Microsoft ERC

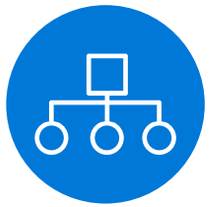
MICROSOFT INTUNE

ВЕБІНАР

Цель вебинара

Настройка архитектуры и параметров проектирования для возможности управления мобильными устройствами с помощью Endpoint Management

Обзор



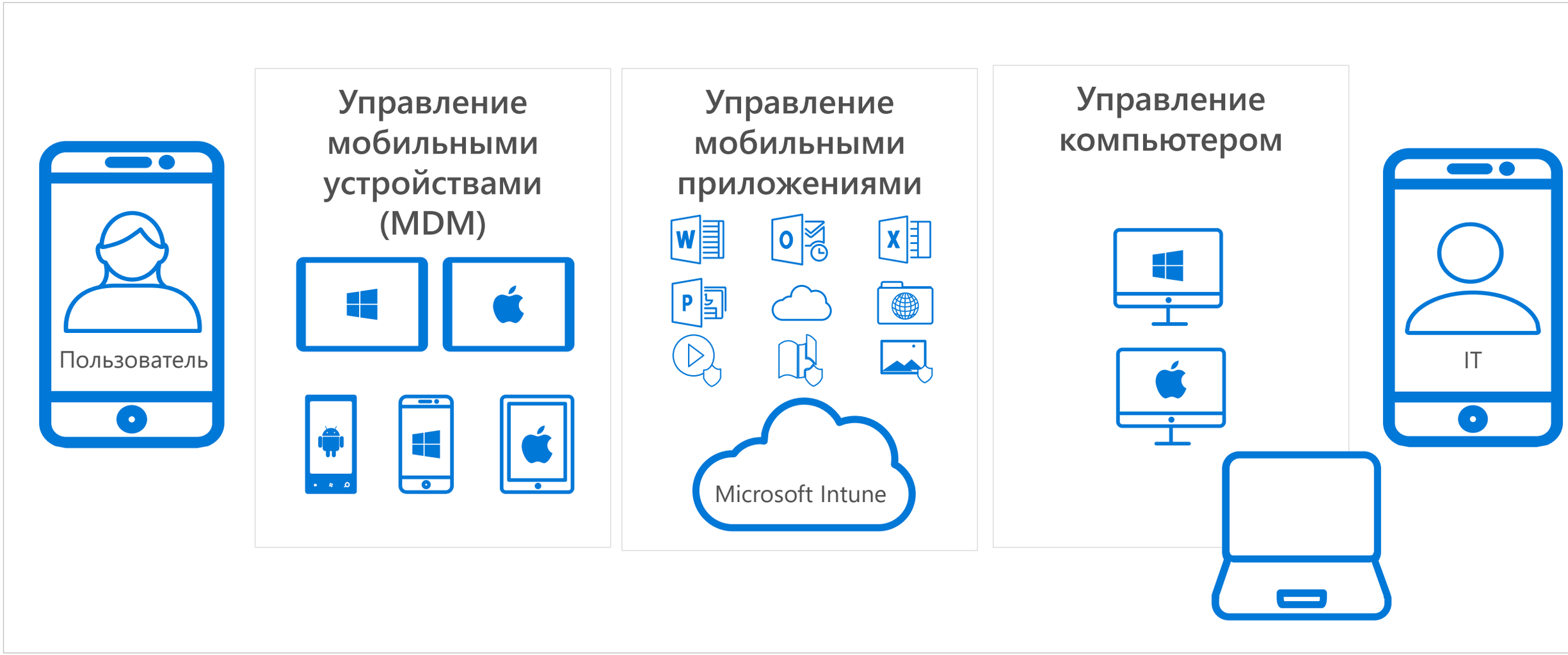
Enterprise Mobility Management

Жизненный цикл устройства

Архитектура решения

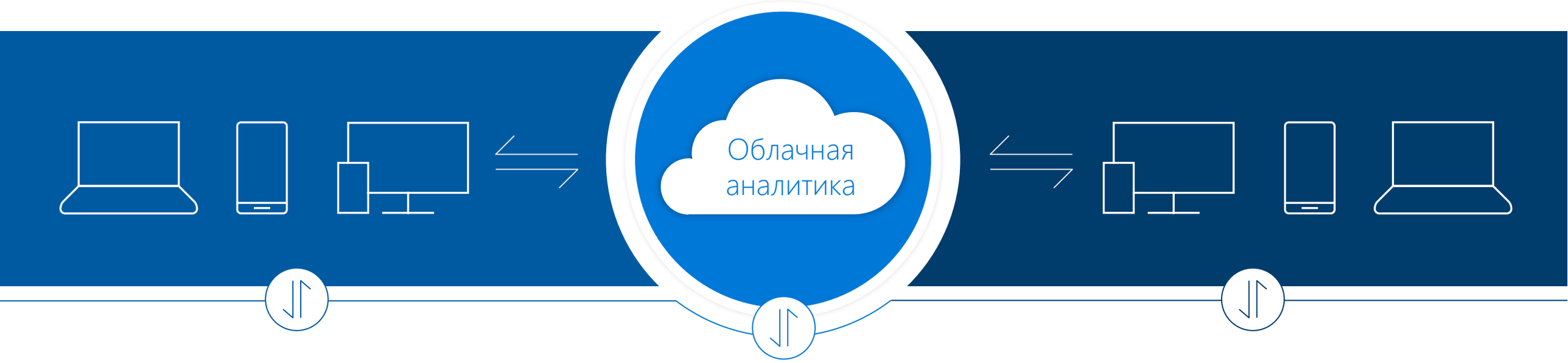
Поддерживаемые платформы устройств

Управление мобильностью предприятия с помощью Microsoft Endpoint Manager



Microsoft Endpoint Manager

Облачная преобразующая платформа для безопасного и унифицированного управления конечными точками



MICROSOFT ENDPOINT MANAGER

Единая консоль администратора

Configuration Manager		Microsoft Intune	
Аналитика рабочего стола	Autopilot Endpoint Security	Политики защиты приложений	Аналитика конечных точек

Дополнительные возможности управления конечными точками в Microsoft 365

Основные возможности Microsoft Endpoint Manager

Безопасность и интеллектуальность

Встроенная интеграция с облачными средствами управления безопасностью и условным доступом к приложениям и данным на основе рисков

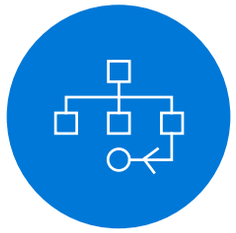
Оптимизация и гибкость

Гибкая поддержка различных корпоративных сценариев и сценариев BYOD при одновременном повышении производительности и совместной работы

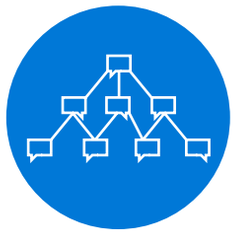
Максимизация инвестиций

Максимизируйте инвестиции и сократите время окупаемости благодаря быстрому развертыванию служб и устройств благодаря сквозной интеграции в знакомый стек Microsoft

Умная Безопасность



Контроль на основе рисков



Унифицированное управление

Инициализация без вмешательства в систему

Продвинутая аналитика

Глубокая интеграция с Microsoft 365

Мобильность

Microsoft Endpoint Manager Основные возможности

Безопасность и интеллектуальность

Умная Безопасность

Windows Hello

Базовые показатели безопасности

BitLocker Управление

Расширенная защита от угроз

Оценка производительности

Контроль на основе рисков

Соответствие требованиям и рискам конечных точек

Условный доступ

Политика защиты приложений

Сигнализация о рисках и соответствии требованиям третьих сторон

Оптимизация и гибкость

Унифицированное управление

Мобильность и управление ПК

Центр администрирования M365

Управляемые развертывания

M365 Корпоративные приложения

Инициализация без вмешательства в систему

Windows Autopilot

Android Enterprise

Apple ADE (Apple Automated Device Enrollment)

Samsung Knox Mobile Enrollment

Сокращение затрат

Продвинутая аналитика

Оценка технологического опыта

Аналитика журналов

Расширенное обнаружение угроз в режиме реального времени

Динамическая оценка рисков пользователей

Глубокая интеграция с Microsoft 365

Администрирование на основе ролей

Graph API

PowerShell

Ревизия

Оптимизация облачного контента

Мобильность

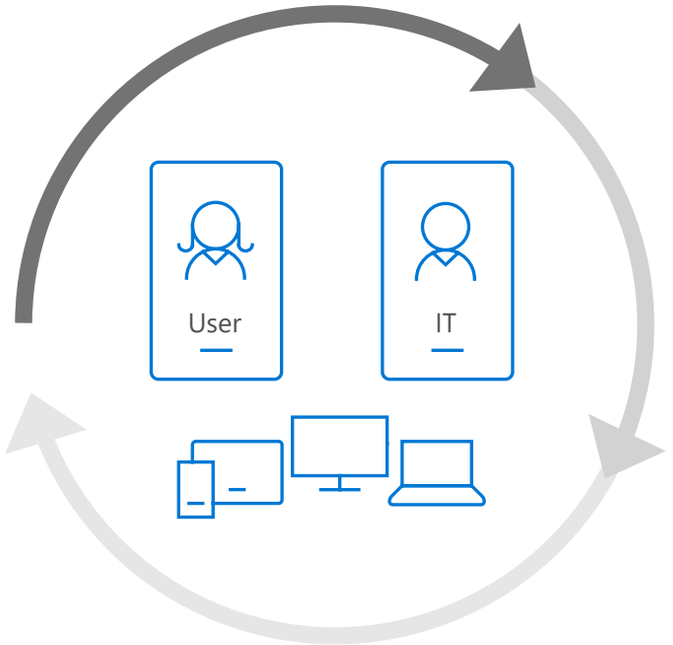
Управление жизненным циклом устройства

Регистрация устройств

- ✓ Выбор специальных методов регистрации для iOS/iPadOS, Android, Windows и macOS
- ✓ Развертывание корпоративного портала самообслуживания пользователей для регистрации личных устройств
- ✓ Автоматическая инициализация с автоматическими вариантами регистрации для корпоративных устройств

Поддержка и блокировка

- ✓ Отзыв доступа к корпоративным ресурсам
- ✓ Выполнение выборочной очистки
- ✓ Аудит потерянных и украденных устройств
- ✓ Устройство, выводящееся из эксплуатаци
- ✓ Предоставление удаленной помощи



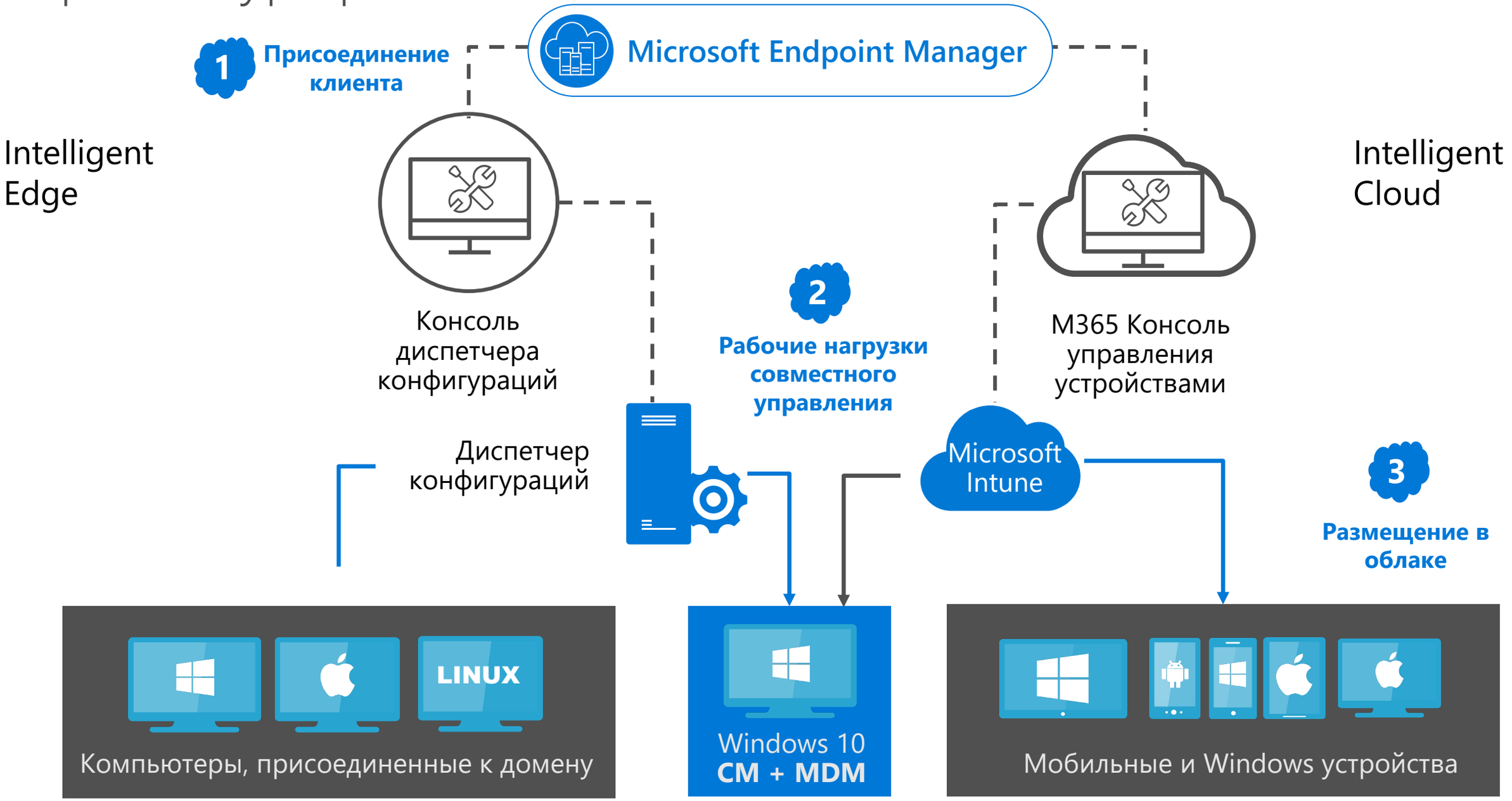
Настройка

- ✓ Развертывание сертификатов, почты, VPN, и профилей Wi-Fi
- ✓ Развертывание параметров политики безопасности устройств
- ✓ Установка обязательных приложений
- ✓ Развертывание политик ограничения устройств
- ✓ Развертывание параметров компонентов устройства

Защита

- ✓ Ограничить доступ к корпоративным ресурсам в случае нарушения политик (например, джейлбрейкнутого устройства)
- ✓ Защита корпоративных данных путем ограничения таких действий, как копирование, вырезание, вставка и сохранение за пределами управляемой экосистемы приложений
- ✓ Отчет о соответствии устройств и приложений требованиям

Архитектура решения



Что такое подключение к облаку?

Использование объединенных возможностей Microsoft Endpoint Manager путем присоединения Configuration Manager к Intune

Подключение к облаку	
Присоединение клиента (Tenant attach)	Присоединение клиента через совместное управление (Co-management)
Подключите сайт Configuration Manager к Intune для мгновенного использования облака.	Зарегистрируйте устройства Configuration Manager в Intune для получения дополнительных облачных преимуществ.
Облачная консоль через EMAC	
Интеграция с ATP	Условный доступ
Служба поддержки	Современная инициализация с помощью автопилота
Аналитика рабочего стола	Управление в любом месте
Аналитика пользовательского опыта	
Размещение в облаке (Cloud-only management)	
Использование Microsoft Azure для размещения компонентов Configuration Manager	

Управление на базе облака Microsoft 365

	Локальная среда	Облако
Традиционное развертывание ОС	✓	✓
Управление приложениями Win32	✓	✓
Конфигурация и объект групповой политики	✓	✓
Управление BitLocker	✓	✓
Инвентаризация оборудования и программного обеспечения	✓	✓
Управление обновлениями	✓	✓
Унифицированное управление конечными точками – Windows, iOS, macOS, Android, Linux (beta)		✓
Современный контроль доступа – Compliance, Условный доступ		✓
Современная инициализация – Autopilot, DEP, Zero Touch, KME		✓
Современная безопасность – Hello, Attestation, ATP, Secure Score		✓
Современная политика – Базовые показатели безопасности, Шаблоны для администраторов, Управляемые развертывания		✓
Современное управление приложениями – M365 Корпоративные приложения, Магазины, SaaS, VPP		✓
Полная интеграция M365 – Аналитика, Графики, Консоль, Управление доступом на основе ролей, Аудит		✓

Поддерживаемые платформы устройств

Apple

iOS 11.0 and later
iPadOS 13.0 and later
macOS X 10.12 and later

Google

Android 5.0 and later (включая Samsung KNOX Стандарт 2.4 и выше)*
Android Enterprise (7.0+)

Google

Microsoft

Surface Hub
Windows 11 (Home, Pro, Education, and Enterprise versions)
Windows 10 (Home, S, Pro, Education, and Enterprise versions)
Windows 10 IoT Enterprise (x86, x64)
Windows Holographic for Business
Windows 10 Teams (Surface Hub)
Sustaining mode:

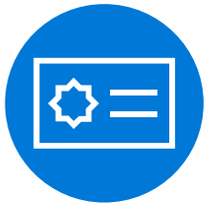
- Windows 10 Mobile
- Windows 10 1709 (RS3) and later, Windows Phone 8.1, Windows 8.1 RT, PCs running Windows 8.1

Подготовка

Подписка
Microsoft Intune

Инфраструктура

Конфигурация



Сертификаты

Подписка на Microsoft Intune

Обзор	Microsoft Endpoint Manager можно настроить в конфигурации Cloud Native, Co-Management или Tenant Attach • Подключение клиентов и совместное управление подключают Configuration Manager (1710 или выше) к облаку Microsoft 365
Варианты подписки	Intune входит в следующие лицензии: • Microsoft 365 E3, E5, F1, F3, Education A3 and A5, Goverment G3 and G5 • Enterprise Mobility + Security E3, E5 • Microsoft 365 Business Premium
Лицензионное соглашение	Варианты лицензионного соглашения • Программа подписки Microsoft Online — рекомендуется для организаций с менее чем 250 пользователями • Соглашение Enterprise, Соглашение о продуктах и услугах Майкрософт, поставщик облачных решений — рекомендуется для организаций для более чем 250 пользователей

Инфраструктура

Предварительные требования только в облаке

Инфраструктура Предварительные требования	Нет предварительных требований к инфраструктуре для облачной конфигурации

Инфраструктура

Предварительные требования Присоединение арендатора или совместное управление

Инфраструктура Предварительные требования

- Совместное управление: поддерживаемая и работоспособная среда Microsoft Endpoint Configuration Manager (версия 1710 или более поздняя)
- Присоединение клиента: поддерживаемая и работоспособная среда Microsoft Endpoint Configuration Manager (версия 2002 или более поздняя)

Инфраструктура

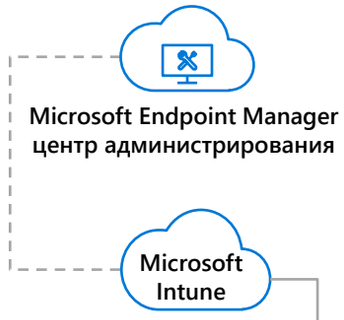
Развертывание сертификатов

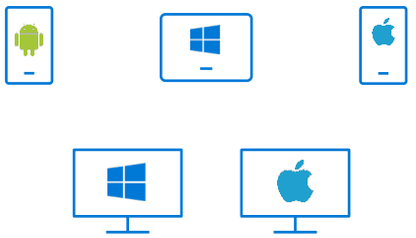
Локальная среда Предварительные требования	Центр сертификации (подчиненный центр сертификации Microsoft Enterprise) Серверы Windows Server 2012 R2 (или более поздней версии) для размещения роли NDES + соединитель Intune Microsoft NDES + прокси приложения Локальная служба Active Directory, синхронизированная с Azure Active Directory Изменение брандмауэра или прокси-сервера для обеспечения подключения Microsoft Intune
Публичный домен компании	Все учетные записи пользователей должны иметь общедоступно проверяемое доменное имя, которое может быть проверено Microsoft Intune Microsoft Intune может поддерживать несколько доменов
Публичный домен UPN	Перед синхронизацией учетных записей пользователей Active Directory убедитесь, что учетные записи пользователей имеют имя участника-пользователя публичного домена

Инфраструктура

Зависимости Intune Standalone (только для облака)

Управление только в облаке





Устройства Windows и
мобильные устройства
(Управление только в облаке)

Управление и защита

Нет необходимости в существующей инфраструктуре

Не требуется развертывание Microsoft Endpoint Configuration Manager

Упрощенное управление политиками

Простая веб-консоль администрирования

Более быстрая частота обновлений

Всегда актуальная информация

Поддержка регистрации устройств

Windows 10, 11

iOS/iPadOS

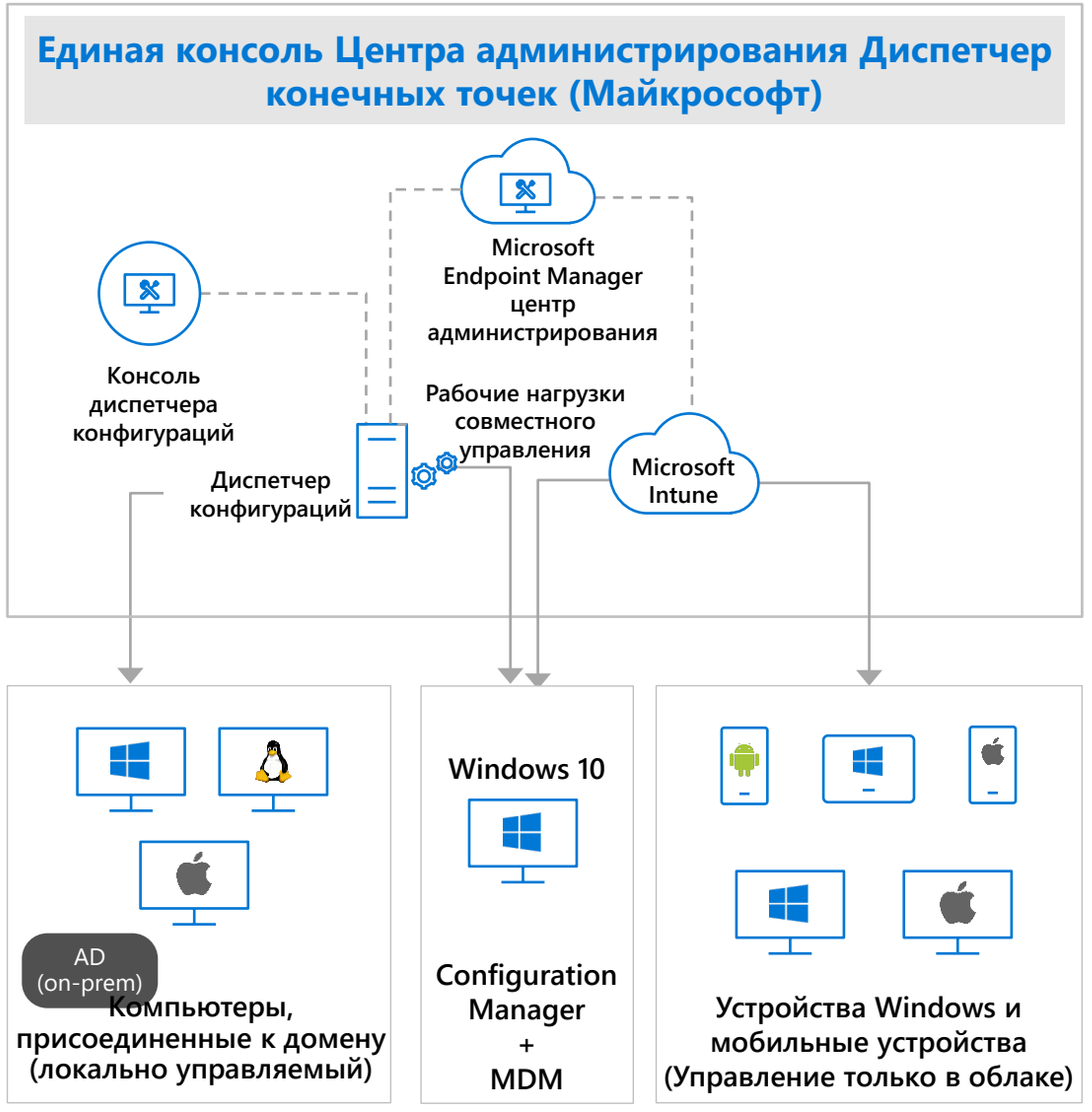
Android

macOS

linux (beta test)

Инфраструктура

Зависимости **Совместное управление** (Co-management)



Microsoft Endpoint Configuration Manager с Microsoft Intune

Подключите существующее развертывание Configuration Manager (версии 1710 или более поздней) к облаку Microsoft 365

Совместно управляемое устройство имеет агент Configuration Manager и зарегистрировано в Intune

Условный доступ с соответствием устройств

Удаленные действия на основе Intune

Современная подготовка с автопилотом Windows

Связывание пользователей, устройств и приложений с помощью Azure Active Directory (Azure AD)

Поддерживаемые устройства (в дополнение к мобильным)

Windows PCs (x86/64, Intel SoC)

Windows Server

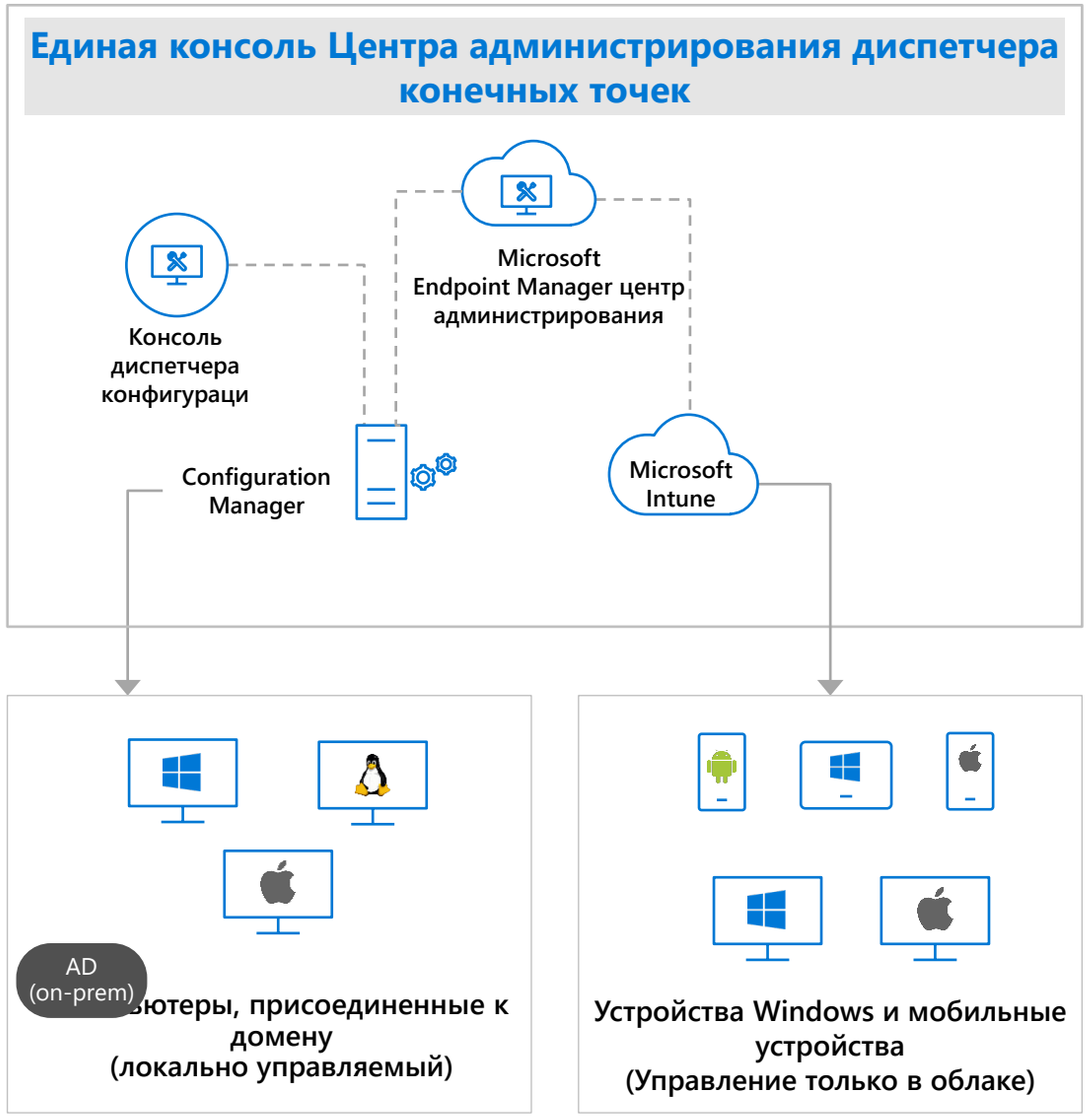
Linux/UNIX server

macOS

linux (beta test)

Инфраструктура

Зависимости **Присоединение клиента** (Tenant Attach)



Присоеденение Microsoft Endpoint Configuration Manager к Microsoft Intune

Подключите существующее развертывание Configuration Manager (версии 2002 или более поздней) к облаку Microsoft 365

Синхронизация агентов Configuration Manager с Intune без регистрации в Intune

Единая панель для управления устройствами в облаке

Интеграция с ATP

Служба поддержки

Аналитика рабочего стола

Аналитика пользовательского опыта

Поддерживаемые устройства (в дополнение к мобильным)

Windows PCs (x86/64, Intel SoC)

Windows Server

Linux/UNIX server

macOS

Конфигурация

Корпоративный портал

Обзор

Корпоративный портал Microsoft Intune предоставляет пользователям доступ к корпоративным данным и приложениям.
Пользователи могут получить доступ к корпоративному порталу с помощью:

- Приложение корпоративного портала
- Веб-сайт корпоративного портала

Цель

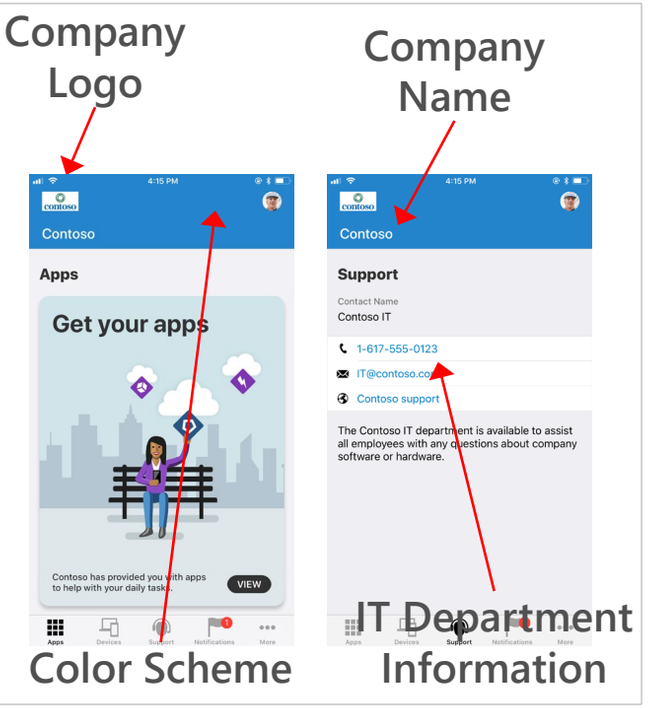
Пользователи могут использовать корпоративный портал для:

- Регистрации устройств
- Просмотр состояния своих устройств
- Загрузка программного обеспечения, развернутого компанией
- Обращения в ИТ-отдел за поддержкой

Настройка

Настройки для корпоративного портала включают:

- Название компании
- URL-адрес документации по конфиденциальности компании
- Цветовая схема для корпоративного портала (RGB)
- Логотип компании (400 x 100 pixels)
- Информация об ИТ-отделе



Конфигурация

Развертывание сертификатов - Прокси приложения

Обзор	Устройствам Microsoft Intune потребуются сертификаты для доступа к ресурсам компании. Прокси-сервер приложения позволяет подключенным к Интернету устройствам безопасно взаимодействовать с корпоративной сетью для достижения этой цели.
Прокси приложения Azure AD	Облачное решение Позволяет пользователям безопасно получать доступ к таким приложениям, как NDES внутри частной сети, через Интернет. Пользователи могут входить в корпоративные приложения на управляемых устройствах Microsoft Intune Соединитель прокси приложения Azure AD устанавливается только в операционной системе Windows Server 2012 R2 или более поздней версии.
Прокси веб-приложения + ADFS	Локальное решение Требуется дополнительная инфраструктура и ОС Windows Server 2012 R2 или более поздней версии для обеспечения функциональности прокси-сервера веб-приложения Рекомендуется для клиентов в сценариях, где ADFS 2012 R2 или более поздняя версия уже настроена

Конфигурация

Управление доступом на основе ролей

Встроенные роли			
Оператор службы поддержки	Оператор только для чтения	Администратор роли Intune	Диспетчер безопасности конечных точек
Менеджер политик и профилей	Менеджер приложений	Школьный администратор	

Пользовательские роли							
Разрешения	Android for Work	Device Compliance Policies	Endpoint Protection Reports	Managed Apps	Organization	Remote Tasks	Security Tasks
	Audit Data	Device Configurations	Enrollment Programs	Managed Devices	Policy Sets	Roles	Telecom Expenses
	Corporate Device Identifiers	Device Enrollment Managers	Intune Data Warehouse	Mobile Apps	Remote Assistance	Security Baselines	Terms and Conditions
Задание	Участники (группы): пользователи, которым назначена эта роль		Область (группы): политики, приложения и задачи пользователей и устройств этой группы областей		Область (теги): Объекты, которым назначен этот тег области		

Роли Azure AD с доступом Intune		
Глобальный администратор	Администратор службы Intune	Администратор условного доступа
Администратор безопасности	Оператор безопасности	Считыватель безопасности
Администратор соответствия требованиям	Администратор данных соответствия требованиям	Глобальный читатель

Конфигурация

Настройка доступа на основе ролей

1. Назначение ролей Azure AD

Роли Azure AD используются в основном для доступа администратора Intune и управления объектами Azure AD (пользователями, группами, лицензиями, условным доступом).

2. Определение ролей Intune

Роли Intune используются для предоставления доступа к подмножеству компонентов в Intune (например, удаленные действия на устройствах, изменение профиля конфигурации и т. д.).

3. Определение тегов области в Intune

Теги области используются для ограничения области действия назначения роли Intune

4. Просмотр групп, используемых для администраторов и пользователей

5. Назначение ролей Intune

Конфигурация

Теги

Обзор	Используйте теги управления доступом и области на основе ролей, чтобы убедиться, что нужные администраторы имеют правильный доступ и видимость к нужным объектам Intune. Роли определяют, какой доступ имеют администраторы к каким объектам. Теги области определяют, какие объекты могут видеть администраторы.
Использование	Создайте в Intune столько тегов области, сколько нужно, чтобы ограничить область разрешений для группы администраторов. Теги области могут быть назначены многим типам объектов в Intune (устройствам, политикам, ограничениям регистрации и т. д.). Тег области по умолчанию автоматически добавляется ко всем объектам без тегов, поддерживающим теги области.
Ограничения	Теги области могут быть назначены группе устройств, чтобы они автоматически получали тег области при регистрации. В настоящее время невозможно назначить тег области группе пользователей, чтобы устройство пользователя автоматически получало тег области. Для этого можно использовать сценарии

Сертификаты

Обзор	Сертификаты позволяют Intune устанавливать аккредитованное и зашифрованное IP-подключение, а также подписывать приложения для защиты устройств от вредоносных программ
Сертификаты инфраструктуры	Шаблон сертификата — настроен в ЦС для поддержки управляемых Intune мобильных устройств Сертификат проверки подлинности клиента — установлен в NDES Сертификат аутентификации сервера — установлен на сервере NDES* Сертификат доверенного корневого ЦС — экспорт в Microsoft Intune
Сертификаты подписи кода	Отправка сертификатов подписи кода при подписании пакетов LOB appx сертификатом, который не получен от доверенного центра сертификации Сертификаты Symantec Phone и лицензионные ключи для загрузки неопубликованных приложений не требуются для загрузки неопубликованных приложений Windows 10, 11 Сертификат подписи кода Symantec, используемый для развертывания мобильных приложений Windows Phone 8.1, был прекращен 28 февраля 2019 г. и больше не доступен для продления от Symantec
iOS	Сертификат службы push-уведомлений Apple необходим для управления устройствами iOS в Microsoft Intune

*If NDES is required , use the NDES module for implementation design

Чек лист для старта

Подписка Intune	Cloud-only, Co-management or Tenant Attach Office 365 and Microsoft Intune integrated tenant
Поддерживаемые платформы	iOS/iPadOS macOS Android/Samsung KNOX Windows
Корпоративный портал	Без кастомизации С кастомизацией
Обратный прокси-сервер	Azure AD Application Proxy Web Application Proxy
RBAC	Необходимые роли и доступ
Сертификаты	Сертификаты инфраструктуры Сертификаты устройств

Спасибо за внимание

Microsoft ERC