

# Moderní správa a nasazení Windows 10

Kamil Roman

[Konzultace@KamilRT.net](mailto:Konzultace@KamilRT.net)

[www.KamilRoman.EU](http://www.KamilRoman.EU)

# Agenda

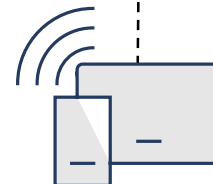
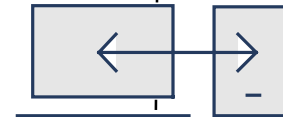
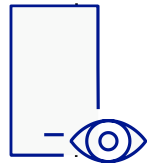
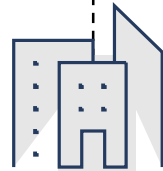
- Modern management introduction
- Windows Autopilot
- Microsoft Intune

# Characteristics of traditional PC management

On-premises Infrastructure

High control

Business-owned devices



# Characteristics of modern device management

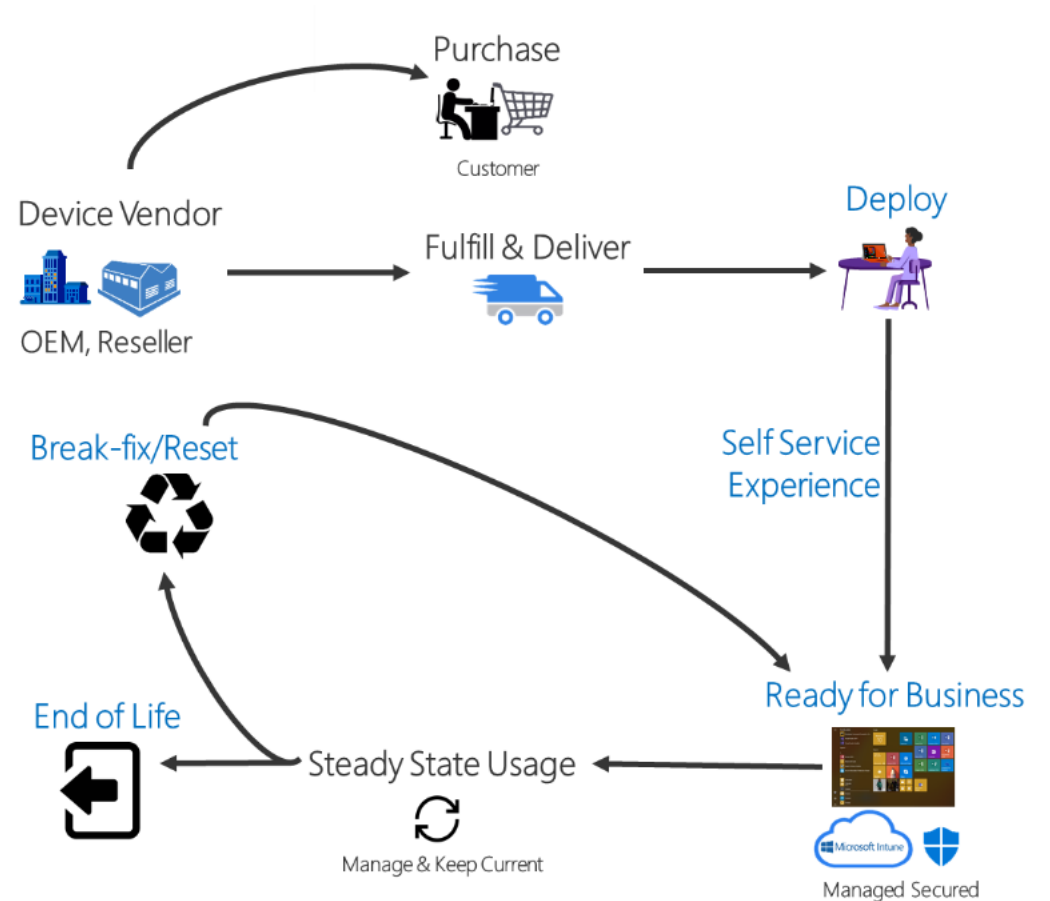
Cloud services

Simpler IT process

Business-owned + BYOD

# Modern Deployment

- Intended to reduce:
  - Image-based deployment
  - Number of images to maintain
  - On-premise infrastructure needed to support deployment
  - Simplify configurations



# IT initiatives enabled by modern management



**Remote users:** Enable remote users



**Wireless-first:** Disable wired ports



**Internet-first:** Remove corporate networks



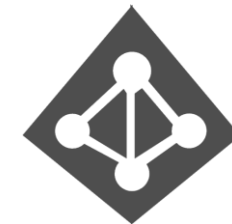
**Server retirements:** Move services to the cloud



**Co-Manage:** Transition from classic to modern with Intune and ConfigMgr

## Modern management

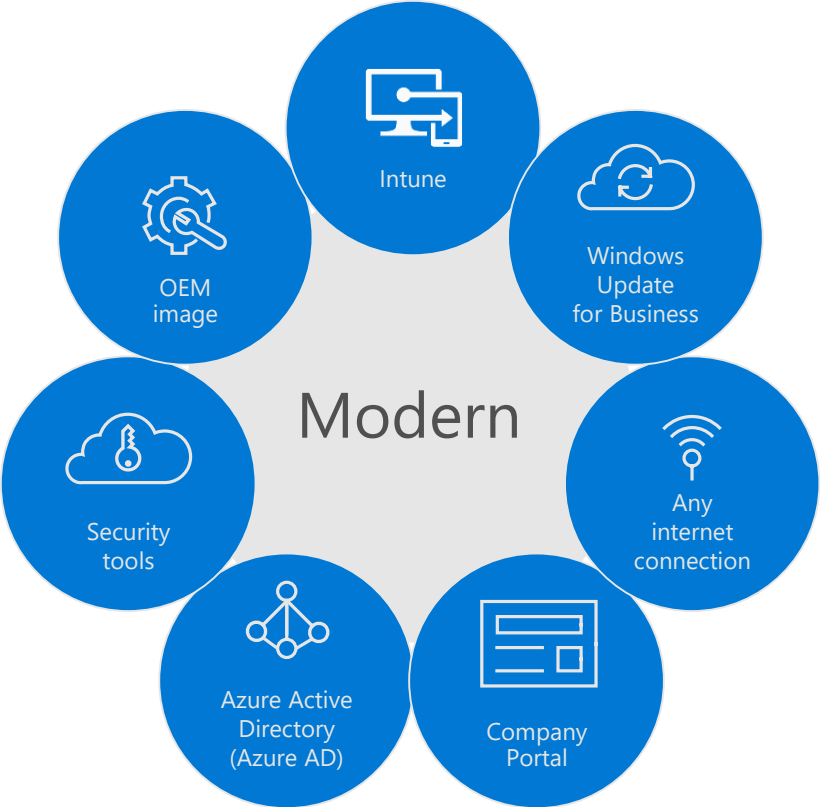
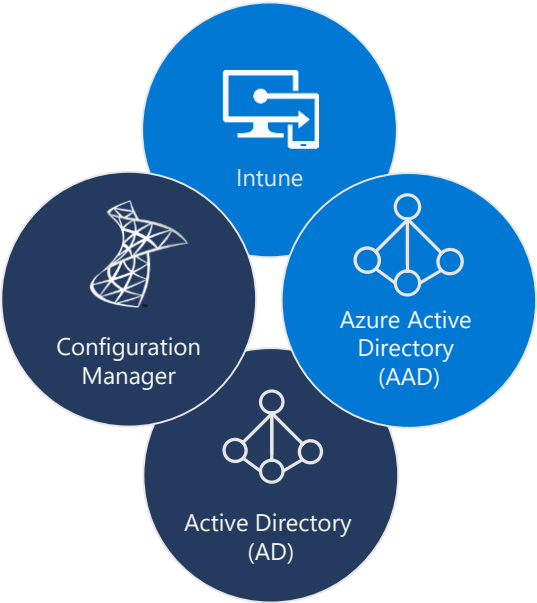
The Enterprise IT infrastructure is cloud-based for identity and device management services.



# Evolution to modern management



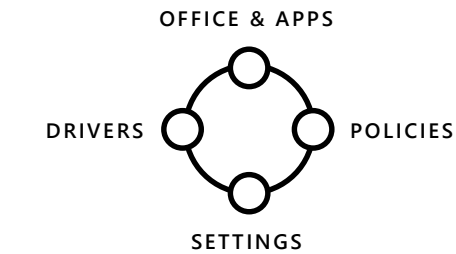
## Co-management





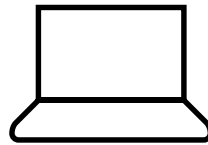
# Windows Autopilot

# Traditional Windows deployment // The old way



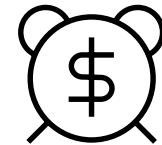
Build a custom image, gathering everything else that's necessary to deploy

+



Deploy image to a new computer, overwriting what was originally on it

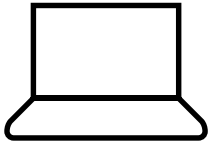
=



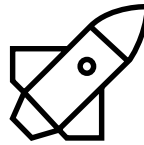
Time means money, making this an expensive proposition



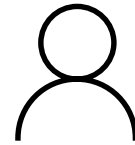
# Modern Windows deployment // The new way



Un-box and turn on  
off-the-shelf Windows PC

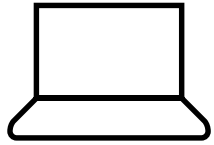


Transform with minimal  
user interaction

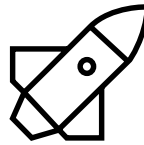


Device is ready  
for productive use

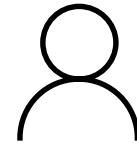
# Modern Windows deployment // The new way



Un-box and turn on  
off-the-shelf Windows PC



Transform with minimal  
user interaction



Device is ready  
for productive use

**Deploying a Windows device should be as simple as getting a new phone.**

# Windows Autopilot // One-time preparation tasks

## Azure Active Directory

- ✓ Configure [automatic MDM enrollment](#).
- ✓ Configure [company branding](#).
- ✓ Enable [Windows Subscription Activation](#) if desired.
- ✓ Ensure users can join devices to Azure AD (for user-driven mode)

## Intune:

- ✓ Enable the enrollment status page
- ✓ Ensure users can enroll devices in Intune
- ✓ Assign licenses to users
- ✓ (Optional) Set up enrollment restrictions so only Autopilot-registered devices can enroll

# Three simple steps



Register devices



Assign a profile



Deploy

# Three simple steps



Register devices



Assign a profile



Deploy

- Have devices registered automatically
  - Request clean images, choice of Windows 10 version at the same time (if available)
  - Specify group tag to help segment devices by purpose
  - Devices are automatically tagged with the purchase order ID
- Register devices yourself via Intune for testing and evaluation using [Get-WindowsAutopilotInfo](#) PowerShell script
- Register (harvest) existing Intune-managed devices automatically

# Three simple steps



Register devices



Assign a profile



Deploy

- Use Intune:
  - Select profile scenario (user-driven, self-deploying)
  - Configure needed settings
  - Assign to an Azure AD group so Intune will automatically assign to all devices in the group
- Use a dynamic Azure AD group to automate this step
  - Consider static Azure AD group for exceptions

# Three simple steps



Register devices



Assign a profile



Deploy

- Boot up each device
- Connect to network (Wi-Fi, Ethernet)
- Enter credentials (if required)

# Participant device manufacturers and resellers

These brands ship devices using Windows Autopilot. When you purchase from them, your employees will receive devices ready to go, just by signing in — requiring no help from IT.



ACER

[Learn more >](#)



CDW

[Learn more >](#)



DELL

[Learn more >](#)



DYNABOOK

[Learn more >](#)



HP

[Learn more >](#)



Lenovo

[Learn more >](#)



Panasonic

[Learn more >](#)



Surface

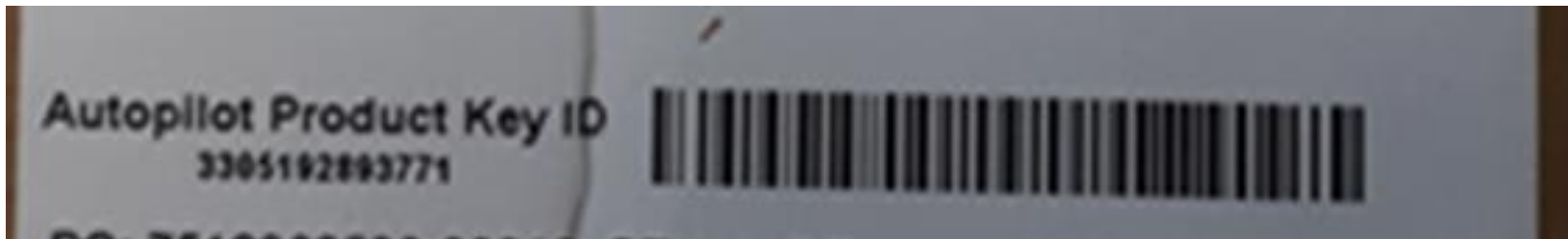
[Learn more >](#)



Fujitsu and Getac coming soon



# Windows Autopilot // Coming soon



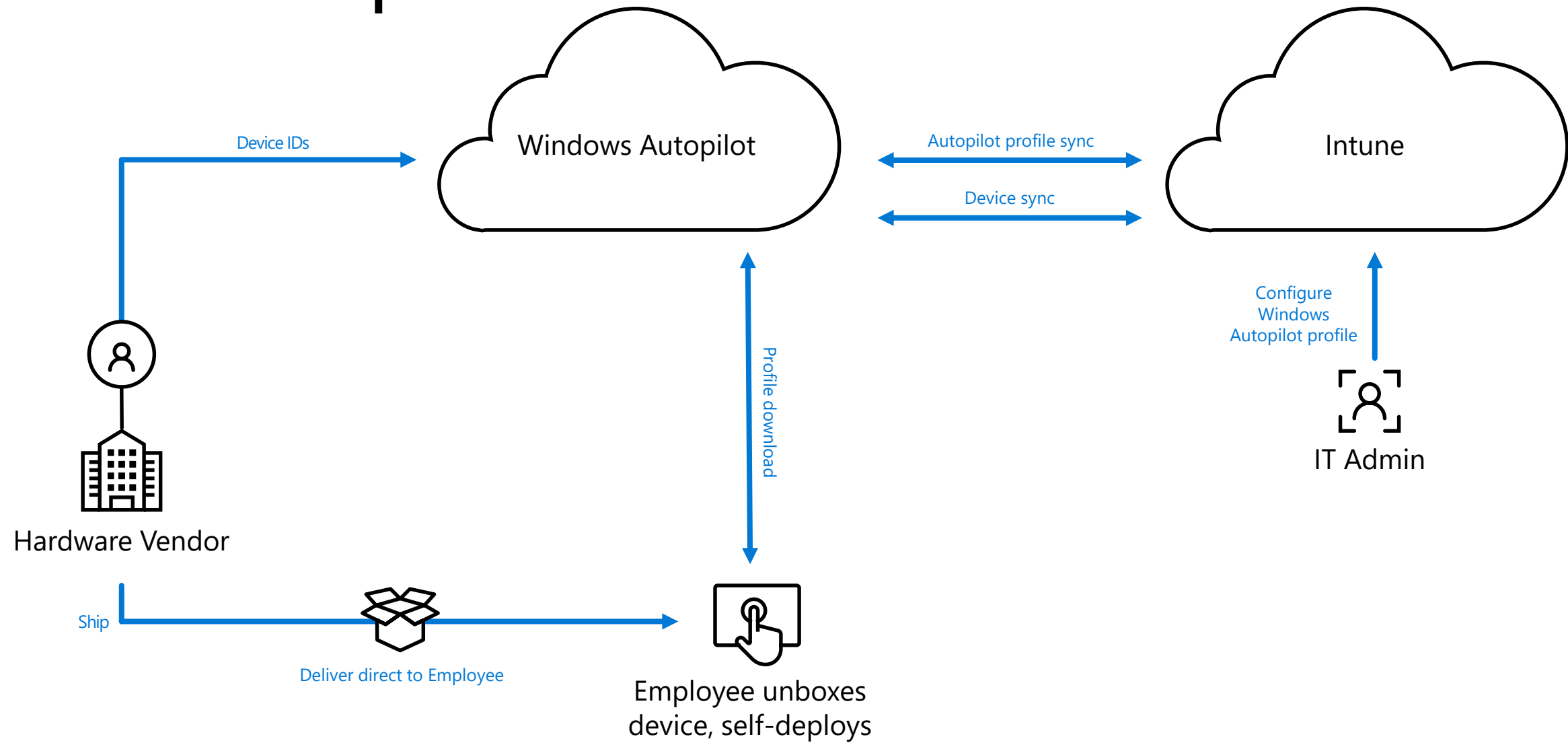
# Windows Autopilot // Deployment Scenarios

AVAILABLE in 1703	AVAILABLE in 1809	AVAILABLE in 1903	AVAILABLE in 1903	AVAILABLE in 1809
User-driven mode with Azure AD Join	User-driven mode with Hybrid Azure AD join	Windows Autopilot white glove (preview)	Self-deploying mode (preview)	Windows Autopilot for existing devices
Join device to Azure AD, enroll in Intune/MDM	Join device to AD, enroll in Intune/MDM <b>Coming soon! Deploy over VPN (preview in Q1CY20, 1903+)</b>	White glove partners or IT staff can pre-provision Windows 10 PC to be fully configured and business-ready for an org or user  <b>General availability targeting CY20</b>	No need to provide credentials, automatically joins Azure AD  <b>General availability targeting CY20</b>	Windows 7/8.1 to Windows 10  ConfigMgr task sequence, followed by Windows Autopilot user-driven mode  <b>New! Hybrid Azure AD Join support</b>

# Windows Autopilot // Cross-scenario features

AVAILABLE in 1803+	AVAILABLE in Intune	AVAILABLE in Intune	ONGOING	ONGOING	AVAILABLE in 1903+
<b>Enrollment status page</b>	<b>Device lifecycle management</b>	<b>Reporting and monitoring</b>	<b>Windows and device config</b>	<b>Delivery optimization</b>	<b>Windows Autopilot update</b>
Track progress of: <ul style="list-style-type: none"><li>• Policies</li><li>• Certificates</li><li>• Win32, MSI and UWP apps</li><li>• Office</li></ul>	Register and de-register devices	See information about Windows Autopilot deployments	Make it easier to set up Windows 10 defaults, features, firmware configuration, etc.	Cache content so it doesn't need to be downloaded repeatedly from the server	Automatically install the latest Windows Autopilot features and updates
<b>New! Disable for Nth users</b>	<b>Coming soon! Improved performance</b>	<b>Coming soon! Windows Autopilot deployment report (Q4CY19)</b>	<b>New! DFCI firmware configuration</b>	<b>New! Office 365 ProPlus install support (preview)</b>	Windows 10 1903 (September KB4517211+) or later
<b>Coming soon! Integration with ConfigMgr (H1CY20)</b>	<b>Coming soon! Edit group tags (Q4CY19)</b>	<b>Coming soon! Windows Autopilot log collection</b>	<b>Planned! Remove list of in-box apps</b>	<b>Planned! Automatic Connected Cache discover for white glove</b>	
<b>Coming soon! Options for skipping user ESP, targeting users and computers</b>	<b>Coming soon! Assign computer names (Q4CY19)</b>		<b>Planned! Add language packs and features</b>		

# Windows Autopilot overview



# The deployment process // Transforming the device



OEM-optimized Windows 10

+ Software

+ Settings

+ Updates

+ Features

+ User data

Ready for productive use

# The deployment process // Transforming the device



- Office 365 ProPlus
- Single-file MSIs (LOB apps)
- Intune Management Extensions
- Security Baselines
- Administrative Templates
- Software Update rings
- OneDrive for Business
- Kiosk templates
- Device Firmware Configuration Interface (DFCI)

# Windows Autopilot

## User-Driven Azure AD join

# Let's start with region. Is this right?



A screenshot of the Azure portal's region selection dropdown menu. The menu is open, showing a list of regions. The 'United States' option is highlighted with a blue background and a dashed border. A mouse cursor is pointing at the 'Yes' button at the bottom right of the screen.

U.S. Minor Outlying Islands
U.S. Virgin Islands
Uganda
Ukraine
United Arab Emirates
United Kingdom
<b>United States</b>

Yes

## User-Driven Azure AD Join

- **Connect to a network**
- **Authenticate to Azure AD**

Password-less with phone sign-in

Coming soon! [Authenticate with FIDO2](#)

- **Enroll in Intune**
- **Track progress with the Enrollment Status Page**

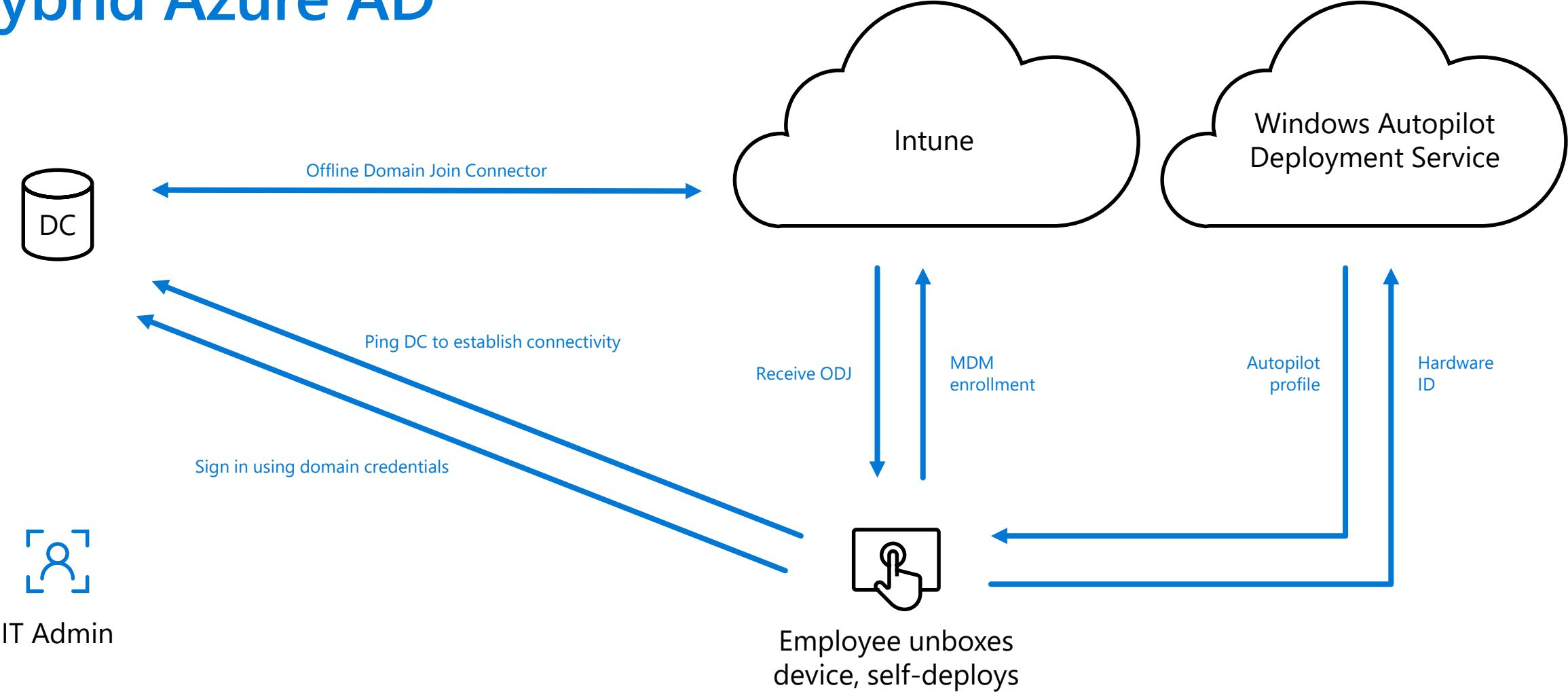
Policies  
Apps (Win32, MSI, UWP)  
Certificates  
Network, VPN connections

Coming soon! [Integration with ConfigMgr task sequences \(H1CY20\)](#)

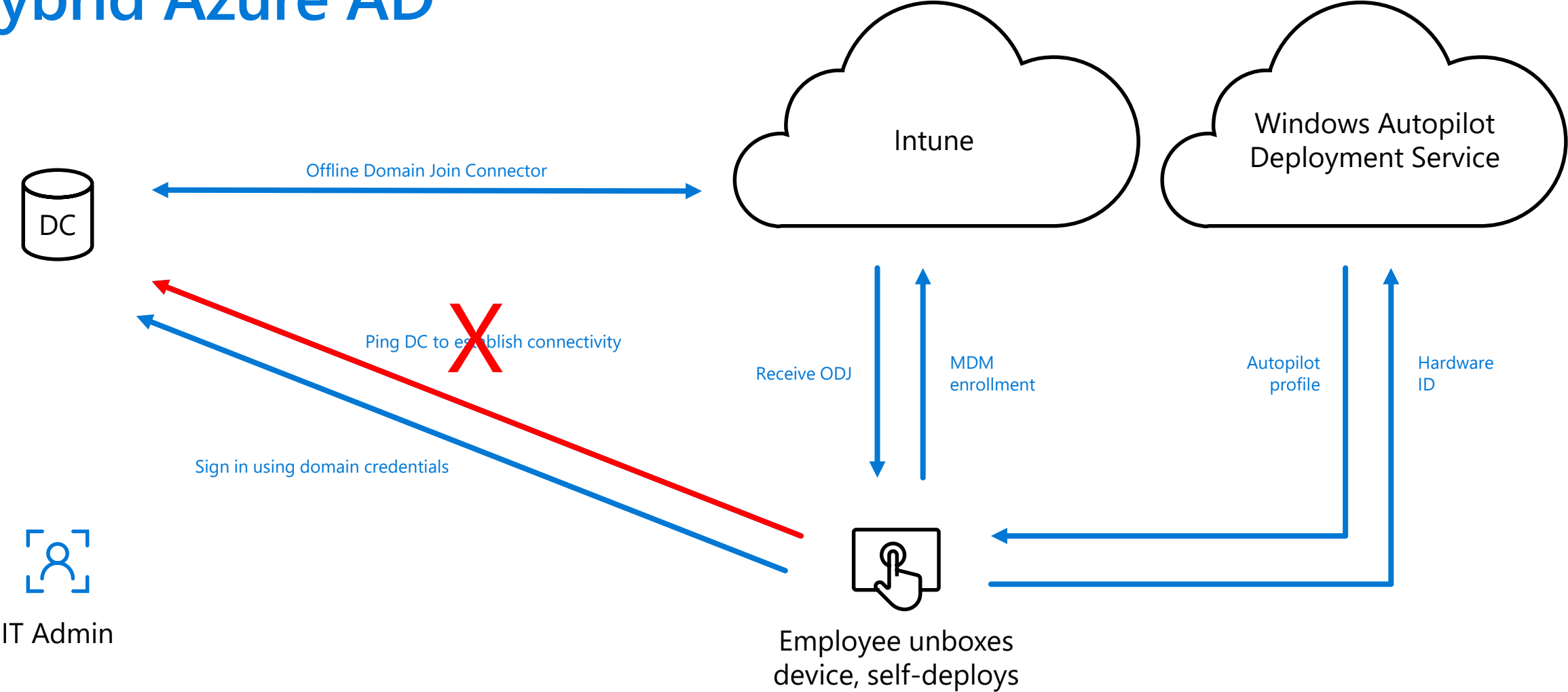


Windows Autopilot  
User-Driven Hybrid Azure  
AD join

# Windows Autopilot // User-Driven deployment with Hybrid Azure AD



# Windows Autopilot // User-Driven deployment with Hybrid Azure AD



# Let's start with region. Is this right?

U.S. Minor Outlying Islands

U.S. Virgin Islands

Uganda

Ukraine

United Arab Emirates

United Kingdom

United States

Yes

## User-Driven Hybrid AAD Join

- **Connect to a network**
- **Authenticate to Azure AD**

Password-less with phone sign-in

**Coming soon! Authenticate with FIDO2**

- **Enroll in Intune**
- **Perform offline domain join**

**Coming soon! VPN support (preview in Q1CY20, 1903+)**

- **Track progress with the Enrollment Status Page**

Policies

Apps (Win32, MSI, UWP)

Certificates

Network, VPN connections

**Coming soon! Integration with ConfigMgr task sequences (H1CY20)**

# Windows Autopilot

## Self-deploying mode (preview)



Just a moment...

### **Self-Deploying Mode (preview)**

- **TPM attestation to authenticate to Azure AD**
- **Enroll in Intune**
- **Track progress with the Enrollment Status Page**

Policies, including Kiosk profiles  
Apps (Win32, MSI, UWP)  
Certificates  
Network, VPN connections

**Coming soon! Integration  
with ConfigMgr task  
sequences (H1CY20)**

**General availability in CY20**

# Windows Autopilot for existing devices



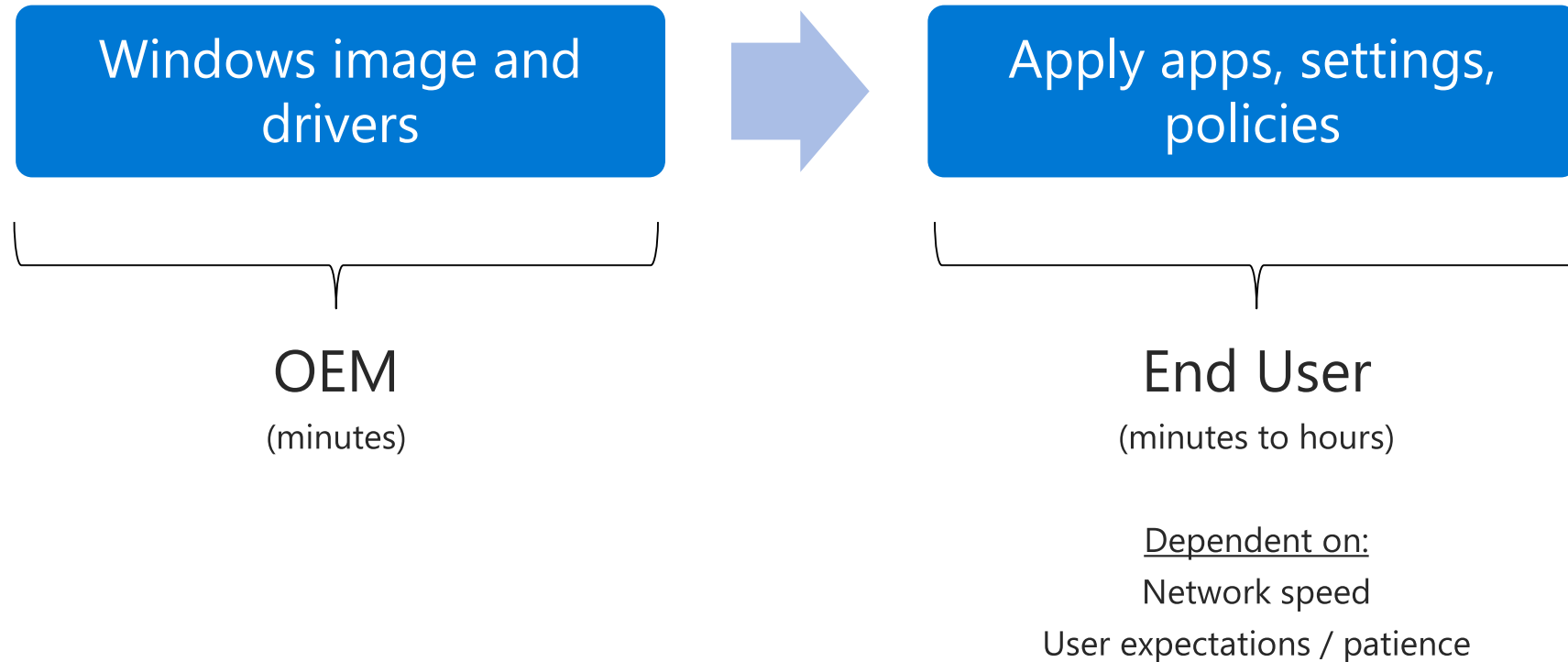
- **New! Support for Hybrid Azure AD Join**
- **ConfigMgr task sequence to deploy Windows 10**
  - No state migration
  - Data is already in the cloud with OneDrive for Business
  - Reformat drive, apply image, inject drivers
  - Drop in AutopilotConfigurationFile.json
- **Standard user-driven process once booted into Windows 10**
  - Coming soon! Integration with ConfigMgr task sequences (H1CY20)**



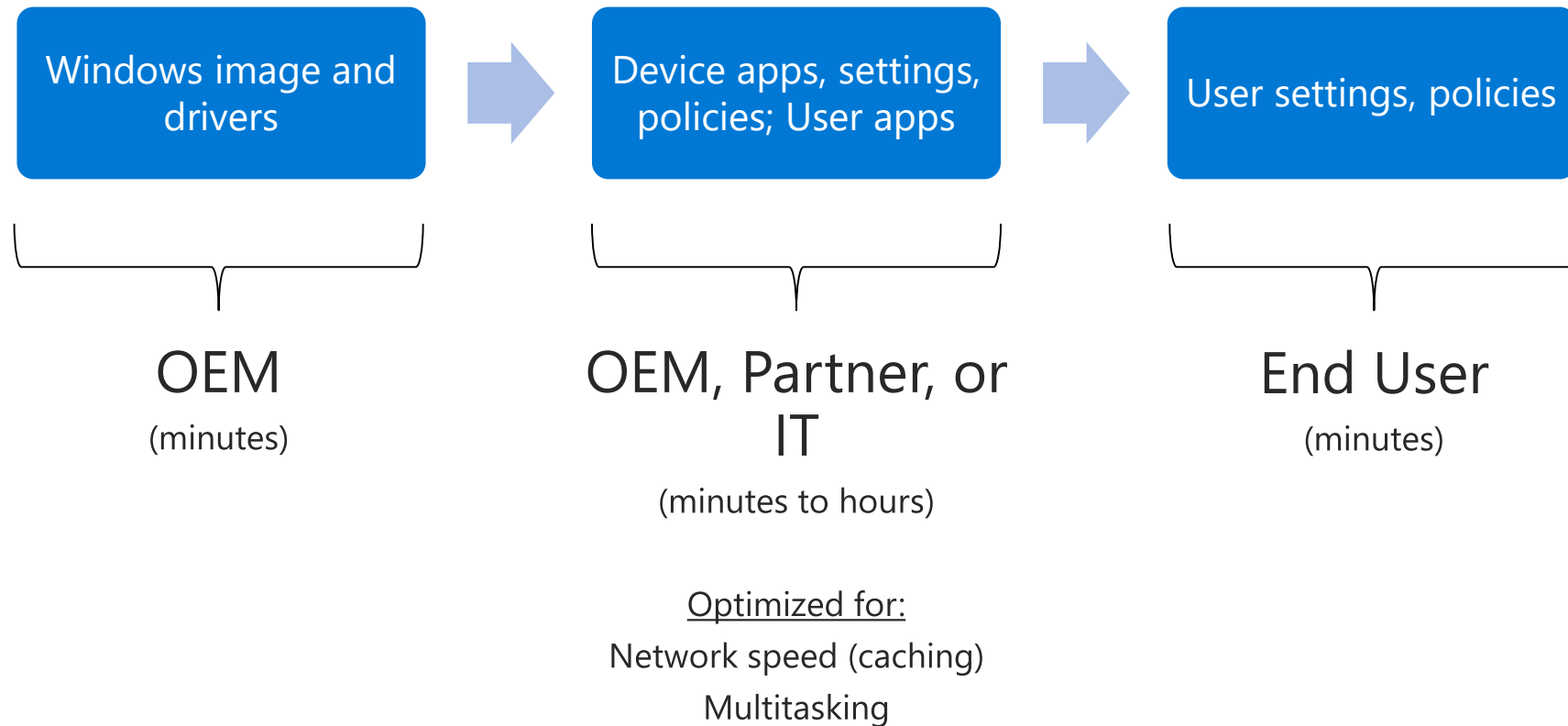
# Windows Autopilot

## White glove (preview)

# Windows Autopilot // Today



# Windows Autopilot // with white glove in Windows 10 1903





**At the Woodgrove warehouse,  
devices are processed...**





**At the Woodgrove warehouse,  
devices are processed...**

First, the technician does  
the pre-provisioning  
work

Let's start with region. Is this right?

Turks and Caicos Islands

Tuvalu

U.S. Minor Outlying Islands

U.S. Virgin Islands

Uganda

Ukraine

United Arab Emirates

United Kingdom

United States

Yes

### White glove (preview) technician flow

- **Press Windows key five times to start**
- **Choose Windows Autopilot provisioning option**
- **Confirm settings**

Configure user with companion app, refresh

**Coming soon! Configure group tag, computer name with companion app (Q4CY20)**



**Now the device (with all apps,  
updates, and policies applied)  
can be shipped to the user...**





Then, the user quickly  
finishes the process

**White glove (preview)**  
**user flow**

- **Standard user-driven process**

For Azure AD Join: Enter credentials, go through device and user ESP

For Hybrid Azure AD Join: Enter AD credentials to sign in, go through user ESP

# Windows Autopilot // Deployment report

Coming soon! New Windows Autopilot deployment report showing results, duration (Q4CY20)

Microsoft 365 Device Management

Restore default configuration

admin@spencersh.onmi...  
SPENCECORP

»

Dashboard > Device enrollment - Autopilot deployments (preview)

Device enrollment - Autopilot deployments (preview)

Microsoft Intune

Search (Ctrl+ /)

Filter Refresh Export

Overview

Quick start

Manage

Apple enrollment

Android enrollment

Windows enrollment

Terms and conditions

Enrollment restrictions

Device categories

Corporate device identifiers

Device enrollment managers

Monitor

Autopilot deployments (prev...

Enrollment failures

Audit logs

Incomplete user enrollments

Data is retained for the last 30 days

Search by Serial number, User, Device name, or AP profile

Enrollment date	Enrollment method	Serial number	Device name	User	Autopilot profile	ESP deployment state	Deployment total time
10/11/19, 5:10 PM	Self-deploying AAD	005318482657	DESKTOP-JQPMHL1	IWUser1@spencersh.onmicrosoft.c...	Self Deploying profile	Success	10 mins 11 secs
10/07/19, 5:48 PM	Self-deploying AAD	005318482657	30dd7430-f391-4f8d-9419-6f9ec9...	IWUser1@spencersh.onmicrosoft.c...	Self Deploying profile	Success	10 mins 13 secs
10/04/19, 3:07 PM	User-driven AAD	005318482657	SCORP-94813618	IWUser1@spencersh.onmicrosoft.c...	User Driven Profile	Success	7 mins 5 secs
10/11/19, 4:40 PM	Self-deploying AAD	005318482657	DESKTOP-PQUMSPI	admin@spencersh.onmicrosoft.com	Self Deploying profile	Success	9 mins 23 secs
10/10/19, 4:40 PM	User-driven AAD	005318482657	SCORP-44611256	admin@spencersh.onmicrosoft.com	User Driven Profile	Success	9 mins 41 secs

# Windows Autopilot // Top 10 new features coming soon

1. User-driven Hybrid Azure AD Join over the internet – VPN support (Q1CY20 preview)
2. Integration with Configuration Manager for running task sequences (H1CY20)
3. Group tag editing (Q4CY19)
4. Direct computer name assignment (Q4CY19 for Azure AD)
5. Windows Autopilot deployment report (Q4CY19)
6. Aligned naming options for Azure AD and Hybrid Azure AD (CY20)
7. Guided scenarios to help with initial setup and configuration
8. ESP enhancements for targeting, disabling user ESP, Nth user
9. Full network documentation (URLs, IP addresses, etc.)
10. Windows 10 configuration for features, language packs, in-box apps





# DEMO

## Windows Autopilot

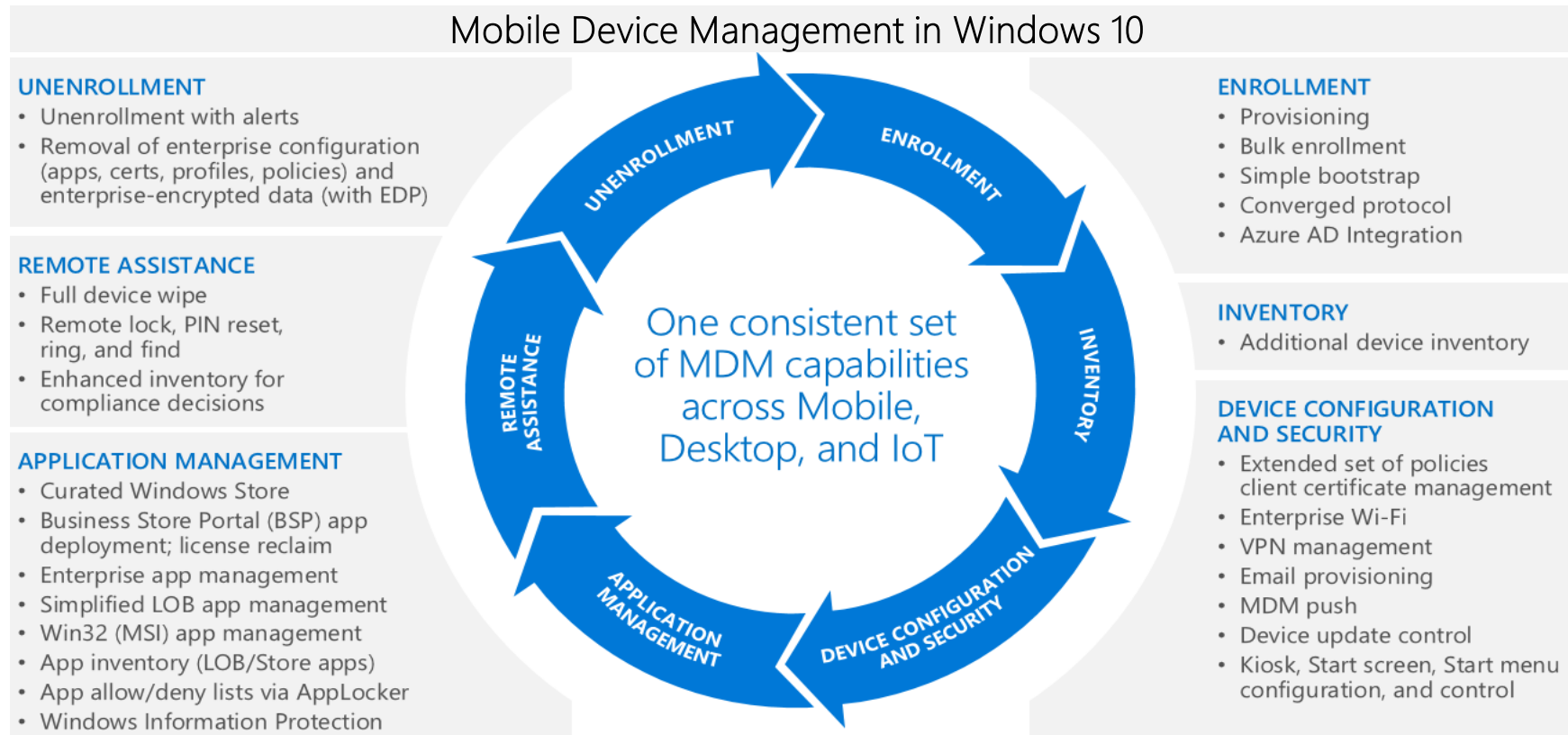


# Microsoft Intune overview

# Managing devices with Mobile Device Management

MDM authority, such as Intune, provides

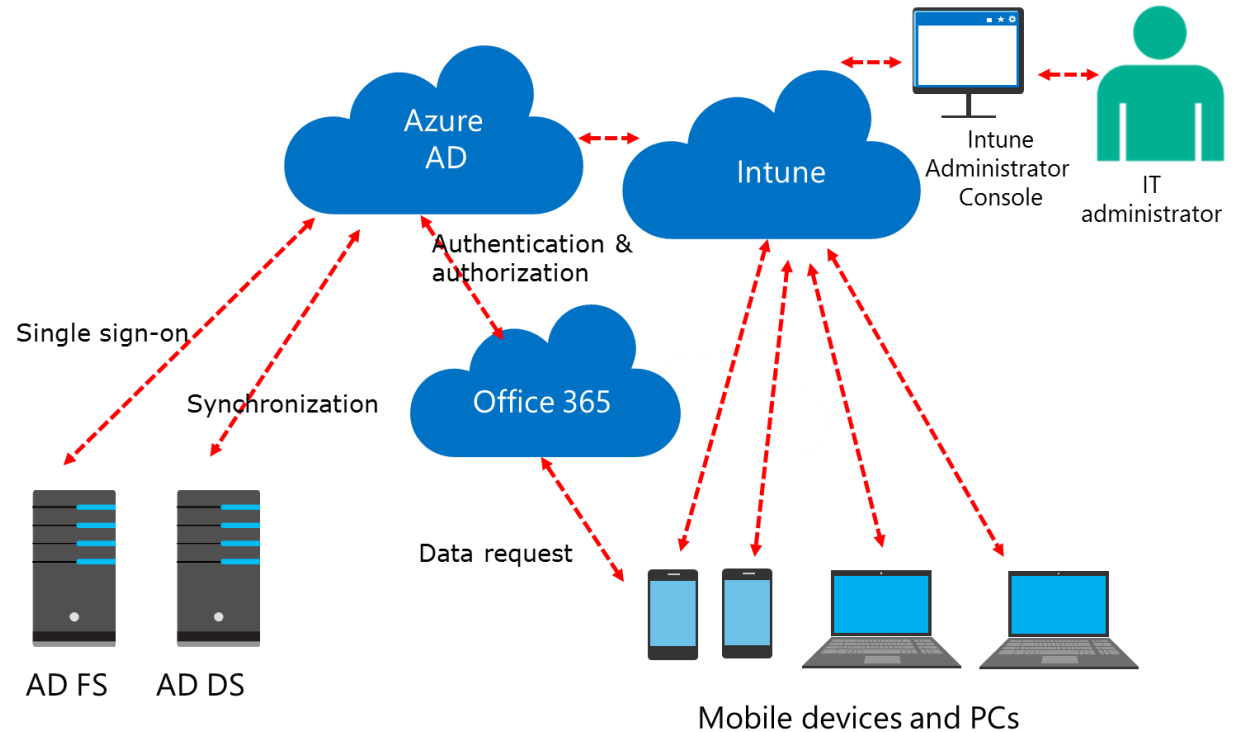
- Device enrollment
- Monitoring and reporting
- Selective delete data
- Configuring devices
- Application Management



# What is Intune?

Intune is a cloud service that you use to:

- Allow BYOD programs
- Manage corporate-owned phones
- Control Office 365 access from kiosks and other unmanaged devices
- Help ensure security compliance of mobile devices





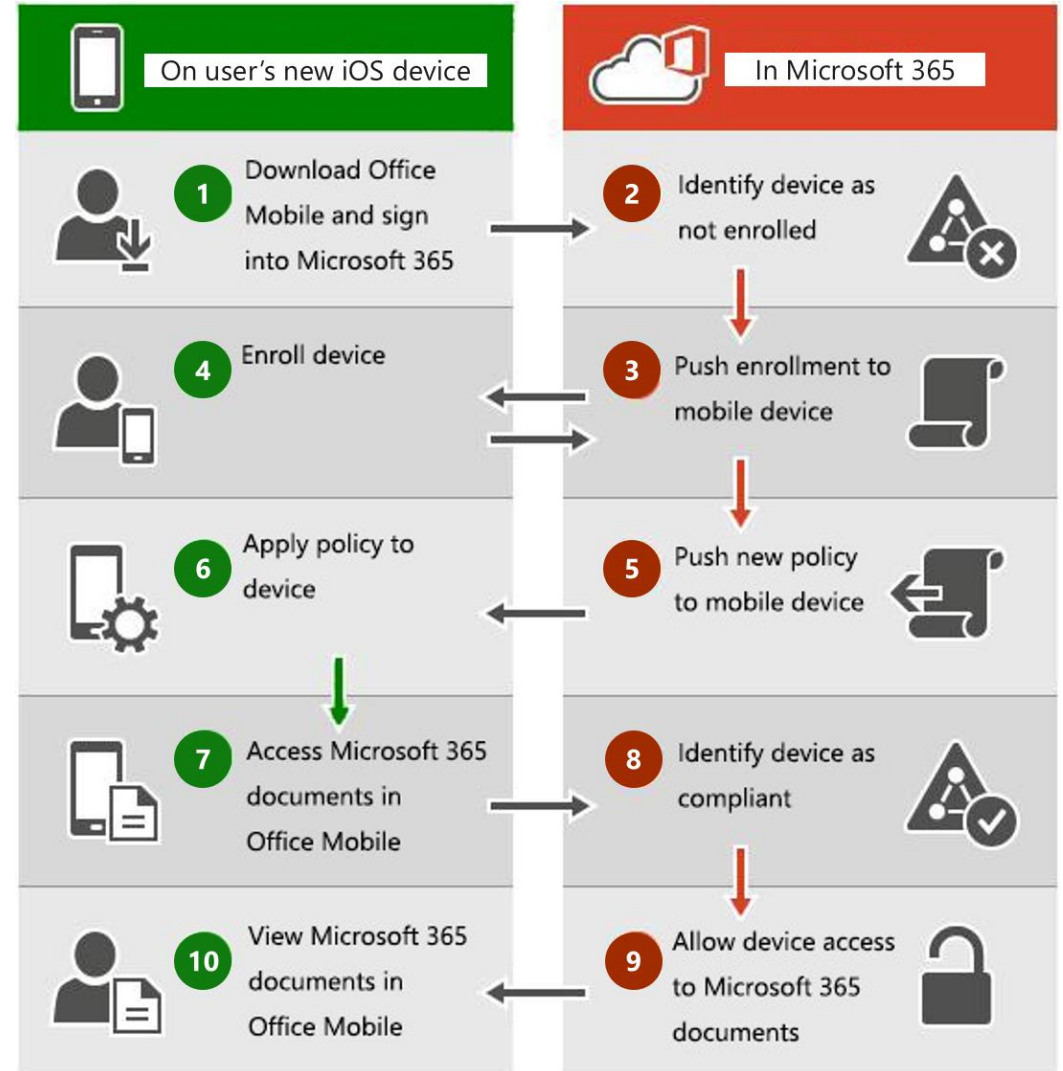
# Comparing MDM for Office 365 and Intune

Category	Feature	MDM for Office 365	Microsoft Intune (cloud only)
Device configuration	Inventory mobile devices that access corporate applications	•	•
	Remote factory reset (full device wipe)	•	•
	Mobile device configuration setting (PIN length, PIN required, lock time, etc.)	•	•
	Self-service password reset (Office 365 cloud only users)	•	•
Office 365	Provides reporting on devices that do not meet IT policy	•	•
	Group-based policies and reporting (ability to use groups for targeted device configuration)	•	•
	Root and jailbreak detection	•	•
	Remove Office 365 app data from mobile devices while leaving personal data and apps intact (selective wipe)	•	•
	Prevent access to corporate email and documents based upon device enrollment and compliance policies	•	•
Premium mobile device & app management	Self-service Company Portal for users to enroll their own devices and install corporate apps		•
	App deployment (Windows Phone, iOS, Android)		•
	Deploy certificates, VPN profiles (including app-specific profiles), email profiles, and Wi-Fi profiles		•
	Prevent cut/copy/paste/save as of data from corporate apps to personal apps (mobile application management)		•
	Secure content viewing via Managed Browser, PDF Viewer, Image Viewer, and AV Player apps for Intune		•
	Remote device lock via self-service Company Portal and via admin console		•
PC management	Client PC management (e.g. Windows 8.1 inventory, antimalware, patch, policies, etc.)		•
	PC software management		•
	Comprehensive PC management (e.g. Group Policy, login scripts, BitLocker management, virtual desktop and power management, custom reporting, etc.)		
	Windows Server/Linux/UNIX/Mac OS X support		
	OS deployment and imaging		

# Intune device communication flow architecture

Intune sends policies to devices and learns the state of the device and app through:

- Device settings
- Device settings and data usage information that the cellular provider reads
- Data protection compliance information
- Device compliance information



# Managing devices with Intune

# Options for managing devices

Device enrollment:

- Preferred for Windows 10
- Required for phones and non-Windows devices
- Highly scalable

Intune client installation, required for:














- Windows 7
- Remote assistance with TeamViewer
- Executable file or similar software installations

# Rules for enrolling devices with Intune

- With Intune, you can manage the following platforms:
  - Apple iOS 9.0 and later
  - Mac OS X 10.9 and later
  - Android 4.4 and later and Android for Work
  - Windows Phone 8.1, Windows 8.1 RT and Windows 8.1 (Sustaining mode) PCs
  - Windows 10 and Windows 10 Mobile
  - Windows 10 IoT Enterprise and Windows 10 IoT Mobile Enterprise
  - You can manage Windows 7 PCs only by using the Intune client software
- You can manage device enrollment by configuring the following enrollment options:
  - Terms and conditions
  - Enrollment restrictions
  - Enable Apple device enrollment
  - Corporate identifiers
  - Multi-factor authentication
  - Device enrollment manager

Configure platforms

Specify the platform configuration restrictions that must be met for a device to enroll. Use compliance policies to restrict devices after enrollment. Define versions as major.minor.build. Version restrictions only apply to devices enrolled with the Company Portal. Intune classifies devices as personally-owned by default. Additional action is required to classify devices as corporate-owned. [Learn More.](#)

	VERSIONS		PERSONALLY OWNED
Android	Allow min/max range: <div>Min  Max </div>	 	<div><div>Allow</div><div>Block</div></div>
iOS	Allow min/max range: <div>Min  Max </div>	 	<div><div>Allow</div><div>Block</div></div>
macOS	Restriction not supported		<div><div>Allow</div><div>Block</div></div>
Windows (MDM) 	Allow min/max range: <div>Min  Max </div>	 	Restriction not supported

# Intune device profile overview

- Manage device features and settings, such as:
  - Device features
  - Device restrictions
  - Email
  - Wi-Fi
  - VPNs
  - Education
  - Certificates
  - Edition upgrades
  - Endpoint protection settings
  - Windows Information Protection
  - Custom settings
- Must be assigned to groups to take affect
- Known as configuration policies in the classic portal

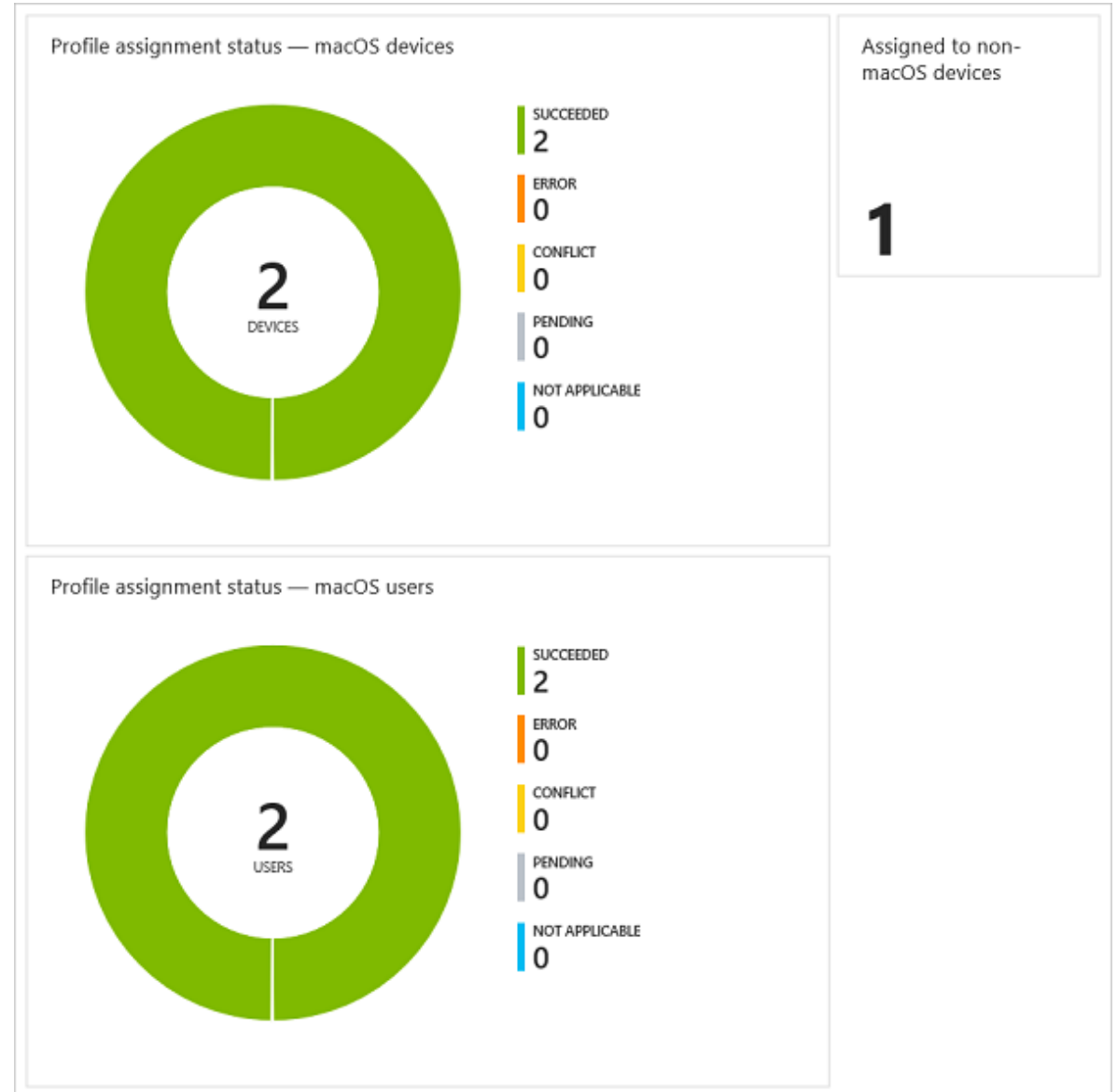
# Managing Intune device profiles

- Device profiles for Windows 10:
  - Email
  - Wi-Fi
  - VPN
  - Education
  - Certificates
  - Edition upgrade
  - Endpoint protection
  - Windows Information Protection

- To create a device profile:
  1. Within the Intune console in the Azure portal, open the **Device Configuration** blade.
  2. Open the **Create Profile** blade.
  3. Provide a name and description for the profile.
  4. Select the device platform.
  5. Select the profile type, which varies based on the platform.
  6. Provide the settings required by the profile type.

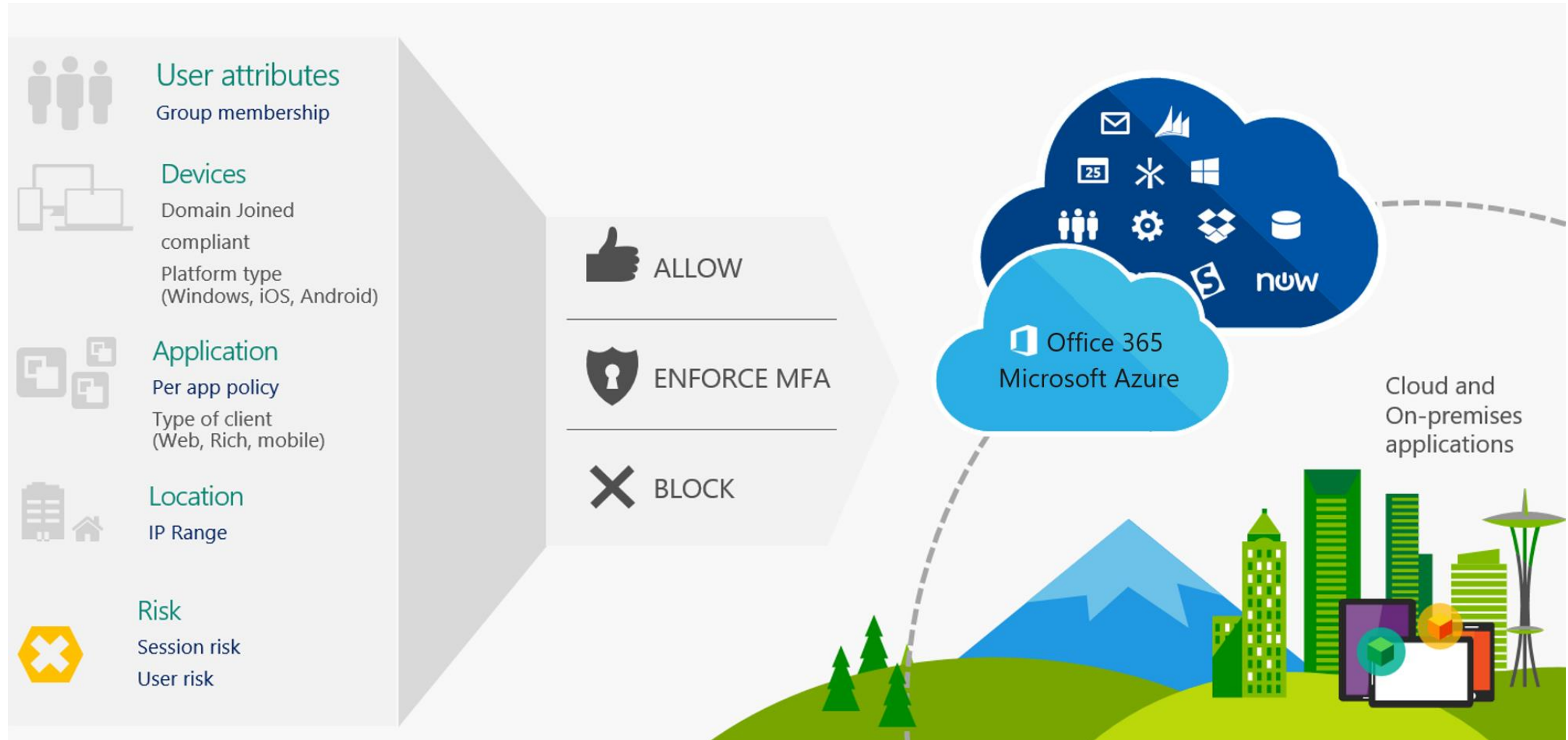
# Monitor profiles

- To view existing profiles:
  1. Sign in to the Azure portal.
  2. Select **All services**, filter on Intune, and select **Microsoft Intune**.
  3. Select **Device configuration** > **Profiles**.
- After you create your device profile, Intune provides graphical charts that display the status of a profile, such as successful assignment, or profile conflict





# Protecting data on devices by using Intune



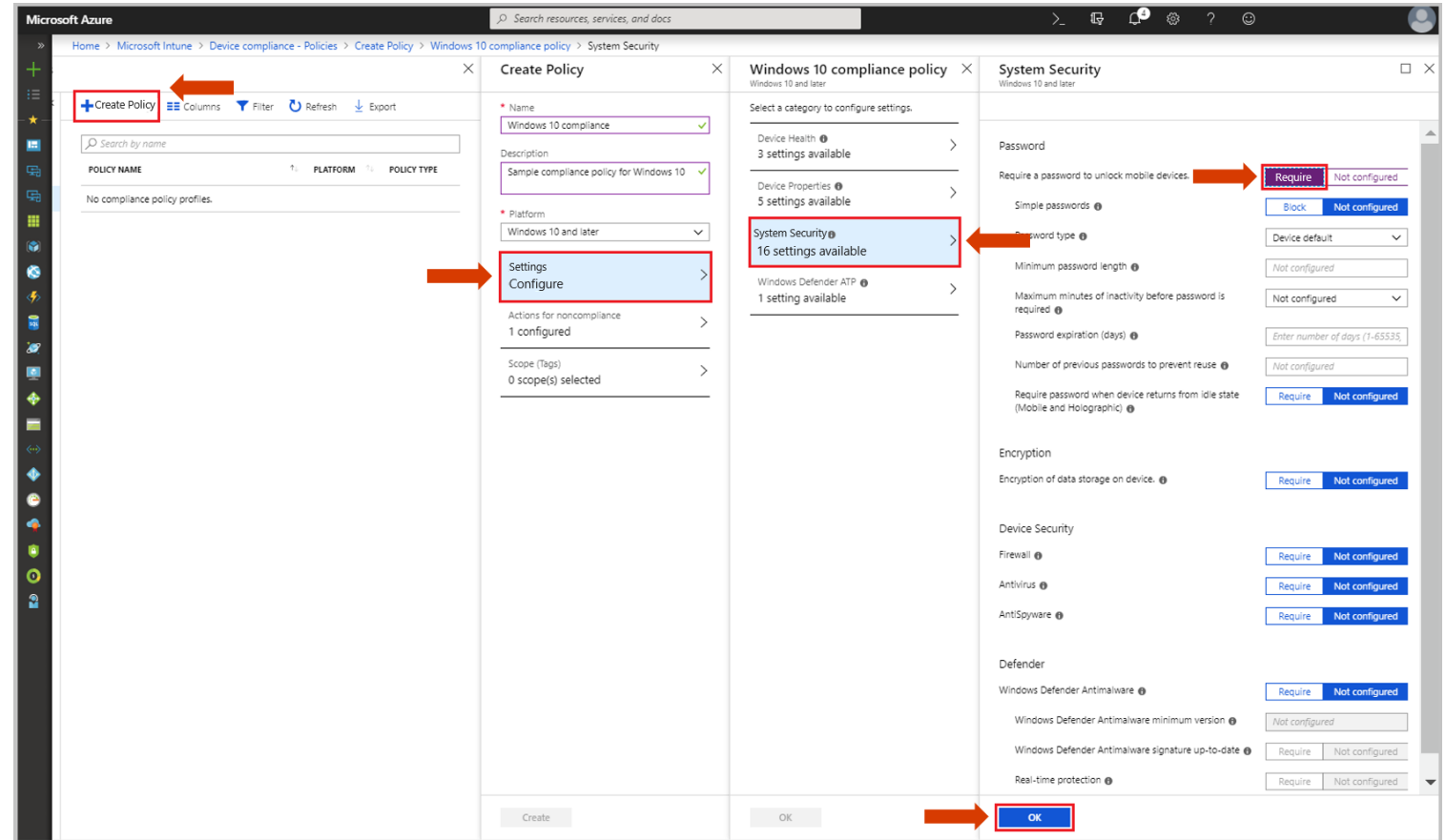
**Implement device compliance policies**

# What is device compliance policy?

- Consists of rules that include:
  - Password settings
  - Encryption settings
- Typically used for conditional access
- Deployed to user groups, not device groups
- Created per platform in the Azure portal
- Created as common across all platforms in the classic portal
- Monitored from the Device Compliance Dashboard

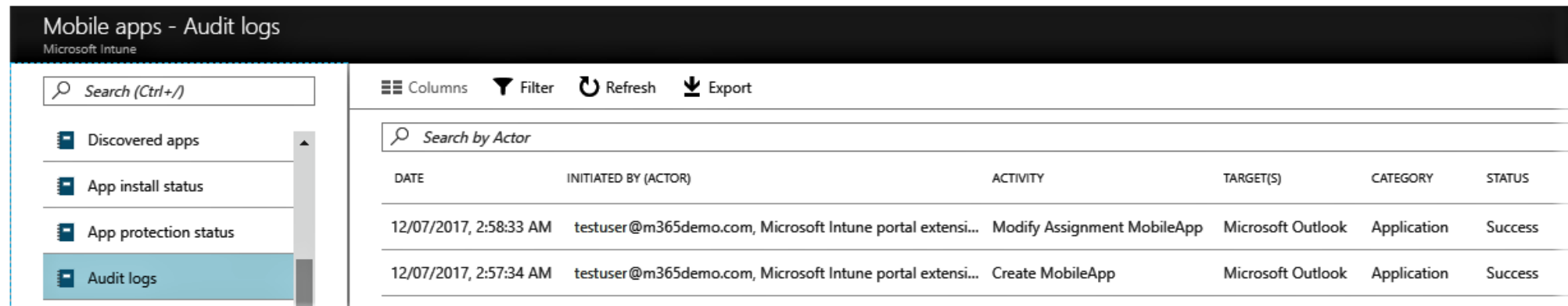
# Deploying device compliance policy

- You can deploy compliance policy to users in user groups or devices in device groups.
- On Windows 10 version 1803 and newer devices, it's recommended to deploy to device groups if the primary user didn't enroll the device



# Monitoring enrolled devices

- You can perform basic device monitoring on the Intune blade in the Azure portal and the Microsoft 365 admin portal
- Intune stores audit logs of all activities that generated changes in Microsoft Intune
- Auditing is enabled by default, and cannot be disabled
- In the Intune blade you can also trigger a device action and view history of the remote actions that were run on different devices



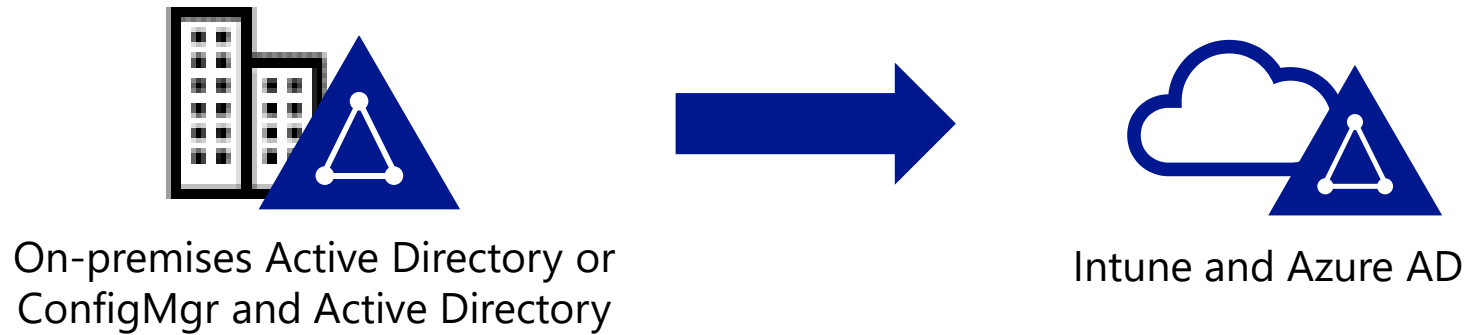
DATE	INITIATED BY (ACTOR)	ACTIVITY	TARGET(S)	CATEGORY	STATUS
12/07/2017, 2:58:33 AM	testuser@m365demo.com, Microsoft Intune portal extensi...	Modify Assignment MobileApp	Microsoft Outlook	Application	Success
12/07/2017, 2:57:34 AM	testuser@m365demo.com, Microsoft Intune portal extensi...	Create MobileApp	Microsoft Outlook	Application	Success

# Device management options

# Benefits of modern management

- Easy to deploy and manage
- Always up to date
- Intelligent security, built-in
- Proactive insights

# Co-management: a practical path to modern management



- Simplifies the transition to modern management
- Benefits of modern management from day one
- Devices managed using both on-premises Active Directory and service and Azure Active Directory (Azure AD) and Intune
- Even when not connected to on-premises environment, devices can be managed by Intune



# Planning co-management

- Maximize your users' productivity through single sign-on (SSO) across your cloud and on-premises resources
- Enable co-management by configuring hybrid Azure AD joined devices
- Decide which workloads, you want to move to Intune:
  - Resource access policies
  - Windows Update policies
  - Endpoint Protection
  - Device configuration
  - Office 365 Click-to-Run apps

# Prerequisites for co-management

- To enable co-management for on-premises Active Directory devices:
  - Devices must be hybrid Azure AD joined
  - Latest Azure AD connect must be installed and configured to sync computer accounts to Azure AD
  - Intune MDM must be setup and automatic enrollment configured
  - All users must have Enterprise Mobility + Security (EMS) or Intune license assigned
  - Windows 10 v1709 or later must be used
  - Azure AD automatic enrollment enabled

# Migrating Group Policy management to MDM

- MDM enables admins to apply broader privacy, security, and application management settings through lighter and more efficient tools
  - MDM ideal for BYOD scenarios and lightweight device management.
  - Group Policy is better suited for devices that require more granular policy management.

# What is the MDM Migration Analysis Tool (MMAT)?

- Created to ease the transition to modern management
- Can analyze Group Policies set for a user or device
- Will cross-reference against its built-in list of supported MDM policies
- Will create reports indicating if a given Group Policy settings can be migrated directly to Intune
- Free and can be downloaded from GitHub

**Manage Intune device enrollment and  
inventory**

# Managing Corporate Enrollment Policy

Configure automatic MDM enrollment and MFA

- Recommendation: configure automatic MDM enrollment - devices automatically enroll in Intune
- Use the Azure Portal, under Azure AD -> Mobility
- Recommendation: protect all Administrator accounts in Azure with Multi-Factor Authentication (MFA)
  - No extra cost
- MFA for normal user accounts requires Azure AD P2 licenses or Enterprise Mobility + Security (EMS) licenses

# Managing Corporate Enrollment Policy

Simplify Windows enrollment without Azure AD Premium

- Create CNAME records to simplify enrollment and device registration when not licensed for Azure AD Premium
- If no CNAME records, users must type the Intune server name during enrollment
- CNAME records must be configured as follows:
  - **EnterpriseEnrollment.yourdomain.com** and point to **EnterpriseEnrollment.s.manage.microsoft.com**
  - **EnterpriseRegistration.yourdomain.com** and point to **EnterpriseRegistration.windows.net**

# Enrolling Windows, Android and iOS devices to Intune

## Enrolling Windows 10 devices

- Many ways to enroll Windows 10 devices in Microsoft Intune:
  - Add work or school account
  - Modern app sign-in (user driven)
  - Enroll in MDM only (user driven)
  - Azure AD join (Out of Box Experience (OOBE))
  - Azure AD join (autopilot – User-driven deployment mode)
  - Enroll in MDM only (Device Enrollment Manager)
  - Azure AD device registration + automatic enrollment Group Policy Object
  - System Center Configuration Manager co-management
  - Azure AD join (bulk enrollment using provisioning package)
  - Azure AD join (autopilot self-deploying mode)



# Enrollment rules

- The device enrollment manager (DEM) can enroll and install devices through the Company Portal on behalf of the user
- A DEM can be used to enroll up to 1000 devices
- A user must exist in Azure AD to be added as a DEM
- Do not use an administrative user as a DEM

# Enrolled devices inventory in Intune

- You can download reports (csv format) for all your devices and applications within the Intune Portal
- For richer reports:
  - Use Intune Data Warehouse and Power BI
  - Microsoft Graph API lets you access all Intune data
    - Create reports using Power BI or Excel based on the data
    - Microsoft Graph also enables you to script almost everything in Azure AD and Intune

# Configuring device profiles

# What are Intune device profiles?

- Microsoft Intune includes settings and features that you can enable or disable on different devices within your organization
- These settings and features are managed using profiles

# Types of device profiles

- The following device profiles are available in Intune:
  - Device features, Device restrictions, Device restrictions (Windows 10 Team)
  - Edition upgrade and mode switch, Email, Email (Samsung KNOX only)
  - Endpoint protection, Identity protection, Kiosk (Preview)
  - Network boundary, Trusted certificate, SCEP certificate
  - PKCS certificate, VPN, Windows Defender ATP (Windows 10 Desktop)
  - Wi-Fi, Education profile, iOS update policies, Certificates
  - Custom

# Manage PowerShell scripts in Intune

- Upload PowerShell scripts to Intune and run them on Windows 10 devices
- Devices must be joined to Azure Active Directory (Azure AD)
- Devices must run Windows 10 version 1607 or later
- To run PowerShell scripts, you must:
  1. Create the script and test it before using it in Intune
  2. Upload the script to Intune
  3. Assign the script to the Azure AD group containing the devices that will run the script
  4. Monitor script execution in the console

# Creating a custom device profile

- Intune may not have all the built-in settings you need or want
- You can create a custom device profile for Windows 10, Android and iOS devices
- Custom settings are configured differently for each platform
- New Open Mobile Alliance Uniform Resource Identifier (OMA-URI) settings are added regularly
- You can find lists online with all the configuration service providers (CSPs) that Windows 10 supports
- You assign the custom profile to an Azure AD group
- You can monitor the status of an assigned profile in Intune

# Assigning and monitoring device profiles

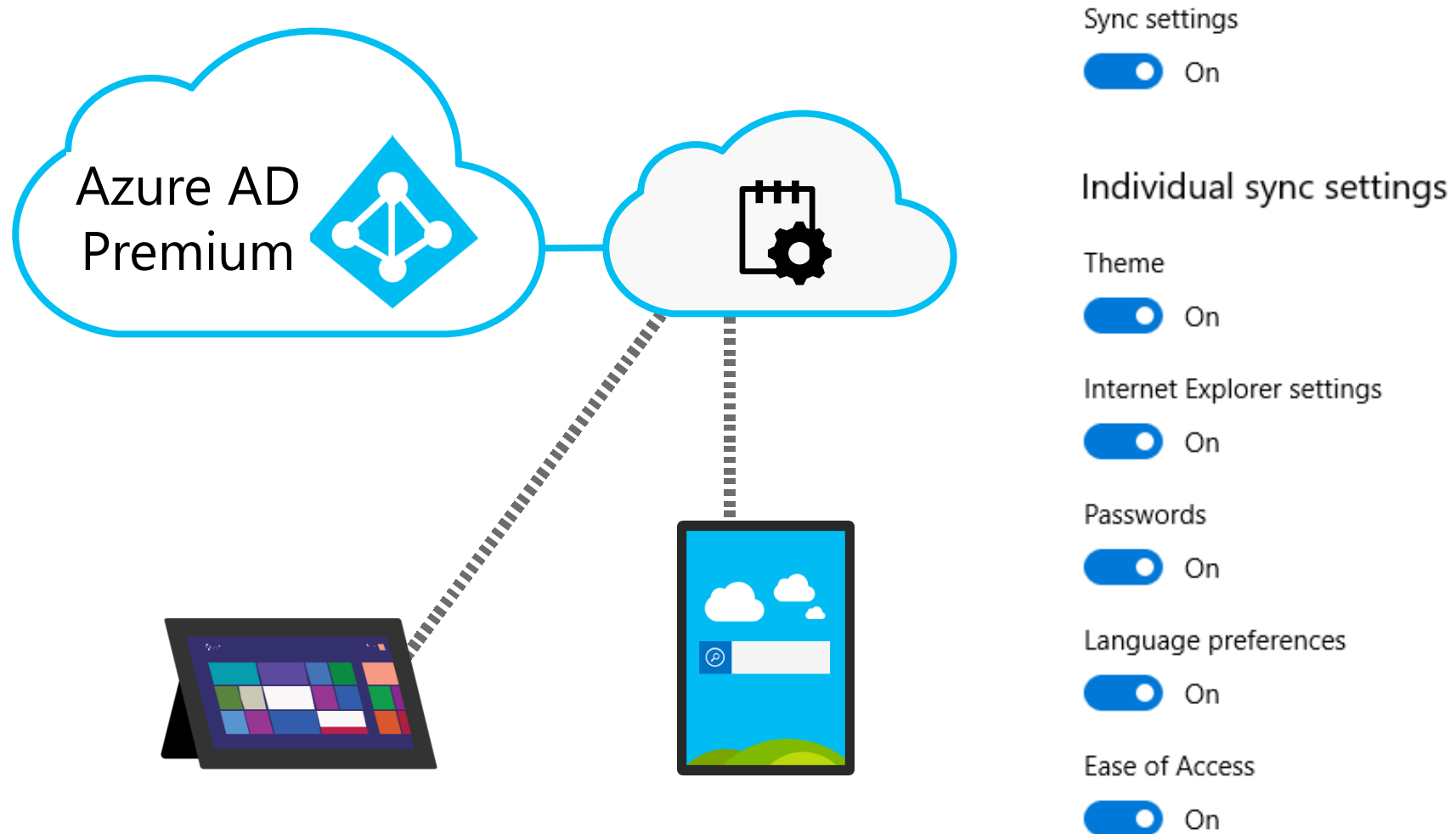
- A profile must be assigned to have any effect on a device
- You can assign it to the following Azure AD groups:
  - Selected Groups
  - All Users & All Devices
  - All Devices
  - All Users
- You can exclude groups from the assignment
- You can check the status of a profile, see which devices are assigned and get a graphical overview of the status
- It's also possible to view settings in a profile that are causing conflicts with settings in another profile



# Managing user profiles

# Enterprise State Roaming overview

Sync settings between Azure AD-joined Windows 10 devices



# Configuring Enterprise State Roaming in Azure

- Enterprise State Roaming benefits:
  - Roaming is based on the Azure AD account
  - Separation of business and private data
  - Enhanced security and data encryption
  - Management and monitoring
  - Synced data is kept in the same region
  - Data retention
- Company must have Azure AD
  - Azure AD Premium P1 or P2 required
  - Windows 10 device must be Azure AD-joined
- Sync is across devices based on Azure AD account

# Monitoring devices

# Monitor and manage devices enrolled to Intune

In Azure portal > Intune > Devices

- You can get a lot of information:
  - Information about the individual devices
  - How many devices are using the different platforms, including Windows, Android and iOS
  - Hardware inventory
  - Apps installed
- You can perform device actions, that you can trigger on your enrolled devices, such as:
  - Wipe, Delete, Remote lock, Restart, Sync, Quick Scan and Full Scan

# Monitor and manage devices enrolled to Intune

Sync devices to get the latest policies and actions with Intune

Enrolled devices get the policy on their next scheduled check-in with the Intune service, as follows:

Platform	Check-in frequency
iOS	Every 6 hours
Mac OS X	Every 6 hours
Android	Every 8 hours
Windows 10 (enrolled as devices)	Every 8 hours
Windows 8.1	Every 8 hours

# Monitor and manage devices enrolled to Intune

Manage settings and features on your devices with Intune policies

- Microsoft Intune policies:
  - Groups of settings that control features on mobile devices and computers
  - You create policies by using templates that include recommended or custom settings
  - You deploy them to device or user groups
- When a device checks in, it immediately receives any pending actions or policies that have been assigned to it
- The Sync device action forces the selected device to immediately check in with Intune

# **Implement Mobile Application Management (MAM)**



# Overview of Mobile Application Management (MAM)

- MAM protects an organization's data within an application and manages the application
- You implement MAM by creating app protection policies in Intune
- Mobile Device Management (MDM) (Intune) manages the device
- App protection policies supported by Android and iOS
  - For windows 10, use Windows information Protection (WIP)
- Intune MAM supports two configurations:
  - Intune MDM + MAM
    - Device are enrolled in Intune
  - MAM without enrollment
    - Devices are not enrolled
    - Devices are not managed, but applications are
    - Typically used in bring your own device (BYOD) scenarios

# Application considerations in MAM

- An app must be “built” to work with MAM
- You can get an updated list of MAM-enabled apps from Microsoft’s website
- Some apps support multi-identity, let you use different accounts (work and personal) to access the same apps, while app protection policies apply only when the apps are used in the work context.

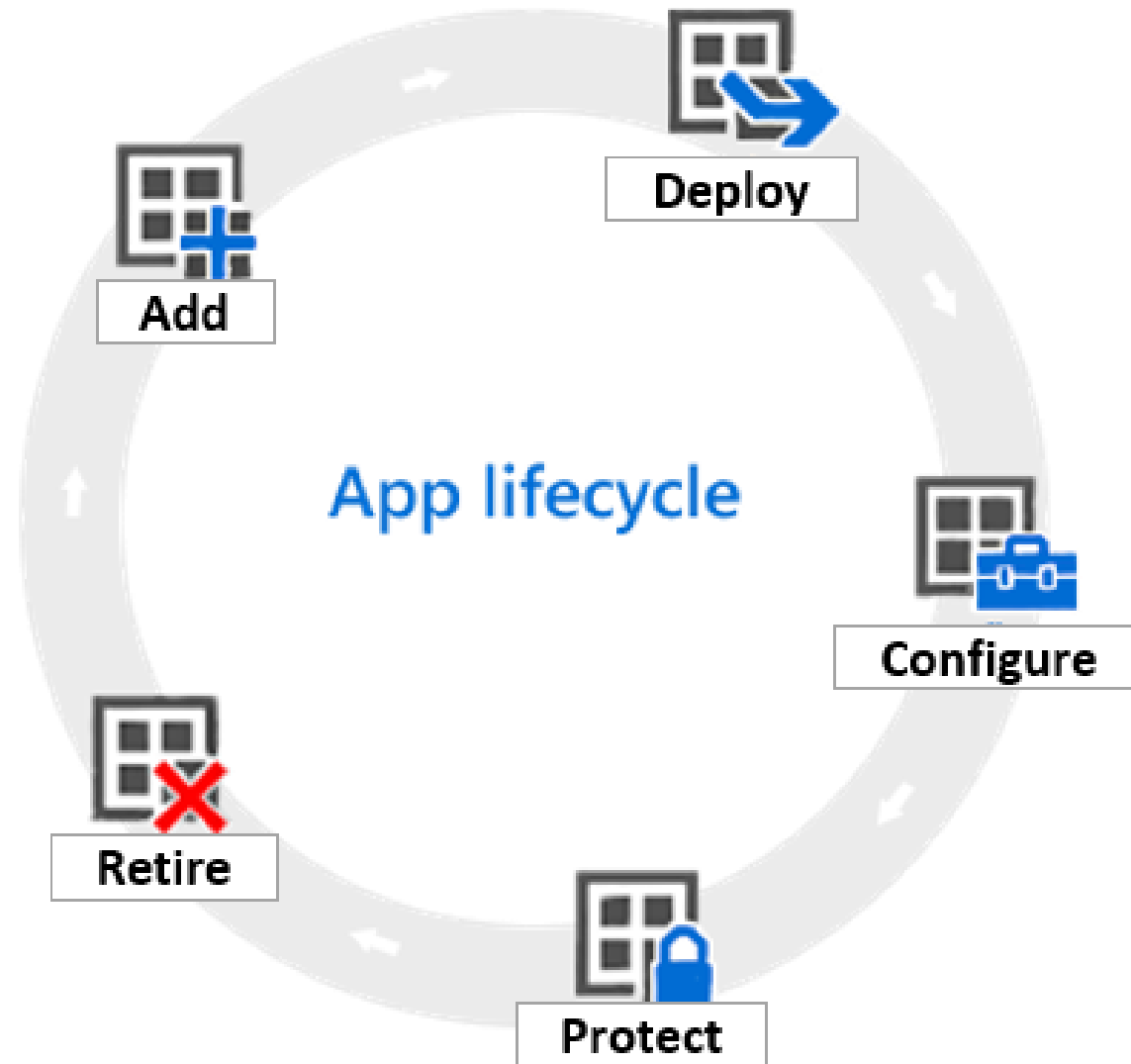
# Implementing and managing MAM policies in Intune

- App protection policies can be applied to apps running on devices that may or may not be enrolled in Intune
- Intune app protection policies are assigned to users
- Intune app protection policies can only be assigned to Android or iOS devices

**Deploying and updating applications**

# Deploying applications with Intune

Intune app lifecycle



# Deploying applications with Intune

Working with apps in Intune

You can add the following app types in Intune:

- Store app
  - Windows, Android and iOS
- Office 365 Suite
  - Windows 10 and macOS
- Other
  - Web link, Build-in app, Line of Business (LOB) apps, and Windows app (Win32)

# Microsoft Store for Business overview

- Microsoft Store (for general audience):
  - Apps, games, music, movies, TV shows, and books
- Microsoft Store for Business (for companies):
  - Business-related modern apps and LOB apps
- Microsoft Store for Business main benefits:
  - Scalable, free, and familiar infrastructure services
  - Private store
  - Bulk app acquisition for company employees
  - App distribution and integration with management tools
  - Support for company LOB apps
  - App license tracking and management
  - Automatic updating of deployed apps

# Configuring Microsoft Store for Business

## Requirements

- **Internet connectivity:**
  - Microsoft Store for Business is a cloud service
- **Windows 10 devices:**
  - Windows 10 devices include Microsoft Store app
  - Microsoft Store for Business apps install only on Windows 10 devices
- **Windows Update service must be enabled:**
  - Service is for downloading and installing updates
- **Azure Active Directory (Azure AD) account:**
  - Required to sign in to the Microsoft Store for Business
- **Web browser for administration:**
  - Not required for accessing Microsoft Store for Business apps



# Configuring Microsoft Store for Business

## Implementing Microsoft Store for Business

- Available for free to organizations that have Azure AD:
  - Azure subscription or Microsoft Office 365
  - Azure AD tenant can be created as part of the sign-up process
- You must sign up for Microsoft Store for Business:
  - <https://www.microsoft.com/business-store>
  - Five apps are added to the private store by default
- Manage Microsoft Store for Business in a web browser
- Access Microsoft Store for Business by using a Microsoft Store app or web browser
- Store permissions are delegated by assigning roles:
  - Role can be assigned only to Azure AD users, not groups

# Using Microsoft Store for Business

## Licensing and apps

- Store apps only work on Windows 10 devices:
  - Universal Windows Platform apps for Windows 10
  - Universal Windows apps, by device: phone, Microsoft Surface Hub, Internet of Things (IoT), and Microsoft HoloLens
- Apps in the private store can be:
  - Obtained from Microsoft Store for Business
  - LOB apps, developed for your organization
- Microsoft Store for Business licensing models:
  - Online licensing
  - Offline licensing

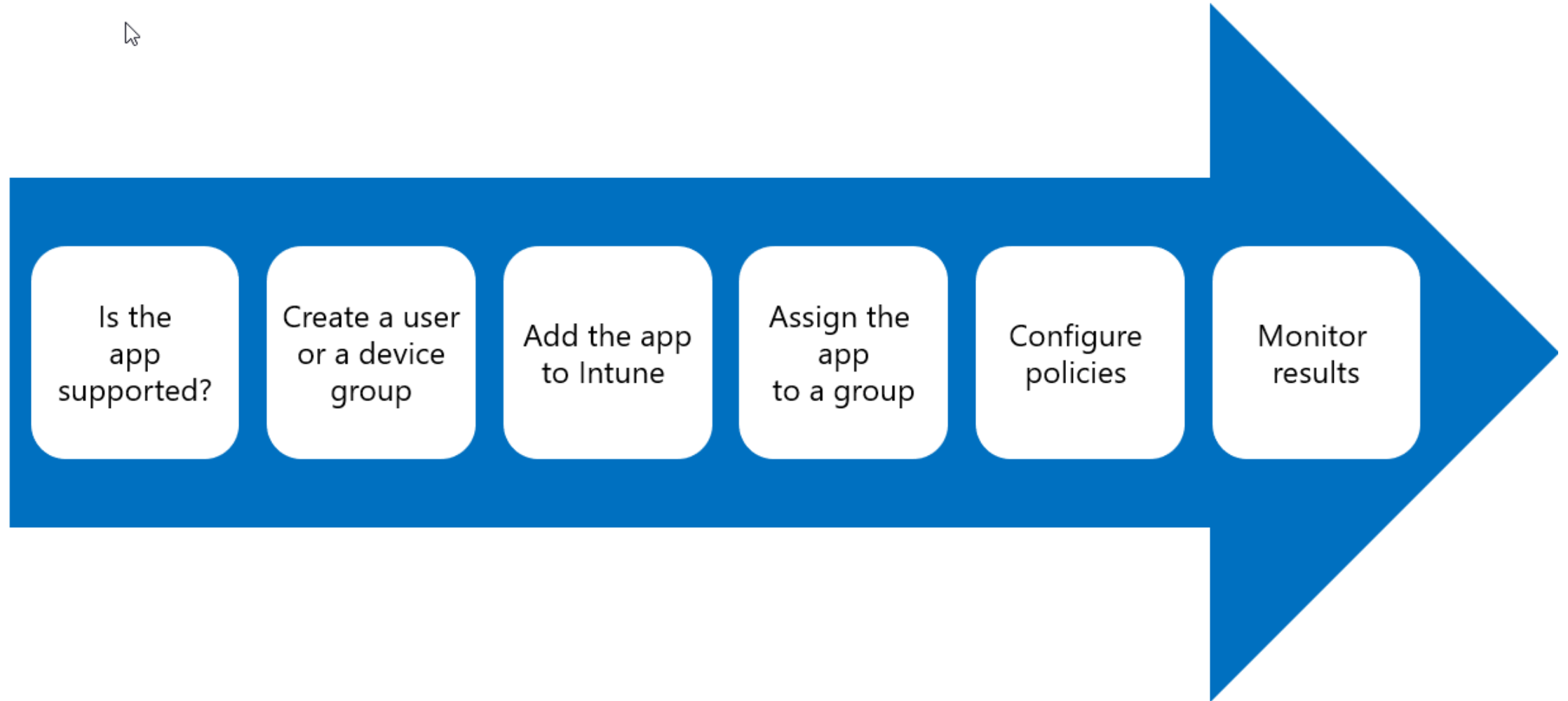
# Using Microsoft Store for Business

## Apps in Microsoft Store for Business

- **Distribute apps by using a private store:**
  - Only for online-licensed apps
  - Add apps to the private store
  - All organizational users can install apps from the private store
- **Assign apps to users:**
  - Only for online-licensed apps
  - Obtained apps can be assigned to users
  - User can install the apps from email notifications
  - Licenses can be reclaimed when no longer needed
- **Distribute apps with a management tool:**
  - Can use for online-licensed and offline-licensed apps
  - Use mobile device management tool such as Microsoft Intune

# Administering applications

# Managing apps with Intune



# Configuring and managing Internet Explorer

- Microsoft Edge is default browser in Windows 10
- Specific websites and apps with compatibility problems with Microsoft Edge can be redirected to Internet Explorer automatically
- You use Enterprise Mode to redirect sites to Internet Explorer
  - Create an Enterprise Mode site list containing sites you want to redirect
  - You use Enterprise Mode Site List Manager to create site lists
- Enable Enterprise Mode by configuring the Group Policy setting  
**Configure the Enterprise Mode Site List** here:
  - Computer Configuration/Administrative Templates/Windows Components/Microsoft EdgeOR
  - User Configuration/Administrative Templates/Windows Components/Microsoft Edge

# App inventory review

## Client apps - Apps

Microsoft Intune

Search (Ctrl+J)

Overview

### Manage

Apps

App protection policies

App configuration policies

App selective wipe

iOS app provisioning profiles

### Monitor

App licenses

Discovered apps

App install status

App protection status

Audit logs

### Setup

iOS VPP tokens

+ Add

Refresh

Export

Columns

Search by name or publisher...

NAME	TYPE	STATUS	ASSIGNED	VPNS
Adobe Reader Touch	Microsoft Store for Business app		No	None
Company Portal	Microsoft Store for Business app		No	None
Download Manager	Windows MSI line-of-business app		No	None
Edge	Built-In iOS app		Yes	None
Excel Mobile	Microsoft Store for Business app		No	None
Fresh Paint	Microsoft Store for Business app		No	None
Microsoft Outlook	iOS store app		No	None
Office 365 ProPlus	Office 365 ProPlus Suite (Windows 10)		Yes	None
OneNote	Microsoft Store for Business app		No	None
PowerPoint Mobile	Microsoft Store for Business app		No	None
Sway	Microsoft Store for Business app		No	None
Word Mobile	Microsoft Store for Business app		No	None





# DEMO

## Microsoft Intune





# DEMO

## Microsoft Store for Business



# Moderní správa a nasazení Windows 10

Kamil Roman

[Konzultace@KamilRT.net](mailto:Konzultace@KamilRT.net)

[www.KamilRoman.EU](http://www.KamilRoman.EU)