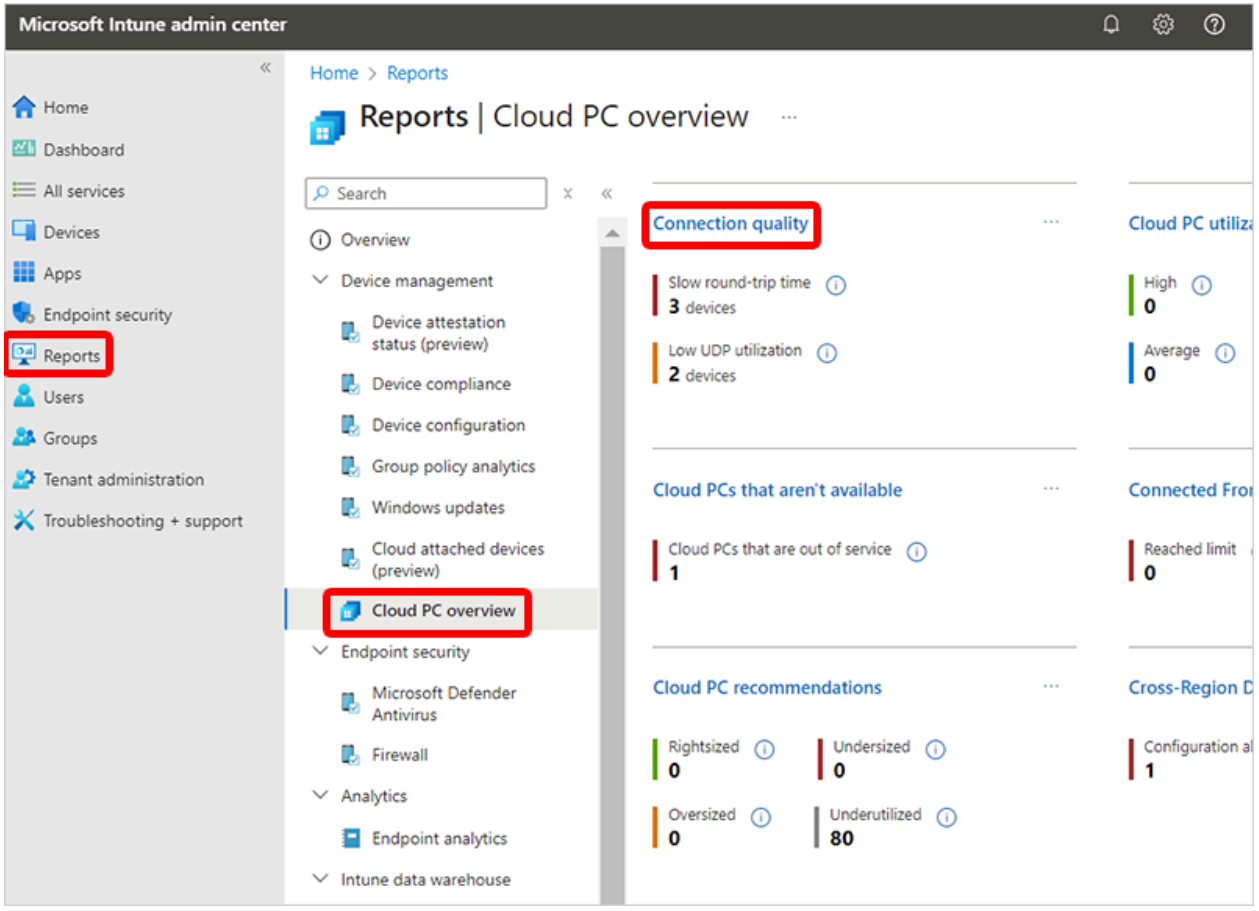
Отчет о качестве подключения к облачному компьютеру

Статья • 31.01.2025

Отчет о качестве подключения помогает администраторам Windows 365 определять устройства, которые могут работать ниже ожидаемых. Качество соединения — это субъективная концепция с множеством переменных, определяющих, что приемлемо в любых обстоятельствах. Администраторы должны использовать объективные данные, предоставляемые этим отчетом, передавать их в свои собственные субъективные критерии производительности, чтобы определить политики и исправления своей организации.

Использование отчета о качестве подключения к облачному компьютеру

Чтобы получить отчет о **качестве подключения к облачному компьютеру**, войдите в центр администрирования Microsoft Intune и выберите **Отчеты Обзор>>облачного компьютераКачество подключения**.



В списке устройств отображаются отдельные облачные компьютеры со следующими столбцами:

- **Имя устройства**
- **Время кругового пути для последнего (или текущего) подключения** (RTT): количество миллисекунда, которое требуется только на транспортном уровне для обмена данными между клиентом и облачным компьютером. Более низкие значения указывают на лучшее подключение в оба пути.
- **Время кругового пути для указанного диапазона дат (P50)**
- **Доступная пропускная способность для последнего (или текущего) подключения**
- **Доступная пропускная способность для указанного диапазона дат (P50):** пропускная способность сети, наблюдаемая во время сеансов с указанным набором примеров CPC.
- **Шлюз подключений**
- **Время входа в удаленном взаимодействии (P50):** количество секунд, в течение которых пользователь завершил процесс входа.
- **IP-адрес клиента**
- **Протокол для последнего (или текущего) подключения**
- **Среднее значение использования UDP в диапазоне дат**
- **Тип устройства**: тип облачного компьютера в зависимости от предложения (Enterprise, Frontline dedicated, Frontline shared).

Каждая строка в отчете содержит ссылки на конкретный облачный компьютер, где можно найти более подробные сведения об журнале подключений устройств и связанной производительности.

Для настройки отчета можно использовать параметры **фильтра Столбцы** и **Добавить** :

- Выберите отображаемые столбцы.
- Отфильтруйте диапазон для каждого столбца.
- Выберите диапазон дат (7 дней или 28 дней).

Эти фильтры можно использовать для выявления подключений, которые не соответствуют требованиям вашей организации. Затем можно оценить потенциальные причины, например:

- Конфигурации сети, узла или клиента, ограничивающие выбор протокола.
- Географическое расстояние.
- Методы и архитектура проверки подлинности.
- Применимость клиента или узла.

Дальнейшие действия

Отчет о качестве подключения к облачному компьютеру

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Отчет о рекомендациях по облачным компьютерам

Статья • 24.02.2025

Отчет **о рекомендациях по облачным компьютерам** — это функция на основе ИИ, которая помогает администраторам Windows 365 определить правильный размер облачных компьютеров. Она предназначена для того, чтобы помочь вам найти оптимальную конфигурацию для облачных компьютеров на основе:

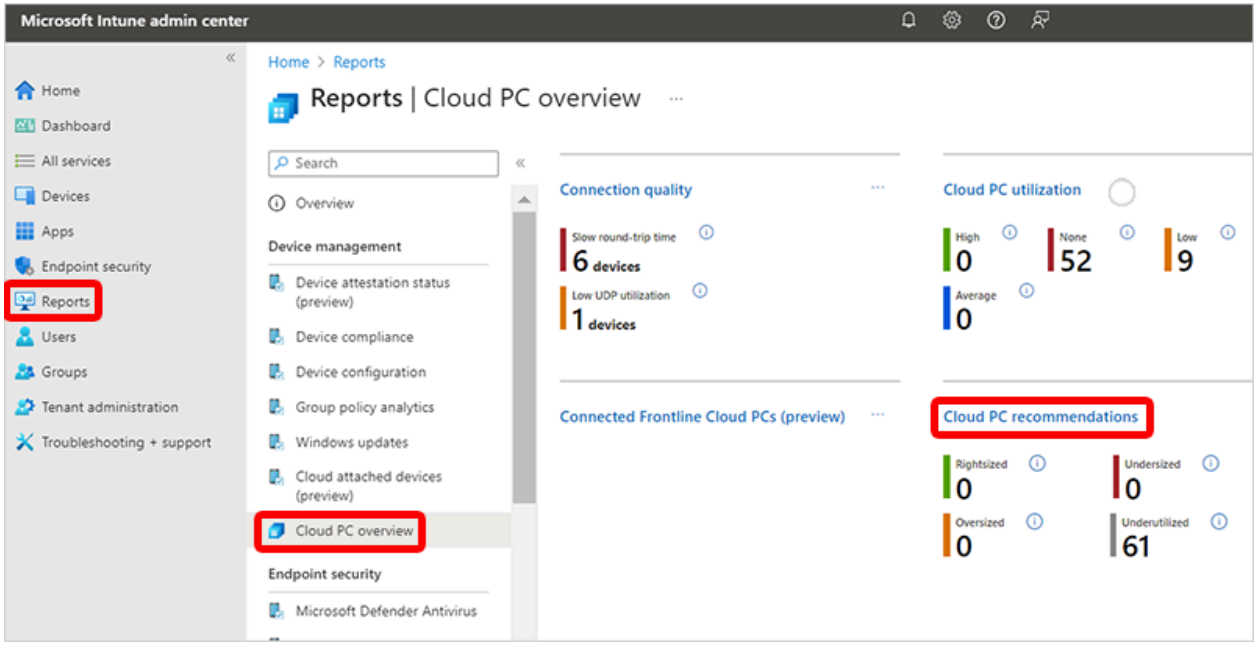
- Шаблоны использования облачных компьютеров конечными пользователями.
- Данные об использовании ресурсов на уровне платформы.
- Требования к производительности.

Развивающаяся модель анализирует эти данные, чтобы определить, являются ли облачные компьютеры:

- Не используется.
- Соответствующий размер.

Использование отчета о рекомендациях по облачным компьютерам

Чтобы получить отчет **о рекомендациях по облачным компьютерам**, войдите в центр администрирования Microsoft Intune, выберите **Отчеты Обзор>>облачных компьютеровРекомендации по облачным компьютерам**.



Вкладка "Обзор"

Вкладка Обзор начинается с различных аналитических сведений об облачных компьютерах.

- **Права:** облачные компьютеры, которые часто используются и имеют соответствующий размер для рабочей нагрузки, которую на них наделяют конечные пользователи.
- **Негабаритный:** облачные компьютеры, которые не поддерживают рабочую нагрузку, которую они поддерживают. Пользователи могут иметь плохой опыт работы. Чтобы улучшить результаты, увеличьте ресурсы устройства, изменив размер номера SKU до большего размера.
- **Негабаритный:** облачные компьютеры, которые перегружены для рабочей нагрузки, которую они поддерживают. Такое же качество взаимодействия может быть доставлено пользователям с меньшим количеством ресурсов. Чтобы освободить ресурсы, измените их на SKU меньшего размера.
- **Недостаточное использование**: облачные компьютеры используются редко или вообще не используются. Возможно, они не нужны. К этой категории относится любой облачный компьютер с активным подключением менее 40 часов в течение 28 дней.

Вкладка "Аналитика по устройствам"

На этой вкладке отображаются рекомендации для конкретных облачных компьютеров. Только облачные компьютеры с некоторым уровнем использования пользователем имеют сведения об используемом ЦП и ОЗУ. Выберите облачный компьютер, чтобы просмотреть дополнительные сведения и описание рекомендации.

В отчете отображаются следующие столбцы:

- **Имя устройства**
- **Имя пользователя**
- **Аналитические сведения**: с правами, с недостаточным, негабаритным или недостаточно используемым.
- **Текущий размер**
- **Рекомендуемый размер**: рекомендуемый размер для изменения классификации облачного компьютера на Rightsized.
- **Общее время подключения (за последние 4 недели)**

Аналитика по моделям

Сводка рекомендаций по типу облачного компьютера. В отчете отображается **тип компьютера** и количество облачных компьютеров в каждой категории. Типы компьютеров с большим количеством облачных компьютеров в столбцах без прав могут указывать на то, что тип не подходит для ваших рабочих нагрузок.

Дальнейшие действия

Отчет о качестве подключения к облачному компьютеру

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Отчет об использовании облачных компьютеров

28.05.2025

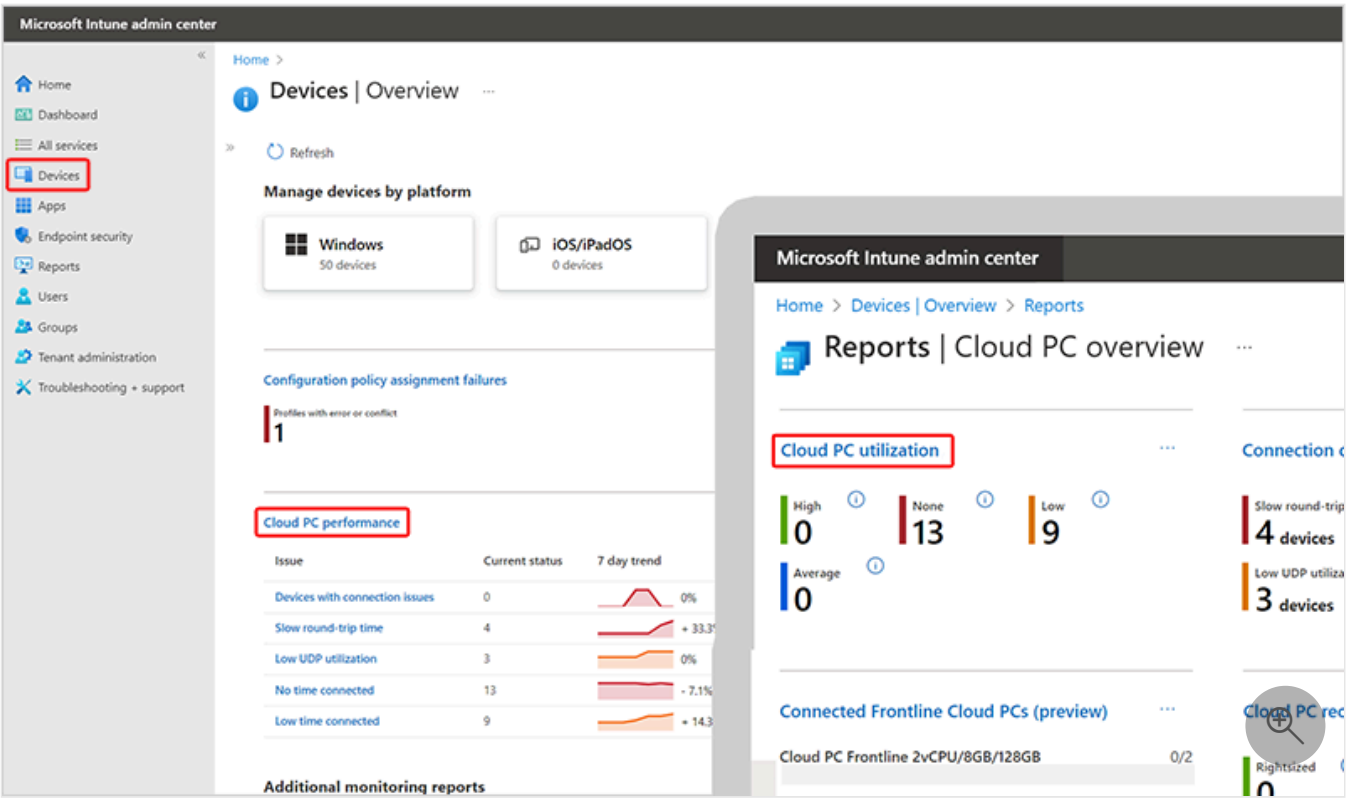
Отчет об использовании облачных компьютеров помогает отслеживать и оптимизировать использование облачных компьютеров в организации. В нем показано, сколько времени пользователи тратят на облачные компьютеры и когда они в последний раз подключаются к ним.

Просмотр облачных компьютеров с низким уровнем использования позволяет снизить затраты на следующие действия:

- Переназначение недостаточно используемых лицензий облачных компьютеров другим пользователям, которые могут использовать их чаще.
- Определение и отзыв облачных компьютеров, которые неактивны в течение длительных периодов времени.

Использование отчета об использовании облачных компьютеров

Чтобы получить отчет об **использовании облачных компьютеров**, войдите в центр администрирования Microsoft Intune и выберите **Устройства** **Производительность** > **облачных компьютеров** > **Использование облачных компьютеров**.



Страница отчета об использовании облачных компьютеров (данные клиента)

В отчете показаны следующие данные клиента, агрегированные для выбранного интервала времени (28, 60 или 90 дней):

- На этой гистограмме показано количество подключенных облачных компьютеров для каждого диапазона:
  - **Время подключения**: более 80 часов.
  - **Среднее время подключения**: 40–80 часов.
  - **Низкое время подключения**: менее 40 часов.
  - **Нет**: ноль часов.
- Список отдельных облачных компьютеров со следующими столбцами:
  - **Имя устройства**
  - **Имя участника-пользователя**: идентификатор пользователя в Active Directory в виде адреса электронной почты.
  - **Тип компьютера**
  - **Время подключения**: общее количество часов, в течение которого пользователь был подключен к облачному компьютеру за последние четыре недели.
  - **Дата последнего подключения**: дата последнего подключения пользователя к облачному компьютеру (в течение последних 60 дней). Если пользователь в настоящее время не подключен к облачному компьютеру, эта дата является

временем выхода. Если пользователь подключен к облачному компьютеру, эта дата является последним временем подключения.
    - **Дата создания**: дата создания облачного компьютера.
    - **Тип устройства**: тип облачного компьютера в зависимости от предложения (Enterprise, Frontline dedicated, Frontline shared).

Фильтры

Элемент управления **Добавление фильтров** позволяет фильтровать таблицу по следующим параметрам:

- **Тип компьютера**
- **Время подключения**
- **Дата последнего подключения**

Эти фильтры помогут вам понять закономерности использования и определить недостаточно используемые облачные компьютеры, которые могут быть отменены или понижены.

Данные на уровне устройства

Аналогичные данные об использовании можно просмотреть для каждого облачного компьютера:

1. Войдите в Центр администрирования Microsoft Intune и выберите **Отчеты Об>использовании облачных компьютеров>**.
2. Выберите устройство, а затем — **Производительность (предварительная версия).**
3. В разделе **Время подключения** отображаются данные об использовании для этого облачного компьютера. Для получения дополнительных сведений в этом разделе выберите **Просмотреть отчет**.

Дальнейшие действия

Отчет о качестве подключения к облачному компьютеру

Отчет о недоступных облачных компьютерах

Статья • 31.01.2025

Отчет о **недоступных облачных компьютерах** помогает администраторам Windows 365 определить облачные компьютеры, которые в настоящее время могут быть недоступны.

В этом отчете отображаются последние условия до 5–15 минут назад. Таким образом, облачные компьютеры в отчете, возможно, уже были восстановлены с момента записи условия. Кроме того, облачные компьютеры, которые недавно стали недоступными, могут быть отсутствуют в отчете.

Использование отчета о недоступных облачных компьютерах

Чтобы открыть отчет о **недоступных облачных компьютерах**, войдите в центр администрирования Microsoft Intune и выберите **Отчеты Обзор**>**облачных компьютеров**>**Облачные компьютеры, которые недоступны**.

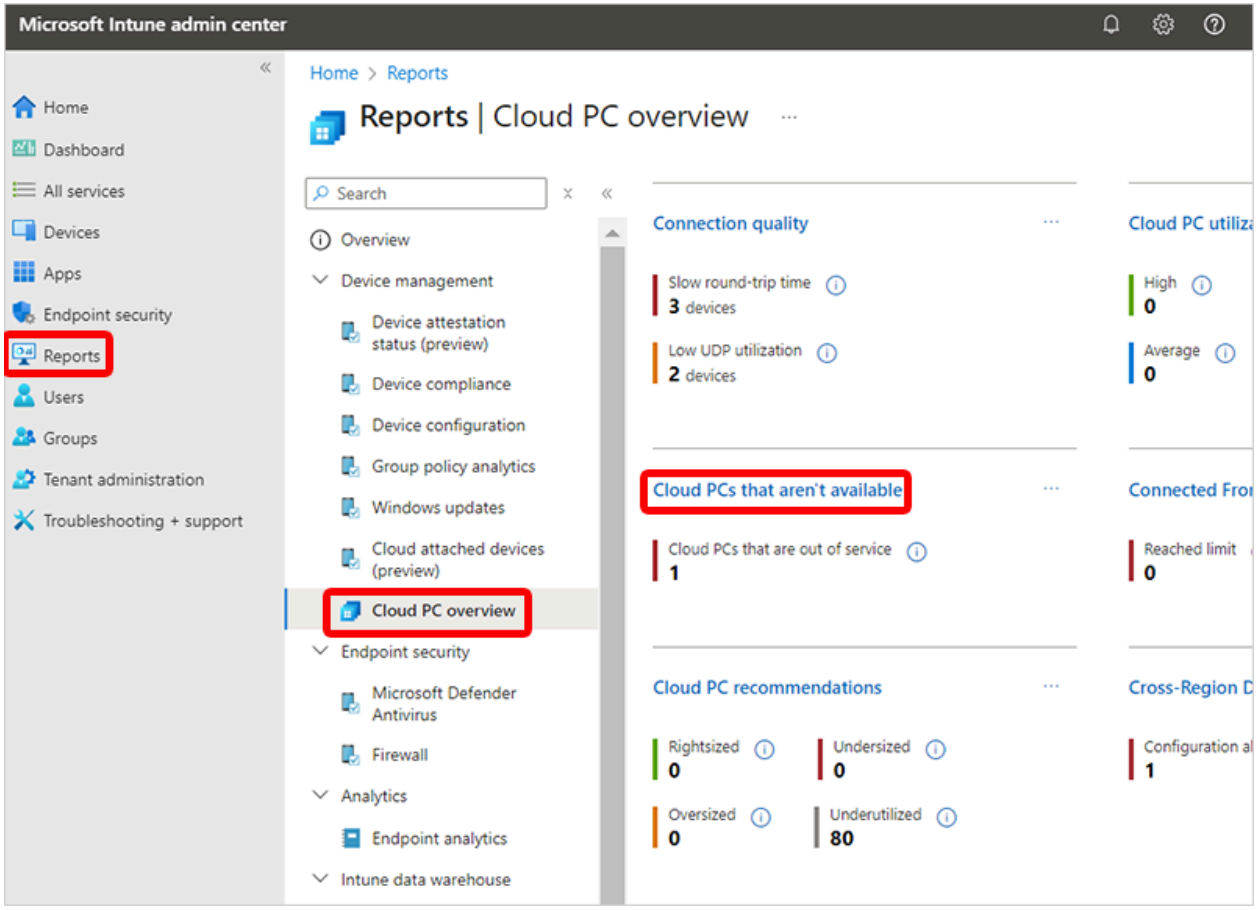


Таблица данных

В списке устройств отображаются отдельные облачные компьютеры со следующими столбцами:

- **Имя устройства**
- **Имя пользователя**
- **Работоспособность узла**. Последняя ошибка работоспособности узла облачного компьютера проверка, если она есть.
- **Ошибка подключения**: последняя ошибка подключения, если она есть.
- **Состояние системы**: текущее состояние системы для облачного компьютера.
- **Регион**: регион Azure, в котором находится облачный компьютер.
- **Состояние устройства**: текущее состояние облачного компьютера.
- **Последнее событие**: дата и время последнего события, предполагающего, что облачный компьютер недоступен.
- **Сведения о проблеме**: сведения о событии.

Отсутствие данных в столбце указывает на то, что для этой области не нужно сообщать. Эта область, вероятно, не является основной причиной недоступности.

Для настройки отчета можно использовать параметры **фильтра Столбцы** и **Добавить** :

- Выберите отображаемые столбцы.
- Отфильтруйте диапазон для каждого столбца.

Вы можете использовать ссылку **Просмотреть сведения** , чтобы просмотреть новейшую историю облачного компьютера. Затем можно перекрестно ссылаться на несколько условий и временных шкал, чтобы найти потенциальные первопричины недоступности облачного компьютера.

Используя различные столбцы вместе, опытный администратор может получить подсказки о состоянии устройства и основной причине любых проблем. Например, пользователь жалуется в службу поддержки, что не может получить доступ к своему облачному компьютеру. Вы проверка этот отчет и не увидите никаких данных в столбцах **Работоспособности узла** или **Состояние системы**, **состояние устройстваподготовлено**, а **ошибка подключения** — "**Отключение клиента**". Другие облачные компьютеры в том же регионе отсутствуют в списке. Эта проблема, вероятно, связана с этим пользователем, возможно, связана с физической конфигурацией клиента, конфигурацией сети или сетевой инфраструктурой.

Массовые действия устройств

Вы можете использовать **массовые действия устройства** для одновременного выполнения действий на нескольких облачных компьютерах.

1. Необязательный параметр. Используйте **команду Добавить фильтры** , чтобы отфильтровать данные таблицы, чтобы просмотреть облачные компьютеры, которыми вы хотите управлять.
2. Выберите облачные компьютеры, которыми вы хотите управлять (не более 100 000 облачных компьютеров).
3. Выберите **Массовые действия**> устройства для конкретного устройства.
4. В зависимости от конкретного действия завершите последующие страницы.

Время, затраченное на выполнение действий, зависит от конкретного действия.

Дальнейшие действия

Удаленное управление Windows 365 устройствами.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Отчет подключенных облачных компьютеров frontline

Статья • 28.04.2025

Этот отчет поможет вам:

- Сведения о максимальном количестве одновременных подключений для каждого размера лицензии облачного компьютера (максимальное ограничение параллелизма).
- Узнайте, какие пользователи в настоящее время подключены к своему компьютеру Frontline Cloud, и просмотрите продолжительность сеанса.
- Узнайте, какие пользователи в настоящее время используют буфер параллелизма (облачные компьютеры frontline только в выделенном режиме).
- Перезапустите компьютеры Frontline Cloud, чтобы получить параллелизм ниже заданного порогового значения.
- Убедитесь, что вы приобрели нужное количество лицензий для пикового использования.

Максимальное ограничение параллелизма

Максимальное ограничение параллелизма определяется общим числом приобретенных лицензий frontline. Если это ограничение достигнуто, последующие пользователи не смогут подключаться к своим облачным компьютерам.

В таких случаях можно выполнить любое из следующих действий, чтобы разблокировать пользователей:

- Перезапустите некоторые облачные компьютеры, чтобы уменьшить параллелизм. Вы можете использовать сведения о длине сеанса, чтобы определить, какие облачные компьютеры следует перезапустить.
- Повторное распространение лицензий между Microsoft Entra назначениями группы.
- Приобретение дополнительных лицензий.

Если общее количество подключений превышает максимальное ограничение параллелизма, это означает, что вы используете буфер параллелизма (только для компьютеров Frontline Cloud в выделенном режиме).

Требования

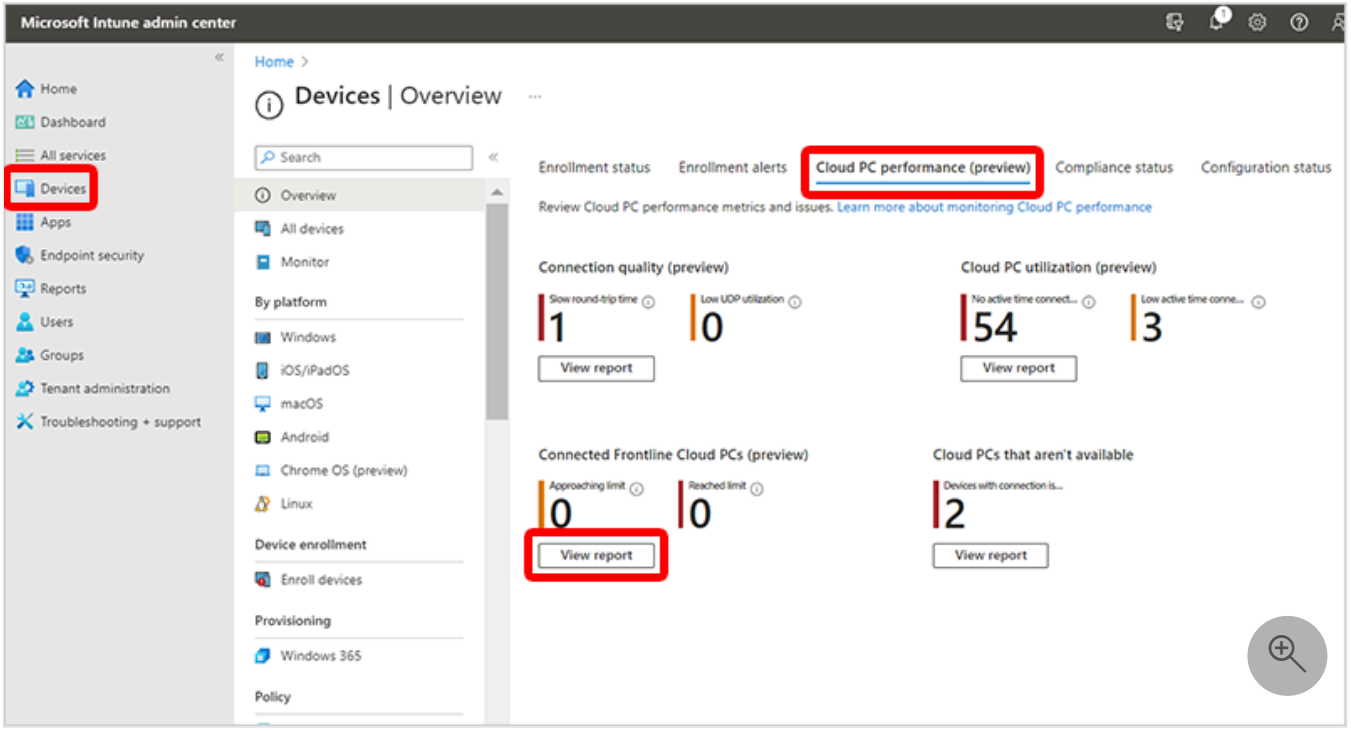
Для просмотра этого отчета требуются следующие разрешения:

- SharedUseLicenseUsageReport
- SharedUseServicePlans

Чтобы назначить эти разрешения, перейдите в раздел**Роли**>**администрирования**> клиента**Создание**>**Windows 365 роль**.

Использование отчета подключенных облачных компьютеров frontline

Чтобы открыть отчет **Подключенные облачные компьютеры frontline**, войдите в центр администрирования Microsoft Intune, выберите **Отчеты Обзор**>>**облачного компьютераПодключенные облачные компьютеры Frontline Cloud PC (предварительная версия)**> выберите размер облачного компьютера.



Если вы подготовили облачные компьютеры Frontline в режиме общего доступа, связанные назначения отображаются под выбранным размером облачного компьютера.

Данные отчета

Этот отчет предназначен для Windows 365 Frontline выделенном и общем режиме. Это не относится к другим планам Windows 365. Если вы не приобрели лицензии на Windows 365 Frontline для клиента, данные в отчете не отображаются.

Журнал одновременных подключений

В отчете показаны следующие данные, агрегированные за последние 28 дней:

- **Текущие подключения**: количество подключенных в настоящее время облачных компьютеров frontline.
- **Журнал одновременных подключений**. Этот график поможет вам решить, нужно ли приобретать больше лицензий, чтобы увеличить ограничение параллелизма.
- **Большинство одновременных подключений**: наибольшее число подключенных облачных компьютеров Frontline для отфильтрованного диапазона:
  - Ежедневно в течение последних 7 или 28 дней.
  - Ежечасно за последние один, три или семь дней.
- **Ограничение**: максимальное ограничение параллелизма, равное количеству приобретенных лицензий.
- **Достигнуто ограничение параллелизма**: предупреждения о приближении и достижении максимального предела параллелизма.

На **диаграмме Журнал одновременных подключений** показано, когда вы достигаете или превышаете максимальное ограничение параллелизма для клиента или выбранного назначения группы. Если общее число подключений превышает максимальное ограничение параллелизма, вы используете буфер параллелизма (только в выделенном режиме frontline). Дополнительные сведения см. в разделе Превышение максимального предела параллелизма.

Подключенные устройства

Чтобы узнать, какие пользователи подключены в данный момент, выберите **Подключено**.

В этом разделе показано, какие облачные компьютеры подключены в настоящее время. Чтобы привести параллелизм ниже максимального предела, можно перезапустить облачные компьютеры, чтобы отключить пользователя от сеанса.

Дальнейшие действия

Отчет о качестве подключения к облачному компьютеру

Отчет о производительности ресурса

Статья • 27.02.2025

Отчет о производительности ресурсов в Аналитике конечных точек помогает оптимизировать ресурсы виртуальных ЦП и ОЗУ на устройствах Облачных компьютеров в вашей организации. Отчет включает четыре вкладки с данными:

- **Оценка производительности ресурса**
- **Производительность модели**
- **Производительность устройства**
- **Журнал устройства**

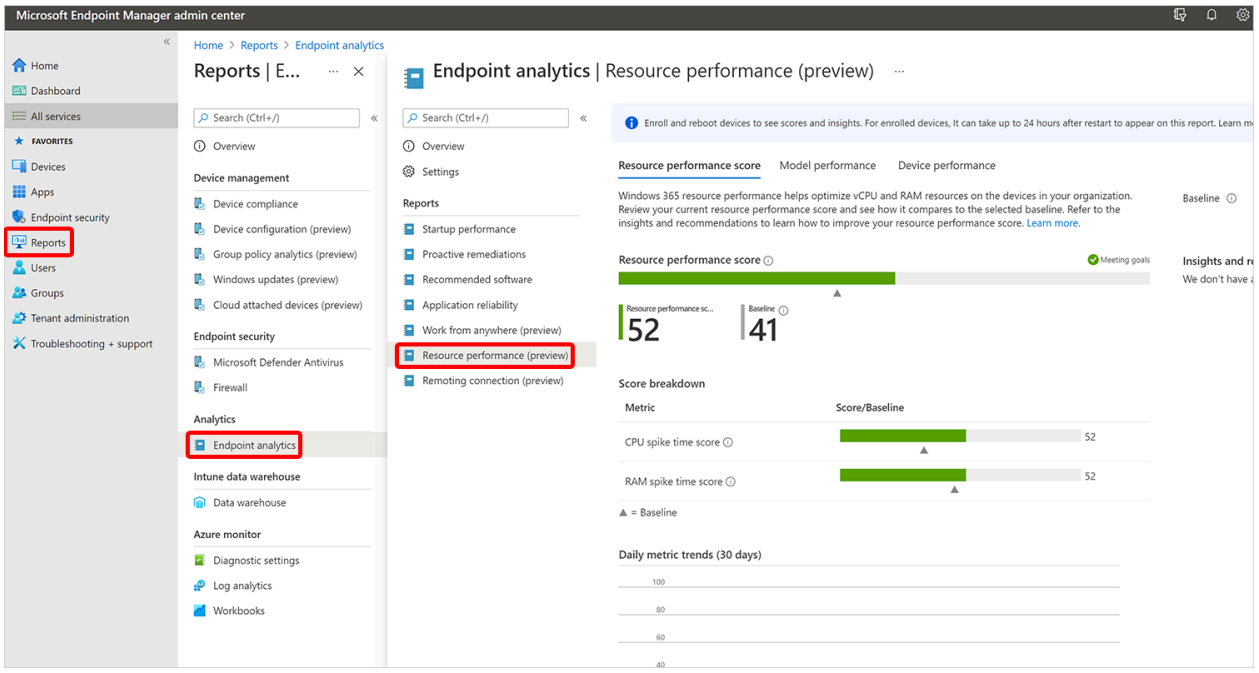
Оценка производительности ресурса также влияет на оценку производительности Майкрософт вашей организации.

Предварительные требования

Прежде чем использовать этот отчет, необходимо зарегистрировать устройства Облачных компьютеров в Аналитике конечных точек.

Использование отчета о производительности ресурсов

Чтобы открыть отчет о **производительности ресурсов**, войдите в центр администрирования Microsoft Intune, выберите **Отчеты**>**Аналитика конечных**> точек**Производительность ресурсов**.



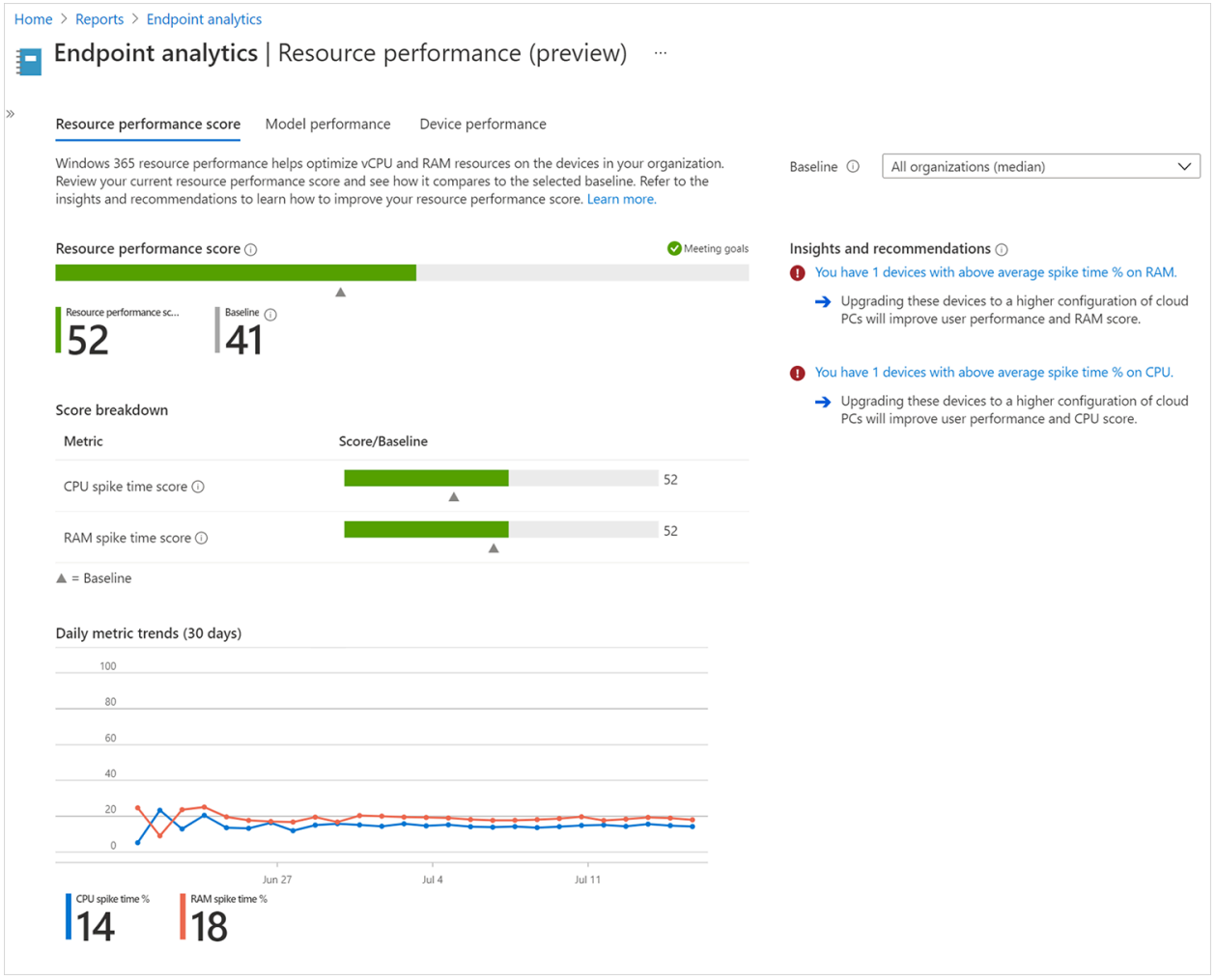
Вкладка "Оценка производительности ресурса"

Оценка производительности ресурса — это общий рейтинг производительности (от 0 до 100) для всех управляемых вами Облачных компьютеров. Эта оценка представляет собой взвешенное среднее значение оценки времени пиковой нагрузки на **ЦП** и **ОЗУ**.

- **Время пиков ЦП** %. На графике тенденций ежедневной метрики отображается отношение времени пиков ЦП к общему времени использования. Эти данные о скачке ЦП в процентах в среднем за 14-дневный период, заканчивающийся на дату в нижней части диаграммы. Использование более 50 % считается пиком.
- **Время пиков ОЗУ** %: на графике тенденций ежедневной метрики отображается отношение времени пиков ОЗУ к общему времени использования. Эти данные о пике ОЗУ в среднем за 14-дневный период, заканчивающийся на дату в нижней части диаграммы. Использование более 50 % считается пиком.

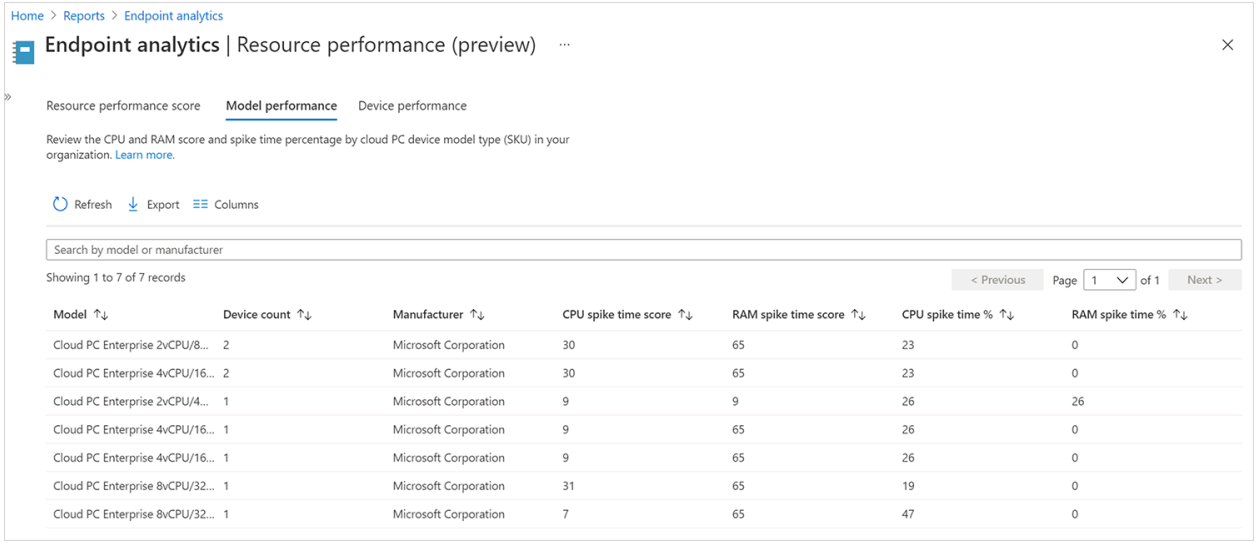
Базовый показатель позволяет понять, добиваетесь ли вы нужных целей. Вы можете задать базовый показатель на уровне медианы для организации или указать собственное значение.

Аналитика и рекомендации позволяют получать предложения о действиях, которые можно предпринять для улучшения оценки.



Вкладка производительности модели

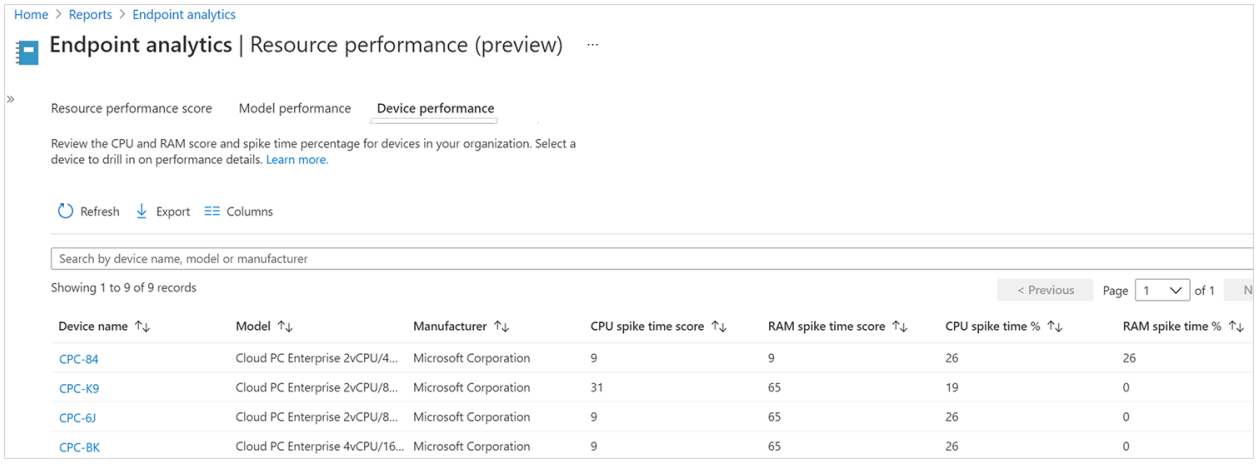
Вы можете просмотреть оценки и проценты времени всплеска ЦП и ОЗУ для каждого номера SKU модели облачного компьютера в вашей организации.



Model	Device count	Manufacturer	CPU spike time score	RAM spike time score	CPU spike time %	RAM spike time %
Cloud PC Enterprise 2vCPU/8...	2	Microsoft Corporation	30	65	23	0
Cloud PC Enterprise 4vCPU/16...	2	Microsoft Corporation	30	65	23	0
Cloud PC Enterprise 2vCPU/4...	1	Microsoft Corporation	9	9	26	26
Cloud PC Enterprise 4vCPU/16...	1	Microsoft Corporation	9	65	26	0
Cloud PC Enterprise 4vCPU/16...	1	Microsoft Corporation	9	65	26	0
Cloud PC Enterprise 8vCPU/32...	1	Microsoft Corporation	31	65	19	0
Cloud PC Enterprise 8vCPU/32...	1	Microsoft Corporation	7	65	47	0

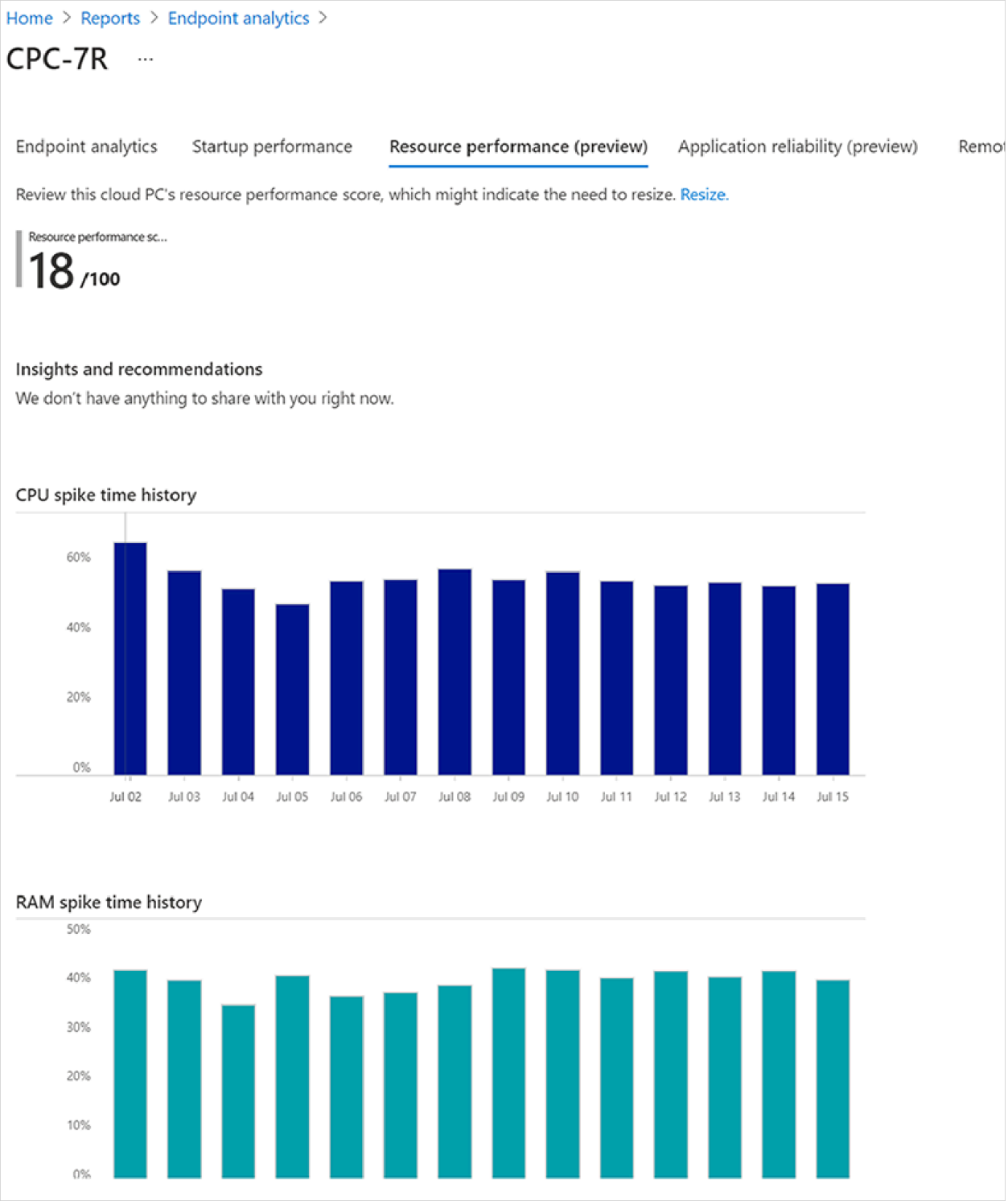
Вкладка "Производительность устройства"

Вы можете просмотреть показатели времени загрузки ЦП и ОЗУ и проценты для каждого устройства облачного компьютера в вашей организации.



История устройств

Когда вы выбираете определенное устройство в одном из отчетов, вы увидите соответствующие сведения об этом устройстве. Если оценка устройства ниже базового показателя, можно улучшить производительность и оценку устройства, добавив дополнительные ресурсы для устройства и изменив размер.



Дальнейшие действия

Отчет о качестве подключения к облачному компьютеру

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Необязательный отчет о состоянии непрерывности бизнес-процессов и аварийного восстановления для облачного компьютера

15.08.2025

В дополнительном отчете о **состоянии непрерывности бизнес-процессов и аварийного восстановления облачного компьютера** содержатся соответствующие сведения о работоспособности аварийного восстановления, а также аварийное восстановление между регионами или аварийное восстановление.

Использование дополнительного отчета о непрерывности бизнес-процессов и аварийном восстановлении облачного компьютера

Чтобы открыть **необязательный отчет о состоянии непрерывности бизнес-процессов и аварийного восстановления на облачном компьютере**, войдите в центр администрирования Microsoft Intune, выберите **Отчеты Обзор**>**облачного компьютера**>**Необязательная непрерывность бизнес-процессов и состояние аварийного восстановления**.

В списке устройств отображаются отдельные облачные компьютеры со следующими столбцами:

- **Имя устройства**
- **Имя участника-пользователя**
- **Оповещение конфигурации**
  - **Здоровый**
  - **Неработоспособное**
- **Тип лицензии**
  - **Между регионами**
  - **DR Plus**
  - **Нет**
- **Состояние аварийного восстановления**
  - **Активный сбой**
  - **Истечение срока действия активации**
  - **Неактивен**

- **Текущая точка восстановления**
- **Состояние резервного копирования CPC**
- **Срок действия активации**
- **Параметры пользователя**

Каждая строка в отчете содержит ссылки на конкретный облачный компьютер, где можно найти более подробные сведения об журнале подключений устройств и связанной производительности. Для настройки отчета можно использовать параметры **фильтра Столбцы** и **Добавить** . Фильтры доступны для:

- **Срок действия активации**
- **Оповещение конфигурации**
- **Состояние аварийного восстановления**
- **Тип лицензии**

Дальнейшие действия

Узнайте, как настроить и активировать и отключить аварийное восстановление между регионами . Узнайте, как настроить и активировать/деактивировать аварийное восстановление плюс.

политика кругов клиентский компонент Центра обновления Windows в Intune

04.03.2025

Создайте круги обновлений, указывающие, как и когда Windows как услуга обновляет устройства с Windows *обновлениями компонентов и качества*. В Windows новые обновления компонентов и исправлений включают содержимое всех предыдущих обновлений. Если у вас установлено последнее обновление, то устройства с Windows обновлены. В отличие от предыдущих версий Windows, теперь необходимо устанавливать не отдельную часть обновления, а полное обновление.

Круги обновления также можно использовать для обновления до Windows 11 подходящих устройств с Windows 10. Для этого при создании политики воспользуйтесь параметром *Обновление устройств с Windows 10 до последнего выпуска Windows 11*, настроив для него значение *Да*. При использовании кругов обновления для перехода на Windows 11 на устройства устанавливаются последние версии Windows 11. Если вы позже присвоите параметру обновления значение *Нет*, устройства, которые еще не приступили к обновлению, не начнут его, а устройства, находящиеся в процессе обновления, продолжат его. На устройствах, завершивших обновление, сохранится Windows 11. Дополнительные сведения о соответствии требованиям см. в разделе Технические характеристики и требования к системе для Windows 11 | Майкрософт.

Круги обновлений Windows поддерживают теги области. Теги области можно использовать с кругами обновлений для фильтрации применяемых наборов конфигураций и управления ими.

Предварительные требования

Чтобы использовать клиентский компонент Центра обновления Windows rings для устройств Windows в Intune, необходимо выполнить следующие предварительные требования.

- Устройства должны иметь доступ к конечным точкам. Подробный список конечных точек, необходимых для связанной службы, см. в статье Сетевые конечные точки.
  - Центр обновления Windows

> **Примечание**
>
> Хотя для настройки политик клиента клиентский компонент Центра обновления Windows не требуется, если служба Помощника по Sign-In учетных записей

Майкрософт (wlidsvc) отключена, клиентский компонент Центра обновления Windows не предлагает обновления компонентов. Дополнительные сведения см. в разделе **Обновления компонентов не предлагаются в отличие от других обновлений**.

- Устройства должны быть одним из следующих поддерживаемых выпусков Windows:
  - Windows Pro
  - Windows Enterprise
  - Windows IoT Enterprise
  - Windows для образовательных учреждений
  - Windows Team — для устройств Surface Hub
  - Windows Holographic for Business — Windows Holographic for Business поддерживает подмножество параметров для обновлений Windows, в том числе:
    - **Автоматическое обновление**
    - **Обновления продуктов Майкрософт**
    - **Канал обслуживания**: любая общедоступная сборка обновления.

    Дополнительные сведения см. в статье Управление Windows Holographic.
  - Windows Enterprise LTSC и IoT Enterprise LTSC- LTSC поддерживаются для обновлений качества, но не для обновлений компонентов. В результате следующие кольцевые элементы управления не поддерживаются для LTSC:
    - Приостановка обновлений *компонентов*
    - Период отсрочки обновления компонентов (в днях)
    - Установка периода удаления обновления компонентов (от 2 до 60 дней)
    - Включение предварительных сборок, что включает следующие параметры сборок.
      - Программа предварительной оценки Windows — предварительный выпуск
      - Бета-канал
      - Канал разработчика
    - Использование параметров крайнего срока для обновлений *компонентов*.

Ограничения для устройств, присоединенных к рабочему месту

Круги обновления Intune для Windows требуют использования клиентский компонент Центра обновления Windows клиентских политик, которые поддерживают устройства,

присоединенные к рабочей области (WPJ). Однако следующие типы политик Intune клиентский компонент Центра обновления Windows используют клиентский компонент Центра обновления Windows клиентские политики и автоматическое исправление Windows, что предоставляет дополнительные возможности, которые не поддерживаются для устройств WPJ.

- Обновления драйверов
- Обновления функций
- Обновления качества (также известные как *ускоренное* обновление)

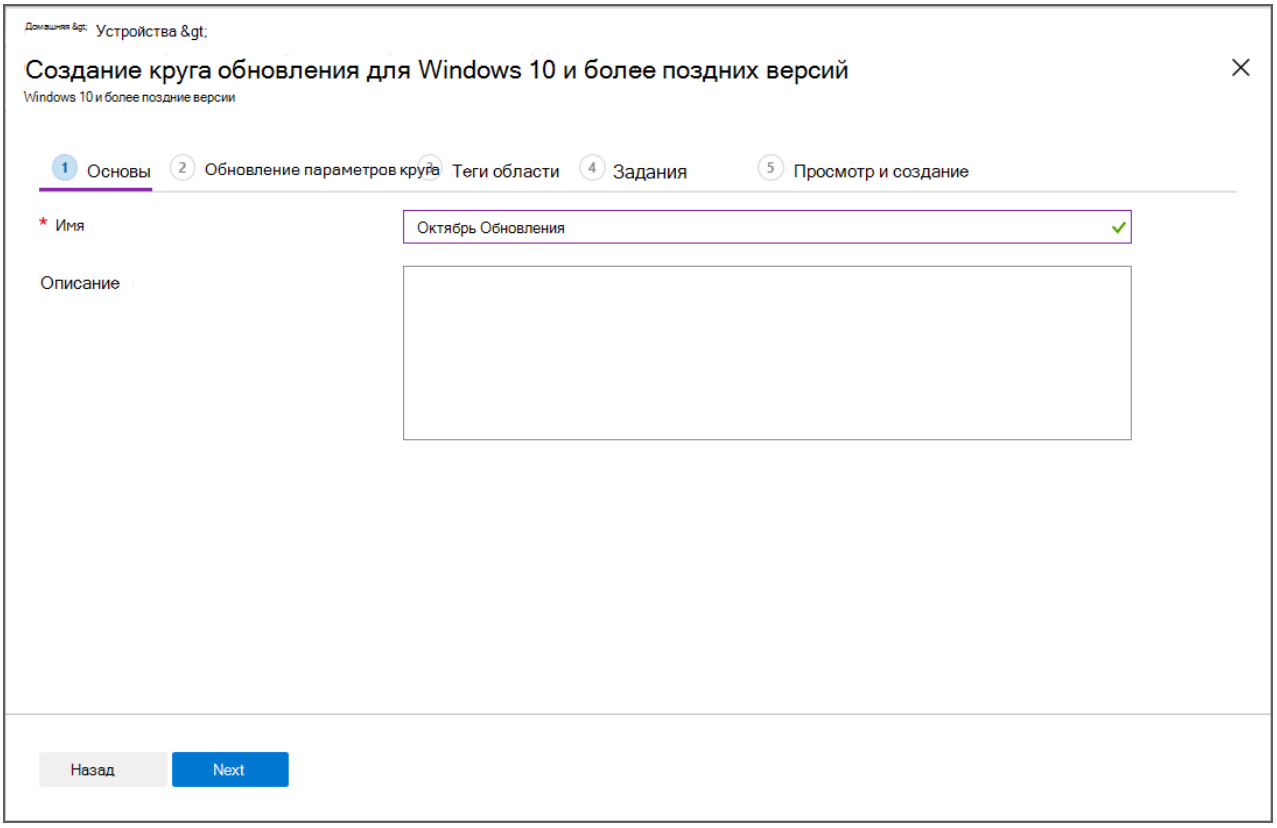
Дополнительные сведения об ограничениях WPJ для политик клиентский компонент Центра обновления Windows Intune см. в разделе Ограничения политик для устройств, присоединенных к рабочей области.

Создание и назначение кругов обновления

1. Войдите в Центр администрирования Microsoft Intune.

2. Выберите **Устройства**>**По платформе**>**Windows**>**Управление обновлениями**>**Windows 10 и более поздними обновлениями**на**вкладке**>**Круги обновлений**> Создать профиль.

3. В разделе *Основные* укажите имя, описание (необязательно), а затем выберите **Далее**.



4. На вкладке **Параметры круга обновления** настройте параметры в соответствии со своими бизнес-потребностями. Дополнительные сведения о доступных параметрах см. в статье Параметры Центра обновления Windows. После настройки параметров *Обновление и взаимодействие с пользователем* выберите **Далее**.

5. На вкладке **Теги области** щелкните **+ Выбрать теги области**, чтобы открыть панель *Выбранные теги*, в которой можно назначить теги области для круга обновления. Выберите теги, а затем нажмите кнопку **Выбрать**, чтобы добавить их в круг обновления и вернуться к панели *Теги области*.

   Когда все будет готово, выберите **Далее**, чтобы перейти к *назначениям*.

   > ⓘ **Примечание**
   >
   > При настройке или изменении политик Intune некоторые типы политик могут не отображать страницу конфигурации "Теги области", если для клиента нет настраиваемых область тегов. Если параметр Тег области не отображается, убедитесь, что в дополнение к тегу область по умолчанию определен хотя бы один тег.

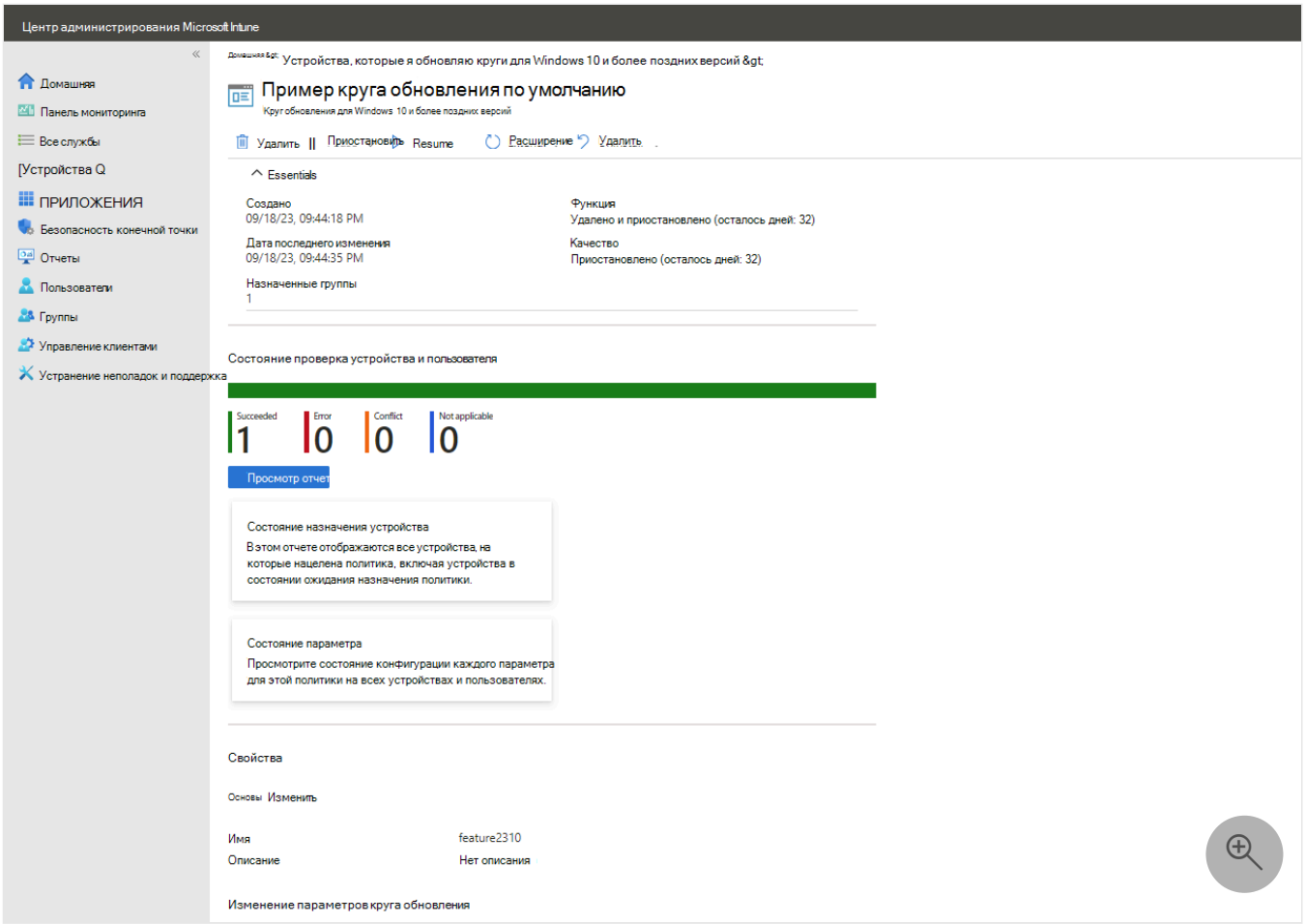
6. На вкладке **Назначения** щелкните **+ Выберите группы для включения** и назначьте круг обновления группам. Используйте функцию **+ Выберите группы для исключения** для точной настройки назначения. Нажмите кнопку **Далее**, чтобы продолжить.

   В большинстве случаев рекомендуется развертывать круги обновления в группах устройств. Использование групп устройств соответствует нашим рекомендациям по развертыванию обновлений компонентов и устраняет необходимость входа пользователя на устройство до применения политики.

7. На вкладке **Проверка и создание** просмотрите параметры, а затем выберите **Создать** при готовности к сохранению круга обновления для Windows. Новый круг обновления отображается в списке кругов обновления.

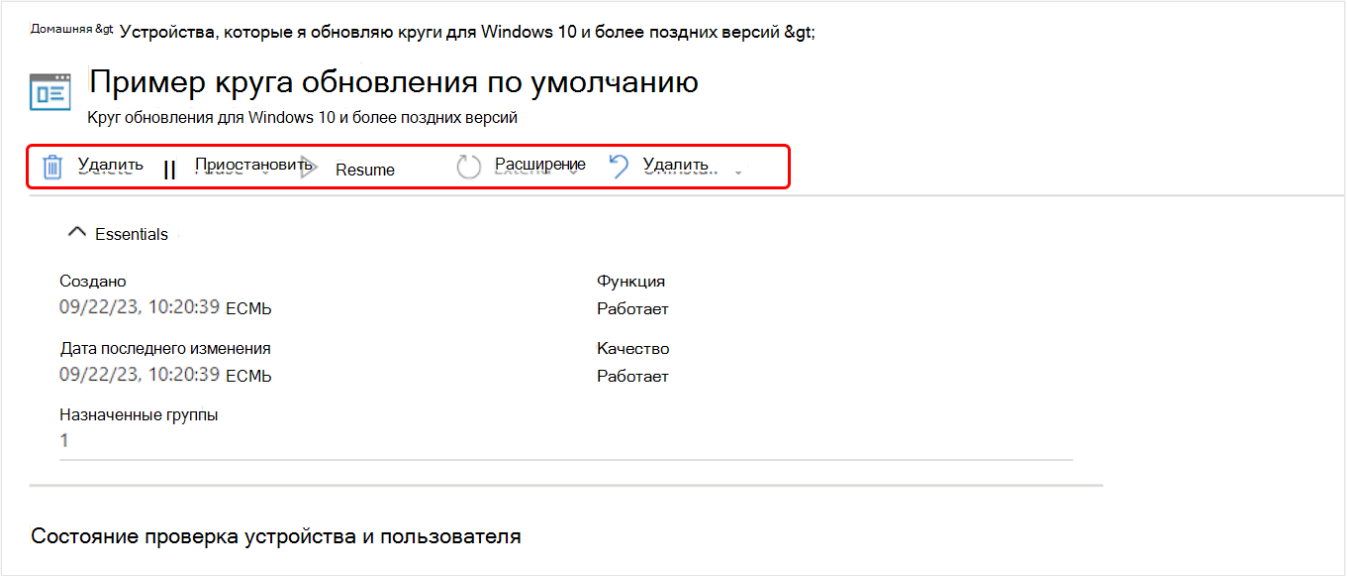
Управление кругами обновлений Windows

На портале перейдите на вкладку **Устройства**>**По платформе**>**Windows**>**Управление обновлениями**>**Windows 10 и более поздними обновлениямиКруги обновлений**> и выберите политику кругов, которой вы хотите управлять. Intune отображает сведения, аналогичные приведенным ниже, для выбранной политики:



Это представление включает в себя:

- **Действия политики**. Используйте следующие параметры в верхней части представления политики для управления политикой круга обновлений:
- Удаление
- Pause
- Resume
- Extend
- Uninstall



Это представление также включает в себя:

- **Essentials**. Список сведений о политике, включая время ее создания, последнего изменения и количество групп, назначенных политике.

- **Состояние проверка устройства и пользователя**: представление отчета по умолчанию для этой политики. В дополнение к этому представлению по умолчанию доступны следующие сведения и параметры отчета:

  - **Просмотр отчета**. Кнопка открывает более подробное представление отчета о *состоянии проверка устройства и пользователя*.

  - **Две дополнительные плитки отчета**. Вы можете выбрать плитки для следующих отчетов, чтобы просмотреть дополнительные сведения:
    - **Состояние назначения устройства** . В этом отчете отображаются все устройства, на которые нацелена политика, включая устройства в состоянии ожидания назначения политики.
    - **Состояние параметра** — просмотр состояния конфигурации каждого параметра для этой политики на всех устройствах и пользователях.

  Дополнительные сведения об этом представлении отчета см. в статье Отчеты для кругов обновления для политики Windows 10 и более поздних версий.

- **Свойства**. Просмотрите сведения для каждой страницы конфигурации политики, включая параметр **Изменить** каждую область политики.

Действия политики

Удалить

Выберите **Удалить**, чтобы остановить применение параметров выбранного круга обновления Windows. При удалении круга из Intune удаляется его конфигурация, поэтому Intune больше не применяет эти параметры.

При удалении круга из Intune его параметры на устройствах, которым назначен круг обновления, не изменяются. Вместо этого устройство сохраняет текущие настройки. Устройства не сохраняют запись журнала о параметрах, которые они удерживали ранее. Устройства могут также принимать параметры из других кругов обновления, которые остаются активными.

Удаление круга

1. На странице "Обзор" для круга обновления выберите **Удалить**.
2. Нажмите кнопку **OK**.

Пауза

Выберите **Приостановить**, чтобы предотвратить получение исправлений или обновлений компонентов на соответствующем устройстве на срок до 35 дней с момента приостановки круга. По истечении максимального числа дней функция приостановки автоматически отключается, и устройство может проверить наличие обновлений в Центре обновления Windows. После этой проверки вы можете снова приостановить обновления. Если возобновить приостановленный круг обновления, а затем снова приостановить его, период приостановки будет сброшен до 35 дней.

Приостановка круга

1. На странице "Обзор" для круга обновления выберите **Приостановить**.
2. Выберите **Компонент** или **Исправление**, чтобы приостановить этот тип обновления, а затем нажмите кнопку **OK**.
3. После приостановки одного типа обновления можно снова выбрать "Приостановить", чтобы приостановить другой тип обновления.

Когда тип обновления приостановлен, в области "Обзор" для этого круга отображается количество оставшихся дней до возобновления типа обновления.

> ⓘ **Важно!**
>
> После подачи команды приостановки устройства получат эту команду при следующей регистрации в службе. Не исключено, что перед регистрацией они могут установить запланированное обновление. Кроме того, если в момент подачи

команды приостановки целевое устройство выключено, при включении оно может скачать и установить запланированное обновление до регистрации в Intune.

Resume

Пока круг обновления приостановлен, можно выбрать **Восстановить**, чтобы восстановить обновления компонентов и исправления для этого круга до активной операции. После возобновления круга обновления можно снова приостановить круг.

Возобновление круга

1. На странице "Обзор" для приостановленного круга обновления выберите **Возобновить**.
2. Выберите один из доступных вариантов, чтобы возобновить обновления **компонентов** или **исправления**, а затем нажмите кнопку **OK**.
3. После возобновления одного типа обновления можно снова выбрать "Возобновить", чтобы возобновить другой тип обновления.

Расширение

Пока круг обновления приостановлен, можно выбрать **Продлить**, чтобы сбросить период приостановки для исправлений и обновлений компонентов для этого круга обновления до 35 дней.

Продление периода приостановки для круга

1. На странице "Обзор" для приостановленного круга обновления выберите **Продлить**.
2. Выберите один из доступных вариантов, чтобы возобновить обновления **компонентов** или **исправления**, а затем нажмите кнопку **OK**.
3. После продления приостановки для одного типа обновления можно выбрать "Продлить" еще раз, чтобы продлить другой тип обновления.

Удалить

Администратор службы Intune может нажать кнопку **Удалить**, чтобы удалить (откатить) последнюю версию обновления *компонента* или последнюю версию *исправления* для активного или приостановленного круга обновления. После удаления одного типа можно удалить другой тип. Intune не поддерживает и не управляет возможностью пользователей удалять обновления.

> **Важно!**
>
> Когда вы используете опцию *Unininstall* (Удалить), Intune немедленно передает запрос на удаление устройствам.
>
> - Устройства Windows начинают удалять обновления сразу после получения изменений в политике Intune. Удаление обновлений не ограничено расписаниями обслуживания, даже если они настроены как часть круга обновления.
> - Если для удаления обновления требуется перезагрузка устройства, устройство перезапускается без предоставления пользователям устройства возможности задержки.

Для успешного удаления:

На устройстве необходимо установить последнее обновление. Так как обновления являются накопительными, устройства, на которых установлено последнее обновление, будут иметь самое последнее обновление компонентов и самые последние исправления. Примером использования этого параметра является откат последнего обновления при обнаружении критической проблемы на компьютерах с Windows.

При удалении учитывайте следующее:

- Удаление обновления компонентов или исправления доступно только для канала обслуживания устройства.
- В результате удаления исправлений и обновлений компонентов политика восстанавливает предыдущее обновление на компьютерах с Windows.
- После успешного отката обновления качества пользователи устройств по-прежнему видят обновление, указанное в **разделе Параметры**> Windows **Обновления**>**Обновить журнал** обновления.
- Если вы удаляете обновления компонентов или исправления в круге обновления, Intune приостанавливает обновления такого же типа в этом круге обновления.
- Когда приостановка обновления компонента или исправления в круге обновления истечет, устройства переустановят удаленные ранее обновления компонентов или исправления, если они еще применимы.
- Удаление не будет успешным, если обновление компонента было применено с помощью пакета включения. Дополнительные сведения о пакетах включения см. в

разделе KB5015684 .

- В частности, для обновления компонентов время, в течение которого можно удалить обновление, ограничено сроком от 2 до 60 дней. Этот период настраивается параметром обновления кругов **Установка периода удаления обновления компонентов (2–60 дней)**. Невозможно выполнить откат обновления компонента, установленного на устройстве, после того как обновление было установлено на период, превышающий настроенный период удаления.

  Например, рассмотрим круг обновлений с периодом удаления обновлений 20 дней. По истечении 25 дней вы решаете откатить последнее обновление компонентов и используете опцию удаления. Устройства, которые установили обновление компонентов более 20 дней назад, не могут выполнить откат, так как они удалили необходимые биты в рамках обслуживания. Однако устройства, которые установили обновление только 19 дней назад, могут удалить его, если они зарегистрированы для получения команды удаления до истечения 20-дневного периода удаления.

Дополнительные сведения о политиках Центра обновления Windows см. в статье Обновление CSP в документации по управлению клиентом Windows.

Удаление последнего обновления Windows

1. На странице "Обзор" для приостановленного круга обновления выберите **Удалить**.
2. Выберите один из доступных вариантов, чтобы удалить обновления **компонентов** или **исправления**, а затем нажмите кнопку **OK**.
3. После запуска удаления для одного типа обновления можно выбрать "Удалить" еще раз, чтобы удалить оставшийся тип обновления.

Проверка и создание отчетов

Существует несколько вариантов получения подробных отчетов об обновлениях Windows 10/11 с помощью Intune. Дополнительные сведения об отчетах для кругов обновления, включая сведения о представлении по умолчанию и дополнительных плитках отчетов, см. в статье Отчеты об обновлении Windows.

Дальнейшие действия

- Использование обновлений компонентов Windows в Intune
- Используйте отчеты о совместимости обновлений Windows
- Использование отчетов об обновлениях Windows для обновлений Windows

- Также см . статью Автозапавание Windows в содержимом развертывания Windows для альтернативного решения.

Политика обновления компонентов для Windows 10 и более поздней версии в Intune

19.09.2025

С помощью *обновлений компонентов для Windows 10 и более поздних версий* Intune можно выбрать версию обновления компонентов Windows, на которой должны оставаться устройства. Intune поддерживает установку уровня компонента для любой версии, которая поддерживается на момент создания политики.

Вы также можете использовать политику обновления компонентов для обновления устройств под управлением Windows 10 до Windows 11.

Политики обновлений компонентов Windows работают с политиками *кругов обновления Windows 10 и более поздних версий*, чтобы предотвратить получение устройством версии компонента Windows, превышающей значение, указанное в политике обновления компонентов.

Когда устройство получает политику для обновлений компонентов.

- Устройство обновляется до версии Windows, указанной в политике. Устройство, которое уже работает под управлением более поздней версии Windows, остается в текущей версии. При замораживании версии набор компонентов устройств остается стабильным в течение всего срока действия политики.

> ⓘ **Примечание**
>
> Обновление не будет установлено на устройстве, если на нем установлена *защитная блокировка* для этой версии Windows. Когда устройство оценивает применимость обновления, Windows устанавливает временную защитную блокировку при наличии известной неразрешенной проблемы. После устранения проблемы блокировка снимается, после чего устройство можно обновить.
>
> - Дополнительные сведения о **защитных блокировках** см. в документации Windows о *состоянии обновления компонентов*.
> - Сведения об известных проблемах, которые могут привести к защитной блокировке, см. сведения о соответствующем выпуске Windows, где следует перейти на соответствующую версию Windows из оглавления для этой страницы:

- Информация о выпуске Windows 11

- В отличие от использования *Паузы* с кругом обновления, срок действия которого истекает через 35 дней, политика обновления компонентов остается в силе. Устройства не устанавливают новую версию Windows, пока не будет изменена или удалена политика обновления компонентов. Если изменить политику, указав более новую версию, то устройства смогут устанавливать компоненты из этой версии Windows.

- Возможность *Удалить* обновление компонентов по-прежнему будет поддерживаться кругами обновления.

- Вы можете настроить политику для управления расписанием, в соответствии с которым Центр обновления Windows делает предложение доступным для устройств. Дополнительные сведения см. в статье Параметры выпуска для Центра обновления Windows.

- При развертывании обновления компонентов Windows на устройстве из облачной службы автоматически включается последнее ежемесячное обновление качества.

Предварительные требования

> ⓘ **Важно!**
>
> Эта функция не поддерживается в облачных средах GCC и GCC High/DoD.
>
> Включение активации подписки с помощью существующего еа не применяется к облачным средам GCC и GCC High/DoD для возможностей автоматического исправления Windows.

Ниже перечислены предварительные требования обновления компонентов Windows для Windows 10 и более поздних версий в Intune.

- Для основных функций создания и нацеливания обновления компонентов требуется только лицензия на Intune. Основные функции включают создание политики и выбор обновления компонентов для обновления устройств, использование параметра **Сделать обновления доступными как можно скорее** или указание даты начала и создание отчетов. Для возможностей, поддерживаемых политиками клиентов на профессиональных устройствах SKU, лицензия не требуется.

- Для дополнительных облачных функций требуется дополнительная лицензия. Чтобы использовать облачную возможность, помимо лицензии на Intune, ваша организация должна иметь одну из следующих подписок, включающих лицензию на автоматическое исправление Windows:
  - Windows Корпоративная E3 или E5 (входит в состав Microsoft 365 F3, E3 или E5)
  - Windows для образовательных учреждений A3 или A5 (входит в состав Microsoft 365 A3 или A5)
  - Доступ к виртуальному рабочему столу Windows E3 или E5
  - Microsoft 365 бизнес премиум

  Облачные возможности, требующие дополнительной лицензии, указаны на странице *Создание развертывания обновления компонентов* или создания политики и включают следующие элементы и потенциально новые функции:

  - Постепенное развертывание. Возможность постепенного развертывания — это только облачная функция, которая включает в себя основные элементы управления для развертывания указанного обновления компонентов и момента, когда следует сделать обновление доступным для устройств.
  - Необязательные обновления компонентов
  - Windows 10 (SxS). Функция Windows 10 (SxS) — это функция только для облака. Если вы заблокированы при создании новых политик для возможностей, для которых требуется автоматическое исправление Windows, и вы получаете лицензии на использование клиентский компонент Центра обновления Windows клиентских политик через Соглашение Enterprise (EA), обратитесь к источнику ваших лицензий, например к вашей группе учетных записей Майкрософт или к партнеру, который продал вам лицензии. Команда по учетным записям или партнер могут подтвердить, что лицензии клиентов соответствуют требованиям к лицензии на автоматическое исправление Windows. См . раздел Включение активации подписки с помощью существующего еа.
- Устройства должны:
  - Запустите версию Windows, которая остается в поддержке.
  - Зарегистрируйтесь в Intune MDM и Microsoft Entra гибридное присоединение или Microsoft Entra присоединение.
  - иметь включенную функцию сбора данных телеметрии с минимальным значением *Обязательные*.

Устройства, которые получают политику обновления компонентов и для которых телеметрия *не настроена*, могут установить более позднюю версию Windows, чем определено в политике обновления компонентов.

Настройка телеметрии в рамках политики ограничения устройств для Windows. В профиле ограничения устройства в разделе *Отчеты и телеметрия* присвойте параметру **Общий доступ к данным об использовании** минимальное значение **Обязательные**. Также поддерживаются значения **Расширенный (1903 и более ранние версии)** или **Необязательно**.

- Должен быть запущен *Помощник по входу в учетную запись Microsoft* (wlidsvc). Если служба заблокирована или *отключена*, получить обновление не удастся. Дополнительные сведения см. в разделе Обновления компонентов не предлагаются в отличие от других обновлений. По умолчанию для службы задано значение *Вручную (запуск по триггеру)*. Это позволит запустить его при необходимости.

- Иметь доступ к конечным точкам. Подробный список конечных точек, необходимых для связанных служб, перечисленных здесь, см. в статье Конечные точки сети.
  - Центр обновления Windows
  - Автоисправление Windows

- Включите сбор данных в Intune для устройств, на которые требуется развернуть обновления компонентов.

- Обновления компонентов поддерживаются для следующих выпусков Windows:
  - Pro
  - Предприятие
  - Pro для образовательных учреждений
  - Образование
  - Pro для рабочих станций

> **Примечание**
>
> **Неподдерживаемые версии и выпуски**: *Windows Enterprise LTSC*: клиентский компонент Центра обновления Windows клиентские политики не поддерживают выпуск *Long Term Service Channel*. Запланируйте использование альтернативных методов исправления, таких как WSUS или Configuration Manager.

Ограничения для устройств, присоединенных к рабочему месту

Политики Intune для *обновлений компонентов для Windows 10 и более поздних версий* требуют использования клиентский компонент Центра обновления Windows клиентских политик и автоматического исправления Windows. Если клиентский компонент Центра обновления Windows клиентские политики поддерживают устройства WPJ, автопатка Windows предоставляет дополнительные возможности, которые не поддерживаются для устройств WPJ.

Дополнительные сведения об ограничениях WPJ для политик клиентский компонент Центра обновления Windows Intune см. в статье Ограничения политик для устройств, присоединенных к рабочей области, *в статье Управление Windows 10 и Windows 11 обновлениями программного обеспечения в Intune*.

Ограничения политики обновления компонентов для Windows 10 и более поздней версии

- При развертывании политики *обновлений компонентов для Windows 10 и более поздних версий* на устройстве, на котором также применяется политика *кругов обновления для Windows 10 и более поздних версий*, проверьте круг обновлений на следующие настройки:
  - Для параметра **Период отсрочки обновления компонентов (в днях)** рекомендуется установить значение **0**. Эта конфигурация гарантирует, что обновления компонентов не будут отложены отсрочками обновлений, которые могут быть настроены в политике круга обновлений.
  - Обновления компонентов для круга обновления должны быть *запущены*. Их не следует приостанавливать.

> **Совет**
>
> Если вы используете обновления компонентов, рекомендуем задать период отсрочки обновления компонентов *равным 0* в связанной политике Круги обновлений. Объединение отсрочек круга обновления с политикой обновления компонентов может привести к задержке установки обновлений.
>
> Дополнительные сведения см. в статье **Переход от отсрочек круга обновления к политике обновления компонентов**

- Обновления компонентов для политик Windows 10 и более поздних версий не могут применяться во время запуска Windows Autopilot(OOBE). Вместо этого политики применяются при первом сканировании Центром обновления Windows после завершения подготовки устройства, которое обычно длится день.

- Если вы совместно управляете устройствами с Configuration Manager, политики обновления компонентов могут не сразу вступить в силу на устройствах при новой настройке рабочей нагрузки политик Центра обновления Windows для Intune. Эта задержка носит временный характер, однако может привести к обновлению устройств до более поздней версии (по сравнению с той, которая была настроена в политике) обновления компонентов.

  Чтобы эта первоначальная задержка не повлияла на совместно управляемые устройства:

  1. Войдите в Центр администрирования Microsoft Intune.

  2. Перейдите на **вкладку Устройства**>**По платформе**>**Windows**>**Управление обновлениями**>**Windows 10 и более поздними обновлениями**>**компонентов** вкладка >**Создать профиль**.

  3. В разделе **Параметры развертывания** введите понятное имя и описание политики. Затем укажите обновление компонентов, которое должно выполняться на устройствах.

  4. Завершите настройку политики, включая назначение политики устройствам. Политика развертывается на устройствах, хотя любое устройство, у которого уже выбранная вами версия или более новая версия, не будет предлагаться обновление.

     Отслеживайте отчет о политике. Для этого перейдите на вкладку >**Отчеты**>**Windows Обновления**> Отчеты **Обновления отчет о функциях**. Выберите созданную политику и сформируйте отчет.

  5. Устройства с состоянием *OfferReady* или более поздним регистрируются для обновления компонентов и защищаются от обновления до чего-либо более нового, чем обновление, указанное на шаге 3. См. статью Использование отчета об обновлениях компонентов Windows 10 (организация).

  6. С помощью устройств, защищенных и зарегистрированных для обновлений, вы можете безопасно изменить нагрузку *Политики Центра обновления Windows* с Configuration Manager на Intune. См. раздел Переключение рабочих нагрузок на Intune в документации по совместному управлению.

- Когда устройство возвращается в службу Центра обновления Windows, его членство проверяется по группам безопасности, назначенным параметрам политики обновления компонентов для всех обновлений функций.

- Управляемые устройства, получающие политику обновления компонентов, автоматически регистрируются с помощью автоматического исправления Windows. Служба управляет обновлениями, получаемыми устройством. Microsoft Intune использует эту службу и работает с политиками Intune для обновлений Windows для развертывания обновлений компонентов на устройствах.

  Если устройство больше не назначено ни одной политике обновления компонентов, устройство остается зарегистрированным в автозаписи. Это изменение позволяет назначить устройству другую политику и убедиться, что в это время устройство не получит обновление компонентов, которое не было предназначено.

В результате, когда политика обновления компонентов больше не применяется к устройству, на этом устройстве не предлагается обновление компонентов до тех пор, пока не произойдет одно из следующих действий:

- Устройство будет назначено новому профилю обновления компонентов.
- Устройство отключено от регистрации в Intune, что отменяет регистрацию устройства из управления обновлениями компонентов с помощью автоматического исправления.
- Чтобы удалить устройство из управления обновлениями компонентов, используйте API графа автоматического исправления Windows.

Создание и назначение политик обновления компонентов для Windows 10 и более поздней версии

1. Войдите в Центр администрирования Microsoft Intune.

2. Выберите **Устройства**>**По платформе**>**Windows**>**Windows 10 и более поздних обновлений**> на вкладке >**Обновления компонентовСоздать профиль**.

3. В разделе **Параметры развертывания**:

   А. **Имя**, **описание**. Укажите имя и описание (необязательно).

   Б. **Обязательные или необязательные обновления**. Эти параметры доступны только в том случае, если целевая версия Windows 11.

- Если выбран параметр по умолчанию **Сделать доступным для пользователей в качестве обязательного обновления** , устройство автоматически установит обновление в зависимости от параметров устройства.
- Когда администратор выбирает параметр **Сделать доступным для пользователей в качестве необязательного обновления**, выбранные обновления становятся доступными для пользователей в качестве необязательных обновлений. Параметры развертывания по-прежнему управляют, когда обновление доступно для устройства, но затем пользователь должен установить обновление, прежде чем оно будет установлено на устройстве.

То, что пользователь видит на своем устройстве Когда администратор делает обновление доступным как **необязательное** обновление, пользователь должен перейти на страницу **параметров обновления Windows** , чтобы просмотреть и выбрать установку обновления. Рекомендуется сообщить конечным пользователям через каналы коммуникации о том, что им доступно необязательное обновление. Когда пользователь переходит на страницу **параметров обновления Windows** , он может увидеть и выбрать установку обновления, когда он захочет принять обновление. Чтобы установить обновление, пользователи должны нажать кнопку **Скачать** . В противном случае он не будет установлен, пока администратор не сделает его **обязательным** . Это тот же необязательный интерфейс обновления, с которым пользователи знакомы на своих персональных компьютерах.

Когда администратор переключается с **необязательный** на **обязательный**, наблюдается следующее поведение:

- Обновления не переустанавливать для пользователей, которые решили установить обновление, когда оно было **необязательным**.
- Если устройство не запустило обновление, при следующей проверке наличия обновлений обновление обрабатывается и автоматически устанавливается как **обязательное** обновление.

Когда администратор переключается с **обязательный** на **необязательный**, наблюдается следующее поведение:

- Устройства, которые уже установили обновление, не затрагиваются.
- Устройства, ожидающие перезагрузки, скорее всего, продолжат устанавливать обновление как **обязательное** .
- Переключение влияет только на устройства, которые еще не запустили обновление или были достаточно ранними в процессе обновления, чтобы их можно было изменить на **необязательное** обновление.

c. **Обновление компонентов для развертывания**. Выберите конкретную версию Windows с набором компонентов, который вы хотите развернуть на своих устройствах. Для выбора доступны только поддерживаемые версии Windows.

d. **Параметры развертывания**. Настройте **параметры развертывания**, чтобы управлять тем, когда Windows Обновления делает обновление доступным для устройств, получающих эту политику. Дополнительные сведения об использовании этих параметров см. в статье Параметры развертывания для Windows Обновления, а затем нажмите кнопку **Далее**.

4. На вкладке **Назначения** щелкните **+ Выберите группы для включения** и назначьте развертывание обновления функций одному или нескольким устройствам или группам устройств. Нажмите кнопку **Далее**, чтобы продолжить.

5. В окне **Проверка и создание** проверьте параметры. Когда все будет готово для сохранения политики обновлений компонентов, выберите **Создать**.

Обновление устройств до Windows 11

Вы можете использовать политику для *обновления компонентов для Windows 10 и более поздних версий* для обновления устройств с Windows 10 до Windows 11.

При использовании политики обновления компонентов для развертывания Windows 11 вы можете нацелить политику на устройства с Windows 10, которые соответствуют минимальным требованиям для перехода на Windows 11. Устройства, которые не соответствуют требованиям для Windows 11, не установят обновление и останутся на текущей версии Windows 10.

Другой вариант — установить флажок **Если устройство не поддерживает работу Windows 11, установите последнее обновление компонентов Windows 10**, а устройства, которые не соответствуют требованиям для Windows 11, получат последнюю Windows 10 обновление компонентов.

Однако если Windows 10 устройство, которое не может работать Windows 11, предназначено для обновления Windows 11, будущие обновления Windows 10 не будут предлагаться на этом устройстве автоматически. В этом случае удалите неподходящее устройство из политики Windows 11 и назначьте устройство политике обновления компонентов Windows 10. См. раздел Поведение обновления, когда устройство является целью нескольких политик.

Подготовка к обновлению до Windows 11

Первым шагом в подготовке к обновлению до Windows 11 является обеспечение соответствия устройств минимальным требованиям к системе для Windows 11.

Вы можете использовать аналитику конечных точек , чтобы определить, какие из ваших устройств соответствуют требованиям к оборудованию. Если некоторые из ваших устройств не соответствуют всем требованиям, вы можете увидеть, какие из них не выполнены. Чтобы использовать аналитику конечных точек, устройства должны управляться Intune, совместно управлять или иметь клиент Configuration Manager с включенным подключением клиента.

Если вы уже используете аналитику конечных точек, перейдите к отчету Работа из любого места и выберите категорию оценка Windows в середине, чтобы открыть всплывающее окно со сводными сведениями о готовности Windows 11. Для получения более подробной информации перейдите на вкладку Windows в верхней части отчета. На вкладке Windows отображаются сведения о готовности устройства к работе.

Лицензирование для версий Windows 11

Windows 11 включает новое лицензионный соглашение, которое можно просмотреть в https://www.microsoft.com/useterms/ . Данное лицензионное соглашение автоматически принимается организацией, которая отправляет политику для развертывания Windows 11.

При настройке политики в Центре администрирования Microsoft Intune для развертывания любой Windows 11 версии Центр администрирования Microsoft Intune отображает уведомление о том, что отправляя политику, вы принимаете условия лицензионного соглашения Windows 11 от имени устройств и пользователей устройств. После отправки политики обновления компонентов конечные пользователи не увидят или не должны будут принимать лицензионное соглашение, что делает процесс обновления более простым.

Это напоминание о лицензии отображается при каждом выборе сборки Windows 11, даже если все ваши устройства с Windows уже работают под управлением Windows 11. Этот запрос предоставляется, так как Intune не отслеживает, какие устройства будут получать политику, и его возможные новые устройства, которые выполняют Windows 10 могут позже зарегистрироваться и быть целевыми для политики.

Дополнительные сведения, включая общие сведения о лицензировании, см. в документации Windows 11.

Создание политики для Windows 11

Чтобы развернуть Windows 11, вы создадите и развернете политику обновлений компонентов так же, как это можно было сделать ранее для Windows 10 устройства. Это тот же процесс, хотя вместо выбора версии Windows 10 вы выберете версию Windows 11 из раскрывающегося списка *Обновление компонентов для развертывания*. В этом списке отображаются поддерживаемые обновления версий Windows 10 и Windows 11.

Кроме того, администратор может развернуть последнее обновление Windows 10 на устройствах, которые не имеют права на Windows 11. Чтобы включить эту функцию, администратор должен установить флажок **Если устройство не поддерживает работу Windows 11, установите последнее обновление компонентов Windows 10** в политике развертывания. Эта возможность доступна только в том случае, если вы выбрали версию Windows 11 из *раскрывающегося списка Обновление компонентов для развертывания* и если клиент соответствует требованиям лицензирования, определенным в начале этого документа.

С помощью этой возможности вам не нужно создавать две разные политики развертывания или два разных обновления компонентов. С помощью одной политики вы можете получить Windows 10 устройств, которые не могут перейти в Windows 11 для обновления до последней версии Windows 10, и все устройства, которые могут перейти на Windows 11 для обновления до выбранной Windows 11 версии.

Невозможно установить флажок для существующей политики, так как изменение значения флажка завершает текущее развертывание и запускает два новых развертывания. Чтобы изменить параметры развертывания, удалите текущую политику обновления компонентов и создайте новую политику с установленным флажком.

- Развертывание более старой версии Windows на устройстве не приведет к понижению версии устройства. Устройства устанавливают обновление только в том случае, если оно более новое, чем текущая версия на устройстве.
- Развертывание обновления Windows 11 на устройстве с Windows 10, которое поддерживает Windows 11, обновляет это устройство.

Поведение обновления, когда несколько политик нацелены на устройство

Учитывайте следующие моменты, когда политики обновления компонентов нацелены на устройство с несколькими политиками обновления или на устройство Windows 10 с обновлением для Windows 11.

- Каждая политика обновления компонентов Windows поддерживает одно обновление. Если устройство является целью нескольких политик, для него могут предназначаться несколько версий обновления.

- Служба Центра обновления Windows может предложить устройству только одно обновление компонентов за раз и всегда предлагает последнюю версию обновления, предназначенную для устройства.
- Так как обновления Windows 11 считаются более поздними версиями, чем Windows 10, служба всегда предлагает обновление Windows 11 для устройства, которое является целью для обновлений Windows 10 и Windows 11. Причиной этого является то, что развертывание обновления Windows 11 на устройстве с Windows 10 является поддерживаемым путем обновления.
- Если **устройство не может работать Windows 11, установите последнее обновление компонентов Windows 10** при использовании нескольких политик, чтобы избежать проблем, упомянутых в этом разделе, и настроить службу, чтобы определить, когда Windows 11 не подходит для устройства, а вместо этого предлагает последнее обновление компонентов Windows 10.

> ⓘ **Примечание**
>
> Если вы создаете две политики с одним и тем же устройством или с, где для одной задано значение **Обязательно** , а для другой — **значение Необязательный** , а обе политики предназначены для одной и той же версии обновления компонентов, обновление будет предложено как **Обязательное**.

Управление политикой обновления компонентов для Windows 10 и более поздних версий

В Центре администрирования перейдите на вкладку **Устройства**>**по платформе**>**Windows**>**Управление обновлениями**>**Windows 10 и более поздними обновлениями**>**компонентов**, чтобы просмотреть профили.

Для каждого профиля отображаются следующие сведения:

- **Версия обновления компонентов** — версия обновления компонентов в профиле.
- **Назначено** — отображается, если профиль назначен одной или нескольким группам.
- **Поддержка** — состояние обновления компонентов:
  - **Поддерживается** — версия обновления компонентов поддерживается и может быть развернута на устройствах.

- **Завершение поддержки** — версия обновления компонентов перестанет поддерживаться через два месяца.
- **Не поддерживается** — срок действия поддержки обновления компонентов истек; обновление больше не развертывается на устройствах.

- **Дата окончания поддержки** — дата окончания поддержки для версии обновления компонентов.

> ⓘ **Примечание**
>
> Указанная дата — для выпусков Windows Enterprise и Education. Сведения о датах поддержки для других выпусков, поддерживаемых автопаттой Windows, см. на сайте жизненного цикла продуктов Майкрософт.

Если выбрать профиль в списке, откроется панель **Обзор** для профилей, где можно выполнить следующие действия:

- Выбрать **Удалить**, чтобы удалить политику из Intune и с устройств.
- Выбрать **Свойства**, чтобы изменить развертывание. На панели*Свойства* выберите **Изменить**, чтобы открыть *Параметры развертывания или назначения*, в которых можно изменить развертывание.

> ⓘ **Примечание**
>
> Значение Состояние обновления конечного пользователя Время последнего сканирования будет возвращать значение "Еще не проверено" до тех пор, пока начальный пользователь не войдет в систему и не будет инициирована проверка оркестратора сеансов обновления (USO). Дополнительные сведения об архитектуре Единой платформы обновлений (UUP) и связанных компонентах см. в статье Начало работы с клиентский компонент Центра обновления Windows.

Проверка и создание отчетов

Существует несколько вариантов получения подробных отчетов об обновлениях Windows 10/11 с помощью Intune. Отчеты об обновлении Windows показывают сведения о ваших устройствах с Windows 10 и Windows 11 бок о бок в одном отчете.

Дополнительные сведения см. в разделе Отчеты о соответствии Intune.

Дальнейшие действия

- Использование кругов обновления Windows в Intune
- Используйте отчеты о совместимости обновлений Windows
- Использование отчетов Центра обновления Windows для обновлений Windows 10/11
- Также см . статью Автозапавание Windows в содержимом развертывания Windows для альтернативного решения.

Настройка клиентский компонент Центра обновления Windows для облачных компьютеров Windows 365 Frontline

Статья • 24.02.2025

Windows 365 Frontline облачные компьютеры полагаются на часы активности клиентский компонент Центра обновления Windows политики, чтобы убедиться, что облачные компьютеры не перезагружаются для клиентский компонент Центра обновления Windows во время активного использования. В следующей таблице перечислены рекомендуемые конфигурации обновлений для облачных компьютеров Frontline. Обязательно используйте функцию Filter или создайте динамическую группу устройств , чтобы использовать политики только для облачных компьютеров frontline.

Развернуть таблицу

параметр политики клиентский компонент Центра обновления Windows	Windows 365 Frontline рекомендации
Обновления продуктов Майкрософт	Разрешить
Драйверы Windows	Разрешить
Период отсрочки обновления качества	9
Период отсрочки обновления компонентов	0
Обновление Windows 10 до последней версии Windows 11	Нет
Установка периода удаления обновлений компонентов	30 дней
Канал обслуживания	Общая доступность
Режим автоматического обновления	Автоматическая установка и перезапуск во время обслуживания*
Проверка перезапуска	Разрешить
Параметр приостановки обновлений	Отключение
Параметр проверка для Windows Обновления	По умолчанию

параметр политики клиентский компонент Центра обновления Windows	Windows 365 Frontline рекомендации
Изменение уровня уведомления об обновлениях	Отключение всех уведомлений, включая предупреждения о перезапуске
Крайний срок обновления компонентов	По умолчанию (не настроено)
Крайний срок обновления качества	По умолчанию (не настроено)
Льготный период	2
Автоматический перезапуск до крайнего срока	Нет
Начало активных часов	Определяется ИТ-администратором
Окончание активных часов	Определяется ИТ-администратором
Максимальный диапазон активных часов	Определяется ИТ-администратором

Эти параметры важны для того, чтобы пользователи не нарушались клиентский компонент Центра обновления Windows в рабочее время.

Автоматическая синхронизация обновлений для компьютеров Frontline Cloud в выделенном режиме, которые не были подключены в течение семи дней

Служба Windows 365 автоматически работает на Windows 365 Frontline облачном компьютере в выделенном режиме, если она не использовалась и не питалась в течение предыдущих семи дней. Когда облачный компьютер Windows 365 Frontline включен, служба Windows 365:

- Синхронизирует облачный компьютер со службой клиентский компонент Центра обновления Windows.
- Выполняет процесс клиентский компонент Центра обновления Windows с учетом конфигураций политики клиентский компонент Центра обновления Windows, заданных в Intune.
- В течение двух часов облачный компьютер будет включен, чтобы убедиться, что установка клиентский компонент Центра обновления Windows может быть завершена.
- Проверяет все ожидающие перезагрузки. Если они есть, облачный компьютер автоматически перезагружается, чтобы завершить любое клиентский

компонент Центра обновления Windows перед отключением облачного компьютера.

Этот процесс позволяет пользователю легко приступить к использованию облачного компьютера при следующем входе.

Дальнейшие действия

Дополнительные сведения о windows Обновления.

клиентский компонент Центра обновления Windows политики, которые следует задать и почему (блог).

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Требования к оборудованию конечного пользователя для доступа к облачному компьютеру

Статья • 31.01.2025

Чтобы получить доступ к облачному компьютеру, оборудование конечного пользователя должно соответствовать определенным требованиям. Эти требования зависят от того, какой клиент Удаленного рабочего стола (Майкрософт) установлен у конечного пользователя.

Windows App

Дополнительные сведения о требованиях к выполнению и использованию Windows App см. в статье Начало работы с Windows App.

Клиент Удаленного рабочего стола (Майкрософт) для Windows

Загружаемые файлы доступны для следующих версий:

- 64-разрядная Windows
- 32-разрядная Windows

Требования к оборудованию:

- **Операционные системы**: Windows 10/11, Windows 8.1, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2
- **ЦП**: 1 виртуальный ЦП с тактовой частотой 1 ГГц или более мощный
- **ОЗУ**: 1024 МБ
- **Жесткий диск**: 100 МБ или более
- **Версия .NET Framework**: 4.6.1 или более поздняя
- **Видео**: DirectX 9 или более поздней версии с драйвером WDDM 1.0

Если вы будете использовать Microsoft Teams на Облачных компьютерах, то к устройствам Windows предъявляются более строгие требования:

- **ЦП**: минимум 2 виртуальных ЦП с тактовой частотой не менее 1,6 ГГц или более мощный. Для более высокого разрешения видео или экрана и частоты

кадров рекомендуется использовать четырехъядерный процессор или более мощный.
- **ОЗУ**: 4096 МБ
- **Жесткий диск**: 3 ГБ или более
- **Версия .NET Framework**: 4.6.1 или более поздняя
- **Видео**: DirectX 9 или более поздней версии с драйвером WDDM 1.0. Для фоновых видеоэффектов требуется Windows 10/11 или процессор с набором инструкций AVX2. Кроме того, производительность выгрузки аудио и видео из Teams на облачный компьютер будет выше при использовании выделенного графического процессора (GPU) на устройстве.

Клиент Удаленного рабочего стола (Майкрософт) для Windows из Microsoft Store

Скачайте из Microsoft Store.

Требования к оборудованию:

- **Операционные системы**: Windows 10 1703 или более поздней версии.
- **ЦП**: процессор с тактовой частотой 1 ГГц и выше
- **ОЗУ**: 1024 МБ
- **Жесткий диск**: 100 МБ или более
- **Видео**: DirectX 9 или более поздней версии с драйвером WDDM 1.0. Производительность выгрузки аудио и видео из Teams на Облачный компьютер будет выше при использовании выделенного графического процессора (GPU) на физическом устройстве.

macOS, iOS/iPadOS и Android

Вы можете установить клиент и найти требования для других платформ здесь:

- macOS
- iOS/iPadOS
- Android

Linux

Вы можете получить доступ к облачным компьютерам Windows 365 с устройств ОС Linux с помощью:

- Веб-клиента, доступного на сайте windows365.microsoft.com.
- Сторонних клиентов для подключения к Виртуальному рабочему столу Azure, в том числе:
  - Dell
  - HP
  - IGEL

  Сторонними клиентскими решениями Linux нельзя управлять с помощью Microsoft Intune. Партнер предоставляет отдельный инструмент управления для устройств Linux.

Дальнейшие действия

Сведения о различных требованиях к сети для каждого сценария см. в разделе Требования к сети.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Доступ к облачному ПК

02.10.2025

Пользователи могут получить доступ к своим облачным компьютерам в соответствии со следующей матрицей:

Развернуть таблицу

Выпуск Windows 365	Windows App	веб-клиент windows.cloud.microsoft	Удаленный рабочий стол (Майкрософт)	LG Web OS
Windows 365 для бизнеса	X	X	X*	X
Windows 365 Корпоративная	X	X	X*	X
Windows 365 Frontline	X	X		
правительство Windows 365		X		

*\ поддержка Удаленный рабочий стол (Майкрософт) завершится в марте 2026 г. Дополнительные сведения см. в разделе Удаленный рабочий стол.

Сведения о требованиях к оборудованию см. в статье Требования к оборудованию конечных пользователей.

Windows App

Windows App — это рекомендуемое приложение для подключения к Windows 365 облачным компьютерам, которое можно использовать на любом устройстве. Дополнительные сведения о требованиях к запуску и использованию Windows App см. в статье Что такое Windows App?

Веб-сайт Windows 365

Windows 365 пользователи могут перейти к windows.cloud.microsoft, чтобы получить доступ к своим облачным компьютерам.

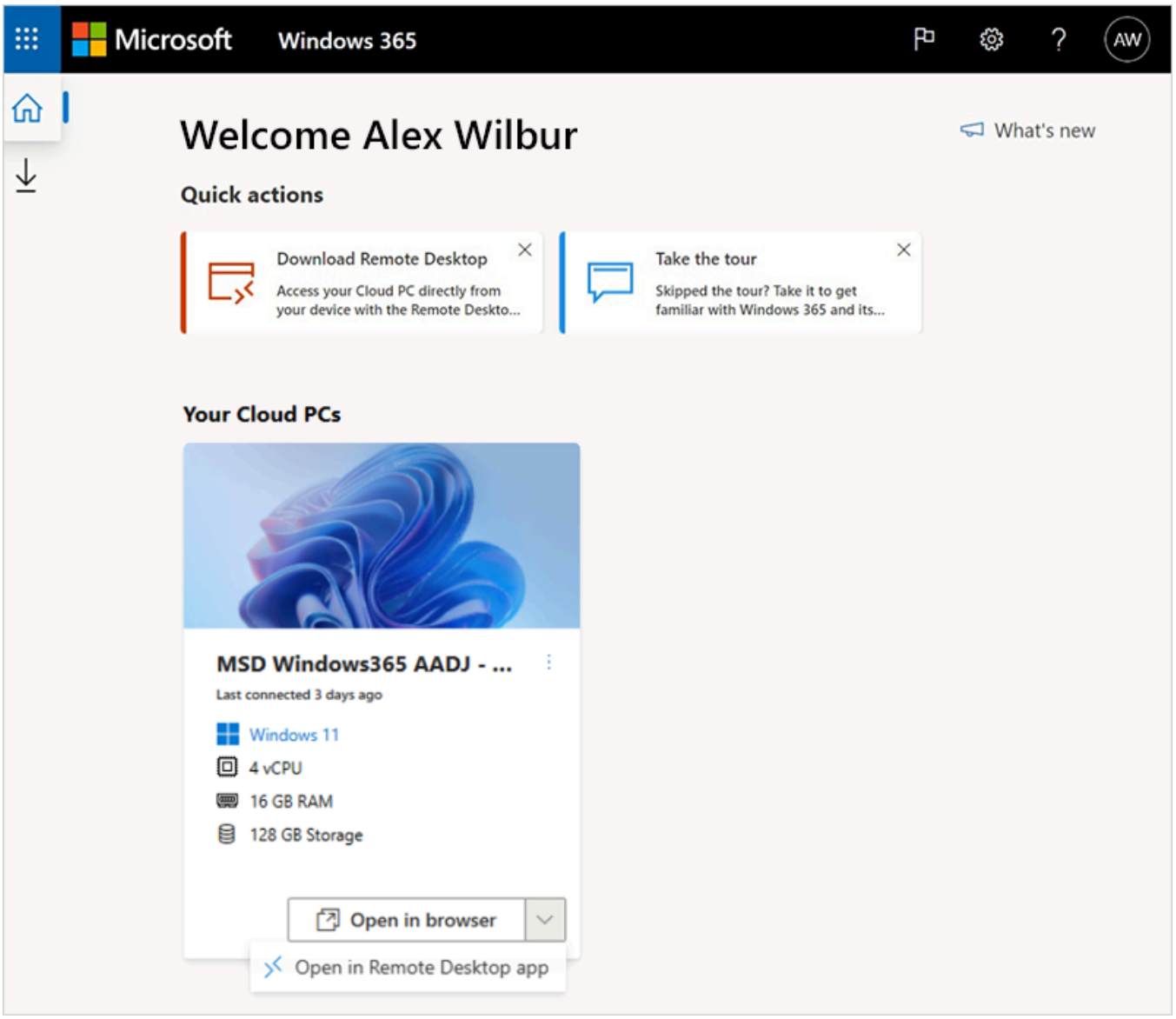
Требования к программному обеспечению

Чтобы получить доступ к облачным компьютерам с этого веб-сайта, устройство конечного пользователя должно соответствовать следующим требованиям:

- Поддерживаемые операционные системы: Windows, macOS, ChromeOS, Linux
- Современный браузер, например Microsoft Edge, Google Chrome, Safari, Mozilla Firefox (версии 55.0 и более поздних версий) или LG webOS 23.

Домашняя страница

На домашней странице Windows 365 в разделе **Ваши облачные компьютеры** пользователи увидят облачные компьютеры, к которым у них есть доступ.



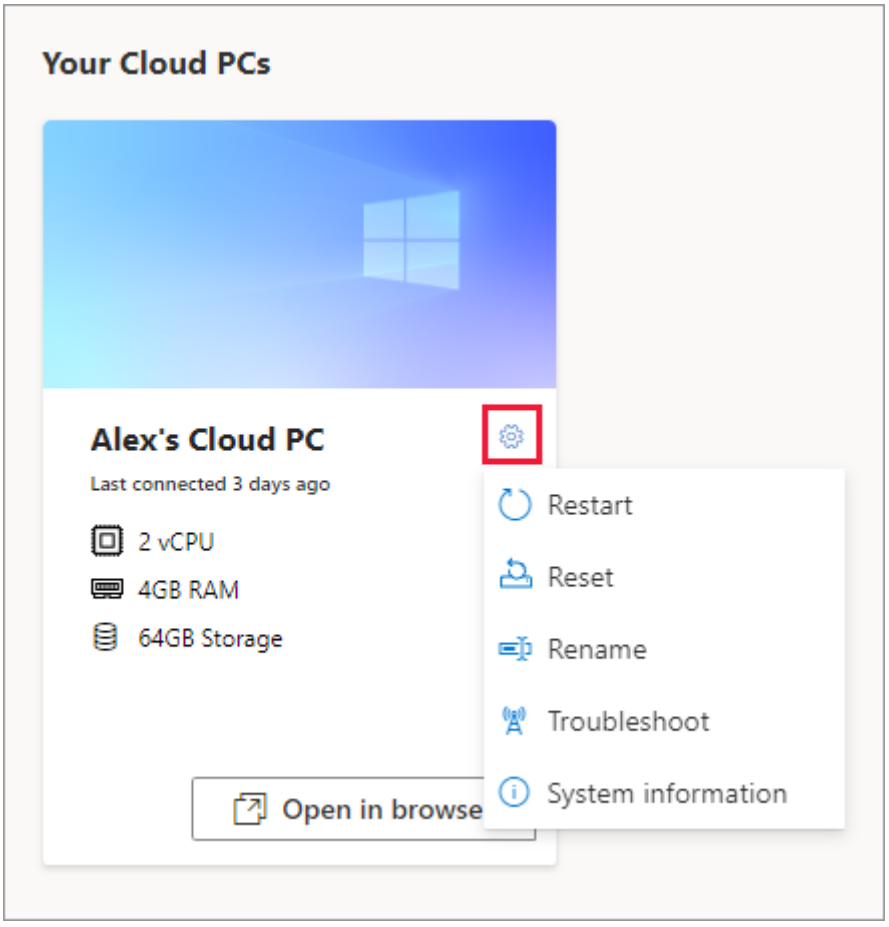
На этой странице у пользователей есть два варианта подключения к облачному компьютеру:

- Выберите **Открыть в браузере** , чтобы открыть облачный компьютер в веб-клиенте (недоступно для мобильных устройств).

- Выберите **Открыть в приложении удаленного рабочего стола,** чтобы открыть облачный компьютер в удаленном рабочем столе. Дополнительные сведения см. в разделе Удаленный рабочий стол.

Действия пользователя

В windows.cloud.microsoft пользователи могут выполнять действия на своих облачных компьютерах, щелкнув значок шестеренки на облачном компьютере карта.



- **Переименовать**: изменяет имя Облачного компьютера, отображаемого пользователю на веб-сайте. Это действие не влияет на имя в Microsoft Intune, Microsoft Entra идентификатор, на устройстве или в приложениях удаленного рабочего стола.

- **Сброс**.

  - Переустанавливает Windows (с возможностью выбора между Windows 11 и Windows 10).

  - Удаление личных файлов.

  - Удаление изменений, внесенных в параметры.

  - Удаление приложений.

> ⓘ **Важно!**
>
> Перед сбросом настроек облачного компьютера сохраните все важные файлы в службе облачного хранения или на внешнем запоминающем устройстве. При сбросе облачного компьютера эти файлы будут удалены.

- **Перезапуск**: перезагружает Облачный компьютер. Для облачных компьютеров, созданных после 31 января 2024 г., можно также перезапустить или завершить работу с помощью сочетания клавиш CTRL+ALT+DEL.
- **Устранение неполадок**: устранение неполадок и попытка решения проблем, которые мешают пользователю подключиться к Облачному компьютеру. Доступны следующие проверки:
  - Проверка того, правильно ли установлены файлы или агенты, необходимые для подключения.
  - Проверка доступности ресурсов Azure.

Развернуть таблицу

Состояние возврата	Описание
Неполадок не обнаружено	Ни одна из проверок не обнаружила проблемы с Облачным компьютером.
Проблемы решены	Проблема обнаружена и исправлена.
Не удается подключиться к облачному компьютеру. Мы работаем над ее исправлением, повторите попытку позже.	Служба Майкрософт, необходимая для подключения, недоступна. Повторите попытку подключения позже.
Не удалось устранить проблемы с облачным компьютером. Обратитесь к администратору.	Проблема найдена, но ее не удалось исправить. Эта проблема возникает из-за текущего обновления Windows или другой проблемы. Если эта ошибка повторяется в течение продолжительного периода времени, может потребоваться сброс настроек облачного компьютера.

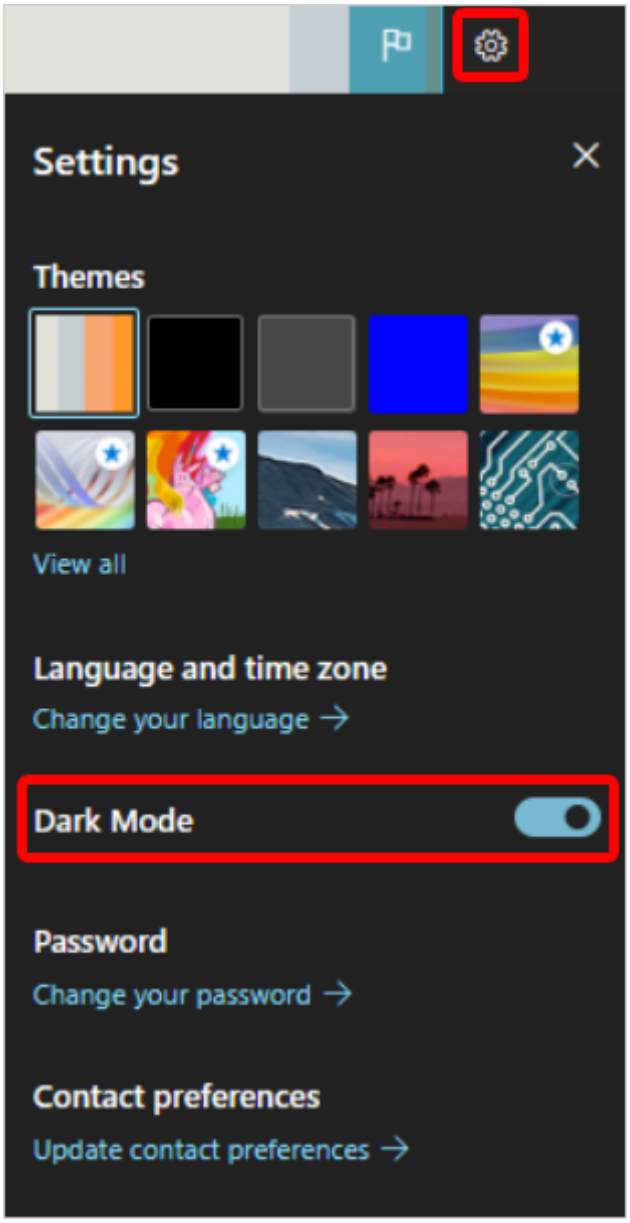
- **Сведения о системе** — отображает сведения о характеристиках облачного компьютера.

Темный режим

Чтобы переключить сайт windows.cloud.microsoft в темный режим, выполните следующие действия:

1. Перейдите на страницу windows.cloud.microsoft.

2. Щелкните значок шестеренки и выберите **Темный режим**.



В параметрах сеанса

При выборе **параметра Открыть в браузере** для облачного компьютера на веб-сайте windows.cloud.microsoft откроется окно **Параметры сеанса** , в котором можно выбрать несколько параметров перед подключением к облачному компьютеру:

1. Выберите устройства и функции на физическом устройстве, к которым может получить доступ облачный компьютер:

    - Принтер
    - Микрофон
    - Буфер обмена
    - Расположение (предварительная версия)

2. Выберите **Показать дополнительные параметры** , чтобы просмотреть следующие параметры:

    - Альтернативная раскладка клавиатуры

3. Нажмите **Подключиться**. Облачный компьютер откроется в веб-клиенте (браузере).

Изменение параметров на облачном компьютере

Чтобы изменить параметры из облачного компьютера, выполните следующие действия:

1. Щелкните значок шестеренки.
2. Выберите параметры, которые требуется изменить >**обновление**.

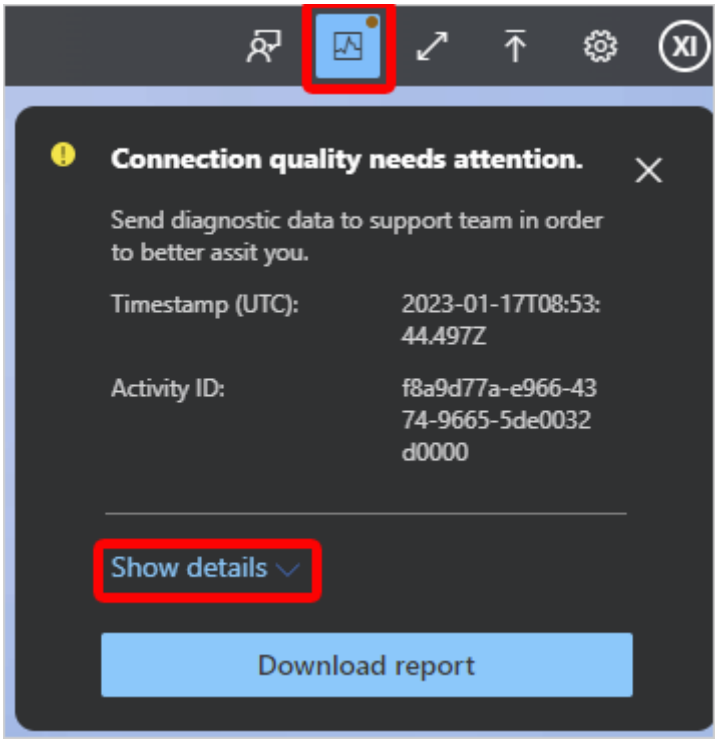
Изменения появятся при следующем перезапуске облачного компьютера.

Пользователи могут оставить отзыв об использовании облачных компьютеров с помощью значка обратной связи в правом верхнем углу.

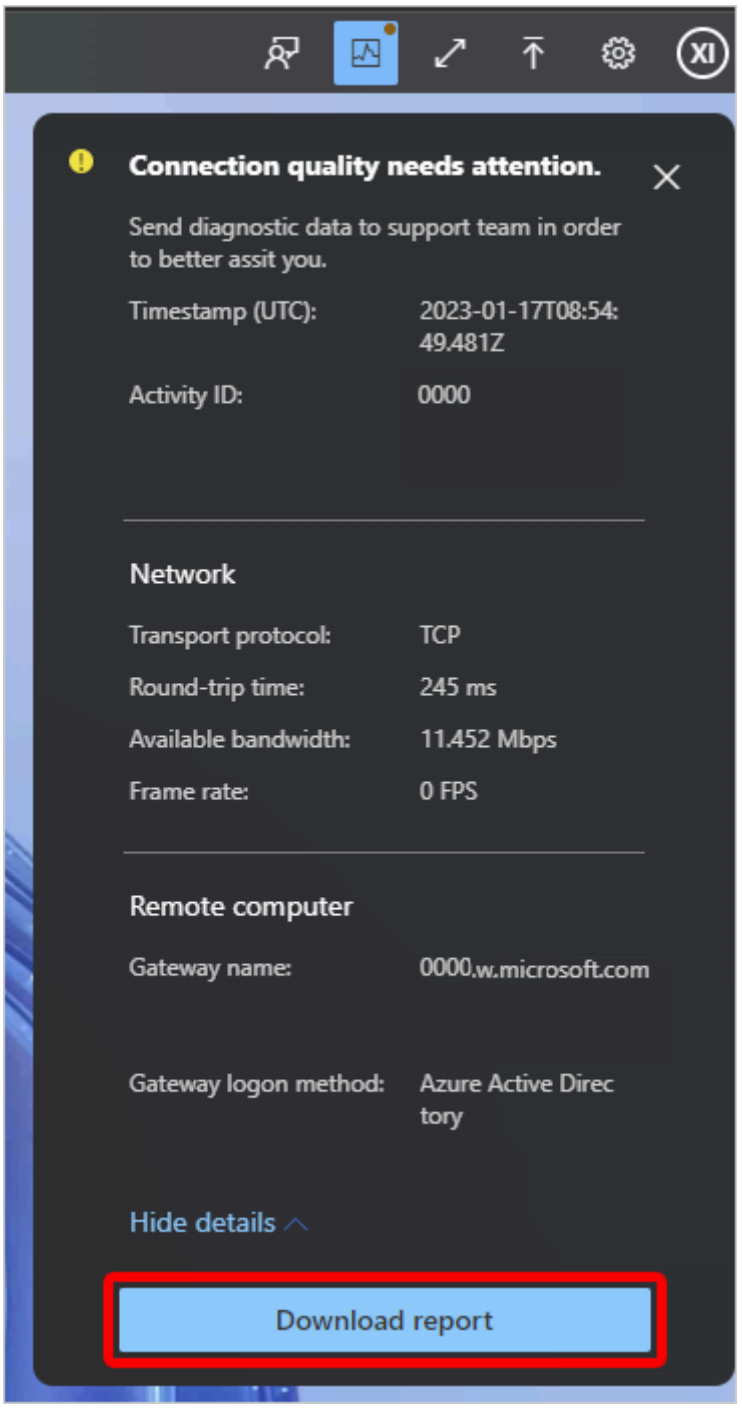
Сведения о подключении

Пользователи могут просматривать и скачивать сведения о подключении.

1. Щелкните значок >**Сведения о подключенииПоказать сведения**.



2. Чтобы скачать текстовый файл, содержащий сведения о подключении, выберите **Скачать отчет**.



Передача файлов на облачный компьютер и с него

Чтобы передать файлы с локального устройства на облачный компьютер, щелкните значок отправки, чтобы запустить проводник. Выберите файлы, чтобы перенести их в папку \Этот компьютер\Виртуальный диск Windows365\Отправки на облачном компьютере.

Чтобы перенести файлы с облачного компьютера на локальное устройство, скопируйте файлы в папку загрузок на облачном компьютере. Файлы автоматически копируются в папку \This PC\Windows365 virtual drive\Downloads на локальном устройстве.

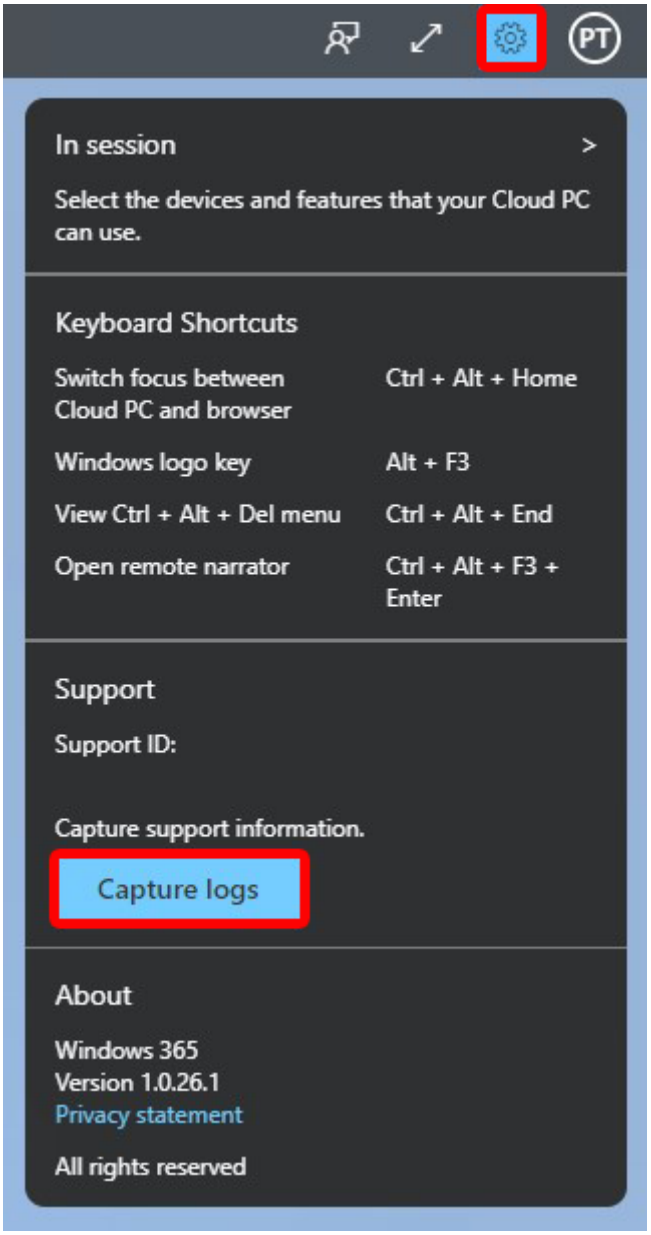
Запрещение пользователям передавать файлы на облачные компьютеры и с них

Вы можете ограничить передачу файлов пользователями с помощью перенаправления диска RDP. Дополнительные сведения см. в разделе Управление перенаправлениями устройств RDP для облачных компьютеров.

Сбор журналов пользователей

Пользователи могут собирать журналы своих сеансов работы на облачных компьютерах. Журналы собираются из браузера, и пользователь может указать место их сохранения.

Чтобы включить сбор журналов, в клиенте щелкните значок > сведений **Запись журналов**.



Аппаратное ускорение

Вы можете включить аппаратное ускорение при использовании веб-клиента для доступа к облачному компьютеру. Этот параметр уменьшает задержку в сети, улучшая взаимодействие с облачным компьютером веб-клиента. Этот параметр включен по умолчанию.

Чтобы включить или отключить аппаратное ускорение, в клиенте щелкните значок > шестеренки **Использовать аппаратное ускорение**.

Высокий точек на дюйм

Переключатель **Высокого разрешения** можно использовать для отображения веб-клиента с помощью собственного разрешения физического устройства. Высокий точек на дюйм — это хороший вариант для включения, если вы используете экран с высоким разрешением, например 4K или UHD-мониторы.

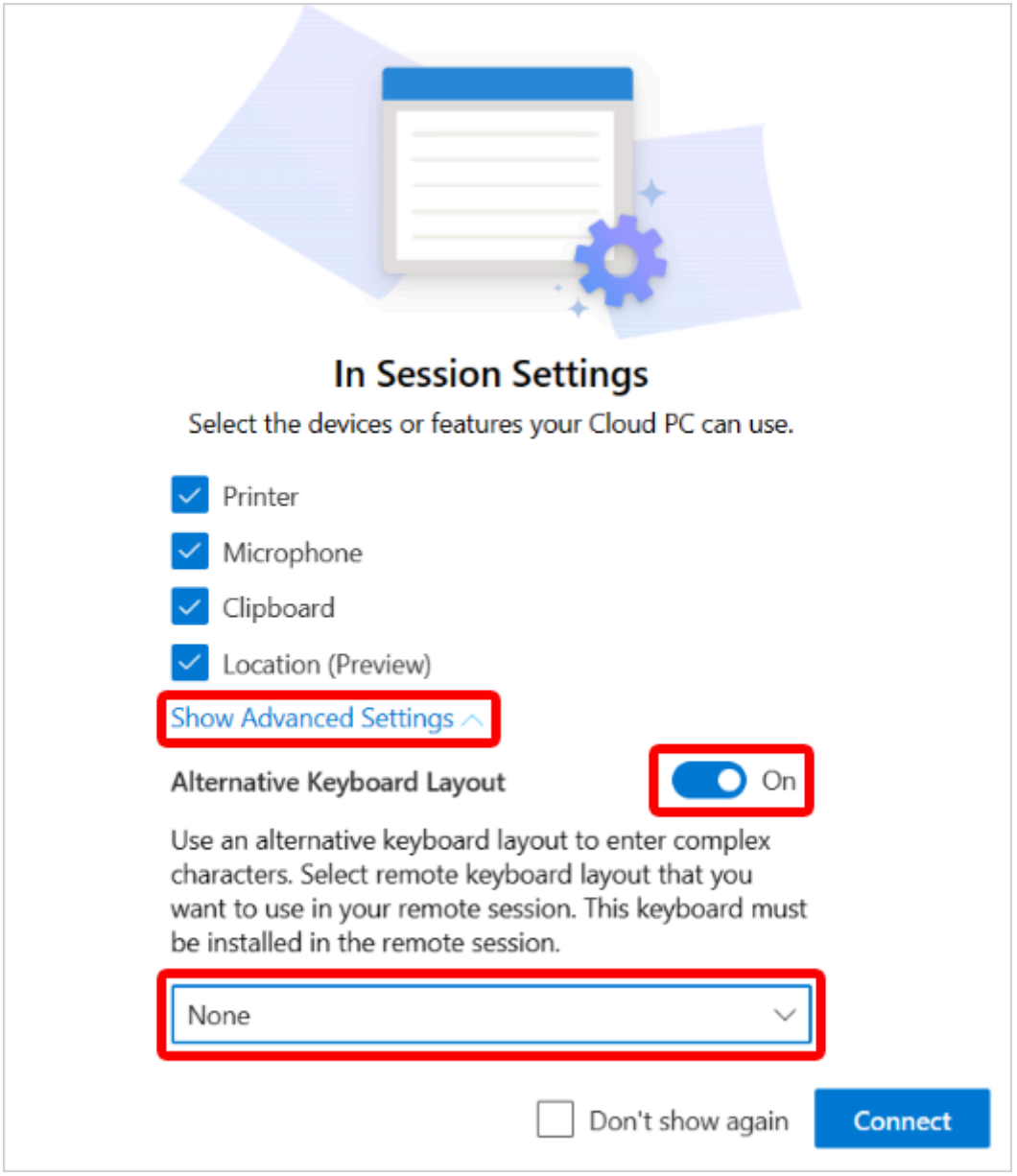
Параметр High Dots per Inch (DPI) настраивает разрешение экрана в соответствии с физическим размером экрана и расстоянием между пользователем и экраном.

Чтобы выбрать этот параметр, щелкните значок шестеренки >**Высокий точек на дюйм**.

Альтернативная раскладка клавиатуры

Используйте этот параметр, если вы используете нестандартную клавиатуру, содержащую специальные символы (например, китайский (традиционное письмо) или испанский (Мексика)).

1. В окне Windows 365 веб-клиент **в параметрах сеанса** выберите **Показать дополнительные параметрыАльтернативная раскладка**> клавиатуры >**Вкл**.



2. В раскрывающемся списке выберите язык, соответствующий клавиатуре.

По умолчанию **альтернативная раскладка клавиатуры** отключена. При использовании стандартной клавиатуры, для которых не требуются специальные макеты, пользователь может отменить выбор этого параметра. Отмена выбора параметра в середине сеанса требует повторного подключения.

Расположение (предварительная версия)

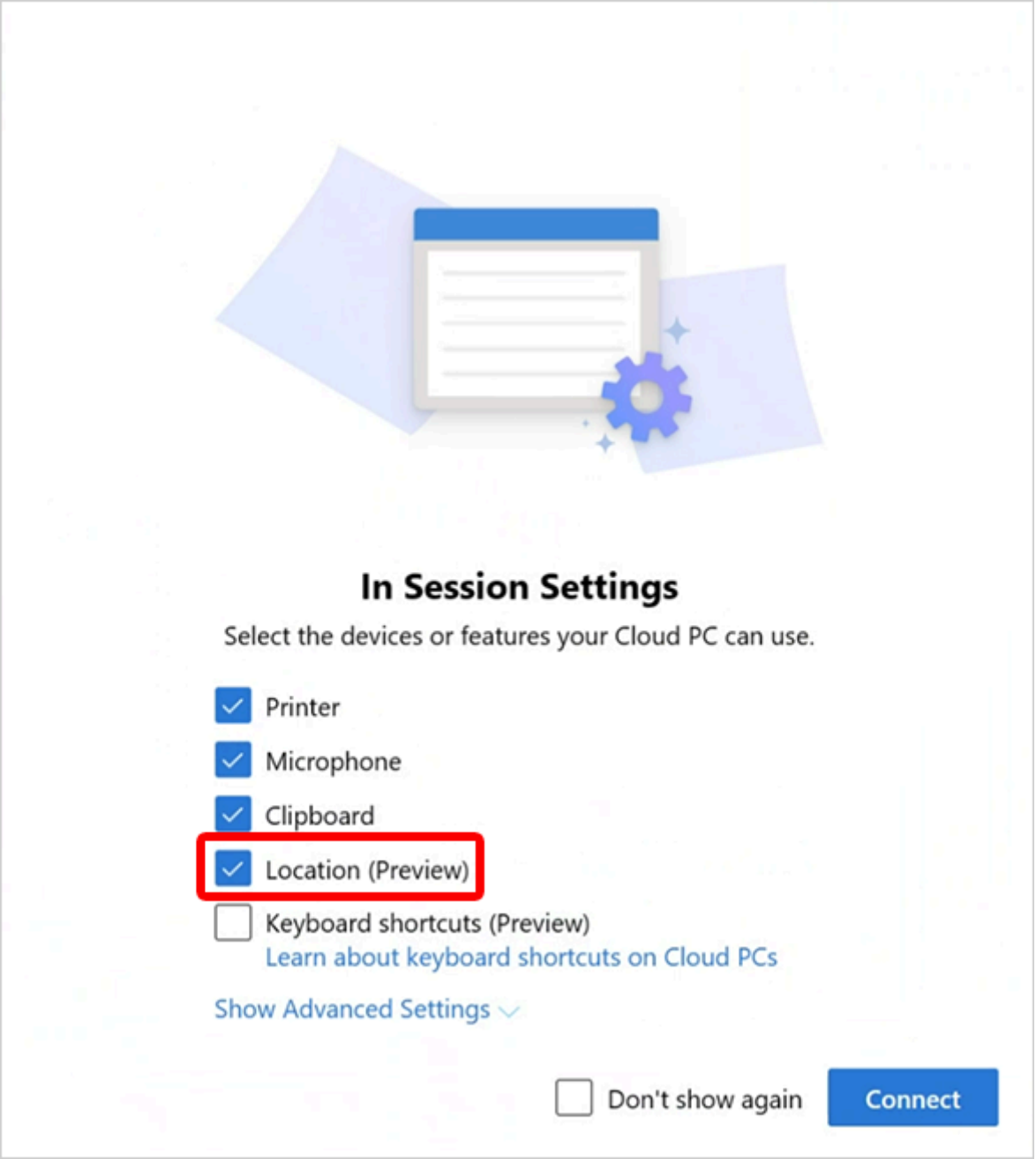
Перенаправление расположения позволяет облачным компьютерам безопасно получать доступ к приблизительному расположению без проблем конфиденциальности. Включив службу определения местоположения, вы позволяете облачному компьютеру использовать расположение физического устройства для большинства приложений (мини-приложение "Погода" в настоящее время не поддерживается).

Дополнительные сведения о службах определения местоположения см. в разделе Служба определения местоположения Windows и конфиденциальность.

Для перенаправления расположения требуются права локального администратора на облачном компьютере. Дополнительные сведения см. в разделе Назначение пользователя в качестве локального администратора.

Чтобы включить перенаправление расположения, выполните следующие действия.

1. На физическом устройстве перейдите в **раздел Параметры**>**Конфиденциальность & Расположение безопасности**>.
2. Для **службы определения местоположения** установите переключатель в **положение Вкл**.
3. Для **параметра Разрешить приложениям доступ к вашему расположению** установите переключатель **в положение Вкл**.
4. Для каждого приложения, в которое вы хотите, чтобы облачный компьютер отображал сведения о расположении, установите переключатель в **положение Вкл**.
5. Перейдите на страницу windows.cloud.microsoft.
6. В разделе **Облачные компьютеры** выберите **Открыть в браузере для облачного** компьютера.
7. **В разделе Параметры сеанса** выберите **Расположение (предварительная версия)**>**Подключить**.



8. В поле подтверждения **windows.cloud.microsoft требуется узнать свое расположение** , выберите **Разрешить**.

Параметры организации могут переопределять параметры расположения устройства. Например, ваша организация может отключить перенаправление расположения для всех облачных компьютеров, которыми они управляют.

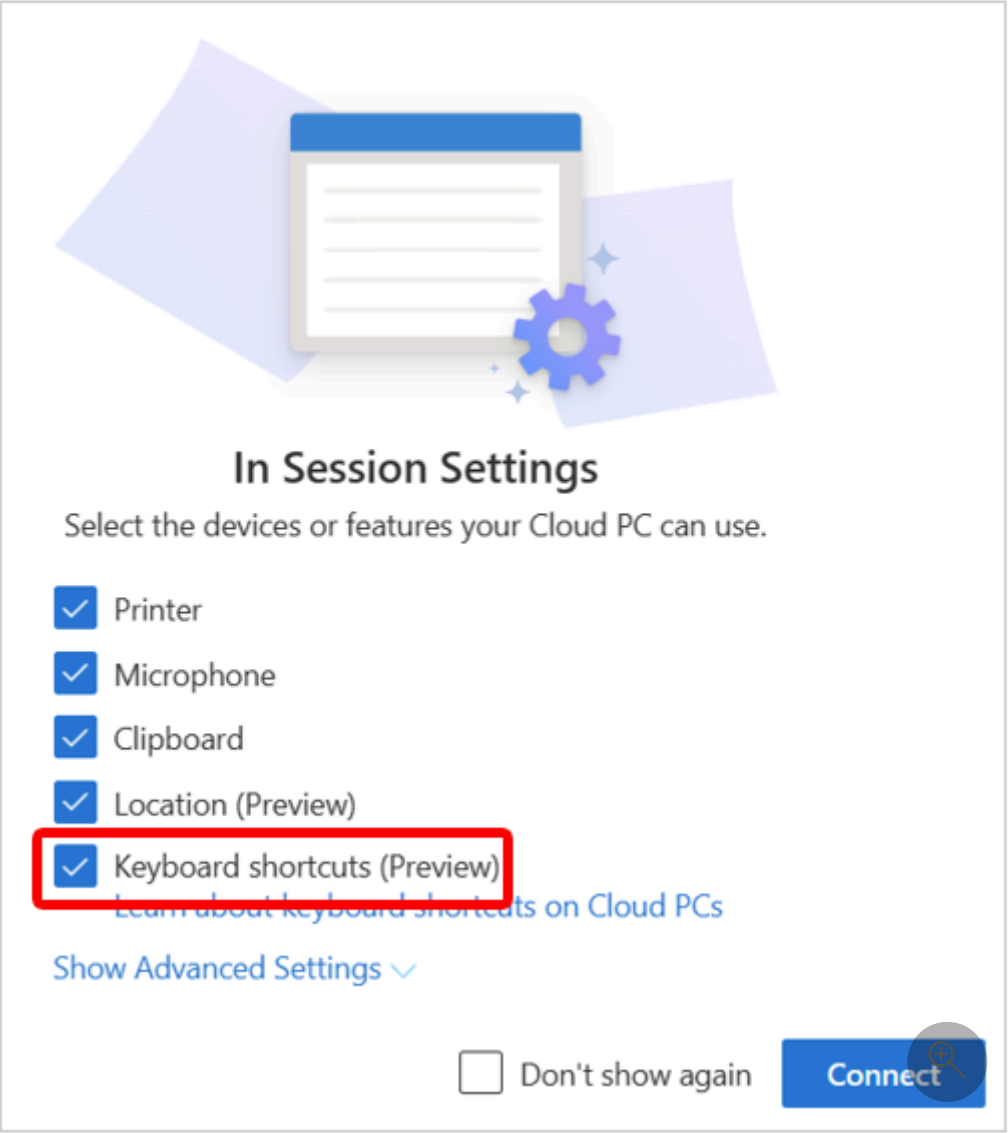
Сочетания клавиш (предварительная версия)

При доступе к облачному компьютеру с помощью веб-клиента можно настроить на облачных компьютерах специальные сочетания клавиш (сочетание клавиш с клавишами Windows, ESC и т. д.). Полный список сочетаний клавиш см. в разделе Сочетания клавиш в Windows .

Сочетания клавиш доступны в общедоступной предварительной версии.

Чтобы включить сочетания клавиш для облачного компьютера, выполните приведенные ниже действия.

1. Перейдите на страницу windows.cloud.microsoft.
2. В разделе **Облачные компьютеры** выберите **Открыть в браузере для облачного** компьютера.
3. **В разделе Параметры сеанса** выберите **Сочетания клавиш (предварительная версия)**>**Подключиться**.



Если **сочетания клавиш** включено, веб-клиент открывается в полноэкранном режиме. Сочетания клавиш работают только в полноэкранном режиме. Полноэкранное использование F11 не поддерживается. На панели инструментов необходимо использовать полноэкранный режим.

Чтобы отключить сочетания клавиш, в веб-клиенте выберите **Параметры**> снимите флажок **Сочетания клавиш**>**Обновление**.

LG webOS 23

Доступ к веб-клиенту Windows 365 можно получить через ТЕЛЕВИЗОР LG с последней версией webOS 23.

Чтобы запустить веб-клиент на телевизоре LG (с LG webOS 23), перейдите в **раздел Home Office**>**Windows 365**.

Следующие Windows 365 функции недоступны на телевизоре LG:

- Передача файлов
- Буфер обмена
- Перенаправление расположения
- Собранные журналы ошибок
- Аппаратное ускорение
- Сочетания клавиш

Удаленный рабочий стол

Приложение Удаленный рабочий стол (Майкрософт) является альтернативой Windows App, которая позволяет пользователям получать доступ к удаленному компьютеру, включая облачный компьютер, и управлять ими.

Список клиентов по операционной системе см. в разделе Клиенты удаленного рабочего стола. Сравнение функций клиентов см. в разделе Сравнение клиентов: функции.

> ⓘ **Важно!**
>
> Начиная с 27 марта 2026 г. клиент удаленного рабочего стола для Windows (MSI) больше не будет поддерживаться. Пользователи должны начать миграцию на Windows App, чтобы убедиться, что они имеют постоянный доступ к виртуальному рабочему столу Azure и Windows 365 ресурсам после этой даты. Дополнительные сведения об известных ограничениях Windows App см. в статье **Известные проблемы и ограничения Windows App**. Этот список обновляется, так как функции клиента удаленного рабочего стола поддерживаются в Windows App. С 27 мая 2025 г. приложение удаленного рабочего стола для Windows из Microsoft Store больше не будет поддерживаться и не будет доступно для скачивания и установки. Пользователи должны перейти на Windows App, чтобы обеспечить им постоянный доступ к Windows 365, Виртуальному рабочему столу Azure и Microsoft Dev Box. Дополнительные сведения см. в статье **Начало работы с Windows App для подключения к устройствам и приложениям**.

Дальнейшие действия

Сведения о различных требованиях к сети для каждого сценария см. в разделе Требования к сети.

Устранение неполадок

Статья • 31.01.2025

В этой статье приводятся рекомендации по устранению неполадок с Windows 365.

Обращение в справочную службу или службу поддержки

Инструкции о том, как получить справку и отправить запрос в службу поддержки, см. в разделе Как получить поддержку в Microsoft Intune. Поддержка входит в состав подписки Windows 365.

Так как облачные компьютеры работают как большинство физических устройств, вы можете использовать имеющуюся документацию по устранению неполадок для устранения неполадок с клиентом Windows, службами Microsoft 365 и Microsoft Intune Центре администрирования.

Перенаправление звука и видео не работает

Чтобы подключения, использующие клиент удаленного рабочего стола для Windows, могли получить доступ к облачным компьютерам, при первом входе пользователя на облачный компьютер устанавливается Microsoft Teams.

После установки оптимизации для перенаправления звука и видео в локальную конечную точку Windows не работают. Чтобы активировать состояние оптимизации, пользователю необходимо закрыть Teams и выйти из системы или перезагрузить облачный компьютер.

Условный доступ

Убедитесь, что политики условного доступа применяются как к выделенному облачному приложению Windows 365, так и к облачному приложению Виртуального рабочего стола Azure. Эти политики можно применить в пользовательском интерфейсе условного доступа центра администрирования Microsoft Intune или Microsoft Entra ID.

Любая политика условного доступа, которую вы применяете, повлияет на:

- Доступ к веб-порталу конечных пользователей

- Подключение к облачному компьютеру из приложений удаленного рабочего стола.

Дополнительные сведения о зависимостях служб в Microsoft Entra условного доступа см. в разделе Зависимости службы условного доступа.

Применение более строгой политики к Виртуальному рабочему столу Azure, чем к облачному приложению Windows 365, приведет к Microsoft Entra ID соблюдение более строгой политики. Эта политика повлияет на возможность подключения пользователей к облачным компьютерам после получения доступа к порталу пользователей Windows 365.

Дополнительные сведения о том, как данная политика может повлиять на вашу среду, см. в разделе Устранение неполадок с помощью инструмента "Что, если" в условном доступе.

Помощь пользователям в вашей организации

Для просмотра проблем с регистрацией, действий по исправлению и сведений о пользователях можно воспользоваться страницей диагностики Intune. Подробнее см. в статье Использование портала устранения неполадок для предоставления помощи пользователям вашей компании.

App Assure — это служба для корпоративных клиентов корпорации Майкрософт, которые сталкиваются с проблемами совместимости приложений. App Assure позволяет исправлять проблемы с приложениями независимых поставщиков программного обеспечения, бизнес-приложениями и приложениями, разработанными корпорацией Майкрософт, без дополнительных затрат. Чтобы отправить обращение в случае возникновения проблем совместимости приложений, выполните приведенные выше инструкции, а также приведите краткое описание проблемы.

Сбой установки языкового пакета

Вы можете попробовать одно из следующих возможных решений:

- Если установка языкового пакета не удалась, попробуйте повторно подготовить облачный компьютер, чтобы снова установить языковой пакет.
- Проверьте, установлено ли в Intune правило сокращения направлений атаки. Если для параметра **Блокировать создание процессов из команд PSExec и**

WMI, установлено значение «Блокировать», установка языкового пакета будет заблокирована. Вы можете удалить правило и повторить подготовку или подготовку с установленным по умолчанию языком en-us. Затем позвольте пользователю изменить язык с помощью приложения «Параметры Windows» на облачном компьютере.

Сеть

Проверки сетевого подключения Azure позволяют убедиться, что оно работает. Если вы подозреваете, что неполадки могут быть вызваны проблемами с сетью, обязательно попробуйте повторно установить сетевое подключение Azure. На первом этапе устранения неполадок следует проводить повторные и согласованные проверки сетевого подключения Azure.

Помните, что проверки сетевого подключения Azure направлены на оценку правильности конфигурации инфраструктуры среды. Они не выполняют проверки для проверки дополнительных конфигураций или приложений, развернутых на облачных компьютерах после подготовки Microsoft Intune или сторонних агентов. Эти агенты или конфигурации могут вызывать другие проблемы, которые сетевое подключение Azure не может протестировать до подготовки.

Например, при развертывании VPN-клиента на всех устройствах в Microsoft Intune убедитесь, что этот клиент не выполняет следующие действия:

- не разрывает подключение к конечным точкам Виртуального рабочего стола Azure, которых требует Windows 365;
- не исключает возможности развертывания VPN-клиента на облачных компьютерах.

Наконец, рассмотрите возможность временного развертывания тестовой виртуальной машины Azure в подсети Azure, которую вы пытаетесь подготовить к работе или подключить к облачным компьютерам. Этот тестовый компьютер позволит выполнить все необходимые тесты сети, которые от нее требуются. Вы можете использовать команду PowerShell Test-NetConnection, чтобы проверить возможность подключения к конкретным портам в конкретных конечных точках или URL-адресах сети.

```
Test-NetConnection <hostname> -Port 443
```

Сетевые подключения Azure

Рекомендуемые исправления см. в статье Устранение неполадок с сетевыми подключениями Azure.

Вопросы подготовки

Рекомендуемые исправления см. в статье Устранение ошибок подготовки.

Устранение неполадок пользователями

Пользователь может устранить некоторые проблемы, которые могут препятствовать подключению к облачному компьютеру. Дополнительные сведения см. в разделе Действия конечных пользователей.

Улучшения воспроизведения видео

Вы можете повысить производительность воспроизведения видео на облачных компьютерах с помощью перенаправления мультимедиа (MMR).

Для облачных компьютеров MMR поддерживается на следующих платформах: Windows, macOS, ChromeOS, Linux.

Дополнительные сведения см. в разделах Перенаправление мультимедиа для Виртуального рабочего стола Azure и Устранение неполадок с перенаправлением мультимедиа для Виртуального рабочего стола Azure.

Ваша организация не назначила вам облачный компьютер

При доступе к windows365.microsoft.com пользователь получает сообщение "Ваша организация не назначила вам облачный компьютер".

Возможная причина. Чтобы получить доступ к облачному компьютеру, пользователю необходимо назначить лицензию и создать политику подготовки.

Действия по устранению неполадок: убедитесь, что:

1. Пользователю назначена лицензия на Windows 365. Дополнительные сведения см. в статье Назначение лицензий и Windows 365 планов и цен.
2. Вы создали политику подготовки, включающую пользователя. Дополнительные сведения см. в статье Создание политик подготовки.

Снижение производительности при вложенной виртуализации

Некоторые пользователи могут столкнуться с снижением производительности облачных компьютеров с 4vCPU при использовании вложенной виртуализации.

Действия по устранению неполадок:

- Повторная подготовка облачного компьютера или
- Удалите Hyper-V на облачном компьютере.

Windows 365 Frontline сообщение пользователя: Облачный компьютер должен быть доступен в ближайшее время

Если вы достигли максимального числа активных сеансов пользователей в клиенте, все пользователи, которые пытаются запустить сеанс пользователя, увидят на портале конечных пользователей сообщение "Ваш облачный компьютер должен быть доступен в ближайшее время".

Действия по устранению неполадок. Используйте отчет об использовании , чтобы оценить правильный объем лицензии для вашей организации.

Дальнейшие действия

Устранение неполадок с сетевыми подключениями Azure.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Известные проблемы: Windows 365 Корпоративная и Фронтлайн

23.05.2025

Следующие элементы являются известными проблемами для Windows 365 для предприятий.

При первой авторизации в Cloud PC активируется оповещение "Невозможное местоположение"

При использовании условного доступа пользователь, который впервые входит в облачный компьютер, может активировать уведомление о невозможном местоположении перемещения.

Решение

Выполните следующие действия, чтобы изучить риск и убедиться, что действие соответствует ожидаемому поведению пользователя в зависимости от их физического расположения и расположения облачного компьютера.

Поддержка водяных знаков в Windows 365

Поддержка водяного знака настраивается на узлах сеансов и обеспечивается клиентом удаленного рабочего стола. Параметры поддержки водяного знака можно настроить с помощью групповой политики (GPO) или каталога параметров Intune. Значение по умолчанию для параметра встроенного содержимого QR-кода не позволяет администраторам искать сведения об устройстве на основе изображений, полученных в результате утечки информации, для облачных ПК.

Решение

Убедитесь, что параметр встроенного содержимого QR-кода настроен на **идентификатор устройства**, как в объекте групповой политики, так и в каталоге параметров Intune для профиля конфигурации Intune, используемого для конфигурации поддержки водяных знаков.

Дополнительные сведения см. в разделе "Административный шаблон" для виртуального рабочего стола Azure.

Отсутствует меню и панель задач при использовании iPad и приложения удаленного рабочего стола для доступа к облачному компьютеру

Если пользователи, не являющиеся локальными администраторами, входят на облачный ПК с помощью iPad и приложения Microsoft Remote Desktop, меню Пуск и панель задач могут отсутствовать в пользовательском интерфейсе Windows 11.

Решение

Убедитесь, что у вас есть последняя версия клиента удаленного рабочего стола, которую можно найти на клиентах удаленного рабочего стола для служб удаленных рабочих столов и удаленных компьютеров.

Кроме того, вы можете войти на облачный компьютер с помощью Windows 365.

Восстановление и автоматическое развертывание учетных данных

Многие устройства, зарегистрированные в Active Directory, могут иметь пароль учетной записи компьютера, который автоматически обновляется. По умолчанию эти пароли обновляются каждые 30 дней. Эта автоматизация применяется к гибридным присоединенным компьютерам, но не к собственным компьютерам Microsoft Entra Native.

Пароль учетной записи компьютера сохраняется на облачном компьютере. Если облачный компьютер восстановлен до точки, в которую сохранен предыдущий пароль, облачный компьютер не сможет войти в домен.

Дополнительные сведения см. в разделе "Процесс пароля учетной записи компьютера".

Видимое расположение курсора смещено от фактической позиции.

В сеансе удаленного рабочего стола при выборе одной позиции в текстовом файле курсор на облачном компьютере имеет некоторое смещение с фактическим положением.

Возможная причина

В режиме высокого DPI как сервер, так и браузер Cloud PC масштабируют курсор. Этот конфликт приводит к смещению между видимой позицией курсора и фактическим фокусом курсора.

Решение

Отключите режим высокого уровня DPI.

Outlook загружает только один месяц почты

Outlook скачивает только один месяц предыдущей почты, который не может быть изменен в параметрах Outlook.

Решение

1. Запустите редактор реестра.
2. Удалите ключ реестра по указанному пути:

   `\HKEY_CURRENT_USER\SOFTWARE\Policies\Microsoft\Office\16.0\Outlook\Cached Mode`

3. Добавьте ключ реестра `syncwindowsetting` со значением `1` в путь:

   `\HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Cached Mode`

После выполнения этих действий значение по умолчанию будет составлять один месяц. Однако период скачивания можно изменить в параметрах Outlook.

Обновление Windows на месте может изменить имя компьютера

Обновление существующего облачного компьютера между версиями Windows 10 до Windows 11 может привести к изменению имени компьютера с префиксом "pps" при сохранении имени устройства Intune без изменений.

Решение

Найдите облачный компьютер в Microsoft Intune и управляйте ими с помощью неизменяемого имени устройства Intune в **списке устройств**>**"Все устройства**" или>**"Все облачные компьютеры".**

Ошибка при настройке Windows 365

Ошибки подготовки Windows 365 могут возникнуть, если выполнены оба следующих условия:

- Расширение "Конфигурация требуемого состояния" (DSC) не подписано.
- Политика выполнения PowerShell установлена на **AllSigned** в объекте групповой политики (GPO).

Решение

1. Проверьте, возникла ли в сетевом подключении Azure (ANC) ошибка "Произошла внутренняя ошибка." Развертывание виртуальной машины завершилось с тайм-аутом. Если это так, просмотрите соответствующий объект групповой политики.
2. Убедитесь, что для политики выполнения PowerShell задано значение **AllSigned**. Если это так, удалите объект групповой политики или сбросьте политику выполнения PowerShell на **неограниченную**.
3. Повторите проверку работоспособности ANC. Если проверка выполнена успешно, повторите настройку.

Облачный компьютер сообщает о несоответствии политике соответствия требованиям

Следующие параметры соответствия устройства выводятся как **Неприменимо** при оценке облачного компьютера.

- **Доверенный модуль платформы (TPM)**
- **Требование шифрования хранилища данных на устройстве**

Следующие параметры соответствия устройств могут сообщать о **несоответствии** при оценке для облачного компьютера:

- **Требовать BitLocker**

- **Требуется включить безопасную загрузку на устройстве**. Поддержка облачного компьютера для функции безопасной загрузки теперь доступна всем клиентам.

Решение

Чтобы включить безопасную загрузку на облачном ПК, перейдите к переподготовке конкретного облачного ПК.

Чтобы удалить несоответствующие параметры, выполните следующие действия.

1. Создайте фильтр для всех облачных компьютеров.
2. Для всех существующих политик соответствия устройств, которые оценивают облачный компьютер и содержат любой из **параметров, не соответствующих требованиям** , используйте этот новый фильтр, чтобы исключить облачные компьютеры из назначения политики.
3. Создайте политику соответствия устройств без параметров '**Несоответствия**' и используйте этот новый фильтр, чтобы включить облачные ПК для назначения политики.

Пользователи единого входа видят диалоговое окно, чтобы разрешить подключение к удаленному рабочему столу во время попытки подключения

При включении единого входа появится запрос на аутентификацию в Microsoft Entra ID и разрешение подключения к удаленному рабочему столу при установлении подключения к новому облачному ПК. Microsoft Entra запоминает до 15 устройств в течение 30 дней перед тем, как запросить еще раз. Если вы видите это диалоговое окно, нажмите кнопку "**Да** ", чтобы подключиться.

Чтобы предотвратить появление этого диалогового окна, можно создать предодобренную группу устройств. Следуйте инструкциям по настройке целевой группы устройств для начала работы.

Подключения пользователей с одноразовым входом блокируются через Условный доступ Microsoft Entra

Возможная причина

Чтобы войти через единый вход, клиент удаленного рабочего стола запрашивает маркер доступа к **приложению Удаленный рабочий стол (Майкрософт)** в Microsoft Entra, что может быть причиной сбоя подключения.

Действия по устранению неполадок

Выполните действия, описанные в руководстве по устранению неполадок при входе.

Пользователи единой аутентификации сразу отключаются при блокировке облачного ПК.

Если единый вход не используется, пользователи могут видеть экран блокировки Cloud PC и вводить учетные данные для разблокировки сеанса Windows. Однако при использовании единого входа облачный компьютер полностью отключает сеанс, чтобы:

- Пользователи могут использовать проверку подлинности без пароля для разблокировки облачного компьютера.
- Политики условного доступа и многофакторная проверка подлинности могут применяться при разблокировке облачного компьютера.

Пользователям, которые используют единый вход, не требуется повторно проходить аутентификацию в Microsoft Entra ID при подключении с неуправляемого устройства

При использовании единого входа все действия проверки подлинности (включая поддерживаемые типы учетных данных и частоту входа) управляются идентификатором Microsoft Entra.

Решение

Чтобы применить периодическую повторную проверку подлинности с помощью Microsoft Entra ID, создайте политику условного доступа с помощью параметра управления частотой входа.

На странице "Обзор устройств >" в Центре администрирования Intune не отображаются отчёты Cloud PC.

Если включить параметр "**Предварительный просмотр использования устройств**" в Центре администрирования Intune, вкладка "**Производительность облачных компьютеров (предварительная версия)**", отчет "**Облачные компьютеры с проблемами качества подключения**" и отчет "**Облачные компьютеры с низким использованием**" не отображаются на странице **Обзор**.

Решение

Отключите переключатель **Предварительный просмотр использования устройств** в правом верхнем углу страницы обзора **устройств**>**Overview**.

Облачный компьютер завис в цикле перезапуска после действия восстановления или изменения размера

Возможная причина

Эта проблема может возникнуть для облачных компьютеров, подготовленных до июля 2022 г., которые используют:

- Правила сокращения поверхностей атак Майкрософт (например, управление параметрами уменьшения поверхности атаки с помощью политик безопасности конечных точек в Microsoft Intune) или
- Сторонние решения, которые блокируют выполнение скрипта языка установки во время процесса последующей подготовки.

Облачные компьютеры, подготовленные после июля 2022 года, не сталкиваются с этой проблемой.

Действия по устранению неполадок

Определите первопричину:

1. Выполните поиск в журнале событий Windows. Если в системе отображается следующее событие перезагрузки (1074), перейдите к шагу 2.

Выходные данные

```
The process C:\WINDOWS\system32\wbem\wmiprvse.exe (<CPC Name>) has initiated
the restart of computer <CPC Name> on behalf of user NT AUTHORITY\SYSTEM for
the following reason: Application: Maintenance (Planned)
Reason Code: 0x80040001
Shutdown Type: restart
Comment: DSC is restarting the computer.
```

2. Запустите `Get-DscConfigurationStatus` в командном окне с повышенными привилегиями. Если в результате отображается ожидание перезагрузки для задания, перейдите к шагу 3.

3. Запустите `Get-DscConfiguration` в командном окне с повышенными привилегиями. Если результаты показывают DSC, устанавливающий язык, перейдите к следующему разделу.

Решение

Чтобы остановить цикл перезапуска, попробуйте выполнить одно из следующих параметров:

- Удалите политики Azure Site Recovery или переключите политики в режим аудита, а затем примените новые политики к облачному компьютеру.

- В командном окне с повышенными привилегиями выполните следующую команду, чтобы перезагрузить задание:

  `Remove-DSCConfiguration -Stage Pending,Current,Previous -Verbose`

Проблемы с подключением к облачному компьютеру для клиентов GCC High для государственных организаций

Некоторые клиенты GCC High для государственных организаций, ресурсы которых развернуты в `microsoft.us` средах, могут столкнуться с проблемами подключения к облачному компьютеру с помощью веб-клиентов или браузера Safari.

Возможная причина

Проблема возникает, когда веб-клиент или браузер Safari блокирует сторонние файлы cookie. Сторонние файлы cookie — это файлы cookie, заданные доменом, отличным от

того, который вы посещаете.

Для клиентов GCC High с ресурсами, развернутыми в средах `microsoft.us`, файлы cookie `microsoft.us` считаются сторонними веб-клиентом или браузером Safari. Это связано с тем, что веб-клиент или браузер Safari использует доменное имя Cloud PC, которое отличается от `microsoft.us` имени домена, чтобы определить первый домен. Если веб-клиент или браузер Safari блокирует сторонние файлы cookie, он запрещает `microsoft.us` файлы cookie:

- Хранится.
- Используется для проверки подлинности и авторизации.

В результате вы не можете подключиться к сеансу облачного пк.

Решение

Разрешите сторонние файлы cookie от `microsoft.us` в настройках вашего веб-клиента, настройках браузера Safari или групповой политики.

Это изменение позволяет веб-клиенту или браузеру Safari сохранять и использовать `microsoft.us` файлы cookie для подключения к сеансу облачного компьютера.

Безопасность Windows сообщает: «Целостность памяти отключена». Ваше устройство может быть уязвимо.

Безопасность Windows сообщает: «Целостность памяти отключена». Ваше устройство может быть уязвимо.

В сведениях о системах Windows в Cloud PC также можно увидеть, что строка Виртуализация на основе безопасности (VBS) показывает **включено, но не запущено**.

Эта проблема может быть вызвана при включении вложенной виртуализации. При включении вложенной виртуализации требуется запущенный вложенный гипервизор, который препятствует защите прямого доступа к памяти (DMA). Защита DMA требуется при запуске VBS.

Решение

Убедитесь, что:

- Вложенная виртуализация отключена для облачного компьютера.
- В политиках безопасности включен VBS с защитой DMA.

Другой вариант заключается в том, чтобы не требовать DMA для VBS, так как они несовместимы друг с другом.

Microsoft Teams не использует защиту захвата экрана

Если защита захвата экрана включена, Microsoft Teams на облачных компьютерах Windows 365 не применяет её.

Действия по устранению неполадок

- Убедитесь, что версия WebRTC обновлена.

- Убедитесь, что политика защиты захвата экрана настроена правильно, чтобы выбран клиент и сервер:

    1. Войдите в Центр администрирования Microsoft Intune, выберите "**Конфигурация устройств**>" и выберите политику.
    2. В разделе **Параметры конфигурации** выберите **Компоненты Windows**>, **Службы удаленных рабочих столов**>, **Узел сеансов удаленных рабочих столов**>, **Azure Virtual Desktop**, а затем убедитесь, что задано следующее:
        - **Включить защиту захвата экрана** = **Включить**
        - **Опции защиты от снятия скриншотов** = **Блокировка снятия скриншотов на клиенте и сервере**

Теги областей Windows 365 и вложенные группы

Windows 365 не поддерживает вложенные группы безопасности. Если вы применяете тег области к верхнему уровню вложенной группы безопасности, облачные ПК во внутренних вложенных группах не получают теги области.

Решение

Примените тег области действия к каждой группе в составе вложенной группы безопасности отдельно.

Windows 365 не поддерживает теги области редактирования для отдельных облачных компьютеров

Пользовательский интерфейс Windows 365 и API Graph не поддерживают редактирование тегов областей для отдельных облачных компьютеров.

Решение

Измените теги области для отдельных облачных компьютеров в области "Все устройства" Intune, чтобы синхронизировать ассоциации тегов области со службой Windows 365.

Теги области для пользовательских образов не могут быть изменены

Теги области, применяемые к пользовательским изображениям, не могут быть изменены или непосредственно добавлены администраторами верхнего уровня.

Решение

Когда администраторы с заданной областью создают пользовательские изображения, эти пользовательские изображения помечаются теми же тегами области, которые связаны с администратором данной области.

Например, если администратор с тегом области "Scope Tag A" создает пользовательский образ, созданный пользовательский образ автоматически помечается тегом "Scope Tag A".

Служба перенаправления WebRTC отсутствует в последних образах из галереи облачного ПК Windows 365

Обновления от 21 мая 2024 г. для образов галереи облачных ПК, в которых отсутствует служба перенаправления WebRTC. Без этого компонента перенаправление мультимедиа в Teams не работает.

Это относится к следующим изображениям коллекции:

- Windows 11 23H2 с приложениями Microsoft 365
- Windows 11 22H2 с приложениями Microsoft 365

Действия по устранению неполадок

Для ново-подготовленных облачных компьютеров убедитесь, что WebRTC доступен. Если это не так, можно использовать любой из следующих вариантов:

- Чтобы добавить приложение Службы перенаправления WebRTC в список приложений для установки по умолчанию на облачные компьютеры, выполните действия, описанные в разделе "Добавление Приложения Microsoft 365 на устройства Windows 10/11 с Помощью Microsoft Intune".

- Чтобы добавить приложение службы перенаправления WebRTC в отдельный облачный компьютер, выполните действия, описанные в разделе "Установка службы перенаправления webRTC удаленного рабочего стола". Чтобы получить самый актуальный установщик, используйте следующую ссылку: https://aka.ms/msrdcwebrtcsvc/msi

Проблемы с Windows 365 Frontline

Ниже приведены проблемы с Windows 365 Frontline:

Пользователи могут не иметь доступа к компьютерам Frontline Cloud в общем режиме

Когда компьютеры Frontline Cloud в общем режиме назначены группе идентификаторов Entra с более чем 10 000 участниками, некоторые пользователи могут не получать доступ и могут не видеть карты облачных ПК в приложении Windows.

Решение

Сократите членство в группе Entra ID, чтобы было меньше 10 000 пользователей.

Невозможно уменьшить количество облачных ПК для Frontline Cloud в общем режиме, если не удается успешно подготовить все облачные ПК.

Если подготовка завершается сбоем из-за сбоя профиля подготовки устройств Autopilot (DPP) (предварительная версия) и в результате все облачные компьютеры не показывают

успешно подготовленных устройств, администраторы не смогут уменьшить количество облачных компьютеров в опции повторного назначения.

Решение

Выполните действие реподготовки в политике распределения.

Запланированное восстановление не происходит, если лицензии Frontline удаляются или истекают у арендатора, а затем добавляются обратно.

Если компьютеры frontline Cloud подготавливаются в общем режиме, а затем срок действия лицензий истекает или удаляется из клиента, облачные компьютеры будут удалены до тех пор, пока не будут добавлены допустимые лицензии. После добавления лицензий облачные компьютеры будут подготовлены в соответствии с конфигурациями, определенными в политике предоставления. Если вы настроили запланированную повторную подготовку для политики подготовки, эта запланированная повторная подготовка не будет повторно активирована. Действие повторной подготовки вручную также завершается ошибкой.

Решение

Чтобы восстановить полную функциональность ручной и запланированной повторной подготовки после истечения срока действия лицензии, удалите назначение политики подготовки и снова добавьте ее.

Следующие шаги

Устранение неполадок Windows 365 Корпоративная облачного компьютера

Известные проблемы с облачным компьютером с поддержкой ИИ

Применяется к: ✅ Supported versions of Windows 365

Если облачный компьютер работает неправильно, сначала убедитесь, что вы выполнили все минимальные требования к функциям искусственного интеллекта (ИИ). Если ваша учетная запись и устройство соответствуют этим требованиям, ознакомьтесь со следующими разделами, чтобы узнать, является ли проблема документирована.

Время активации состояния с поддержкой ИИ

После того, как вы активируете ИИ для облачного компьютера, фоновые процессы могут выполняться до 48 часов, прежде чем поддерживаемые функции ИИ будут готовы к использованию.

Sparkles отсутствует в поле поиска Windows после установки обновления Windows

После установки обновления Windows блёстки могут исчезнуть из значка увеличительного стекла.

Чтобы восстановить значок, выберите поле поиска Windows. Если искры по-прежнему отсутствуют, перезапустите облачный компьютер.

Функции искусственного интеллекта отсутствуют после установки обновления Windows

После установки обновления Windows функции ИИ могут быть недоступны.

Чтобы восстановить все функции с поддержкой ИИ, перезапустите облачный компьютер.

Курсор мыши "Click to Do" кажется медленным

Когда вы используете функцию "Click to Do" или после ее отключения, курсор вашего облачного ПК может задерживаться.

Чтобы восстановить скорость реагирования курсора, перезапустите облачный компьютер.

Результаты семантического поиска не отображаются на вкладке "Все" поиска Windows

Результаты поиска могут занять время для загрузки на вкладке "**Все** " окна поиска Windows.

Если результаты поиска не отображаются в первой попытке поиска, повторите поиск. Возможно, вам придется повторить поиск несколько раз, чтобы просмотреть полные результаты.

Поиск семантических файлов не работает на облачном компьютере, использующем вложенную виртуализацию

Если поиск семантических файлов не работает, убедитесь, что облачный компьютер не использует вложенную виртуализацию.

Чтобы проверить этот параметр и отключить его при необходимости, выполните следующие действия.

1. Нажмите клавишу с логотипом Windows+R и введите **панель управления**.
2. В строке поиска панели управления введите **включение или отключение функций Windows**.
3. Убедитесь, что следующие функции не выбраны. Если какой-либо из них выбран, снимите их флажки.
    - Платформа виртуальной машины
    - Платформа гипервизора Windows
    - Hyper-V
    - Средства управления Hyper-V
    - средства управления графическими интерфейсами Hyper-V
    - Модуль Hyper-V для Windows PowerShell
    - платформа Hyper-V
    - Гипервизор Hyper-V
    - службы Hyper-V
4. Чтобы применить изменения, нажмите **кнопку "OK**" и перезапустите облачный компьютер.

"Click to Do" не работает, если облачный ПК находится в оконном режиме

Функция "Click to Do" может не работать, если ваш облачный ПК не находится в полноэкранном режиме. Попробуйте максимизировать окно облачного компьютера (на полный экран), прежде чем использовать кнопку "Сделать".

Дополнительная помощь по вопросам, связанным с использованием облачных компьютеров с поддержкой ИИ

Для проблем, которые не рассматриваются в этой статье, участники программы предварительной оценки Windows могут перейти к дополнительным сведениям в статье "Устранение неполадок" программы предварительной оценки Windows.

Last updated on 18.11.2025

Устранение неполадок сетевых подключений Azure

10.06.2025

Сетевое подключение Azure (ANC) периодически проверяет среду, чтобы убедиться, что выполнены все требования и что она находится в работоспособном состоянии. Если проверка завершается ошибкой, в Центре администрирования Microsoft Intune отображаются сообщения об ошибках. В этом руководстве содержатся дополнительные инструкции по устранению неполадок, которые могут привести к сбою проверок.

Присоединение к домену Active Directory

При подготовке облачного компьютера он автоматически присоединяется к указанному домену. Для проверки процесса присоединения к домену объект компьютера домена создается в определенном подразделении с именем, аналогичным CPC-Hth при каждом запуске проверок работоспособности Windows 365. Эти объекты компьютера отключены при завершении проверки работоспособности. Сбой присоединения к домену Active Directory может возникать по многим причинам. Если присоединение к домену завершается ошибкой, убедитесь, что:

- Пользователь, присоединенный к домену, имеет достаточные разрешения для присоединения к указанному домену.
- Пользователь, присоединенный к домену, может записывать данные в указанную подразделение.
- Пользователь присоединения к домену не ограничивается количеством компьютеров, к которым они могут присоединиться. Например, максимальное число соединений по умолчанию для каждого пользователя равно 10, и это максимальное значение может повлиять на подготовку облачных компьютеров.
- Используемая подсеть может получить доступ к контроллеру домена.
- Вы проверяете `Add-Computer` использование учетных данных присоединения к домену на виртуальной машине, подключенной к виртуальной сети или подсети облачного компьютера.
- Устранение неполадок при присоединении к домену, таких как любой физический компьютер в организации.
- Если у вас есть доменное имя, которое можно разрешить в Интернете (например `contoso.com`), убедитесь, что серверы системы доменных имен (DNS) настроены как внутренние. Кроме того, убедитесь, что они могут разрешать записи DNS домена Active Directory, а не имя общедоступного домена.

Если при проверке работоспособности ANC возникают следующие ошибки, рассмотрите рекомендации в следующих двух разделах, чтобы обеспечить успешное достижение необходимых конечных точек Windows 365 в Azure и локальных конфигурациях:

> Внутренняя ошибка сервера

> Внутренняя ошибка сервера: Невозможно выполнить скрипт DSC

Линия видимости контроллера домена

Успешное взаимодействие с контроллером домена в вашей организации важно для настройки ANC, чтобы разрешить использование гибридных облачных ПК, присоединённых к домену. Убедитесь, что виртуальная сеть Azure, используемая для подключения ANC, имеет сетевой маршрут к контроллеру домена и убедитесь, что настройка DNS может успешно разрешить ее.

> **Примечание**
>
> Этот раздел применяется только к гибридным средам.

Требования к удаленному управлению Windows (WinRM) для ANC

Для завершения установки ANC требуется WinRM.

Чтобы обеспечить успешное предоставление ресурсов, убедитесь, что WinRM не ограничен конкретными IP-адресами, как посредством объекта групповой политики (GPO), так и через поставщика услуг конфигурации Microsoft Intune (CSP), для групп, которые используются в ваших политике подготовки. WinRM следует настроить для разрешения сетевых запросов с любого IP-адреса.

Дополнительные сведения см. в разделе конфигурации GPO или CSP Intune.

Доступ к конечной точке ANC

Во время настройки ANC служба должна скачать данные конфигурации из различных конечных точек Майкрософт, как указано в требованиях к сети. Сбой доступа к этим конечным точкам из-за неправильно настроенных параметров сети может привести к сбою. Чтобы обеспечить успешный доступ, необходимо избежать проверки протокола TLS в любой виртуальной сети, используемой для подключений ANC. Убедитесь, что вы

сможете успешно разрешить и достичь этих конечных точек через виртуальную сеть Azure, используемую и убедитесь, что любой брандмауэр, прокси-сервер или другие сетевые службы, используемые в сети, разрешают им доступ.

Синхронизация устройств Microsoft Entra

Перед регистрацией управления мобильными устройствами (MDM) во время подготовки объект идентификатора Microsoft Entra должен присутствовать для облачного компьютера. Эта проверка предназначена для своевременной синхронизации учетных записей компьютеров организаций с идентификатором Microsoft Entra.

Убедитесь, что объекты компьютера Microsoft Entra отображаются быстро в идентификаторе Microsoft Entra. Рекомендуется отображать их в течение 30 минут и не более 60 минут. Если объект компьютера не поступает в идентификатор Microsoft Entra в течение 90 минут, подготовка завершается ошибкой.

Если подготовка завершается ошибкой, убедитесь, что:

- Конфигурация периода синхронизации в идентификаторе Microsoft Entra ID настроена соответствующим образом. Обратитесь к группе удостоверений, чтобы убедиться, что каталог синхронизируется достаточно быстро.
- Идентификатор Microsoft Entra активен и работоспособен.
- Microsoft Entra Connect работает правильно, и нет проблем с сервером синхронизации.
- Вы вручную выполняете `Add-Computer` вход в подразделение, предоставленное для облачных компьютеров. Время, сколько времени требуется для отображения этого объекта компьютера в идентификаторе Microsoft Entra.

> **Примечание**
>
> Если вы получаете предупреждение **Entra ID Sync** после подтверждения правильно установленной рекомендуемой конфигурации и отсутствия проблем с обеспечением, никаких дальнейших действий не требуется. Это предупреждение может возникать, если проверка выполняется непосредственно после завершения синхронизации.

Использование диапазона IP-адресов подсети Azure

В рамках установки ANC необходимо предоставить подсеть, к которой подключается облачный компьютер. Для каждого облачного компьютера подготовка создает

виртуальный сетевой адаптер и использует IP-адрес из этой подсети.

Убедитесь, что достаточное выделение IP-адресов доступно для количества облачных компьютеров, которые требуется подготовить. Кроме того, запланируйте достаточное адресное пространство для подготовки сбоев и потенциального аварийного восстановления.

Если эта проверка завершается ошибкой, убедитесь, что вы:

- Проверьте подсеть в виртуальной сети Azure. У него должно быть достаточно адресного пространства.
- Убедитесь, что достаточно адресов для обработки трех повторных попыток подготовки, каждый из которых может храниться на сетевых адресах, используемых в течение нескольких часов.
- Удалите все неиспользуемые карты виртуальной сети (виртуальные сетевые адаптеры). Рекомендуется использовать выделенную подсеть для облачных компьютеров, чтобы убедиться, что другие службы не используют выделение IP-адресов.
- Разверните подсеть, чтобы сделать больше адресов доступными. Это невозможно сделать, если подключены устройства.

Во время попыток подготовки важно учитывать любые блокировки CanNotDelete, которые могут применяться на уровне группы ресурсов или выше. Если эти блокировки присутствуют, сетевые интерфейсы, созданные в процессе, не удаляются автоматически. Если они не удаляются автоматически, необходимо вручную удалить виртуальные сетевые адаптеры, прежде чем повторить попытку.

Во время попыток подготовки важно учитывать все существующие блокировки на уровне группы ресурсов или выше. Если эти блокировки присутствуют, сетевые интерфейсы, созданные в процессе, не будут автоматически удалены. При возникновении события необходимо вручную удалить виртуальные сетевые адаптеры, прежде чем повторить попытку.

Готовность клиента Azure

При выполнении проверок убедитесь, что указанная подписка Azure действительна и работоспособна. Если это недопустимо и работоспособно, мы не можем подключить облачные компьютеры к виртуальной сети во время подготовки. Такие проблемы, как выставление счетов, могут привести к отключению подписок.

Многие организации используют политики Azure, чтобы убедиться, что ресурсы подготовлены только в определенных регионах и службах. Убедитесь, что все политики

Azure рассматривают службу облачных компьютеров и поддерживаемые регионы.

Войдите в портал Azure и убедитесь, что подписка Azure включена, действительна и работоспособна.

Кроме того, посетите портал Azure и просмотрите **политики**. Убедитесь, что политики не блокируют создание ресурсов.

Готовность виртуальной сети Azure

При создании ANC мы блокируем использование любой виртуальной сети, расположенной в неподдерживаемом регионе. Список поддерживаемых регионов см. в разделе "Требования".

Если эта проверка завершается ошибкой, убедитесь, что виртуальная сеть указана в регионе в списке поддерживаемых регионов.

DNS может разрешить домен Active Directory

Для успешного присоединения к домену Windows 365 облачные компьютеры, подключенные к виртуальной сети, должны иметь возможность разрешать внутренние DNS-имена.

Этот тест пытается разрешить указанное доменное имя. Например, contoso.com или contoso.local. Если этот тест завершается ошибкой, убедитесь, что:

- DNS-серверы в виртуальной сети Azure правильно настроены на внутренний DNS-сервер, который может успешно разрешить доменное имя.
- Подсеть или виртуальная сеть правильно направляется таким образом, чтобы облачный компьютер смог получить доступ к предоставленному DNS-серверу.
- Облачные компьютеры и виртуальные машины в объявленной подсети могут `NSLOOKUP` на DNS-сервере и отвечают внутренним именам.

Наряду со стандартным поиском DNS по указанному доменному имени мы также проверяем наличие `_ldap._tcp.yourDomain.com` записей. Эта запись указывает, что DNS-сервер предоставляется контроллером домена Active Directory. Запись является надежным способом подтверждения доступности DNS домена AD. Убедитесь, что эти записи доступны через виртуальную сеть, предоставленную в ANC.

Подключение к конечной точке

Во время подготовки облачные компьютеры должны подключаться к нескольким общедоступным службы Майкрософт. К этим службам относятся Microsoft Intune, идентификатор Microsoft Entra и виртуальный рабочий стол Azure.

Необходимо убедиться, что все необходимые общедоступные конечные точки можно получить из подсети, используемой облачными компьютерами.

Если этот тест завершается ошибкой, убедитесь, что:

- Средства устранения неполадок с виртуальной сетью Azure используются для обеспечения доступа к конечным точкам службы, перечисленным в документации.
- Dns-сервер, предоставленный, может правильно разрешать внешние службы.
- Прокси-сервер между подсетью Cloud PC и Интернетом отсутствует.
- Нет правил брандмауэра (физических, виртуальных или в Windows), которые могут блокировать необходимый трафик.
- Вы рассмотрите возможность тестирования конечных точек из виртуальной машины в той же подсети, объявленной для облачных компьютеров.

Если вы не используете Azure CloudShell, убедитесь, что политика выполнения PowerShell настроена для разрешения неограниченных сценариев. Если вы используете групповую политику для установки политики выполнения, убедитесь, что объект групповой политики , предназначенный для подразделения, определенного в ANC, настроен для разрешения неограниченных сценариев. Дополнительные сведения см. в разделе Set-ExecutionPolicy.

Среда и конфигурация готовы

Эта проверка используется для многих проблем, связанных с инфраструктурой, которые могут быть связаны с инфраструктурой, за которую отвечают клиенты. Она может включать такие ошибки, как время ожидания внутренней службы или ошибки, вызванные удалением или изменением ресурсов Azure во время выполнения проверок.

Рекомендуется повторить проверку, если возникла эта ошибка. Если он сохраняется, обратитесь в службу поддержки.

Разрешения приложения первой стороны

При создании ANC мастер предоставляет определенный уровень разрешений для группы ресурсов и подписки. Эти разрешения позволяют службе плавно подготавливать облачные компьютеры.

Администраторы Azure, имеющие такие разрешения, могут просматривать и изменять их.

Если какие-либо из этих разрешений отозваны, эта проверка завершается ошибкой. Убедитесь, что следующие разрешения предоставляются субъекту-службе приложение Windows 365 ликации:

- Роль читателя в подписке Azure.
- Роль участника сетевого интерфейса Windows365 в указанной группе ресурсов.
- Роль сетевого пользователя Windows365 в виртуальной сети.

Назначение ролей в подписке предоставляется субъекту-службе Cloud PC.

Кроме того, убедитесь, что разрешения не предоставляются в качестве ролей администратора классических подписок или ролей (классических). Эта роль недостаточно. Это должна быть одна из встроенных ролей управления доступом на основе ролей Azure, как указано ранее.

Следующие шаги

Узнайте о проверках работоспособности ANC.

Проверка работоспособности сетевого подключения Azure

Статья • 20.01.2025

Уникальной функцией Windows 365 является проверка работоспособности подключения к сети Azure (ANC). Проверки работоспособности периодически выполняются, чтобы убедиться, что:

- Подготовка облачных компьютеров выполнена успешно.
- Интерфейсы облачных компьютеров конечных пользователей являются оптимальными.

Состояние сетевого подключения Azure

На вкладке сетевого **подключения** Azure каждый созданный ANC отображает состояние. Это состояние помогает определить, могут ли новые облачные компьютеры быть успешно подготовлены и имеют ли существующие конечные пользователи оптимального интерфейса облачного компьютера.

К состояниям относятся:

- **Выполнение проверок**: проверки работоспособности выполняются в настоящее время. Представление списка ANC автоматически обновляется каждые пять минут. Дождитесь завершения проверок перед попыткой назначить его политике подготовки.
- **Проверяет успешно:** все проверки работоспособности пройдены. ANC готов к использованию.
- **Проверяет успешное выполнение предупреждений: все критически важные проверки работоспособности пройдены**. Однако по крайней мере одна некритическая проверка может иметь проблемы. Пример проверки, которая может активировать это состояние, — это проверка синхронизации гибридного соединения Microsoft Entra. Синхронизация гибридного соединения Microsoft Entra может занять до 90 минут. Поэтому мы проверили большую часть службы синхронизации гибридного соединения Microsoft Entra, но не смогли подтвердить, что синхронизация устройства выполнена до конца. Политики подготовки могут использовать ANCs с таким состоянием.
- **Сбой** проверок: сбой одной или нескольких обязательных проверок. Не удается использовать ANC, если он находится в состоянии сбоя. Устраните основную проблему и повторите проверки работоспособности.

- **Неактивно**: ANC неактивен и проверки работоспособности приостановлены. Повторно активируйте ANC, чтобы перезапустить проверки работоспособности. После прохождения проверок работоспособности anC будет готов к использованию.

Сведения об ошибке состояния

Каждый неудачный ANC или успешное выполнение с состоянием ошибки предупреждения включает технические сведения за сбоем. Выберите ссылку **"Просмотр сведений"** для каждой неудачной проверки, чтобы просмотреть дополнительные сведения о сбое. После устранения базовой проблемы повторите проверку работоспособности, чтобы повторно запустить тесты. Чтобы повторить проверку работоспособности, необходимо иметь роль администратора Intune или администратора Windows 365.

Поддерживаемые проверки

- **DNS может разрешить домен** Active Directory: устраните предоставленное доменное имя Active Directory.
- **Присоединение** к домену Active Directory: присоединение к домену с использованием учетных данных, домена и подразделения.
- **Подключение конечной точки: подключение** к необходимым URL-адресам или конечным точкам.
- **Синхронизация устройств Microsoft Entra (предупреждение)**: синхронизация идентификатора устройства включена в клиенте Microsoft Entra, а объект компьютера синхронизируется в течение 90 минут.
- **Использование** IP-адресов подсети Azure: в предоставленной подсети Azure доступны достаточные IP-адреса.
- **Готовность** клиента Azure: определенная подписка Azure включена и готова к использованию. Ограничения политики Azure не блокируют создание ресурсов Windows 365
- **Готовность** к виртуальной сети Azure: определенная виртуальная сеть находится в регионе, поддерживаемом Windows 365.
- **Разрешения приложения первой стороны существуют в подписке Azure: в подписке** Azure существуют достаточные разрешения.
- **Разрешения приложения первой стороны существуют в группе ресурсов Azure: в группе** ресурсов Azure существуют достаточные разрешения.
- **Разрешения приложения первой стороны существуют в виртуальной сети Azure: в виртуальной сети** Azure существуют достаточные разрешения.

- **Среда и конфигурация готовы**: базовая инфраструктура готова к успешной подготовке.
- **Ограничения регистрации** Intune позволяют регистрации Windows. Убедитесь, что ограничения регистрации Intune настроены для разрешения регистрации Windows.
- **Готовность** языкового пакета локализации: убедитесь, что доступ к операционной системе и языковым пакетам Microsoft 365 можно достичь. Кроме того, убедитесь, что ссылка на скачивание пакета локализации недоступна.
- **Проверка** подключения UDP: конфигурация сети позволяет использовать прямое подключение протокола UDP (STUN).
- **Конфигурация** единого входа. Определите, правильно ли настроена сеть для единого входа в гибридные компьютеры Microsoft Entra, присоединенные к облачным компьютерам, обеспечивая наличие объекта Kerberos Server.

Следующие шаги

Дополнительные сведения о сетевых подключениях Azure.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Проверки работоспособности подключения

Статья • 31.01.2025

Проверки работоспособности подключения выполняются на отдельных облачных компьютерах и предоставляют сведения о состоянии подключения облачного компьютера. Эти проверки постоянно выполняются службой Windows 365 в серверной части. Если какая-либо из этих проверок завершается ошибкой, пользователь не сможет подключиться к своему облачному компьютеру.

Вы можете проверить все неудачные проверки подключения и воспользоваться кнопкой **Устранение неполадок этого подключения** для устранения неполадок.

Просмотр состояния подключения к облачному компьютеру

1. Войдите в центр >администрирования Microsoft Intune **устройства**> Windows 365 >**Все облачные компьютеры**.
2. Выберите облачный компьютер в списке >**Обзор**>**производительности**.

Если облачный компьютер подключен, состояние отображается как **Доступно**.

Если возникла проблема с подключением облачного компьютера из-за неисправных компонентов, состояние отображается как **Недоступно**. Выберите **Устранение неполадок с этим подключением** , чтобы устранить проблему.

Ошибки подключения

При сбое подключения проверка отображается одно из следующих сообщений. Дополнительные сведения см. в области состояния. Для устранения неполадок можно использовать кнопку **Устранение неполадок с этим подключением** .

- **DomainJoin**: этот облачный компьютер не присоединен к домену.
- **DomainReachable**. Этот облачный компьютер не может подключиться к домену. Проверьте проверки виртуальная сеть Azure.
- **DomainTrust**: домен не доверяет этому облачному компьютеру. Убедитесь, что пароль локального устройства соответствует паролю устройства в домене.
- **SxSStackListener**: параллельный стек, установленный на облачном компьютере, неисправен или заблокирован.

- **Неизвестно**: этот облачный компьютер может не работать или сеть не подключена к общедоступному Интернету.
- **UrlsAccesibleCheck**. Этот облачный компьютер блокирует трафик к этим URL-адресам.

Если какая-либо из этих проблем сохранится, обратитесь в службу поддержки Майкрософт.

Ошибки подключения могут возникать, даже если все проверки работоспособности подключения успешно пройдены.

Отчет журнала подключений пользователей

В отчете журнала подключений пользователей показано, когда пользователь начал подключение и когда подключение было завершено. Существует несколько способов запуска и завершения подключения, и эти подключения регистрируются в отчете как действия.

Просмотр отчета о журнале подключений

1. Войдите в центр >администрирования Microsoft Intune **устройства**> Windows 365 >**Все облачные компьютеры**.
2. Выберите облачный компьютер в списке >**Обзор**>**представленияпроизводительности**> в разделе **Состояние подключения**.

Действия

В отчете показаны следующие действия:

Развернуть таблицу

Действие	Описание
Подключение запущено	Пользователь успешно подключен к своему облачному компьютеру.
Подключение завершено	Пользователь выходит из облачного компьютера или завершает рабочий сеанс. Если подключение завершается сбоем из-за непредвиденной ошибки сетевого подключения, оно отображается как **подключение завершено** с состоянием **Сбоя** .
Проверка	Если подключение завершается сбоем из-за проверка подключения,

Действие	Описание
подключения	отображается сбой проверка.

Выберите любое действие, чтобы получить дополнительные сведения о событии.

Отчет о журнале подключений обеспечивает видимость других действий в течение одного часа после ошибки подключения или сбоя проверка. Например, если пользователь пытается подключиться к своему облачному компьютеру и не может это сделать, также отображаются проверки работоспособности и успешный вход в систему в течение 1 часа до или после ошибки. Эти сведения позволяют администратору оценить ошибку, возможную причину и время восстановления работоспособности системы.

Дальнейшие действия

Дополнительные сведения о сетевых подключениях Azure.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Устранение ошибок подключения к облачному компьютеру

Статья • 20.01.2025

При подключении к облачному компьютеру могут возникать следующие ошибки.

Ошибки при подключении к облачному компьютеру, присоединенном к Microsoft Entra

Неудачная попытка входа

Потенциальная причина 1

Облачный компьютер или физическое устройство пользователя отказано в запросах протокола PKU2U. Протокол PKU2U активируется только в следующих случаях:

- Облачный компьютер присоединен к Microsoft Entra.
- Пользователь подключается из классического клиента Windows.
- Физическое устройство пользователя зарегистрировано в Microsoft Entra, присоединено к Microsoft Entra или гибридное присоединение Microsoft Entra к той же организации, что и облачный компьютер.

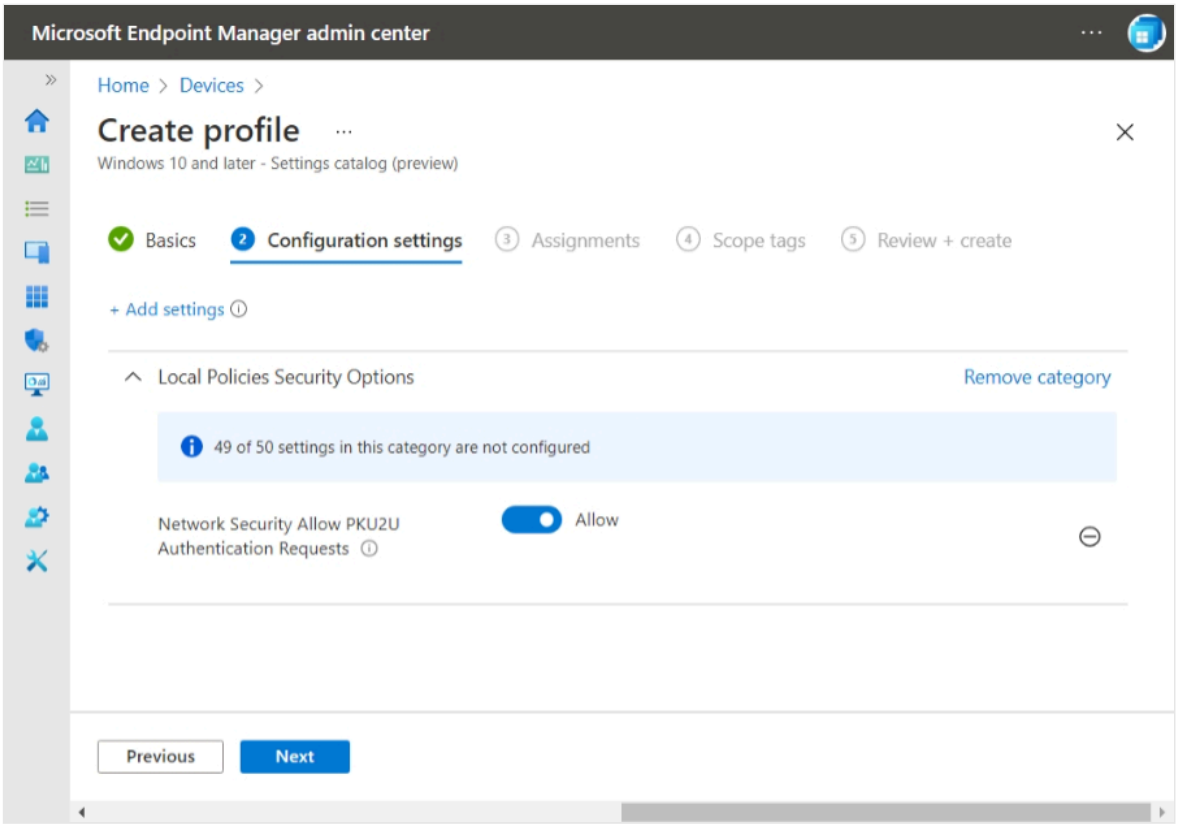
Возможное решение

Включите запросы протокола PKU2U как на облачном компьютере, так и на физическом устройстве пользователя:

1. Создайте фильтр для всех облачных компьютеров.

2. Создайте политику конфигурации устройства с помощью каталога параметров.

3. **На странице параметров конфигурации найдите и выберите "Разрешить запросы проверки подлинности** PKU2U" и выберите пункт **"Разрешить проверку**>подлинности сети".



4. **На странице "Назначения"** выберите **"Добавить все устройства>"Изменить фильтр>"Включить фильтр" в назначении**, а затем выберите фильтр, созданный для всех облачных компьютеров.

5. **На странице "Назначения"** также выберите группу Microsoft Entra, содержащую пользователя или физическое устройство пользователя.

6. Завершите создание политики конфигурации устройства.

Если вы управляете физическим устройством пользователя с помощью групповой политики или не управляете физическим устройством пользователя, вы (или пользователь) можете управлять этим параметром с помощью запросов проверки подлинности PKU2U на этот компьютер для использования политики удостоверений в Сети.

Потенциальная причина 2

Для учетной записи пользователя включена многофакторная проверка подлинности на пользователя. Так как он блокирует вход, многофакторная проверка подлинности для пользователей, подключающихся к облачным компьютерам, присоединенным к Microsoft Entra, не поддерживается.

Возможное решение

Удалите многофакторную проверку подлинности для всех пользователей, подключающихся к облачным компьютерам. Затем задайте политику условного доступа Microsoft Entra и назначьте ее соответствующим пользователям.

Конкретные ошибки подключения

Не удалось подключиться, так как в настоящее время нет доступных ресурсов

Возможная причина

На облачном компьютере может возникнуть проблема с ресурсом.

Возможное решение

Войдите в Windows 365, щелкните значок шестеренки рядом с облачным компьютером и нажмите кнопку "**Перезапустить**".

Не удалось подключиться к шлюзу из-за ошибки. Если это продолжает происходить, обратитесь к администратору или технической поддержке.

Возможная причина

Эта ошибка может быть вызвана параметрами конфигурации сети, например:

- Пользовательские параметры DNS
- Блокировка сетевого виртуального устройства
- Конфигурация группы безопасности сети
- Блокировки ресурсов
- Блоки для обязательных конечных точек

Возможное решение

Просмотрите параметры и убедитесь, что они не вмешиваются в подключения.

Удаленный компьютер завершил сеанс. Если это происходит, обратитесь к администратору сети за

помощью. Код ошибки: 0x3

Возможная причина

Эта ошибка может возникать, когда процессор Cloud PC чрезмерно используется.

Возможное решение

Если проблема сохраняется, войдите в Windows 365, щелкните значок шестеренки рядом с облачным компьютером и нажмите кнопку "**Перезапустить**".

Время ожидания попытки подключения, повторная попытка или ошибка при доступе к этому ресурсу

При возникновении этих ошибок убедитесь, что у вас нет настроенного поставщика облачных служб (CSP) или объекта групповой политики (GPO), который блокирует подключения к удаленному рабочему столу.

Политика CSP Intune:

Каталог параметров: **административные шаблоны\Компоненты Windows\Службы удаленных рабочих столов\Узел сеанса удаленного рабочего стола\Подключения**

Разрешить пользователям удаленно подключаться с помощью служб удаленных рабочих столов

Путь к конфигурации группового объекта:

Конфигурация компьютера\Компоненты Windows\Службы удаленных рабочих столов\Узел сеанса удаленного рабочего стола\Подключения

Разрешить пользователям удаленно подключаться с помощью служб удаленных рабочих столов

Если вы продолжаете сталкиваться с проблемами, запустите **параметр "Проверить подключение** " в приложении Windows или **параметр "Устранение неполадок** " в разделе "**Управление облачным компьютером** ", расположенным под тремя точками.

Другая ошибка подключения вызывает

Ниже приведены некоторые другие возможные причины сбоев подключения к облачному компьютеру:

Устаревшие версии VPN-клиента сторонних производителей

Возможное решение

Обновите VPN-клиенты до самых актуальных версий.

Вход на облачный компьютер с помощью учетных записей пользователей, доступных только для microsoft Entra ID

Возможное решение

Windows 365 в настоящее время является устройством гибридного соединения Microsoft Entra, требующим входа пользователей с помощью учетной записи локальная служба Active Directory.

Использование клиентского компьютера с поддержкой Remote Credential Guard

Возможное решение

Remote Credential Guard требует подключения к контроллеру домена локальная служба Active Directory на клиентском компьютере, используемом для доступа к облачному компьютеру. Это подключение возможно только с помощью VPN-решения. Использование прокси-сервера KDC в настоящее время недоступно для Windows 365.

Azure WireServer может быть заблокирован

Облачный компьютер Windows 365 требуется доступ к каналам коммуникации Azure.

Убедитесь, что IP-адрес 168.63.129.16 доступен через любое программное обеспечение безопасности, установленное на облачном компьютере или на

устройствах шлюза, используемых в виртуальной сети, подключенной к сетевому подключению Azure (ANC).

Дополнительные сведения см. в разделе "Что такое IP-адрес 168.63.129.16".

Другие действия по устранению неполадок

Перемещение облачного компьютера в новое подразделение (подразделение) без групповых политик

Проблемы с подключением могут быть вызваны параметрами, предоставляемыми групповыми политиками. Чтобы проверить эту возможную причину, вы можете переместить облачный компьютер в отдельную подразделение, которое заблокировано для получения групповых политик.

Локальный объект групповой политики может повлиять на подготовку или поведение облачного компьютера

Параметры, предоставляемые групповыми политиками, могут вызвать проблемы с подключением. Чтобы проверить эту проблему, вы можете переместить облачный компьютер в отдельную подразделение, которое заблокировано для получения групповых политик.

Периодические отключения

Если пользователи сталкиваются с периодическими проблемами подключения, рассмотрите следующее:

Возможное решение

- Убедитесь, что проверка и завершение SSL отключена для сетей, используемых облачными компьютерами. Дополнительные сведения см. в руководстве по прокси-серверу для виртуального рабочего стола Azure.
- При использовании сторонних веб-шлюзов программного обеспечения убедитесь, что исключения принудительного туннеля применяются для критического трафика виртуального рабочего стола Azure (AVD).

Дополнительные сведения см. в статье "Оптимизация подключения RDP для Windows 365 ".

Следующие шаги

Просмотрите другие действия по устранению неполадок

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Устранение ошибок подготовки

Статья • 20.01.2025

Следующие ошибки могут возникать во время подготовки облачных компьютеров.

Неправильно настроена точка подключения службы идентификатора Microsoft Entra

Точка подключения службы (SCP) используется облачными компьютерами для обнаружения сведений о клиенте Microsoft Entra. Необходимо настроить scPs с помощью Microsoft Entra Connect для каждого леса, к которому планируется присоединить облачные компьютеры.

Если конфигурация SCP не существует или не может быть обнаружена с помощью объявленной виртуальной сети, подготовка завершается ошибкой.

Дополнительные сведения о SCP и его настройке см. в документации по Microsoft Entra.

Предлагаемое решение

Убедитесь, что группа удостоверений существует SCP для всех целевых лесов.

Сетевое подключение Azure не работает

Подготовка облачных компьютеров блокируется, если связанное сетевое подключение Azure (ANC) не работает.

AnC обновляется каждые шесть часов. Подготовка завершается ошибкой, если обновление ANC завершается ошибкой во время подготовки.

Предлагаемое решение

Убедитесь, что ANC работоспособен и повторите подготовку.

Ошибка выделения диска

Windows 365 подготовил облачный компьютер, но не выделил полное хранилище ОС в соответствии с тем, что пользователь должен был получить на основе

назначенной лицензии Windows 365. В результате пользователь не может видеть или использовать полное хранилище, которое им было назначено.

Предлагаемое решение

Повторная подготовка.

Сбой присоединения к домену

Windows 365 не удалось присоединить облачный компьютер к домену локальная служба Active Directory (AD). Многие факторы могут вызвать этот сбой.

- Убедитесь, что домен AD, подразделение (подразделение) и учетные данные в связанном ANC верны.
- Убедитесь, что пользователь присоединения к домену имеет достаточные разрешения для присоединения к домену.
- Убедитесь, что виртуальная сеть и подсеть могут правильно связаться с контроллером домена.

`JsonADDomainExtension` — это функция Azure, используемая для присоединения к этому домену. Убедитесь, что все, что требуется для присоединения к этому домену, выполняется успешно.

Предлагаемое решение

Подключите виртуальную машину Azure к настроенной виртуальной сети и выполните присоединение к домену с помощью предоставленных учетных данных.

Сбой гибридного соединения Microsoft Entra

Windows 365 не выполняет функцию гибридного соединения Microsoft Entra для клиента. Гибридное соединение Microsoft Entra должно быть настроено и работоспособно в качестве необходимых компонентов для облачного компьютера.

Если подготовка завершается сбоем из-за гибридного соединения Microsoft Entra, скорее всего, из-за недостаточного периода синхронизации, настроенного в службе синхронизации AD. Убедитесь, что Microsoft Entra Connect настроена для синхронизации объектов компьютеров AD каждые 30 минут и не более 60 минут. Этот шаг истекает, если объект Microsoft Entra не отображается в течение 90 минут.

Еще одним фактором, который следует учитывать, является ваше локальное время репликации AD. Убедитесь, что контроллер домена, используемый для Windows 365, реплицируется достаточно быстро, чтобы сделать его в идентификатор Microsoft Entra ID в течение этого пятичасового периода ожидания.

Если ваша организация использует службы федерации Active Directory (AD FS) (ADFS), этот процесс регистрации оптимизирован и может привести к тому, что подготовка облачных ПК выполняется быстрее, чем может быть выполнена синхронизация Microsoft Entra Connect.

Предлагаемое решение

Проверьте, является ли объект AD:

- Отображается в правильном подразделении.
- Успешно синхронизируется с идентификатором Microsoft Entra, прежде чем время ожидания подготовки.

Сбой регистрации в Intune

Windows 365 выполняет регистрацию управления мобильными устройствами (MDM) в Intune.

Если регистрация Intune завершается ошибкой, убедитесь, что:

- Все необходимые конечные точки Intune доступны в виртуальной сети облачных компьютеров.
- В клиенте нет ограничений на регистрацию MDM. Регистрация корпоративных устройств Windows разрешена в пользовательских политиках и политиках по умолчанию.
- Клиент Intune активен и работоспособен.
- Если совместное управление облачными компьютерами с Intune и Configuration Manager, убедитесь, что подразделение cloud PC не предназначено для принудительной установки клиента. Вместо этого разверните агент Configuration Manager из Intune. Дополнительные сведения см. в разделе "Методы установки клиента" в Configuration Manager.

Предлагаемое решение

Попробуйте выполнить регистрацию Intune с помощью тестового устройства или виртуальной машины.

Лицензия не найдена

Во время подготовки пользователь удалил лицензию на Windows 365.

Предлагаемое решение

Убедитесь, что у пользователя есть действительная лицензия.

Ошибка разрешений локального администратора

Windows 365 подготовил облачный компьютер, но не предоставил пользователям разрешения локального администратора, как определено политикой параметров пользователя. В результате пользователь не будет администратором на облачном компьютере. Таким образом, они не могут вносить изменения на уровне системы или устанавливать приложения в контексте системного уровня.

Предлагаемое решение

Повторите подготовку или создайте новую политику параметров пользователя.

Ошибка оптимизации Microsoft Teams

Windows 365 подготовил облачный компьютер. Однако он не настроил облачный компьютер для использования Microsoft Teams в режиме, оптимизированном для запуска на удаленной виртуальной машине. Эта оптимизация не устанавливает Microsoft Teams и все его компоненты. Он задает только конфигурацию, которая вступает в силу при установке Microsoft Teams на облачном компьютере. Если эта оптимизация не задана, и Microsoft Teams устанавливается на этом устройстве, Microsoft Teams не выполняется в оптимизированном режиме для удаленных подключений.

Предлагаемое решение

Повторная подготовка.

Недостаточно доступных IP-адресов

При предоставлении подсети ANC убедитесь, что есть более чем достаточно IP-адресов.

Каждый процесс подготовки облачных компьютеров использует один из IP-адресов, предоставленных в диапазоне.

Если подготовка завершается ошибкой, она выполняется в общей сложности в три раза. Каждый раз выделяется новая виртуальная карта и IP-адрес. Эти IP-адреса выпускаются в часах, но это выделение может вызвать проблемы, если адресное пространство слишком узко.

Предлагаемое решение

Проверьте виртуальную сеть на наличие доступных IP-адресов и убедитесь, что для успешного выполнения процесса повторных попыток доступно более чем достаточно IP-адресов.

Политика подготовки не найдена

Во время подготовки кто-то удалил политику подготовки.

Предлагаемое решение

Убедитесь, что политика подготовки доступна и назначена правильной группе пользователей.

Запрос запрещен политикой

Windows 365 использует виртуальную сеть, предоставляемую клиентом, для выполнения приема виртуальных сетевых карт из облачного компьютера в виртуальную сеть клиента. Иногда предприятие реализует Политика Azure, чтобы ограничить создание определенных объектов Azure. Убедитесь, что нет политик Azure, которые могут ограничить создание объектов Azure от имени Windows 365.

Предлагаемое решение

Просмотр **политики в портал Azure и поиск любых событий политики**, останавливающих службу Windows 365 от подготовки облачного компьютера.

ошибка меню значков питания

Windows 365 подготовил облачный компьютер, но не скрывал значки завершения работы и перезапуска в меню . В результате пользователь видит значки завершения работы и перезапуска в меню . Если пользователь завершает подключение к облачному компьютеру, выбрав значок завершения работы, может потребоваться перезапустить облачный компьютер на портале Cloud PC, прежде чем снова подключиться.

Предлагаемое решение

Повторите подготовку или создайте политику конфигурации устройства, чтобы скрыть кнопку завершения работы и скрыть кнопку перезапуска.

Поддерживаемые регионы Azure для облачных компьютеров, не перечисленные в пользовательском интерфейсе подготовки

Если определенный регион не указан в пользовательском интерфейсе подготовки облачных компьютеров, но указан в документации по требованиям Windows 365, Windows 365 может развернуться в новом регионе. Если сетевая инфраструктура находится в таком регионе, выберите **новый запрос на поддержку, чтобы открыть запрос** в службу поддержки для оценки.

Ошибка перенаправления часового пояса

Windows 365 подготовил облачный компьютер, но не настроил перенаправление часового пояса. В результате пользователь не видит локальное время, отражаемое при подключении к облачному компьютеру. Вместо этого они видят стандартное время в формате UTC.

Предлагаемое решение

Повторите подготовку или создайте объект групповой политики с **настроенной политикой разрешения перенаправления часового пояса** . Чтобы узнать больше о политике, скачайте справочную таблицу параметров групповой политики.

Не удалось найти пользователя.

Во время подготовки пользователь удалил связанного пользователя.

Предлагаемое решение

Убедитесь, что назначенная учетная запись пользователя действительна.

Ошибка сброса Windows

Windows 365 подготовил облачный компьютер, но не отключил встроенный параметр сброса Windows. В результате пользователь может вручную активировать встроенный параметр сброса Windows в разделе "**Параметры**". Облачный компьютер никогда не завершит сброс, что делает облачный компьютер непригодным для использования.

Предлагаемое решение

Повторная подготовка.

Блокировка портов высокого риска: не удалось отключить один или несколько портов высокого риска

Windows 365 подготовил облачный компьютер, но не удалось заблокировать все порты высокого риска на основе стандартов безопасности Майкрософт. Windows 365 отключает порты с высоким риском, используемые для управления ресурсами или незащищенной или незашифрованной передачи данных и не должны предоставляться в Интернете по умолчанию.

Если вы получите эту ошибку, некоторые факторы, которые следует учитывать:

- Иногда предприятие реализует групповую политику Intune, которая включает один из этих портов по умолчанию.
- Убедитесь, что нет политик Intune, которые могут переопределить значение по умолчанию Windows 365, чтобы отключить эти порты с высоким риском.

Предлагаемое решение

Попробуйте любое из этих решений:

- Повторная подготовка.
- Если устройство зарегистрировано в Intune, можно применить политику Intune, чтобы отключить порты.

- Пользователь также может отключить порты вручную, добавив локальное правило брандмауэра на свое устройство. Список портов с высоким риском, рекомендуемых для блокировки, см. в правилах администратора безопасности в Azure виртуальная сеть Manager.

Другие сбои подготовки

Если вы столкнулись с другими ошибками подготовки, не описанными ранее, убедитесь, что все необходимые конечные точки разрешены в виртуальной сети, используемой для AC и любого устройства шлюза.

Следующие шаги

Устранение неполадок с Windows 365.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Устранение неполадок соединителей партнеров в Windows 365

Статья • 20.01.2025

В этой статье приведены некоторые действия по устранению неполадок и возможные решения проблем, связанных с соединителями партнеров в Windows 365.

Устранение неполадок при установке агента партнера

При включении соединителя партнера (Citrix HDX Plus, Omnissa Horizon или HP Anyware) для пользователя агент партнера автоматически устанавливается на облачных компьютерах этого пользователя. Агент включает соответствующий сторонний протокол.

Если при установке возникла проблема, в **списке "Все облачные компьютеры** " появится сообщение об ошибке, предоставив рекомендации по устранению ошибки.

Несмотря на сбой установки, пользователь по-прежнему может подключиться к облачному компьютеру с помощью удаленного рабочего стола.

Действия по устранению неполадок

При устранении ошибки убедитесь, что следующие действия выполняются успешно.

- Состояние лицензии пользователя синхронизируется с партнерской службой с Microsoft Intune, включая идентификатор пользователя Microsoft Entra.
  - Необходимые условия выполнены.
  - Соединитель партнера включен и работоспособен в Microsoft Intune.
  - Правильные разрешения задаются для сторонних приложений партнера в идентификаторе Microsoft Entra.
  - Пользователь Microsoft Entra добавляется и обнаруживается в консоли Partner Cloud.
- Агент партнера скачан на облачном компьютере.
  - Облачный компьютер может получить доступ к URL-адресам для скачивания партнеров.

    - Политика безопасности не блокирует PowerShell или установку приложения или агента как **system**.
- Агент партнера установлен.
    - Проверьте **приложения и компоненты** , чтобы узнать, установлен ли агент партнера на облачном компьютере.
    - Проверьте журналы Windows Просмотр событий (**eventvwr.msc**), чтобы убедиться, что установка агента выполняется.
    - Проверьте журналы установки для любых сбоев:
        - Citrix: **%TEMPsystemdrive%\Windows\Temp\Citrix\XenDesktop Installer**
        - Omnissa Horizon:
            - Проблемы с установкой: **C:\Windows\Temp\Omnissa_Horizon_Agents_Installer_**.log**.
            - Выполните этот скрипт для сбора журналов для проблем после установки: **C:\Program Files\Omnissa\Horizon Agent\Horizon Agent\DCT\support.bat**.
        - HP Anyware:
            - **C:\Teradici\provisioning.log**.
            - Или выберите " **Создать пакет** поддержки" на стороне клиента.
- Облачный компьютер зарегистрирован в клиенте облака партнера.
    - Проверьте состояние регистрации облачного компьютера в консоли конфигурации партнера.
    - Если облачный компьютер не зарегистрирован, проверьте **события входа приложения** в Windows Просмотр событий (**eventvwr.msc**) для ошибок и предупреждений службы партнеров.

После поиска основной причины удалите назначенную лицензию из консоли партнера, а затем добавьте лицензию обратно, чтобы активировать переустановку агента партнера.

> ⓘ **Примечание**
>
> Если другое решение не работает, вы можете **повторно представить** облачный компьютер для повторного просмотра включения. Повторное создание удаляет облачный компьютер и создает новый. Все данные на исходном облачном компьютере будут потеряны. Таким образом, повторная подготовка должна быть последним способом для устранения проблемы.

Устранение неполадок с подключением

Если у вас возникли проблемы с подключением к облачному компьютеру, подготовленному партнером, проверьте подключение на основе RDP по умолчанию, чтобы определить, связана ли проблема с облачным компьютером или подключением партнера.

Включение протокола удаленного рабочего стола (RDP)

Если протокол партнера включен, удаленный протокол Windows 365 по-прежнему включен, но неактивен. Это неактивность означает, что пользователи, пытающиеся подключиться к клиентам удаленного рабочего стола Под управлением Windows 365 (включая браузер HTML5), блокируются по умолчанию. Пользователи могут подключаться только с помощью протокола партнера. Пользователи, пытающиеся подключиться к клиентам, не являющихся партнерами, получают универсальное сообщение об ошибке.

Вы можете включить протокол RDP, чтобы пользователи могли войти в систему с помощью RDP, чтобы проверить подключение к облачному компьютеру. Протокол RDP можно включить следующими способами:

- Создание пользователя локального администратора на облачном компьютере.
- Добавление пользователя в группу пользователей Direct Access на облачном компьютере.

После выполнения любого из этих действий может потребоваться перезапустить облачный компьютер, чтобы обновления членства в группе вступили в силу. Затем пользователь может подключиться с помощью протокола RDP или партнера.

Теперь вы можете проверить подключение с помощью RDP и вызвать обращение в службу поддержки с соответствующей группой поддержки, если проблемы сохраняются.

Следующие шаги

- Дополнительные сведения о Citrix HDX Plus для Windows 365 см. в статье Настройка Citrix HDX Plus для Windows 365 Корпоративная.
- Дополнительные сведения о HP Anyware для Windows 365 см. в статье Настройка HP Anyware для Windows 365 Корпоративная.
- Дополнительные сведения о Omnissa Horizon для Windows 365 см. в разделе "Настройка Omnissa Horizon для Windows 365 Корпоративная".

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Устранение неполадок синхронизации пользовательского интерфейса для Windows 365 Frontline в общем режиме.

В этой статье приведены инструкции по устранению неполадок, связанных с синхронизацией взаимодействия пользователей в средах общего режима Windows 365 Frontline.

Пользователи получают предупреждение о временном изменении пользовательского опыта.

Когда пользователь входит в систему, Windows может уведомить их о том, что они вошли с помощью временного профиля вместо обычного профиля пользователя. В Windows также отображается другое уведомление о том, что "Мы не можем войти в свою учетную запись". В результате у пользователя есть временный интерфейс пользователя.

> ⓘ **Примечание.**
>
> Временный профиль: это непостоянный профиль пользователя Windows, который создает Windows, когда система не может загрузить или создать обычный профиль пользователя Windows. Временный профиль предоставляет основные функциональные возможности, но любые изменения, внесенные во время сеанса (например, изменения параметров, изменения файлов или настроек), удаляются при выходе пользователя. Пользователи видят уведомление о том, что они вошли с помощью временного профиля, а их классическое меню и меню "Пуск" используют параметры Windows по умолчанию вместо персонализированной конфигурации.

Чтобы начать устранение этой проблемы, проверьте состояние отдельного хранилища пользователя, как описано в следующих разделах.

Не удалось подключить хранилище отдельного пользователя к их сеансу

Во время процесса входа в Windows пользователи следуют одному из двух потоков:

- Создание и присоединение нового отдельного хранилища пользователей
- Присоединение существующего хранилища отдельных пользователей

Оба процесса требуют, чтобы служба подключила диск к облачному компьютеру во время входа пользователя. Сбои вложений являются редкими, но могут возникать, когда хранилище пользователей в пуле превышает ограничение хранилища.

Хранилище пользователей в пуле превысило установленный лимит.

Синхронизация пользовательского опыта предоставляет ограниченное количество общего пользовательского хранилища в пуле в зависимости от расчета объема хранилища.

Понимание ограничений пулового хранилища

Каждая политика подготовки определяет ограничение хранилища пользователей в пуле, вычисляемое с помощью следующей формулы:

Общее хранилище в пуле = размер диска ОС × количество подготовленных облачных компьютеров

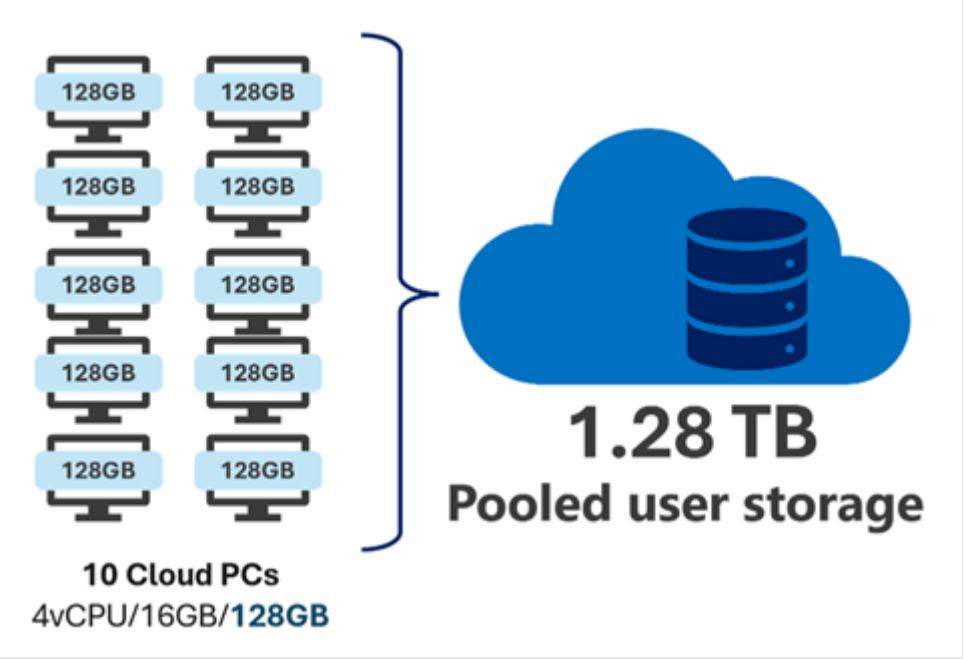


Рис. 1. Вычисление хранилища в пуле на основе размера и количества облачных компьютеров

Обычное потребление хранилища

В обычных условиях резервное хранилище пользователей расходуется по мере создания пользователями отдельных хранилищ. Когда хранилище достигает емкости:

- **Общий размер** и **используемый размер** равны
- **Доступный размер** : **0 ГБ**

- Вкладка "**Хранилище пользователей**" отображает эти метрики в политике подготовки

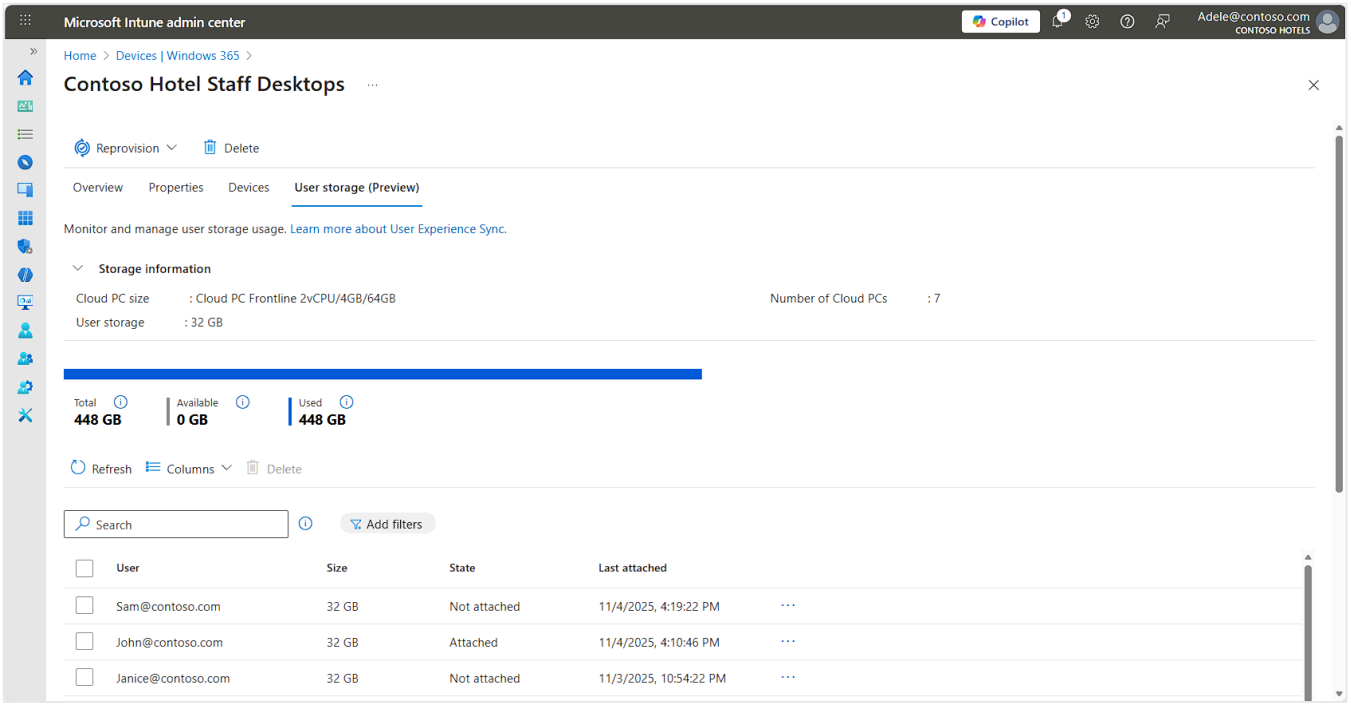


Рис. 2. Общее пользовательское хранилище, достигло предела установленной политики

Превышены условия хранения

Если емкость хранилища пользователей в пуле близка к полному заполнению и несколько пользователей одновременно входят в систему, все пользователи успешно входят в систему и создают свое индивидуальное хранилище. Этот процесс приводит к состоянию превышения со следующими характеристиками:

- **Используемый размер** становится **большеобщего размера**
- **Доступный размер** остается **0 ГБ**
- Появится новое свойство "**Превышено** ", показывающее объем, превышающий ограничение политики.

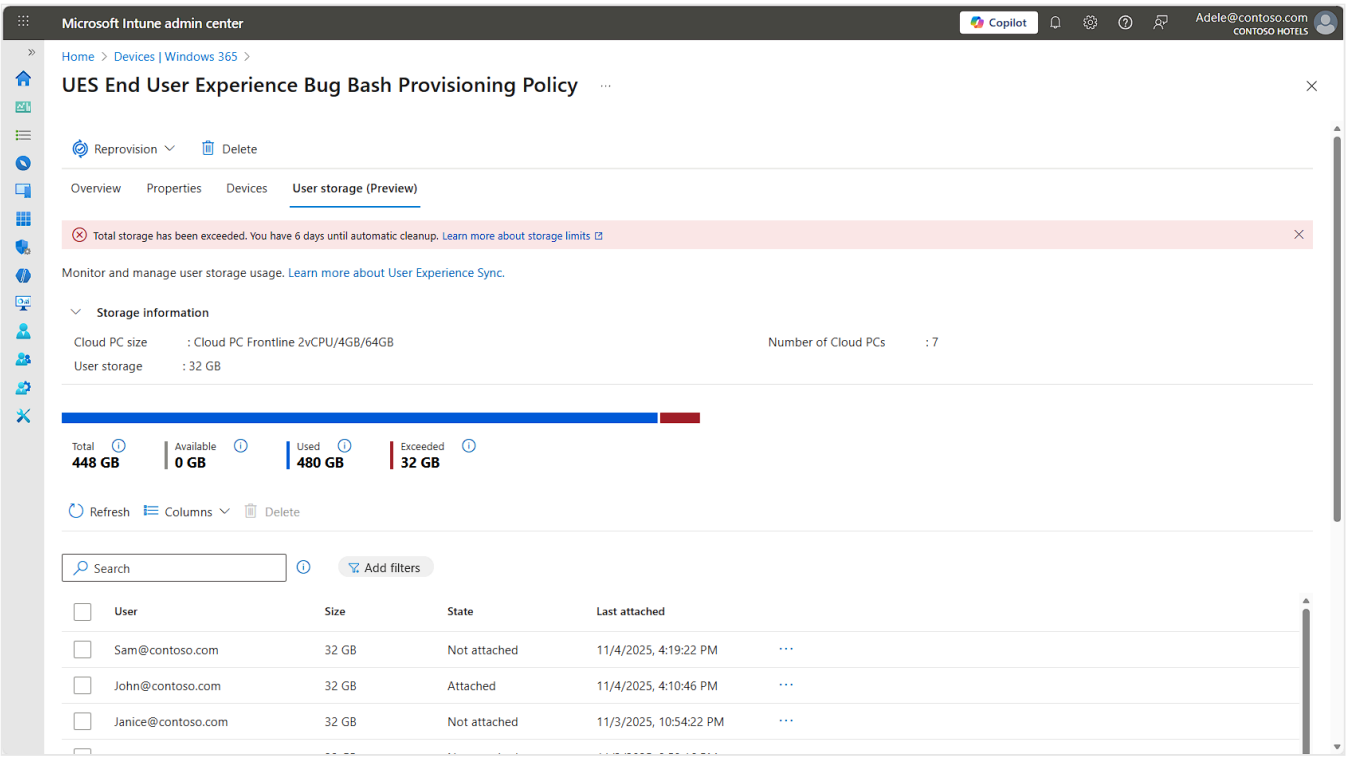


Рис. 3. Хранилище пользователей в пуле, превышающее ограничение политики

Превышен период допустимости

Если объединённое хранилище пользователей превышает свой предел, политика предоставления переходит в период терпимости, чтобы предотвратить дальнейший рост хранилища. В течение этого периода:

- **Длительность**: период допустимости длится **в течение 7 дней** после первого возникновения превышенного условия.
- **Влияние на пользователей**: существующие пользователи, имеющие индивидуальное хранилище, могут продолжать входить и получать доступ к персонализированному пользовательскому опыту.
- **Новые ограничения пользователей: новые пользователи**, пытающиеся войти в систему, получают временный интерфейс пользователя, пока не будет освобождено хранилище.
- **Действия администратора**. Вручную удалите отдельное хранилище пользователей или увеличьте количество облачных компьютеров для назначения.
- **Автоматическое разрешение**: если использование хранилища снижается ниже предела в период допустимости, обычные операции немедленно возобновляются.

После истечения семидневного периода допустимости:

- **Защита службы**: служба начинает удалять отдельное хранилище пользователей, начиная с самого старого (на основе последней метки времени подключения).

Количество хранилища отдельных пользователей, которое удаляется, определяется объемом необходимого пространства для соблюдения лимита политики.

> ⓘ **Примечание.**
>
> Регулярно отслеживайте использование хранилища и настраивайте оповещение о ограничениях службы синхронизации взаимодействия с пользователем Frontline Cloud PC , чтобы избежать достижения превышенного условия. Прежде чем достичь емкости, рассмотрите возможность увеличения объема хранилища, чтобы обеспечить непрерывное взаимодействие с пользователем.

Проблемы с нехваткой или заполнением хранилища у пользователей

Когда хранилище отдельных пользователей становится низким или полным, пользователи могут столкнуться с проблемами с производительностью или не смогут сохранить свою работу. Используйте следующие решения для решения ограничений хранения.

- Освобождение места в OneDrive
- Просмотр содержимого папки загрузки и удаления файлов и папок, которые не нужны
- Запустить Storage Sense вручную
- Удаление хранилища пользователей (администрирование)

  > ⚠ **Предупреждение**
  >
  > Удаление хранилища пользователей окончательно удаляет все пользовательские данные и параметры. Прежде чем продолжить, убедитесь, что пользователь создал резервные копии важных данных.

  Администраторы могут выполнить следующие действия, чтобы удалить хранилище пользователей с помощью портала управления Windows 365:

  1. Войдите в **Центр администрирования Microsoft Intune**.
  2. Перейдите к **Устройства**>**Windows 365**>**Политики подготовки**.
  3. Выберите соответствующую политику подготовки.
  4. Перейдите на вкладку "**Хранилище пользователей** ".
  5. Найдите хранилище пользователей для удаления.

6. Выберите "**Удалить** " и подтвердите действие.

Last updated on 18.11.2025

Устранение неполадок с приложение Windows 365

Статья • 20.01.2025

Эта статья поможет вам определить и решить проблемы с приложение Windows 365.

Ограничения

> **Примечание**
>
> В настоящее время приложение Windows 365 не поддерживается:
>
> - Windows 11 IoT
> - Настройка свойств протокола удаленного рабочего стола (RDP)

Ошибка "Не удается подключиться к облачному компьютеру"

При нажатии кнопки "**Подключиться" для подключения** к облачному компьютеру может появиться сообщение об ошибке "Не удается подключиться к облачному компьютеру".

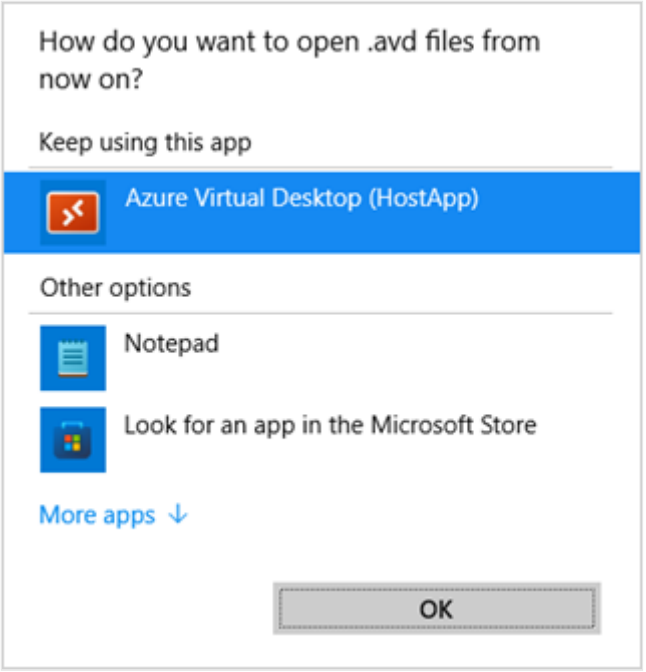
Чтобы устранить эту проблему:

1. **В приложении "Параметры"** на устройстве с Windows выберите **приложения по умолчанию.**>
2. **Найдите ведущее приложение** AVD и обновите приложение по умолчанию для `.avd` файлов.
3. Выполните следующую команду, чтобы очистить старый кэш клиента удаленного рабочего стола:

   ```
   reg delete "HKEY_CLASSES_ROOT\progF3672D4C2FFE4422A53C78C345774E2D" /f
   ```

Приложение Windows 365 запрашивает выбор нового приложения по умолчанию

При установке клиента удаленного рабочего стола может появиться сообщение об сопоставлении типов файлов после попытки подключиться к облачному компьютеру. Выберите параметр "Виртуальный **рабочий стол Azure" (HostApp),** чтобы запустить сеанс облачного компьютера.



Изменение сеанса облачного пк с полноэкранного режима на режим окна

Приложение Windows 365 поддерживает режим окна для более эффективной работы параллельно с локальным компьютером. Чтобы активировать режим окна, нажмите кнопку "**Режим** окна" на панели подключения.

В приложение Windows 365 не отображаются облачные компьютеры

Если приложение Windows 365 не отображает облачные компьютеры, вы можете войти с неправильной учетной записью пользователя. Убедитесь, что вы войдите с учетной записью, зарегистрированной в учетной записи Microsoft Entra, которая подготовлена для облачных компьютеров.

Следующие шаги

Дополнительные сведения о приложение Windows 365 см. в разделе "Установка приложение Windows 365".

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Известные проблемы Windows 365 BCDR

17.10.2025

В этой статье рассматривается известная проблема, связанная с сценариями непрерывности бизнес-процессов Windows 365 и аварийного восстановления (BCDR).

Классический Outlook поврежден после дисастера восстановления переключения на резервный сервер или возврата на основной сервер.

После восстановления облачного компьютера из моментального снимка в процессе аварийного восстановления при переключении на резервный сервер или при возврате после аварии в основной регион пользователи могут столкнуться с сообщением о технической ошибке при запуске классического Outlook.

Эта проблема возникает из-за повреждения автономного кэша Outlook, так как клиент и сервер оказываются без синхронизации во время резервного переключения. Клиент на моментальном снимке отражает прошлое состояние относительно текущего состояния сервера. Процесс повторной синхронизации файла автономной таблицы хранилища (OST) может занять время.

Этот процесс не приводит к потере данных.

Обходной путь

После завершения операции переключения на резерв или возврата после восстановления удалите OST-файл компьютера в облаке.

Это действие заставляет Outlook перестроить индекс поиска и автономный кэш почтового ящика. Этот процесс не приводит к потере данных.

Резолюция

Используйте новое приложение Outlook. Новое приложение Outlook использует другой механизм кэширования, который устраняет эту проблему синхронизации.

Устранение неполадок загрузки Windows 365

Статья • 20.01.2025

В этой статье приведены инструкции по устранению неполадок, возникающих при настройке или управлении устройствами загрузки Windows 365.

Пользователь не может получить доступ к облачному компьютеру с физического устройства загрузки Windows 365

Если пользователь не может получить доступ к облачному компьютеру с физического устройства Windows 365 Boot, попробуйте выполнить следующие действия.

1. Проверьте, можно ли войти на облачный компьютер с помощью одного из следующих вариантов:
   - Перейдите к Windows 365.
   - Приложение Windows на другом устройстве (не windows 365 Boot).
2. Если у пользователя несколько облачных компьютеров, убедитесь, что они выбрали облачный компьютер по умолчанию для использования при каждом входе. Чтобы задать этот параметр по умолчанию, выполните указанные ниже действия.
   a. Перейдите к Windows 365.
   b. В карточке для облачного компьютера, который вы хотите задать в качестве значения по умолчанию, выберите многоточие (...) >Параметры.
   c. На вкладке "Интегрированные **возможности" в разделе "Загрузка на этот облачный компьютер" выберите "Подключиться" во время входа на устройство.**
   d. Выберите **Сохранить**.
3. Если вы можете войти на облачный компьютер из приложения или интернета, а облачный компьютер по умолчанию установлен, то возникла проблема с физическим устройством загрузки Windows 365. В этом случае убедитесь, что физическое устройство настроено правильно и имеет необходимые версии программного обеспечения. Дополнительные сведения см. в статье о требованиях к физическому устройству загрузки Windows 365.
4. Администраторы могут попытаться вручную выбрать **синхронизацию** устройств, чтобы получить политики, доставленные быстрее на устройстве. Пользователи могут попытаться перезапустить устройство.

Конфигурация раздела реестра физических устройств

Убедитесь, что физическое устройство правильно настроено для запуска загрузки Windows 365, задав следующие разделы реестра:

Развернуть таблицу

Имя раздела реестра	Имя параметра реестра	Значение реестра
HKLM\Software\Microsoft\PolicyManager\current\device\CloudDesktop	BootToCloudMode	1
HKLM\Software\Microsoft\PolicyManager\current\device\WindowsLogon	ПереопределениеShellProgram	1
HKLM\Software\Microsoft\Windows\CurrentVersion\SharedPC\NodeValues	18	1
HKLM\Software\Microsoft\Windows\CurrentVersion\SharedPC\NodeValues	01	1

Физические версии устройств Windows 365, приложения виртуального рабочего стола Azure и Windows

Для загрузки Windows 365 требуется, чтобы физическое устройство запускал определенные версии приложений Windows 365 и Виртуального рабочего стола Azure (HostApp). Чтобы проверить установленные версии, выполните следующий командлет PowerShell от имени администратора:

Azure PowerShell

```
Get-AppxPackage -AllUsers -name *MicrosoftCorporationII*
```

Этот командлет отображает все поддерживаемые Корпорацией Майкрософт приложения (например, QuickAssist и Microsoft Family) на физическом устройстве. Чтобы убедиться, что загрузка Windows 365 работает правильно, подтвердите следующие версии:

- Приложение Windows версии 2.0.285 или более поздней версии.
- Приложение Виртуального рабочего стола Azure (HostApp) версии 1.2.4159 или более поздней версии.
- Последняя версия Windows 11.

Удаление и добавление загрузки Windows 365 на физическое устройство снова

Если вы не можете определить источник проблемы, попробуйте удалить и добавить Windows 365 Boot на физическое устройство еще раз.

Удаление загрузки Windows 365 с физического устройства

1. Войдите в Центр администрирования Microsoft Intune и выберите **группы**>**"Все группы"**.

2. Выберите группу для устройств загрузки Windows 365 и выберите "**Участники**".
3. Выберите физическое устройство и нажмите кнопку "**Удалить>да**".
4. Выберите "**Все устройства**">, выберите физическое устройство и выберите "**Синхронизация обзора**".>

Удаление займет около 10 минут. После этого физическое устройство больше не будет настроено для загрузки Windows 365.

Добавление загрузки Windows 365 обратно на физическое устройство

1. Войдите в Центр администрирования Microsoft Intune и выберите **группы**>"**Все группы**".
2. Выберите группу для устройств загрузки Windows 365 и выберите "**Участники**".
3. Выберите "**Добавить участников**" и выберите физическое устройство.
4. Подождите около 10 минут.
5. Выберите "**Все устройства**">, выберите физическое устройство и выберите "**Синхронизация обзора**".>

Физическое устройство снова будет настроено для загрузки Windows 365. Повторите тестирование, чтобы узнать, работает ли он.

Обращение в службу поддержки Майкрософт

Если проблемы по-прежнему не удается устранить, обратитесь в службу поддержки Майкрософт. Чтобы ускорить решение, заранее соберите журналы и идентификаторы сеансов.

Сбор локальных журналов

Сбор сведений журнала идентификатора Windows 365 и Microsoft Entra ID из следующих расположений:

- **C:\Users\{username}\AppData\Local\Temp\DiagOutputDir\Windows365\Logs**
- **C:\Users\{username}\AppData\Local\Temp\DiagOutputDir\RdClientAutoTrace**

Поместите эти журналы в ZIP-файл и предоставьте его группе поддержки Майкрософт для дальнейшего изучения.

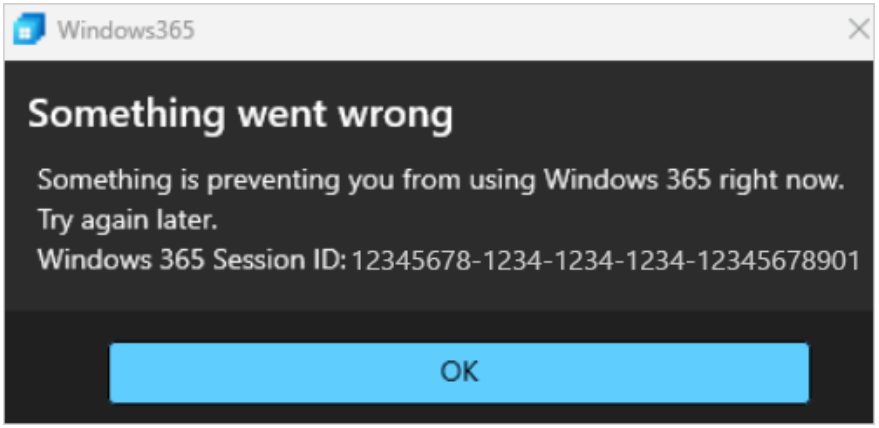
Ошибки и идентификаторы сеансов Windows 365

При обращении в службу поддержки Майкрософт о проблемах загрузки Windows 365 соберите соответствующие идентификаторы, чтобы помочь в расследовании.

На физическом устройстве получите Значение CorrelationId, SessionID или ActivityID.

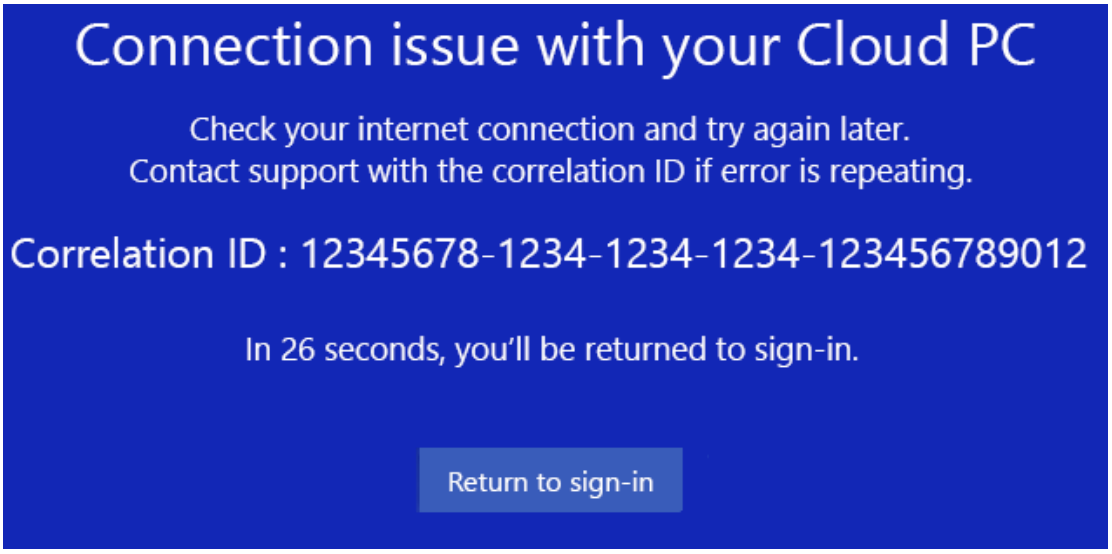
ИД сеанса

Идентификатор сеанса Windows 365 можно найти в диалоговом окне ошибки. Например, диалоговое **окно ошибки "Что-то пошло не так** ".



Идентификатор корреляции

Идентификатор корреляции можно найти на промежуточном экране, отображаемом в течение пятиминутного времени ожидания.



Следующие шаги

Дополнительные сведения о загрузке Windows 365 см. в статье "Что такое загрузка Windows 365?".

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Известные проблемы с загрузкой Windows 365

Статья • 20.01.2025

В этой статье приводятся решения недавних известных проблем с загрузкой Windows 365.

Подключение Wi-Fi

Подключения Wi-Fi, требующие проверки подлинности на основе браузера или согласия, не поддерживаются.

Профили Wi-Fi на основе пользователей, для которых пользователь должен войти в систему, чтобы подключиться к Wi-Fi, не поддерживаются. Новые пользователи, которые никогда не вошли перед преобразованием устройства в устройство загрузки Windows 365, не могут использовать устройство для подключения к сети.

Поддержка VPN

Загрузка Windows 365 поддерживает только VPN-клиенты, для которых не требуется установка приложения. VPN-клиенты на основе приложений, требующие входа пользователей, не поддерживаются, так как пользователи не могут взаимодействовать с VPN-клиентом с устройства загрузки Windows 365.

Выход из сеанса в спящий режим или закрытие устройства

Пользователь не полностью выписывается после закрытия крышки ноутбука. Когда они открывают ноутбук, они видят черный экран или приложение пытается отключиться. В конечном итоге он подписывает пользователя из сеанса.

Повторяющиеся диалоги для некоторых сочетаний клавиш и липких клавиш

Повторяющиеся диалоги могут отображаться для физического устройства и облачного компьютера. Эта проблема может возникнуть для:

- Некоторые сочетания клавиш, такие как Win+G или липкие клавиши.
- Включение параметров ключа специальных возможностей, таких как высокая контрастность, клавиши Num или переключатель ключей.

Загрузка Windows 365 не поддерживается в режиме киоска

Загрузка Windows 365 в настоящее время не поддерживается в режиме киоска в Windows.

Ограниченный доступ к физическому устройству

Загрузка Windows 365 не полностью ограничивает доступ пользователя к физическому устройству. Дополнительные сведения см. в разделе "Ограничение доступа пользователей к физическому устройству с Windows 365".

Другие параметры входа, кроме имени пользователя и пароля, отображаются на экране входа

Загрузка Windows 365 используется с поставщиком службы конфигурации общего компьютера (CSP). Основной поддерживаемый метод входа — имя пользователя или пароль.

Решение

Если вы включили Windows Hello для бизнеса для устройства загрузки Windows 365, вы можете отключить его с помощью Microsoft Intune. Дополнительные сведения см. в разделе "Включение ключей безопасности для входа в Windows".

Если физическое устройство загрузки Windows 365 позволяет пользователям входить с помощью удобного ПИН-кода, вы можете отключить его. Дополнительные сведения см. в разделе AllowPINLogon.

Поставщик учетных данных по умолчанию имеет значение "Ключ безопасности" на

экране входа

Если включен параметр политики использования ключей безопасности для входа, он может быть поставщиком учетных данных по умолчанию. Эта политика может привести к тому, что пользователь видит вход для физического устройства.

Решение

Проверьте, настроен ли параметр политики в Microsoft Intune. Дополнительные сведения о том, как проверить, см. в разделе "Включение ключей безопасности для входа в Windows".

Если он задан, исключите устройства загрузки Windows 365 из политики.

Локальное устройство имеет фоновые приложения и предыдущие конфигурации политик, влияющие на загрузку Windows 365 пользователя

Загрузка Windows 365 использует "чистые" устройства с Windows 11, которые не имеют предварительно настроенных приложений или политик, назначенных устройству.

Решение

Сбросьте устройство в состояние "очистки". Дополнительные сведения см. в статье о требованиях к физическому устройству загрузки Windows 365.

Пользователи единого входа видят диалоговое окно, чтобы разрешить подключение к удаленному рабочему столу во время попытки подключения

При использовании единого входа пользователям предлагается пройти проверку подлинности в идентификаторе Microsoft Entra и разрешить подключение к удаленному рабочему столу при запуске подключения к новому облачному

компьютеру. Microsoft Entra запоминает до 15 устройств в течение 30 дней до запроса еще раз.

Решение

Если вы видите это диалоговое окно, нажмите кнопку "**Да** ", чтобы подключиться.

Пользователи не могут запустить веб-браузер для входа в сеть Wi-Fi.

Загрузка Windows 365 предназначена для подключений Ethernet или подключений Wi-Fi, управляемых через CSP Wi-Fi.

Решение

Настройте профиль Wi-Fi физического устройства Windows 365 через Microsoft Intune. Дополнительные сведения см. в разделе "Добавление параметров Wi-Fi для устройств Windows 10/11" в Microsoft Intune.

Пользователи видят черный экран после использования команды "Отключить/выйти из сети" и "Блокировка" на облачном компьютере

Эта известная проблема находится под следствием.

Решение

Нажмите клавиши CTRL + ALT+DEL **и выберите параметр выхода.**

Вызовы Microsoft Teams имеют низкую производительность

Решение

Убедитесь, что оптимизации Microsoft Teams используются, как описано в Microsoft Teams на облачном компьютере.

Доступ к камере запрещен на облачном компьютере

Разрешения камеры должны быть предоставлены приложению Виртуального рабочего стола Azure (HostApp), чтобы использовать камеру настроенного устройства Windows 365 в Microsoft Teams.

Решение

1. Удалите загрузку Windows 365 с физического устройства.
2. На физическом устройстве откройте **раздел "Параметры>конфиденциальности" и "Камера безопасности>">позволяет приложениям получать доступ к камере.**
3. Установите для **виртуального рабочего стола Azure (HostApp)** значение **On**.
4. Добавьте загрузку Windows 365 обратно на физическое устройство.

Пользователи по-прежнему могут взаимодействовать с функциями физического устройства, такими как параметры, диспетчер задач и уведомления

В настоящее время пользователи заблокированы доступом к большинству функций на физических устройствах с Windows 365. Однако для устранения неполадок некоторые функции не блокируются.

Решение

Сведения об ограничении доступа пользователей к физическому устройству см. в статье "Ограничение доступа пользователей к физическому устройству загрузки Windows 365".

Пользователи отключены от облачного компьютера после простоя в течение

слишком долгого времени

Физические устройства загрузки Windows 365 могут выйти из системы из-за политик простоя экрана, применяемых к физическому устройству или облачному компьютеру.

Решение

Чтобы использовать профиль конфигурации устройства Intune, измените или настройте политику CSP DeviceLock (MaxInactivityTimeDeviceLock). Внесите эти изменения как для физического устройства, так и для облачного компьютера.

Пользователи видят несколько диалоговых окон проверки подлинности, даже если включен единый вход

Решение

Проверьте политику подготовки Windows 365, связанную с облачным компьютером, чтобы узнать, включен ли единый вход . Если это не так, включите единый вход для политики подготовки. Это изменение политики требует повторной подготовки облачного компьютера.

Политики условного доступа также могут вызвать другие диалоги проверки подлинности. Дополнительные сведения см. в разделе "Устранение неполадок при входе с условным доступом".

При использовании единого входа пользователям предлагается:

- Проверка подлинности в идентификаторе Microsoft Entra.
- Разрешить подключение к удаленному рабочему столу при запуске подключения к новому облачному компьютеру.

Microsoft Entra запоминает до 15 устройств в течение 30 дней до запроса еще раз.

Если вы видите это диалоговое окно, нажмите кнопку "**Да** ", чтобы подключиться.

Пользователи видят черный экран после входа

Загрузка Windows 365 настраивается с помощью CSP CloudDesktop.

Решение

Если вы настроили устройство для загрузки Windows 365 с помощью сценария загрузки Windows 365:

1. Войдите в Центр администрирования Microsoft Intune и выберите **профили конфигурации устройств**>.
2. Найдите профиль конфигурации устройства, содержащий политику конфигурации загрузочного устройства Windows 365 в его имени.
3. Убедитесь, что конфигурация "Облачный рабочий стол" настроена с параметром **режима** загрузки Windows 365 для **включения windows 365 Boot Desktop**.
4. Выберите **состояние** назначения устройства и убедитесь, что политика конфигурации успешно применена к ней.
5. Если состояние регистрации не выполнено, см. статью "Устранение неполадок" в Microsoft Intune.

Если проблема сохранится, переустановите операционную систему физического устройства, как описано в требованиях к физическому устройству загрузки Windows 365.

Пользователи видят локальный компьютер при реагировании на диалоговые окна проверки подлинности

Загрузка Windows 365 настраивается с помощью CSP Windowslogon.

Решение

Если вы настроили устройство для загрузки Windows 365 с помощью сценария загрузки Windows 365:

1. Войдите в Центр администрирования Microsoft Intune, выберите >**профили конфигурации устройств**>.
2. Найдите профиль конфигурации устройства, содержащий политику конфигурации загрузочного устройства Windows 365 в его имени.
3. Убедитесь, что конфигурация "Вход в Windows" настроена с параметром "**Переопределение программы оболочки** " для **применения упрощенной**

оболочки.

4. Выберите **состояние** назначения устройства и убедитесь, что политика конфигурации успешно применена к ней.
5. Если состояние регистрации не выполнено, см. статью "Устранение неполадок" в Microsoft Intune.

Если проблема сохранится, переустановите операционную систему физического устройства, как описано в требованиях к физическому устройству загрузки Windows 365.

Сообщение об ошибке: Windows 365 не может подключиться к ресурсам, которые он использует для правильного выполнения

Решение

Проверьте сетевое подключение устройства и повторите попытку. Если вы используете сетевое подключение Azure (ANC) для облачного компьютера, проверьте состояние ANC, как описано в состоянии сетевого подключения Azure.

Дополнительные сведения см. в разделе "Устранение ошибок подключения к облачному компьютеру".

Сообщение об ошибке: что-то не позволяет использовать приложение Windows 365

Решение

Дополнительные сведения см. в разделе "Устранение неполадок с загрузкой Windows 365".

Пользователи не могут подключиться к облачному компьютеру и продолжать ждать на экране перехода

Решение

Убедитесь, что устройство имеет приложения, поддерживающие загрузку Windows 365.

Если приложения соответствуют минимальным требованиям к версии, соберите журналы диагностики и обратитесь в службу поддержки Майкрософт.

Сообщение об ошибке: сервер шлюза удаленных рабочих столов временно недоступен

Решение

Эта проблема может быть временной проблемой из-за перегрузки сети. Повторите вход после ожидания некоторого времени. Если проблема сохранится, соберите журналы диагностики и обратитесь в службу поддержки Майкрософт.

Сообщение об ошибке: необходимо назначить облачный компьютер

Начальная загрузка Windows 365 требует, чтобы для них были подготовлены Облачный компьютер Windows 365.

Решение

Создайте и назначьте политику подготовки Windows 365. Дополнительные сведения см. в разделе "Создание политик подготовки".

Экран ошибки возникает при первом входе пользователей на устройство

Этот экран ошибки возникает при удалении устройства, а затем повторной регистрации в режиме загрузки Windows 365. Исходная регистрация еще не завершила удаление.

Решение

Пользователи должны попробовать войти во второй раз на устройстве. В большинстве случаев они должны иметь возможность подключаться к их Облачный компьютер Windows 365. Если экран ошибки по-прежнему отображается, обратитесь в службу поддержки Майкрософт с отображаемым идентификатором корреляции.

Ресурсы, созданные в интерактивном сценарии загрузки Windows 365, отображаются как "не применимые" в Microsoft Intune

Ресурсы, созданные в интерактивном сценарии загрузки Windows 365, можно применить к обоим:

- Устройства, присоединенные к Microsoft Entra.
- Гибридные устройства, присоединенные к Microsoft Entra, в клиентах, где определенные рабочие нагрузки переключаются на Microsoft Intune. Для гибридных устройств, присоединенных к Microsoft Entra, необходимо переключить политики Обновл. Windows, конфигурацию устройства и рабочие нагрузки клиентского приложения в Microsoft Intune.

Решение

Сведения о том, является ли устройство гибридным присоединенным к Microsoft Entra, см. в разделе "Использование портал Azure". Если устройство присоединено к гибридному присоединению к Microsoft Entra, ознакомьтесь с рабочими нагрузками совместного управления, чтобы узнать, какие рабочие нагрузки настроены в вашей среде.

Пользователи не могут сбросить пароль на устройстве загрузки Windows 365

Если пользователю нужно сбросить пароль, на устройстве загрузки Windows 365 невозможно.

Решение

Пользователи должны сбросить пароль на другом устройстве, отличном от Windows 365.

Сообщение об ошибке: не удалось найти приложение поставщика

Пользователь пытается подключиться к облачному компьютеру, но получает следующее сообщение об ошибке:

> Не удается подключиться к облачному компьютеру с этого устройства
> Не удалось найти приложение поставщика. Попробуйте выполнить сход с другого устройства.
> Чтобы устранить эту проблему, обратитесь в службу поддержки.

Эта ошибка возникает в следующих сценариях:

- Приложение поставщика удаляется.
- Приложение поставщика недоступно или установлено на физическом устройстве конечного пользователя.
- Приложение поставщика устанавливается в области пользователя вручную перед настройкой устройства для загрузки.

Решение

Конечный пользователь может использовать один из следующих вариантов:

- Войдите с другого устройства.
- Дождитесь установки приложения на физическом устройстве.
- Обратитесь к ИТ-администраторам пользователя и попросите их отправить приложение на устройство.
- Если вы подозреваете, что приложение установлено в области пользователя, выполните следующие действия.

    1. Обратитесь к ИТ-администраторам пользователя, чтобы удалить устройство из режима загрузки, удалив его из группы устройств.
    2. Удалите приложение поставщика, установленное в области пользователя.
    3. Поместите устройство обратно в группу устройств в режиме загрузки (приложения области системы должны доставляться Microsoft Intune при

настройке с помощью интерактивного сценария).

Если проблема не исчезла, обратитесь в службу поддержки.

Не удается предоставить общий доступ к локальному экрану физического устройства при использовании Microsoft Teams на облачном компьютере

Если у пользователя есть локальный экран параметров (например, локальные параметры Bluetooth), открытый на физическом устройстве, он не может предоставить общий доступ к экрану на видеозвонке в Microsoft Teams.

Решение

Если пользователь должен предоставить общий доступ к локальному экрану параметров, используйте другое средство, например Быстрая поддержка.

Следующие шаги

Дополнительные сведения см. в разделе "Устранение неполадок с загрузкой Windows 365".

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Известные проблемы с Windows 365 Switch

22.05.2025

В этой статье приведены инструкции по устранению неполадок с последними известными проблемами с Коммутатором Windows 365.

Поддержка только одного облачного компьютера

В настоящее время Коммутатор Windows 365 поддерживает только один облачный компьютер с поддержкой коммутатора. Пользователь автоматически войдет в первый доступный облачный компьютер, поддерживаемый коммутатором, из списка назначенных облачных компьютеров. Чтобы войти в другой облачный компьютер, пользователи могут выбрать многоточие (...), выбрать облачный компьютер и выбрать **режим "Добавить в представление** задач". Одновременно в представление задач можно добавить только один облачный компьютер. Если вы пытаетесь закрепить несколько облачных компьютеров в представлении задач, они добавляются в стек. Например, если удалить первый добавленный облачный компьютер, второй будет его место. Так как в представлении задач отображается только первый добавленный облачный компьютер, мы не рекомендуем закреплять несколько облачных компьютеров в представлении задач.

Удаление или замена устаревшего облачного компьютера из представления задач

Если в представлении задач нет доступа к облачному компьютеру, его можно удалить и заменить.

Решение

1. Удалите приложение Windows.
2. Переустановите приложение Windows.
3. Нажмите кнопку "Добавить приложение **Windows в представление** задач" на облачном компьютере, который вы хотите добавить.

Ограниченные жесты

Некоторые жесты, такие как жесты с тремя пальцами, чтобы изменить приложения или жесты с четырьмя пальцами, чтобы открыть представление задач и показать рабочий стол, не поддерживаются на облачном компьютере. Эти жесты активируются на физическом устройстве. Поддерживаются все остальные обычные жесты Windows 11.

Параметры Bluetooth и оборудования не могут управляться с облачного компьютера

Облачные компьютеры не имеют аппаратных компонентов, таких как адаптеры Bluetooth. Пользователи не могут изменять параметры из приложения параметров облачного компьютера или быстрых параметров.

Решение

Пользователи должны вернуться на физическое устройство и изменить параметры в **приложении "Параметры** ".

Кнопка повторного подключения не работает

Если используется параметр повторного подключения в диалоговом окне сообщения об отключении, повторное подключение может не работать должным образом или привести к неиспользуемому сеансу облачного компьютера.

Решение

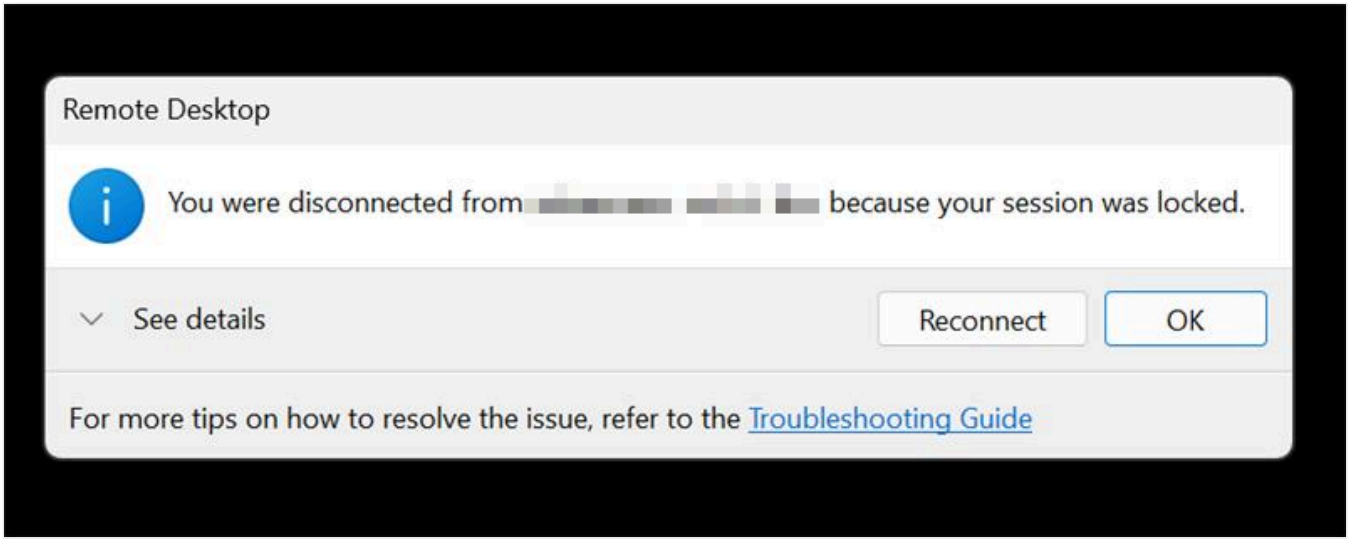
Пусть отключение завершится, а затем запустите новое подключение с помощью **представления** задач.

Отключение облачного компьютера во время работы на локальном компьютере

Облачные компьютеры, подключенные через **представление задач** Windows, тихо отключаются, чтобы избежать нарушения сеанса локального компьютера. В отключенном сеансе облачного компьютера отображается черный экран с полем сообщения.

Решение

При возникновении сообщения о возможности повторного подключения, можно повторно подключиться через окно сообщения, которое похоже на следующий снимок экрана:



Навигация между запросами входа и облачным компьютером

После выбора облачного компьютера в представлении задач пользователи могут получить запрос на вход с помощью учетных данных учетной записи. В некоторых сборках Windows после предоставления учетных данных пользователи могут не возвращаться к подключению к облачному компьютеру.

Решение

Снова нажмите кнопку "**Представление** задач" для облачного компьютера. Подключение продолжается в фоновом режиме. Пользователь должен быть подключен к облачному компьютеру в течение нескольких минут.

Локальный компьютер, отсутствующий в строке представления задач Cloud PC

Если локальный компьютер отсутствует в строке представления задач Cloud PC, виртуальный рабочий стол Azure (HostApp) может быть устаревшим.

Решение

Удалите и переустановите приложение Виртуального рабочего стола Azure (HostApp) из Microsoft Store.

Следующие шаги

Устранение неполадок с Windows 365

Получение журналов аудита Windows 365

Статья • 23.04.2025

Журналы аудита для Windows 365 содержат записи действий, приводящих к изменениям на облачном компьютере. Действия создания, обновления (редактирования), удаления, назначения и удаленные действия приводят к созданию событий аудита, которые администраторы могут просматривать для большинства действий облачных компьютеров, выполняющихся через Graph. По умолчанию аудит включен для всех клиентов. Отключить его невозможно.

У кого есть доступ к данным?

Пользователи со следующими разрешениями могут просматривать журналы аудита:

- Администратор службы Intune
- Глобальный администратор
- администраторы, которым назначена роль Intune с разрешениями **Данные аудита — чтение**.

> ⓘ **Важно!**
>
> Microsoft рекомендует использовать роли с наименьшим количеством разрешений. Это помогает повысить безопасность вашей организации. Глобальный администратор — это роль с высокими привилегиями, которую следует ограничивать экстренными сценариями, когда вы не можете использовать существующую роль.

Отправка журналов аудита Windows 365 в параметры диагностики в Azure Monitor

Параметры диагностики Azure Monitor позволяют экспортировать журналы платформы и метрики в выбранное место назначения. Вы можете создать до пяти различных параметров диагностики для отправки различных журналов и метрик в независимые назначения. Дополнительные сведения см. в статье Параметры диагностики в Azure Monitor.

Создание параметра диагностики для отправки журналов

1. Убедитесь, что у вас есть учетная запись Azure.
2. Войдите в Центр администрирования Microsoft Intune, выберите **Отчеты**>**Параметры диагностики** (в разделе **Azure Monitor**)>**Добавить параметры диагностики**.
3. В разделе **Журналы** выберите **Windows365AuditLogs**.
4. В разделе **Сведения о назначении** выберите назначение и укажите сведения.
5. Выберите **Сохранить**.

Использование API Graph и PowerShell для получения событий аудита

Чтобы получить события журнала аудита для клиента Windows 365, выполните следующие действия.

Установка пакета SDK

1. В PowerShell выполните команду `Install-Module Microsoft.Graph.Beta -Scope CurrentUser -AllowClobber`.
2. Проверьте установку, выполнив команду `Get-InstalledModule Microsoft.Graph.Beta`.
3. Чтобы получить все конечные точки Graph для облачного компьютера, выполните команду `Get-Command -Module Microsoft.Graph* *virtualEndpoint*`.

Вход

1. Выполните одну из следующих команд.

   - `Connect-MgGraph -Scopes "CloudPC.ReadWrite.All"`
   - `Connect-MgGraph -Scopes "CloudPC.Read.All"`

2. На открывшейся веб-странице войдите в свой клиент с помощью учетной записи пользователя, имеющей соответствующие разрешения на чтение и (или) запись.
3. Переключитесь на среду Graph (бета-версия) с помощью команды `Select-MgProfile -Name "beta"`.

Получение данных аудита

Просмотреть данные аудита можно несколькими способами.

Получение всего списка событий аудита, включая субъект аудита

Чтобы получить полный список событий аудита, включая субъект (пользователя, выполнившего действие), используйте следующую команду.

```
Get-MgBetaDeviceManagementVirtualEndpointAuditEvent | Select-Object -Property Actor,ActivityDateTime,ActivityType,ActivityResult -ExpandProperty Actor | Format-Table UserId, UserPrincipalName, ActivityType, ActivityDateTime, ActivityResult
```

Получение списка событий аудита

Чтобы получить список событий аудита без субъекта аудита, используйте следующую команду.

```
Get-MgBetaDeviceManagementVirtualEndpointAuditEvent
```

Чтобы получить все события, используйте параметр **-All**: `Get-MgBetaDeviceManagementVirtualEndpointAuditEvent -All`.

Чтобы получить только N первых событий, используйте следующие параметры: `Get-MgBetaDeviceManagementVirtualEndpointAuditEvent -All -Top {TopNumber}`.

Получение отдельного события по идентификатору события

Для получения одного события аудита вы можете использовать следующую команду, в которой необходимо указать {event ID}: `Get-MgBetaDeviceManagementVirtualEndpointAuditEvent -CloudPcAuditEventId {event ID}`

Дальнейшие действия

Непрерывность бизнес-процессов и аварийное восстановление

Обзор непрерывности бизнес-процессов и аварийного восстановления

Статья • 31.01.2025

Windows 365 предоставляет высокоустойчивые Облачные компьютеры для пользователей, в том числе:

- На 99,9 % высокодоступные пользовательские сеансы Облачных компьютеров Windows 365 согласно определению в соглашении об уровне обслуживания Windows 365 .
- Хранилище дисков с устойчивостью объектов данных "одиннадцать девяток".
- Автоматизированное аварийное восстановление в зоне для вычислений.
- Целевая точка восстановления (RPO) около 0.

Windows 365 является частью Microsoft 365 и полноценно использует решения, возможности и инструменты Windows и Microsoft 365. Эта интеграция обеспечивает переносимость и устойчивость пользовательских данных и пользовательского контекста. К важным необязательным решениям Windows и Microsoft 365 относятся:

- OneDrive
- OneDrive для бизнеса
- Перемещение известных папок OneDrive
- Синхронизация параметров Windows
- Enterprise State Roaming

Использование этих решений Windows и Microsoft 365 сохраняет контекст пользователя и пользовательские данные в случае, если на отдельном Облачном компьютере происходит сбой, не связанный с Azure. Из-за таких сбоев, как сбой обновления ОС или ошибки конфигурации пользователя, Облачный компьютер может быть недоступен, даже если базовая система работоспособна. При использовании Windows 365 с этими решениями вы можете использовать преимущества высокоустойчивых и переносимых данных пользователя и пользовательского контекста, даже если конкретный Облачный компьютер придется подготавливать повторно из базового образа.

Устойчивость данных

Если происходит серьезный сбой, например, полное отключение зоны или региона, предоставленное хранилище дисков обеспечивает устойчивость объектов данных на дисках ОС облачных компьютеров от потери данных в течение заданного кода на уровне 99,999999999 %.

Автоматизированное аварийное восстановление в зоне для вычислений

Сбои в зонах происходят редко, но могут нарушить работу Облачного компьютера. Примеры подобных сбоев:

- Сбой vNic
- Сбой вычислений
- Сбой плоскости хранилища
- Сбой вычислительной мощности

Azure автоматически выявляет сбои вычислений и перемещает рабочую нагрузку пользователя в другой ресурс в зоне.

Если пользователь активно использует сеанс, то во время восстановления службы может возникнуть небольшое нарушение работы пользователя. После восстановления пользователь должен снова установить подключение, повторно войдя в сеанс Облачного компьютера. Если во время входа пользователя в систему и активного использования сеанса облачного компьютера происходит сбой в зоне, пользователь теряет доступ до восстановления системы.

Системы хранилища отделены от функций вычислений и используют избыточность хранилища, чтобы обеспечить аварийное восстановление Windows 365 с показателем RPO около 0. Автоматическое аварийное восстановление Windows 365 основано на актуальной копии диска ОС с показателем RPO около 0. Таким образом, процесс восстановления запускается автоматически, поскольку нет необходимости принимать потерю данных, связанную с восстановлением на момент времени.

OneDrive, OneDrive для бизнеса и OneDrive с перемещением известных папок

Использование Windows 365 с OneDrive и OneDrive с перемещением известных папок дает следующие преимущества:

- Доступ к переносимым данным пользователей на всех физических и Облачных компьютерах.
- Устойчивость данных пользователя между регионами по модели "активный/активный" доступна на Облачных компьютерах и в других рабочих областях, прошедших проверку подлинности.
- Переносимость контекста пользователя и устойчивость между регионами с помощью перемещения известных папок.
- Устойчивость контекста на основе данных пользователя и перемещении известных папок с целевым временем восстановления (RTO) и RPO, равными 0.
- Управление версиями данных, защита от повреждения и случайного удаления и восстановление на момент времени.

Дополнительные сведения о развертывании OneDrive и управлении им для малого и среднего бизнеса и предприятий см. в этой статье.

Синхронизация параметров и Enterprise State Roaming в Windows

Синхронизация параметров и Enterprise State Roaming сохраняют параметры пользователя клиента Windows для обеспечения переносимости и/или устойчивости (резервное копирование). Сведения о различиях между синхронизацией параметров и Enterprise State Roaming см. в статье Что такое Enterprise State Roaming?

Общие сведения о параметрах Windows см. в разделе Обзор параметров Windows в документации по Enterprise State Roaming. Сведения о параметрах, таких как группирование и применимость, см. в разделе Сведения о параметрах Windows в документации Enterprise State Roaming.

Служба управления Облачными компьютерами

Служба управления Облачными компьютерами включает следующие компоненты:

- Центр администрирования Microsoft Intune
- Портал конечного пользователя Облачных компьютеров

Служба управления Облачными компьютерами имеет архитектуру с региональной избыточностью, высоким уровнем доступности и целевым временем доступности

99,99 %. В случае сбоя службы управления для службы действуют следующие целевые показатели:

- RTO < 6 часов.
- RPO <30 минут для изменений, внесенных в службу управления.

Если в службе управления возникают сбои, но других сбоев нет, пользователи не смогут получить доступ к своим сеансам Облачных компьютеров через портал конечного пользователя. Пользователи по-прежнему могут получать доступ к экземплярам облачных компьютеров с помощью любого из следующих вариантов:

- Собственное приложение.
- Напрямую из закладки для сеанса Облачного компьютера.
- https://rdweb.wvd.microsoft.com/webclient/index.html

Сводка

Windows 365 предлагает организациям пользовательские рабочие области со следующими преимуществами:

- Высокий уровень доступности и поддержка Соглашения об уровне обслуживания с финансовыми гарантиями.
- Автоматически восстанавливается, если произошел сбой вычислений Azure в зоне с ожидаемым RTO <10 минут, а RPO — ~0.
- Автоматическое восстановление после сбоя основного региона или зоны с RPO около 0.

Когда организации используют Windows 365 с указанными решениями и функциями Windows и Microsoft 365, им пользуются:

- Еще более высокий уровень устойчивости данных и контекста пользователя.
- Переносимые данные и контекст пользователя.
- Устойчивость данных по модели "активный/активный", обеспечивающая постоянный доступ к данным пользователей через OneDrive даже во время сбоя Windows 365.

Дальнейшие действия

Узнайте, как устранять неполадки с Windows 365.

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте

Использование Microsoft Entra ID для доступа к API Windows 365 в Microsoft Graph

Статья • 31.01.2025

Microsoft API Graph поддерживает Windows 365 как бета-версии и рабочие нагрузки версии 1.0 с определенными API и ролями разрешений. Microsoft API Graph использует Microsoft Entra ID для проверки подлинности и управления доступом. Для доступа к API-интерфейсам Windows 365 в Microsoft Graph требуется следующее.

- Идентификатор приложения со следующими характеристиками:
  - Разрешение на вызов Microsoft Entra ID и API Microsoft Graph.
  - Области разрешений, соответствующие задачам конкретного приложения.
- Учетные данные пользователя со следующими характеристиками:
  - Разрешение на доступ к клиенту Microsoft Entra, связанному с приложением.
  - Разрешения ролей, необходимые для поддержки областей разрешений приложения.
- Конечный пользователь для предоставления приложению разрешений на выполнение задач приложения для своего клиента Azure.

В этой статье:

- Демонстрируется порядок регистрации приложения с доступом к API Microsoft Graph и соответствующими ролями разрешений.
- Описываются роли разрешений API Windows 365.

Дополнительные сведения о версиях API см. в статье Управление версиями, поддержка и политики критических изменений для Microsoft Graph.

Регистрация приложений для использования API Microsoft Graph

Чтобы зарегистрировать приложение для использования API Microsoft Graph, выполните следующие действия:

1. Войдите в Центр администрирования Microsoft Intune, используя учетные данные администратора. При необходимости можно использовать следующие

учетные записи:

- Учетная запись администратора клиента.
- Учетная запись пользователя клиента с включенным параметром **Пользователи могут регистрировать приложения**.

2. Выберите **Все службы**>**Приложения**>**Azure Active Directory**>**Регистрация приложений**.
3. Щелкните **Новая регистрация**, чтобы создать новое приложение, или выберите существующее приложение.
4. Если вы выбрали новую регистрацию, в области **Регистрация приложения** укажите следующие сведения.

   - Имя приложения.
   - Поддерживаемый тип учетной записи.
   - Значение URI перенаправления (необязательно).

5. Нажмите **Зарегистрировать**.
6. В области **Приложение** выполните следующие действия.

   - Запомните значение **Идентификатор приложения (клиента)**.
   - Выберите **Разрешения API**.

7. В области **Разрешения API** выберите **Добавить разрешение**>**Microsoft API Microsoft**>**Graph**> выберите тип разрешений, необходимых приложению.
8. Выберите роли, необходимые для приложения, установив флажки рядом с соответствующими именами. Рекомендуется выбирать наименьшее количество ролей, необходимых для реализации приложения. Дополнительные сведения о Windows 365 и других областях разрешений API Graph см. в справочнике по разрешениям Microsoft Graph.
9. По завершении щелкните **Добавить разрешения**, чтобы сохранить изменения.

Можно также предоставить всем учетным записям клиента разрешения на использование приложения без ввода учетных данных. Для этого можно предоставить разрешения и подтвердить действия в появившемся окне запроса. При первом запуске приложения появится запрос на предоставление ему разрешений на выполнение выбранных ролей.

Дальнейшие действия

Авторизация доступа к веб-приложениям с помощью OAuth 2.0 и Microsoft Entra ID.

Начало работы с проверкой подлинности Microsoft Entra.

Интеграция приложений с Microsoft Entra ID.

Общие сведения об OAuth 2.0

Обратная связь

Были ли сведения на этой странице полезными? Да Нет

Отзыв о продукте