

Tech Summit Roadshow

Build your cloud Skills with the latest in
Azure, Microsoft 365 & Dynamics 365

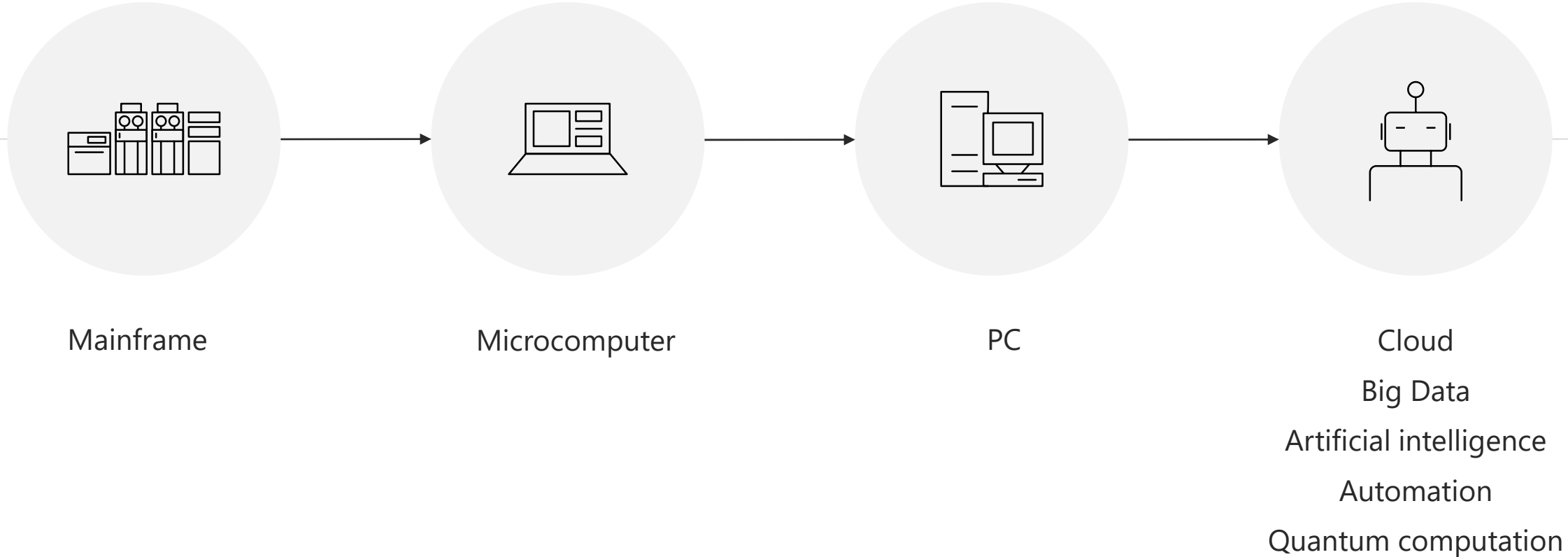


Modern IT with Co- Management

Technical Solution Professional
Modern Desktop



Transformative Tools



IT USE EVOLVED

Classic Workplace

Single Device Platform

Business Owned

Work in the office

Manual

Reactive

Full Service tailored to
Boomers & Gen-Xers

Modern Workplace

Multiple Device Platforms

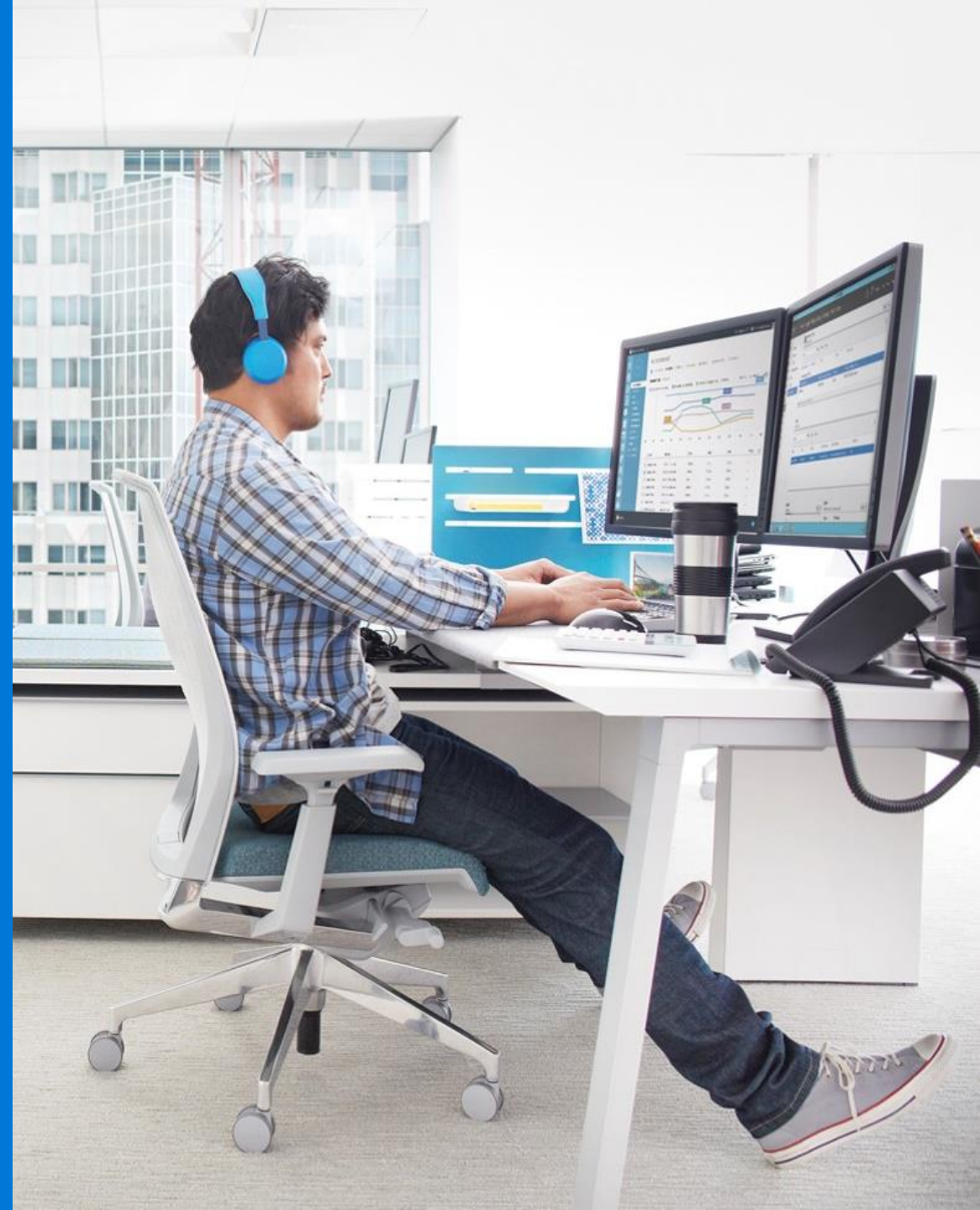
User and Business Owned

Work anywhere

Automated

Proactive

Self-Service tailored to
Millennials & Gen-Yers



On-premises



Legacy devices

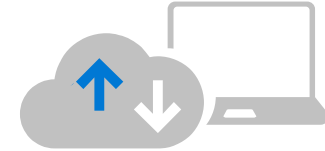
Windows 7

Office

Active Directory

ConfigMgr

Windows Defender



Modern Workplace

Modern devices

Windows 10

Office 365

Azure Active Directory

Microsoft Intune

Microsoft Threat Protection

Bridging the Classic & Modern Workplaces



The Promises of Modern Management



Modern Workplace

- Work from anywhere
- Choose the device you want or bring your own
- Quick, friendly out-of-box experience
- Self-service



Cloud IT

- Integrated and cloud-based security
- Simpler application delivery through Store/SaaS
- Data intelligence for better business insights



Lower TCO

- Minimize on-prem infrastructure costs
- Unified identity, device and app management
- Self-service deployment without imaging

Simplify Windows 10 management and lower TCO

Simplified management & security

Embrace cloud-based management and transition at your pace while staying in control.

- Agentless
- Unified identity, device and O365 ProPlus mgmt.
- Office 365 ProPlus MGMT
- Integrated data protection



Always up to date

Deliver the latest features and security.

Cloud updates mean you don't need to have on-premise update servers.

Control what updates are deployed, to whom and when.



Self-service deployment

Make any new PC enterprise-ready via a simple self-service experience.



Automatically configure devices when your users login with their company credentials.



Proactive insights

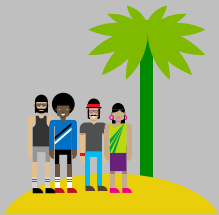
Get ongoing proactive insights to diagnose and fix issues before they happen.

Use cloud intelligence to upgrade Windows 10 and Office 365 ProPlus with confidence.

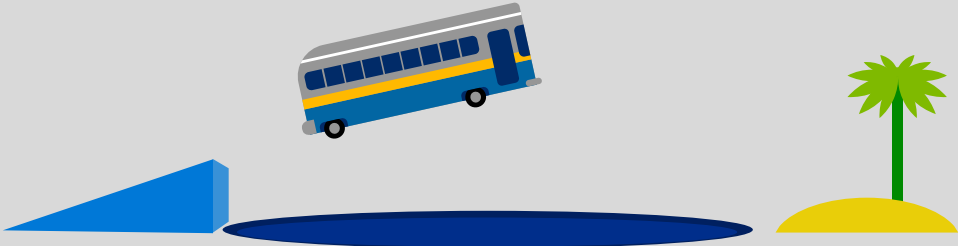


Paths to Modern Management

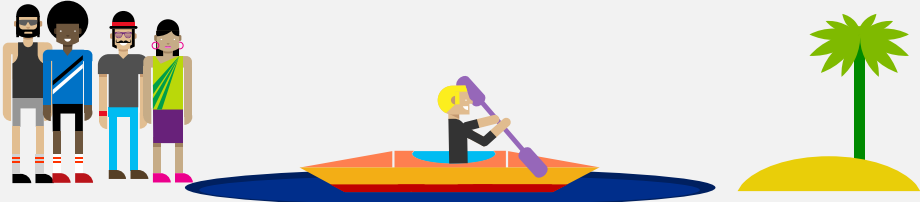
Cloud-first



Big Switch Transition



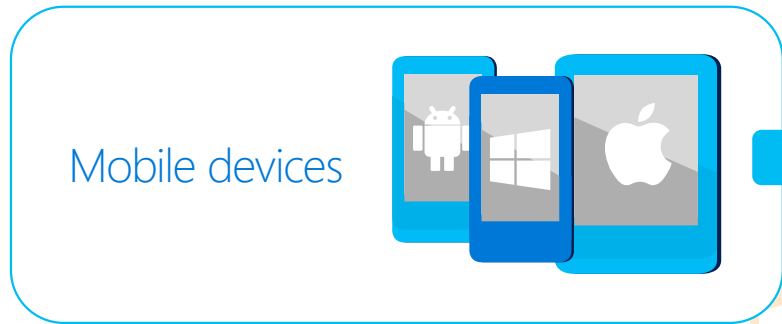
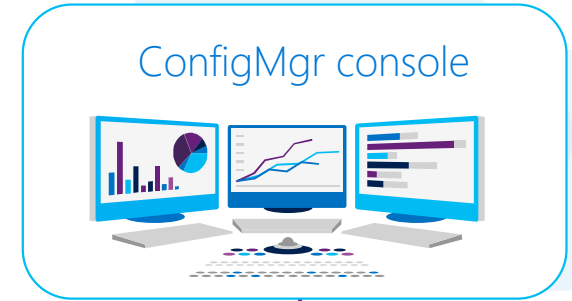
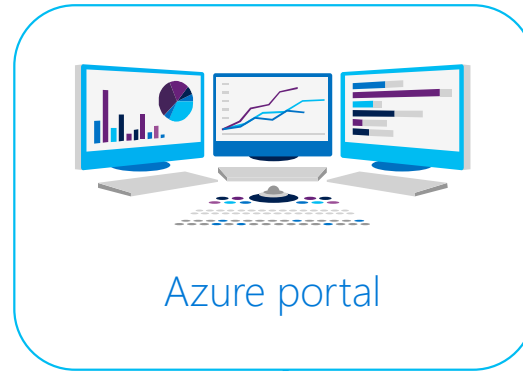
Group by Group Transition






Iterative ("Co-management")



Co-Management Architecture With ConfigMgr and Intune



Management Powered

	 On-premises	 Cloud attached	 Cloud only
Traditional OS Deployment	✓	✓	
Win32 app management	✓	✓	✓
Configuration and GPO	✓	✓	✓
Bitlocker Management	✓	✓	✓
Hardware and software inventory	✓	✓	✓
Update management	✓	✓	✓
Unified Endpoint Management – Windows, iOS, macOS, Android		✓	✓
Modern access control – Compliance, Conditional Access		✓	✓
Modern provisioning – Autopilot, DEP, Zero Touch, KME		✓	✓
Modern security – Hello, Attestation, ATP, Secure Score		✓	✓
Modern policy – Security Baselines, Guided Deployments		✓	✓
Modern app management – O365 Pro Plus, Stores, SaaS, VPP		✓	✓
Full M365 integration – Analytics, Graph, Console, RBAC, Audit		✓	✓

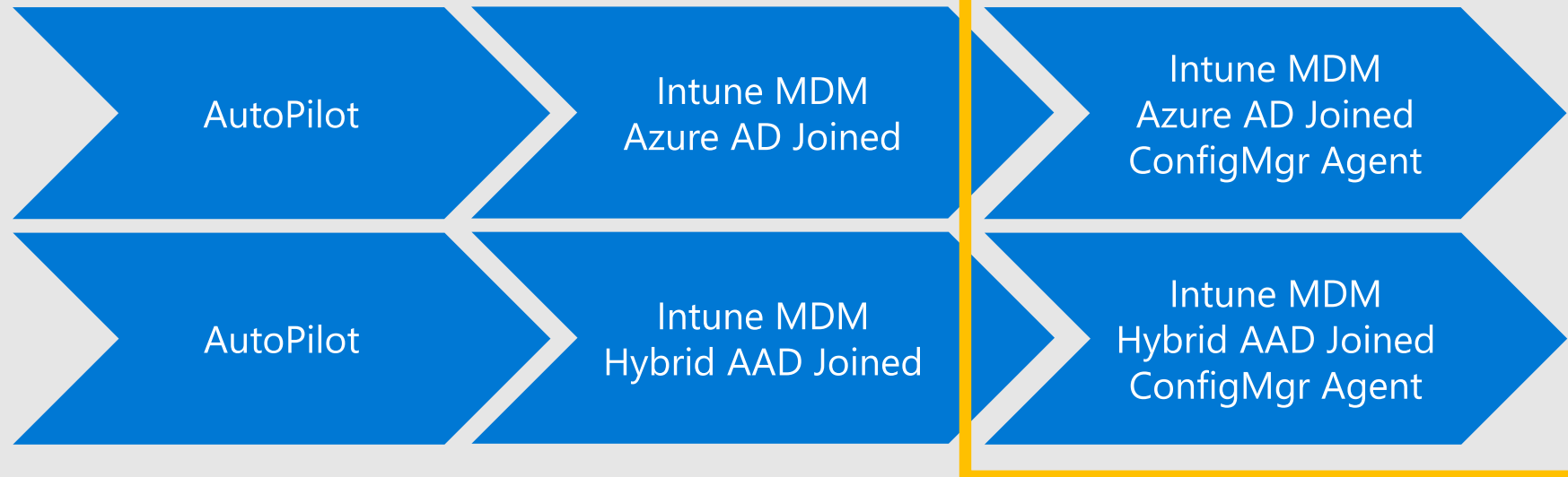
Two main paths to attach to the cloud for existing ConfigMgr customers

1. Existing ConfigMgr managed devices auto-enroll into Intune

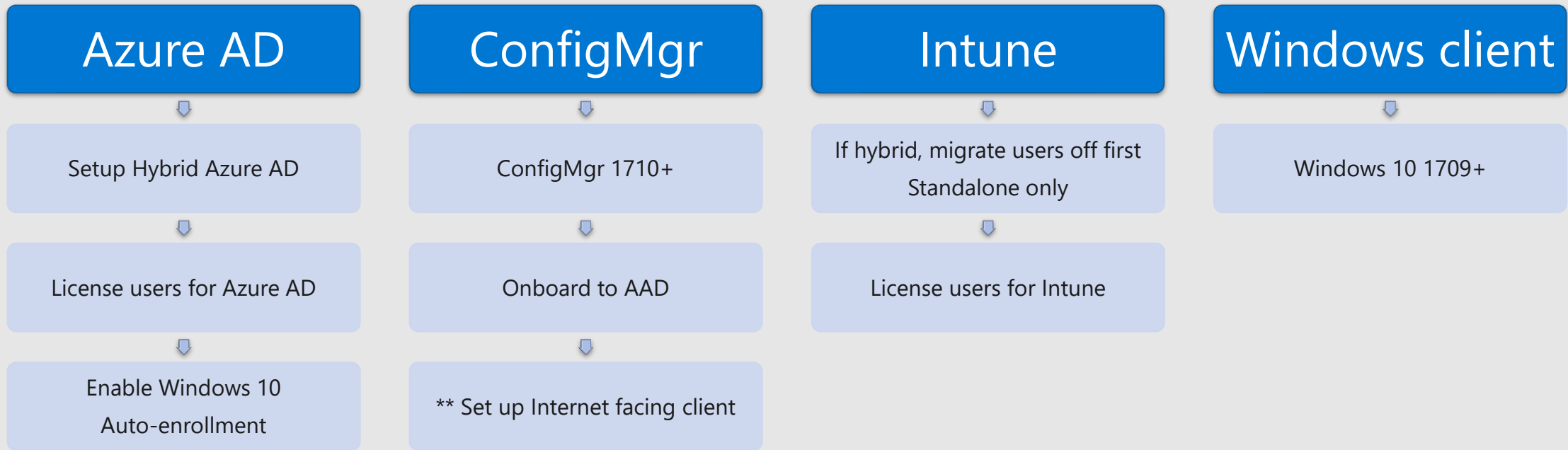
- Transparent
- At scale



2. Modern Provisioning bootstrap ConfigMgr agent

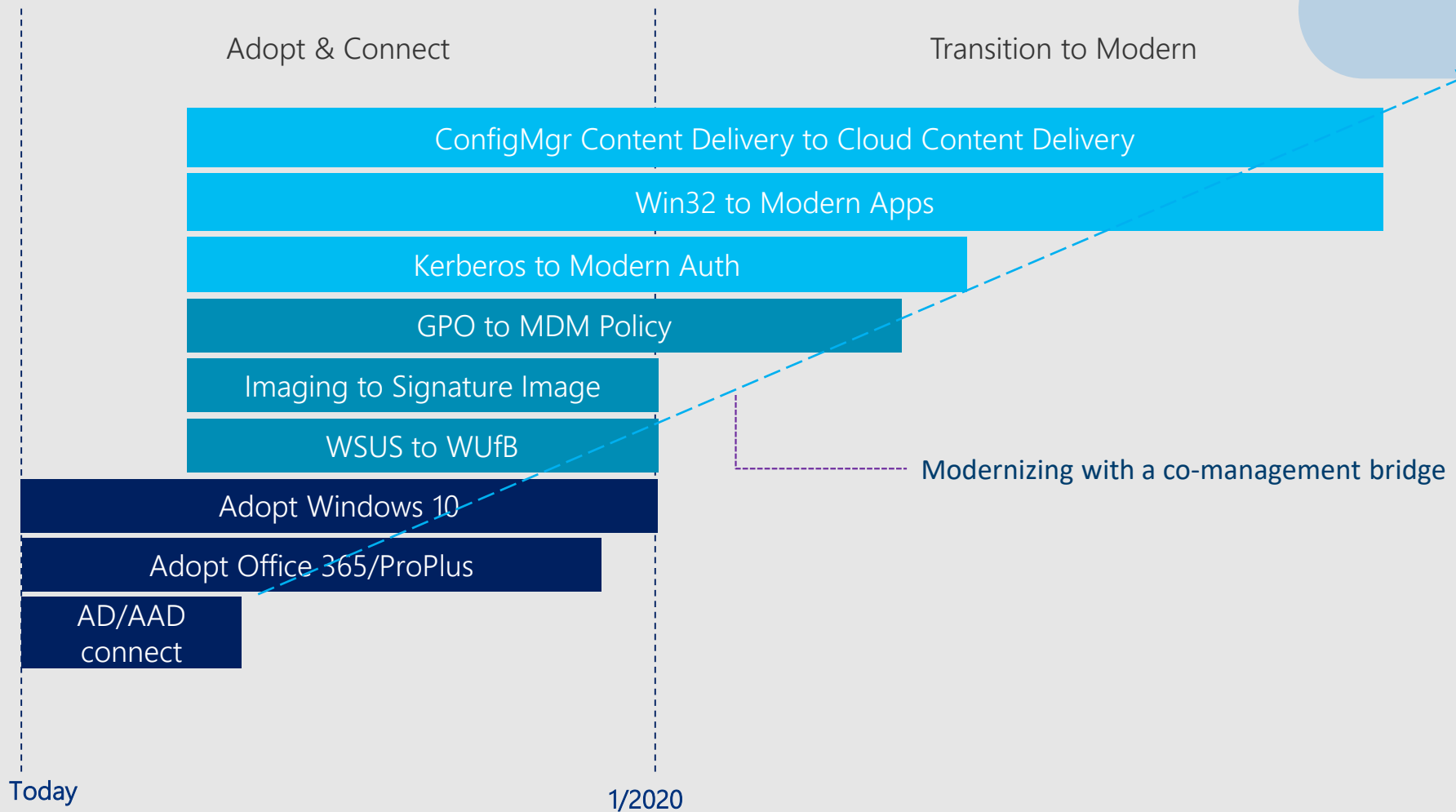


Getting Ready for Cloud Attach

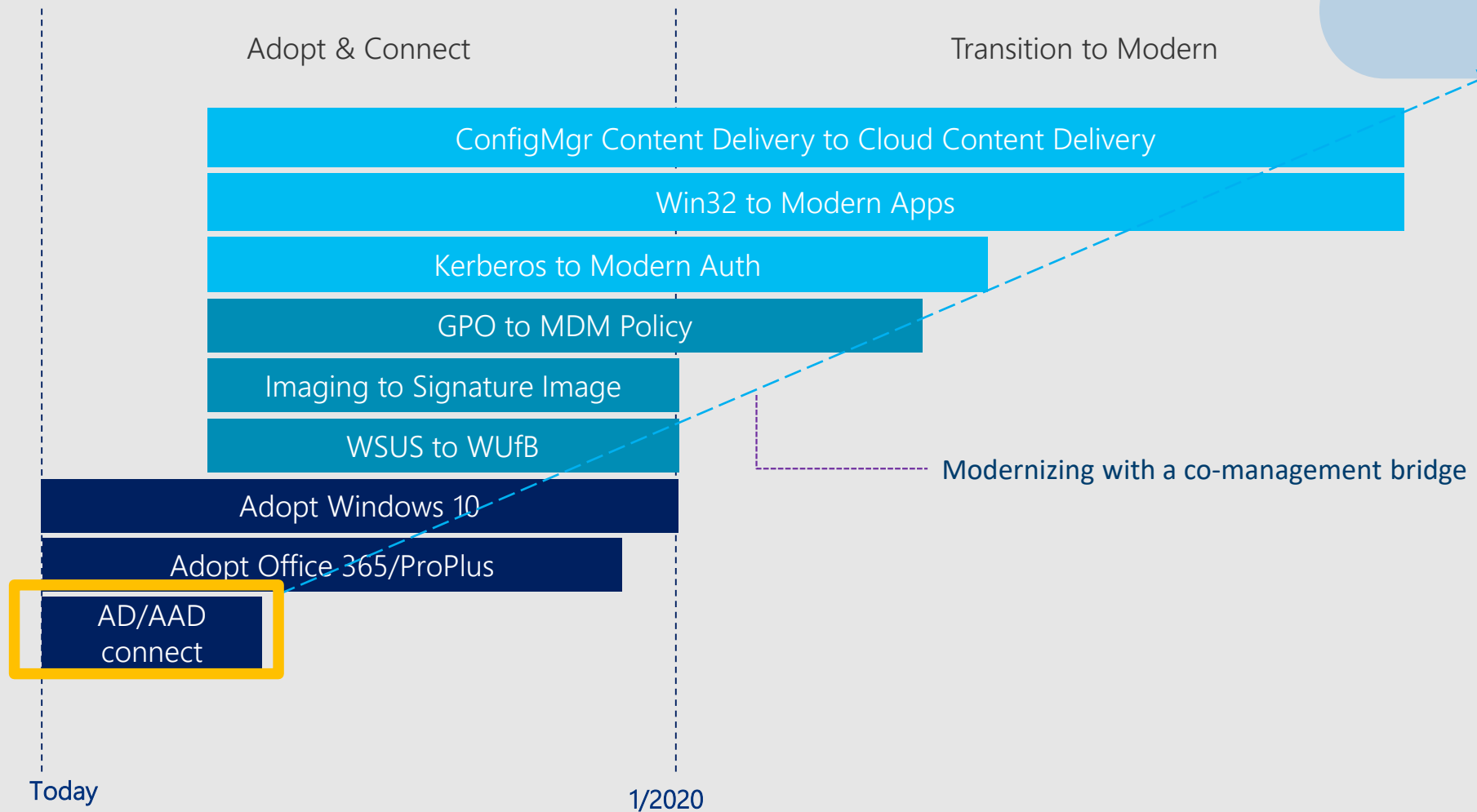


** Optional, only for cloud born devices bootstrapping ConfigMgr client

Bridging to Modern Management



Bridging to Modern Management



From Domain Joined to Azure AD Joined Devices

AD Domain Joined

- Extend your on-premises directory with Azure AD.
- Azure AD Join your AD domain-joined devices
- AD + Azure AD Join new devices through Auto Pilot

Hybrid Azure AD Joined

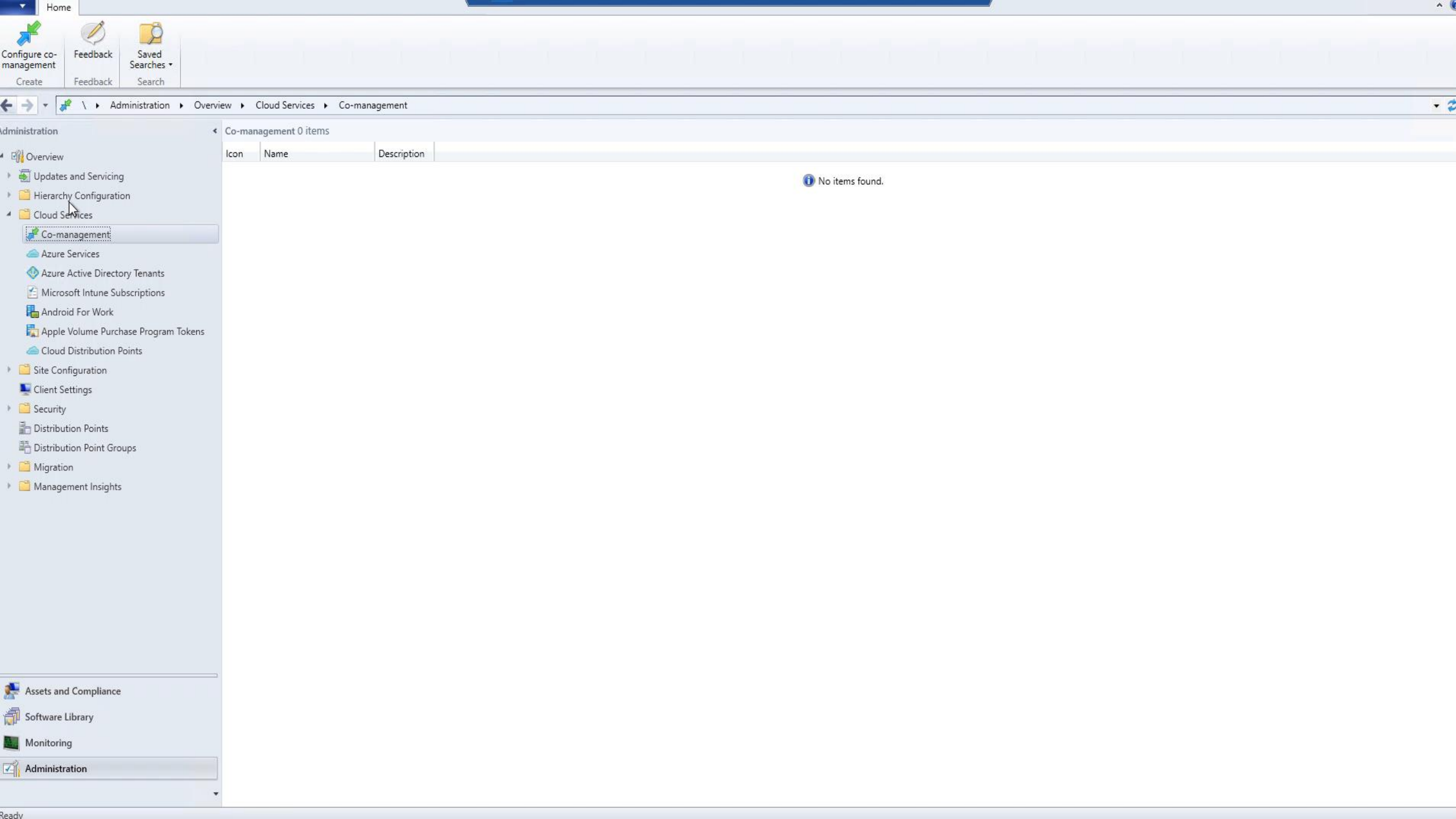
- Transition GPO to MDM
- Pilot Azure AD Join to identify AD auth dependencies
- Gradually move traditional management tools that rely on computer identity to their cloud equivalents or AAD enlightened versions (e.g. ConfigMgr with CMG, WSUS to WUfB)
- AAD Join new devices (AD Joined machines remain AD joined until retired)

Azure AD Joined

... settings are... devices (Enter...
... of Settings...
... can control access...
... Azure AD device-ba...
... conditional access.
Users sign-in conveniently and securely with Windows Hello for Business.

... PC dependency...
... main controllers...
... battery life and...
... performance of the device

Demo: Co-Management



- Administration
 - Overview
 - Updates and Servicing
 - Hierarchy Configuration
 - Cloud Services
 - Co-management**
 - Azure Services
 - Azure Active Directory Tenants
 - Microsoft Intune Subscriptions
 - Android For Work
 - Apple Volume Purchase Program Tokens
 - Cloud Distribution Points
 - Site Configuration
 - Client Settings
 - Security
 - Distribution Points
 - Distribution Point Groups
 - Migration
 - Management Insights
-
- Assets and Compliance
 - Software Library
 - Monitoring
 - Administration**

Co-management 0 items

Icon	Name	Description
------	------	-------------

No items found.

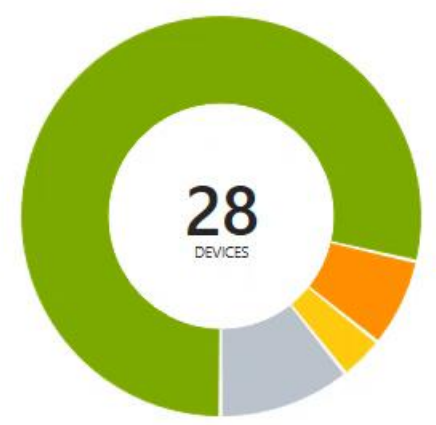
- New
- Dashboard
- Intune
- Azure Active Directory
- All resources
- Resource groups
- App Services
- Function Apps
- SQL databases
- Azure Cosmos DB
- Virtual machines
- Load balancers
- Storage accounts
- Monitor
- Virtual networks
- Advisor
- Security Center
- Billing
- More services >

- Microsoft Intune
- Search (Ctrl+)
- Overview
 - Quick start
- MANAGE
- Device enrollment
 - Device compliance
 - Device configuration
 - Devices
 - Mobile apps
 - eBooks
 - Conditional access
 - On-premises access
 - Users
 - Groups
 - Intune roles
 - Software updates
- HELP AND SUPPORT
- Help and support

Classic portal

Status

Device compliance



Device configuration



Quick tasks

- Find a user
- Find a device
- Add an app
- Create a group
- Create a compliance policy
- Create a configuration policy

Learn more about Intune

- Microsoft Intune overview**
Follow these steps to manage devices, Windows PCs, and apps in your organization
- Protect on-premises email and data**
Take advantage of Intune's conditional access solution to ensure emails can only be accessed by enrolled devices
- Offer bring your own device program**
Use Intune to protect employee owned devices so they can access company data
- Issue corporate owned devices**
Pre-provision multiple corporate owned devices with Intune's bulk enrollment solution

Intune Data Warehouse



Recycle Bin

- ☰
- 🏠
- ☰
- 😊
- 🔍
- ⚙️
- 👤

Apps

Your apps are located in Software Center.
[Open Software Center to get these apps.](#)

Software Center
— □ ×


SCCM PG On-Premises Dogfood

📁 Applications


🔍

All Required


Filter: All
Sort by: Most recent



MSIT AutoVPN
package - MSIT...
MSIT and SCCM Dog...
1.0



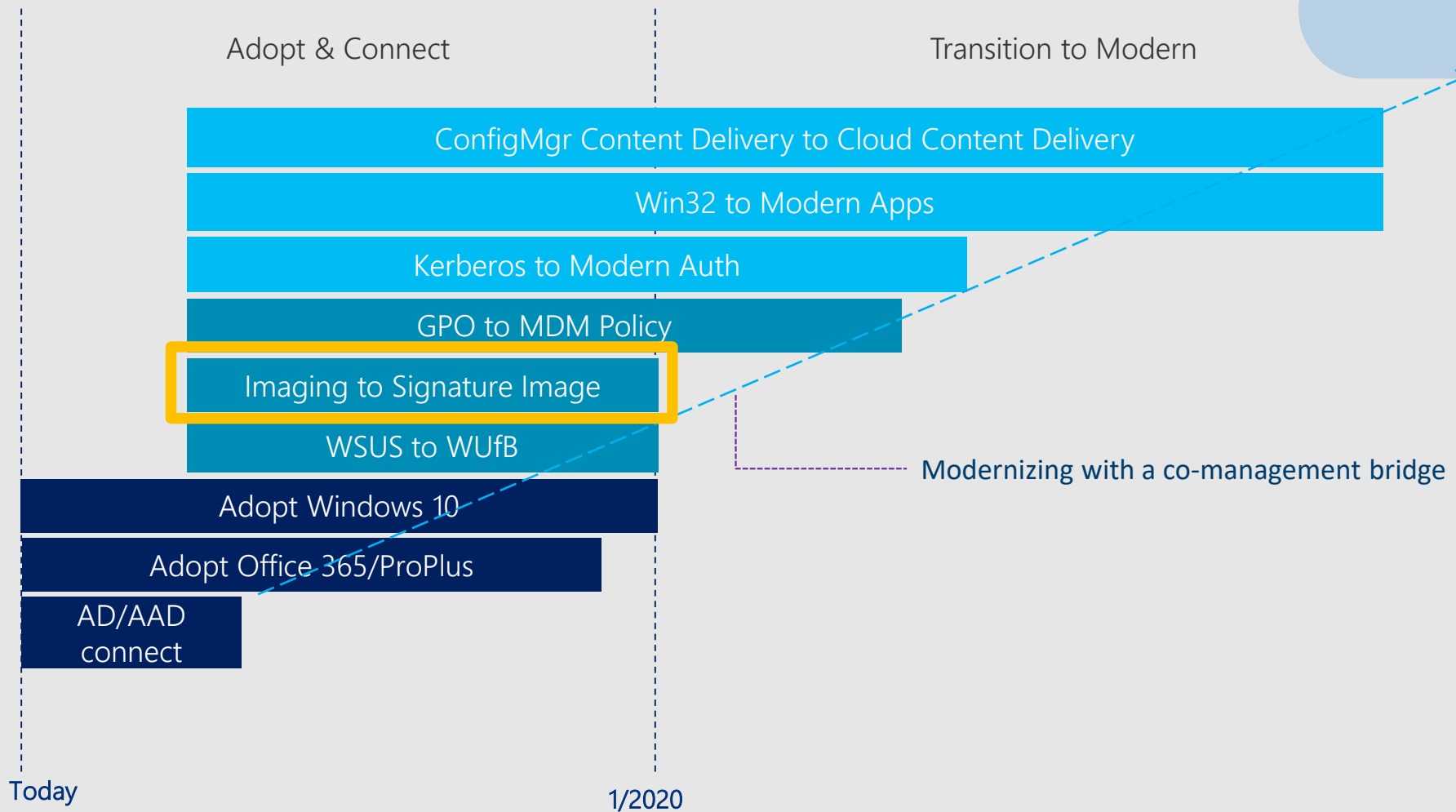
Company Portal
(x86/x64)
Microsoft Corporation
4.0.14621.0



Virtual Smart Card
Certificate Mana...
Microsoft
1.0.191.104

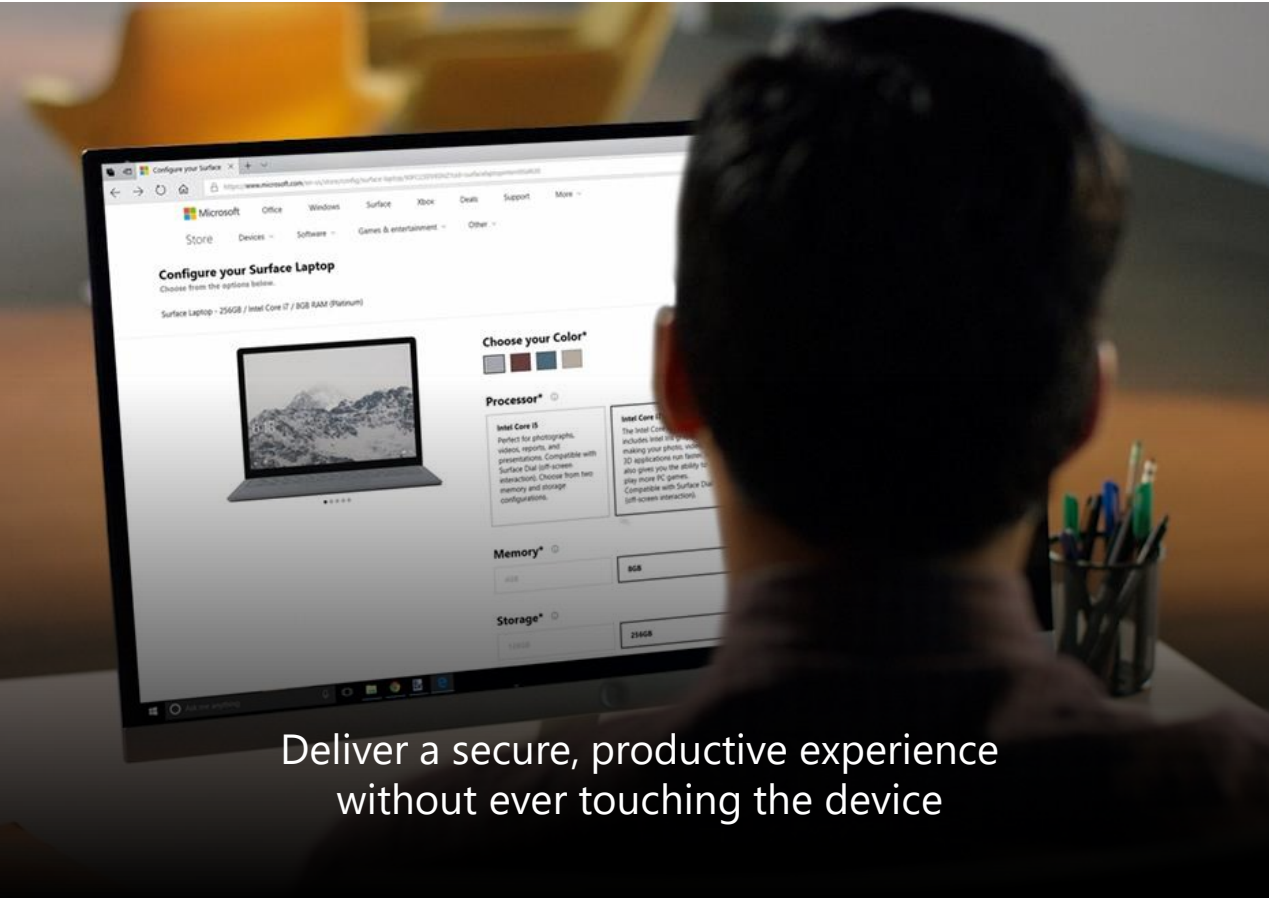


Bridging to Modern Management



Transform device deployment with Windows Autopilot

Great for IT and end users

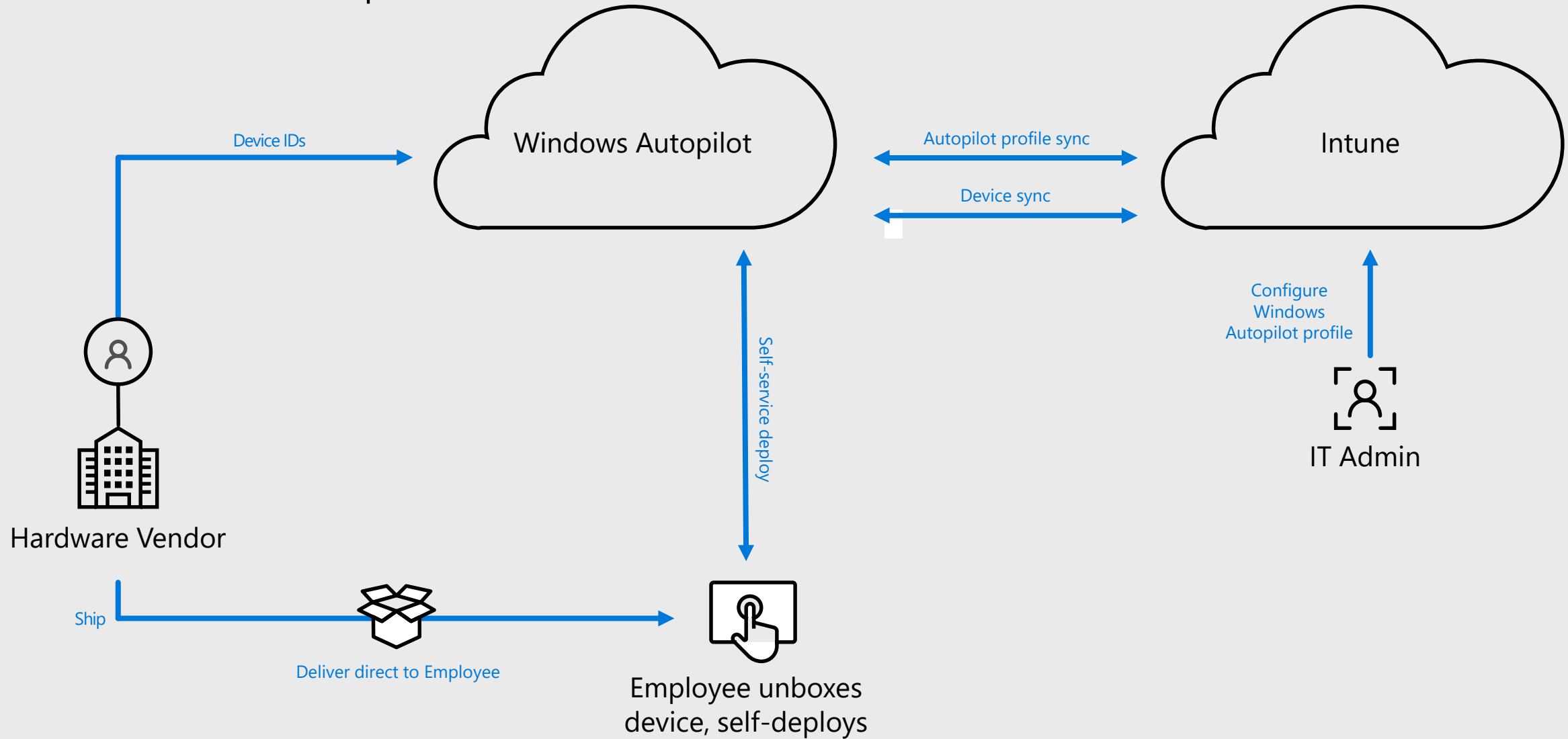


Deliver a secure, productive experience without ever touching the device



Be productive from the start with a personalized out of box experience

Windows Autopilot overview

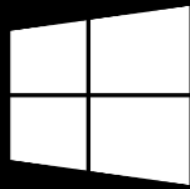


Windows Autopilot Scenarios

AVAILABLE	AVAILABLE	AVAILABLE in 1809	AVAILABLE in 1809	AVAILABLE in 1809	AVAILABLE in 1809
User-driven mode	Windows Autopilot reset - local	Self-deploying mode	Windows Autopilot reset - remote	Hybrid Azure AD Join	Autopilot for existing devices
Windows 10 1703 and above	Windows 10 1709 and above	Windows 10 1809 and above	Windows 10 1809 and above	Windows 10 1809 and above	Windows 10 1809 and above
Join device to AAD, enroll in Intune/MDM	Join device to AAD, enroll in Intune/MDM	No need to provide credentials, automatically joins AAD	Execute a device reset via Intune and maintain AAD join and MDM enrollment	Join device to AD, enroll in Intune/MDM	Windows 7 to Windows 10 ConfigMgr task sequence, followed by Windows Autopilot user-driven mode

Windows Autopilot

User-driven Mode



Continue in English?

English

Français

Español

中文繁体

中文简体

Next



Let's start with region. Is this right?

United Arab Emirates

United Kingdom

United States

Uruguay

Uzbekistan

Vanuatu

Vatican City

Yes



Listening...



Is this the right keyboard layout?

US

United States-Dvorak for left hand DVORAK L

United States-Dvorak for right hand DVORAK R

United States-International QWERTY

Albanian QWERTZ

Azerbaijani PUSUDB

Azeri Latin QUERTY

Yes



Listening...





Want to add a second keyboard layout?



Add layout

Skip




Listening...







Let's connect you to a network


 ContosoGuestWiFi
Open

Connect automatically

[Connect](#)

 Contoso Corp
Secured

 Contoso Corp 2
Secured

 Network4
Open

Skip for now




Now let's get you connected to a network. That way you get updates, apps and cat videos as soon as possible. How about the first one on the list? Want to use that one?







Let's connect you to a network


 ContosoGuestWiFi
Open

Connect automatically

[Connect](#)

 Contoso Corp
Secured

 Contoso Corp 2
Secured

 Network4
Open

Skip for now



Now let's get you connected to a network. That way you get updates, apps and cat videos as soon as possible. How about the first one on the list? Want to use that one?





http://captiveportalwi-fi/eula/1234.htm



Welcome to our Guest Wi-Fi

Agree & Connect

By clicking on the connect button you agree to our [Terms of Service](#) and have reviewed the [Contoso Privacy Policy](#).





http://captiveportalwi-fi/eula/1234.htm



Welcome to our Guest Wi-Fi

Agree & Connect

By clicking on the connect button you agree to our [Terms of Service](#) and have reviewed the [Contoso Privacy Policy](#).





Alright, you're connected. Just a moment...





Now we'll check for any updates...





 Welcome, Anna!

Enter password for your Contoso email account



anna@contoso.com

[Start over with a different account](#)

[Forgot password?](#)

Next



Listening...





 Welcome, Anna!

Enter password for your Contoso email account



anna@contoso.com

[Start over with a different account](#)

[Forgot password?](#)

Next



Listening...





Setting up your work account...



Setting up your device for work

This could take a while and your device may need to reboot.



Device preparation

Complete



Device setup [Hide details](#)

Identifying

Security policies (Identifying)

Certificates (Identifying)

Network connections (Identifying)

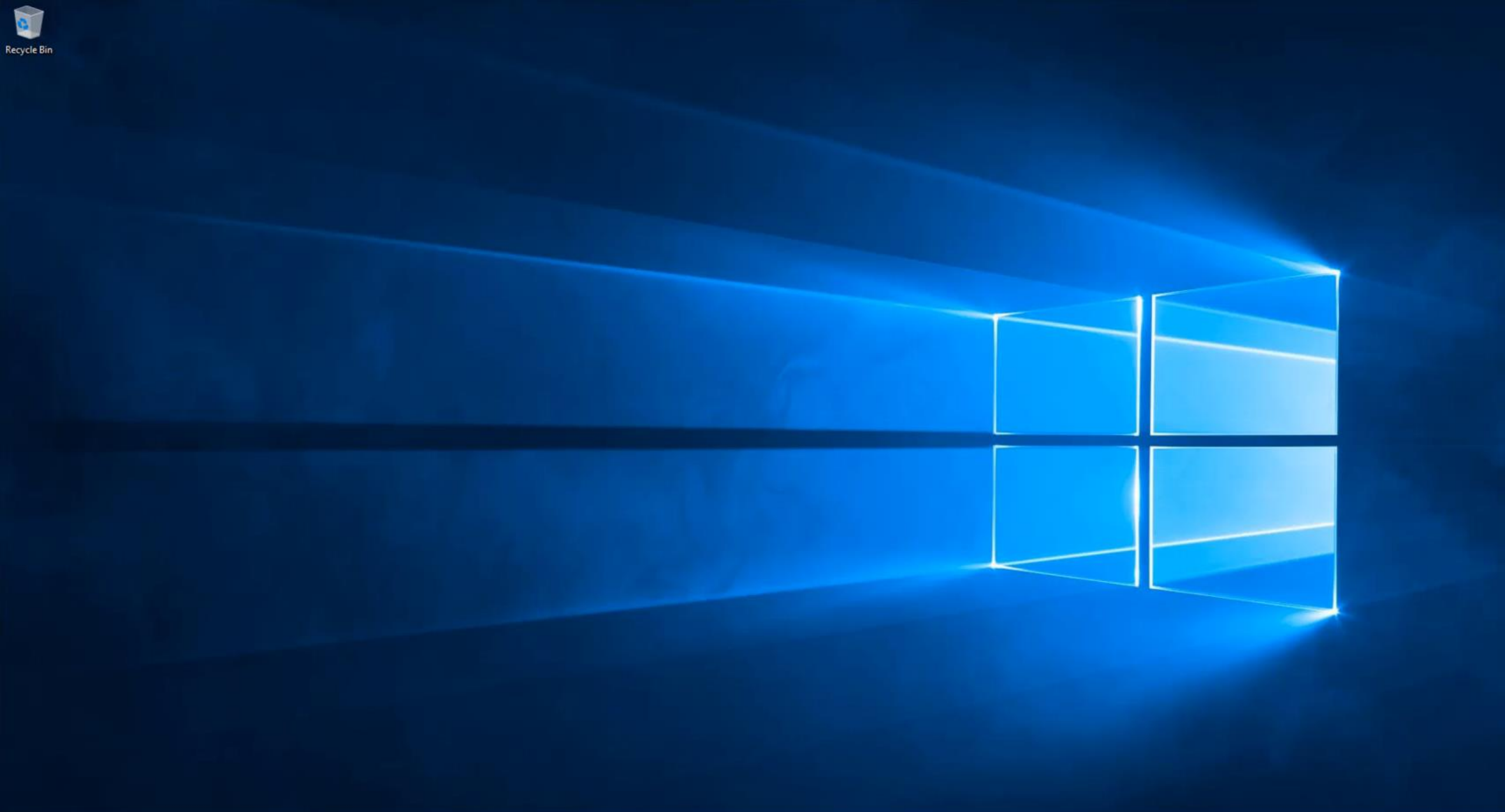
Apps (Identifying)

We're getting everything ready for you.

Don't turn off your PC



Recycle Bin



Taskbar area containing the Start button, search bar with the text "Ask me anything", taskbar icons for File Explorer, Microsoft Edge, and Mail, and the system tray with the time "2:22 PM 6/2/2017" and notification icons.

Windows Autopilot Reset

Local

Windows Autopilot Reset - local

(previously Windows Automatic Redeployment)

Simple process to prepare a device for a different purpose:

Remove all apps, settings, and personal files

Preserve Azure Active Directory join and MDM enrollment so the device is still managed

Preserves provisioning packages

Keeps keyboard, language, wi-fi settings*

Initiated by an admin via a simple Windows-Control-R keystroke from logon screen

Takes 20-30 minutes to complete on typical hardware

*Does not support certificate based Wifi/802.1x



Windows Autopilot Reset - local

(previously Windows Automatic Redeployment)

Requirements:

Windows 10, version 1709 or later

Needs to be enabled on devices (off by default)

- MDM policy and provisioning package support available

Azure Active Directory-joined devices

Active Directory or Azure Active Directory administrators perform this task

- All users who can add devices to Azure AD are considered Administrators
- Configure via Azure Portal to restrict





Settings

Managed by Contoso MN

Areas managed by Contoso MN

Contoso MN manages the following areas and settings. Settings marked as Dynamic might change depending on device location, time, and network configuration.
[More information about Dynamic Management](#)

Policies

- Experience
- Update
- Start

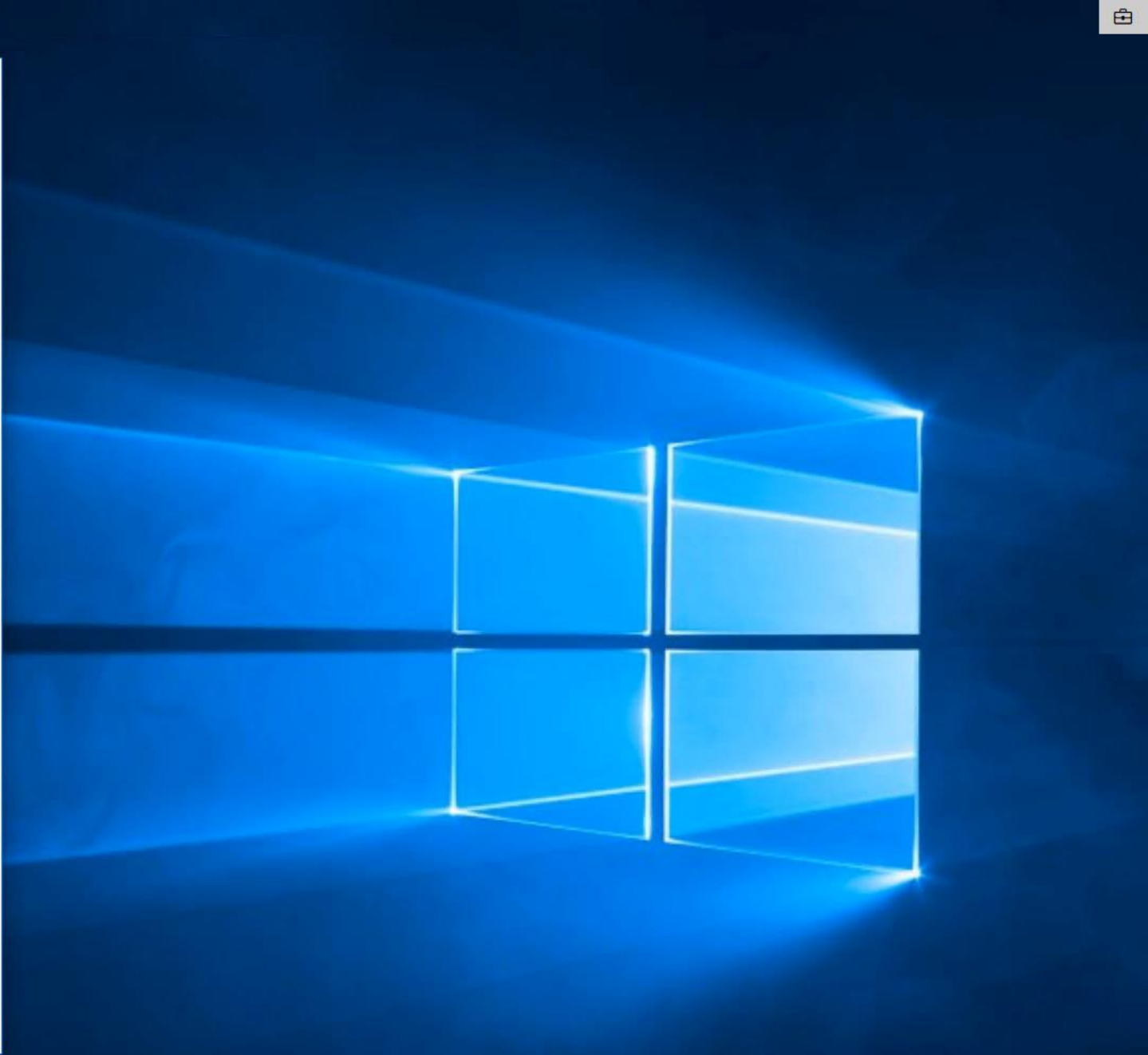
Applications

- Sway
- Delve
- Expenses
- Dynamics 365

Connection info

Management Server Address:
`https://r.manage.microsoft.com/devicegatewayproxy/cimhandler.ashx`

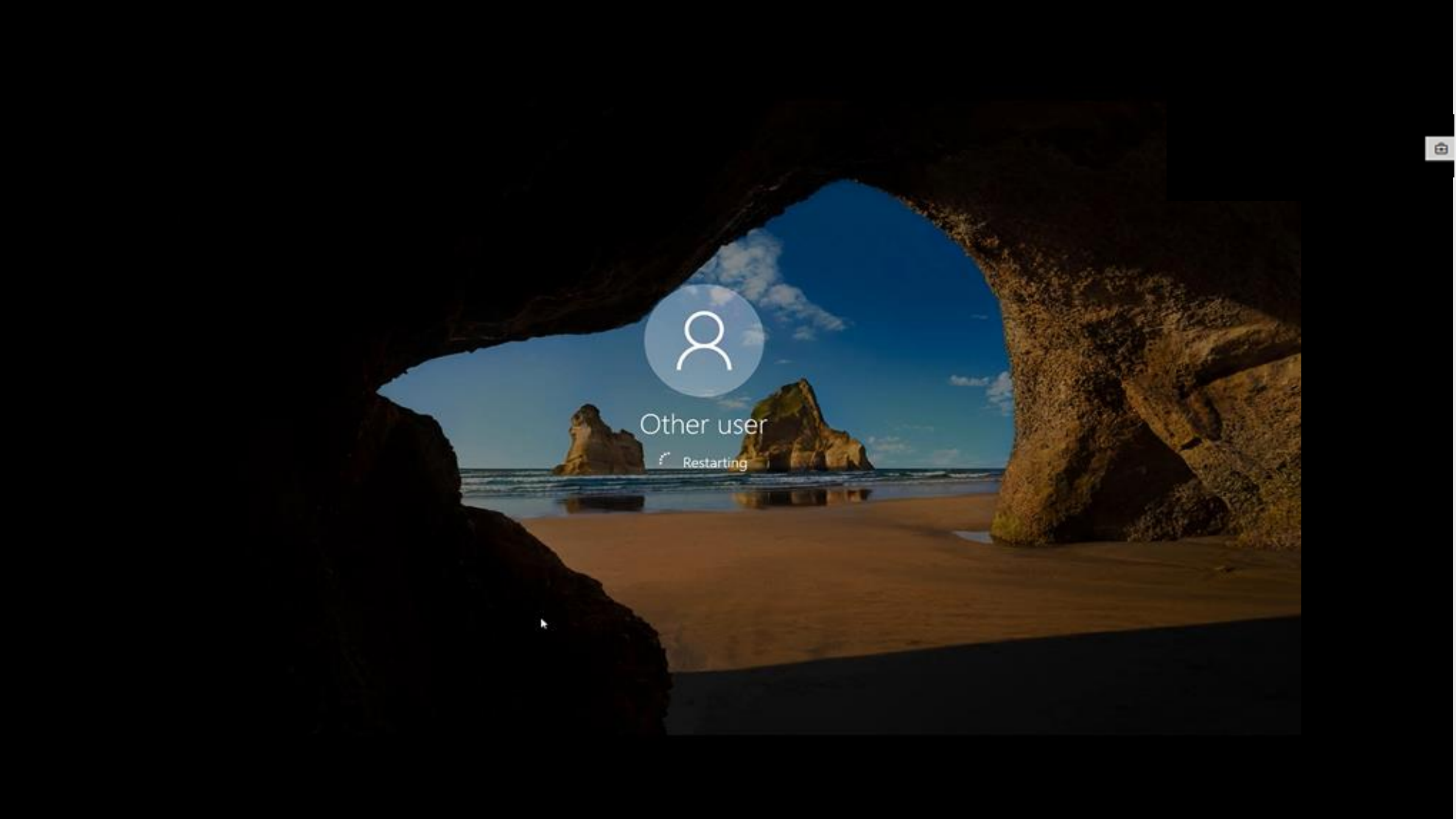
Exchange ID:
`A257859D4D45D63E828035209C4628C1`





Other user

Restarting



Hyper-V™

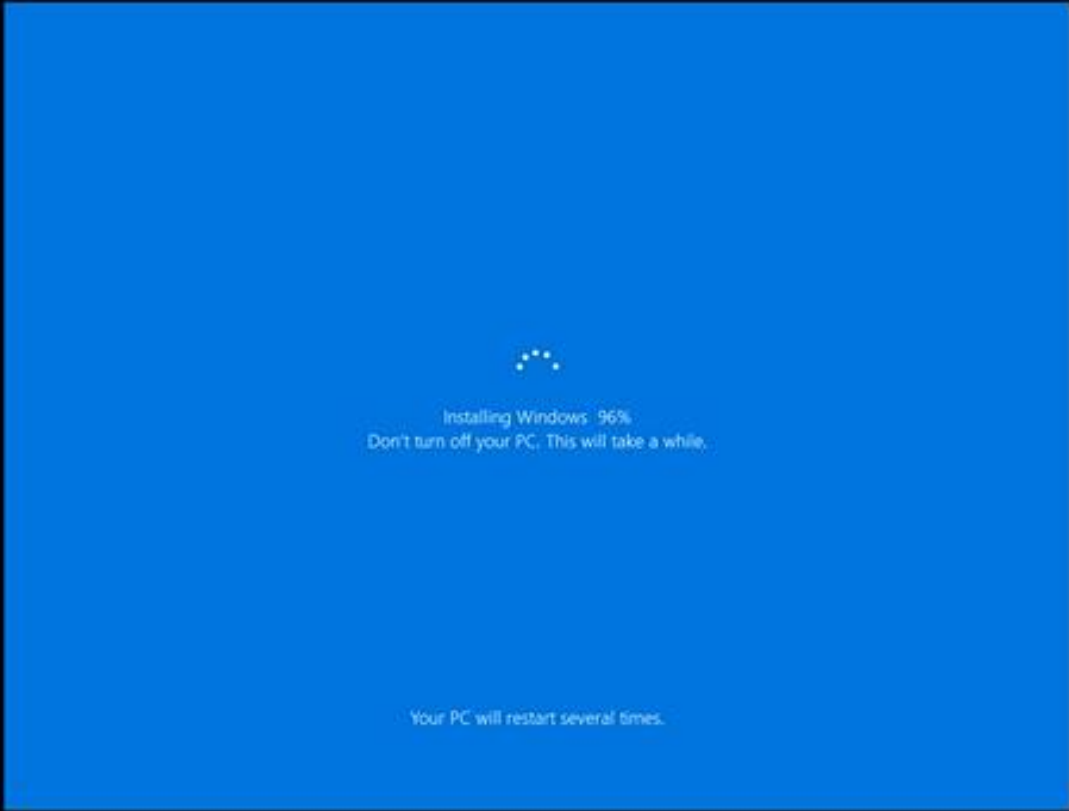


Resetting this PC



Hyper-V™


Resetting this PC 42%



Installing Windows 96%

Don't turn off your PC. This will take a while.

Your PC will restart several times.

The image shows a blue Windows installation progress screen. At the top center, there is a loading icon consisting of five white dots in an arc. Below the icon, the text reads "Installing Windows 96%". Underneath that, a warning message says "Don't turn off your PC. This will take a while." At the bottom of the screen, it states "Your PC will restart several times." The entire screen is a solid blue color.





Success! Windows is set up and ready to go.

12:45

Thursday, August 31



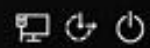


Other user

anna@contosomn.com

Password

Sign in to: Your work or school account





Anna Anderson

Welcome

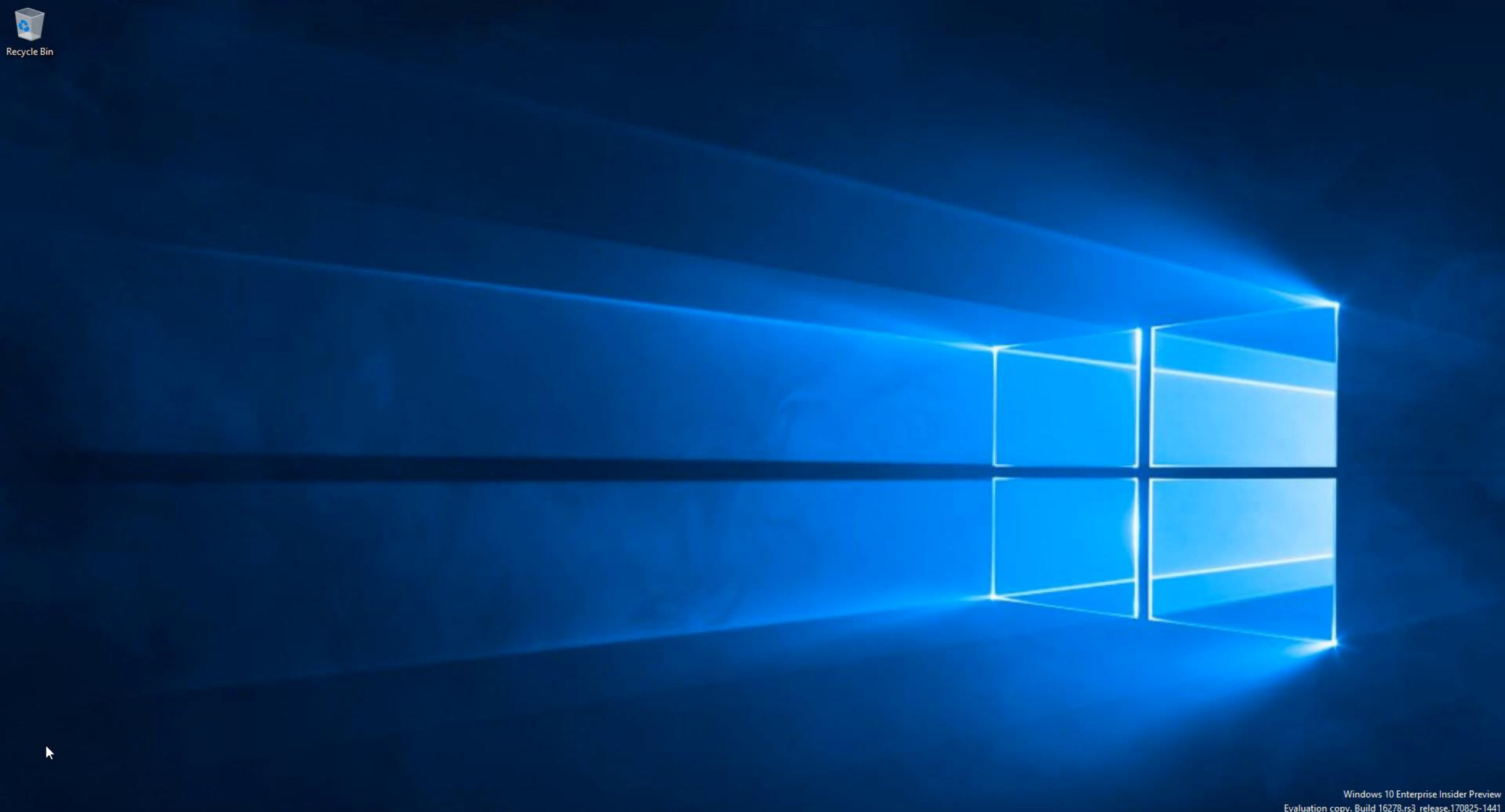


We're getting everything ready for you.

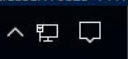
Don't turn off your PC



Recycle Bin



Windows 10 Enterprise Insider Preview
Evaluation copy. Build 16278.rs3_release.170825-1441



Windows Autopilot Reset

Remote via Microsoft Intune

Windows Autopilot Reset - remote

Simple process to prepare a device for a different purpose:

Remove all apps, settings, and personal files

Preserve Azure Active Directory join and MDM enrollment so the device is still managed

Preserves provisioning packages

Keeps keyboard, language, wi-fi settings

Initiated via Microsoft Intune

Takes 20-30 minutes to complete on typical hardware

PUBLIC PREVIEW



Microsoft Azure

Search resources, services, and docs

Home > Microsoft Intune > Devices - All devices > DESKTOP-JDT6CSO

DESKTOP-JDT6CSO

Search (Ctrl+)

Overview

MANAGE

Properties

Monitor

Hardware

Discovered apps

Device compliance

Device configuration

App configuration

- Retire
- Wipe
- Delete
- Remote lock
- Sync
- Reset passcode
- Restart
- Fresh Start
- AutoPilot Reset (preview)
- Quick Scan
- Full Scan
- Update Windows Defender
- New Remote Assistance Ses

Device name DESKTOP-JDT6CSO	Associated user Megan Bowen
Management name MeganB_Windows_9/21/2018_12:06 AM	Compliance Compliant
Ownership Corporate	Operating system Windows
Serial number 8651-5228-2150-4865-5044-8879-02	Device model Virtual Machine
Phone number	Last check-in time 9/20/2018, 7:24:12 PM

Device actions status

ACTION	STATUS	DATE/TIME
No results		

- Create a resource
- All services
- FAVORITES
- Azure Active Directory
- Intune
- All resources
- Resource groups
- App Services
- Function Apps
- SQL databases
- Azure Cosmos DB
- Virtual machines
- Load balancers
- Storage accounts
- Virtual networks
- Monitor
- Advisor
- Security Center

Windows Autopilot Reset - remote

Requirements:

Windows 10 Insider Preview Build 17672 and later

Needs to be enabled on devices (off by default)

- MDM policy and provisioning package support available

Azure Active Directory-joined devices

Administrators to perform the task

- All users who can add devices to Azure AD are considered Administrators
- Configure via Azure Portal to restrict
- Enrollment status page must be switched on in Intune

Roadmap:

Support for Active Directory-joined devices

PUBLIC PREVIEW



Windows Autopilot

Self-deploying devices

How would you use Autopilot to deploy...

Digital signage



Multi app kiosk



Shared PC



Single app kiosk



VDI clients



Design notes

Technicians usually set up these types of devices

No defined user to auth or set up the device

May not have peripherals (keyboards, mice, etc.)

Typically involve “walk up and use” scenarios



It is as easy as....



Registering your device with Autopilot



Assigning a Self-Deploying Autopilot Profile using Intune



Connecting to a network and booting your device

Demo: Self-Deploying

Mode

Kiosk

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



Just a moment...





Now we have some important setup to do.

Welcome! We'll take it from here.

Getting you set up for work may take a while, but leave everything to us.
Please don't turn off this device.

Not your company's device?

Next





Just a moment...



Please wait while we set up your device...



Setting up your device for work

This could take a while and your device may need to reboot.



Device preparation
Complete



Device setup [Hide details](#)
Identifying

Security policies (Identifying)

Certificates (Identifying)

Network connections (Identifying)

Apps (Identifying)

This might take several minutes

Don't turn off your PC

Self-Deploying mode

Prerequisites:

Windows 10 1809 and later

TPM 2.0

Azure Active Directory Premium

Microsoft Intune

Steps:

1. Register device with Autopilot
2. Assign Autopilot Profile configured for "self-deploying mode" within Intune
3. Boot device, click OK (for now)

Windows Autopilot

Hybrid Azure AD Join

What is Hybrid Azure AD Join?

Devices joined to on premises Active Directory and registered in Azure Active Directory

If you deployed **AAD Connect** and use **Windows 10 1607 or later**, you likely already use this

Some refer to this state as "DJ++"

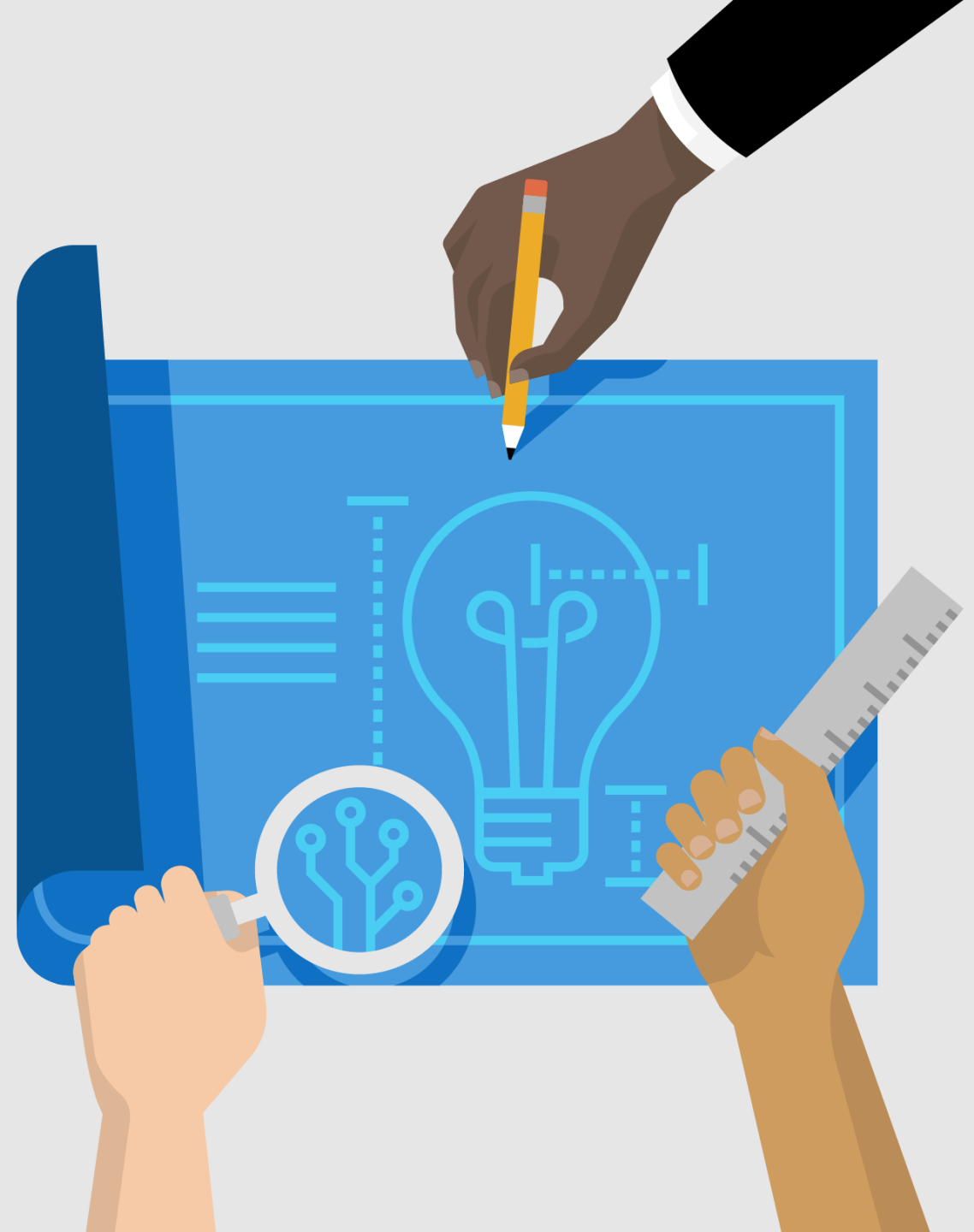
Learn more at - <https://docs.microsoft.com/en-us/azure/active-directory/devices/overview#hybrid-azure-ad-joined-devices>

Design notes

Customers routinely ask for the ability to join on premises domains via OOBE

Need for the same customizations Autopilot provides:

- Auto-accept EULA
- Skip Privacy pages
- Admin vs. standard user
- Device naming



It is as easy as...



Registering your device with Autopilot



Assigning a Hybrid Azure AD Autopilot Profile using Intune



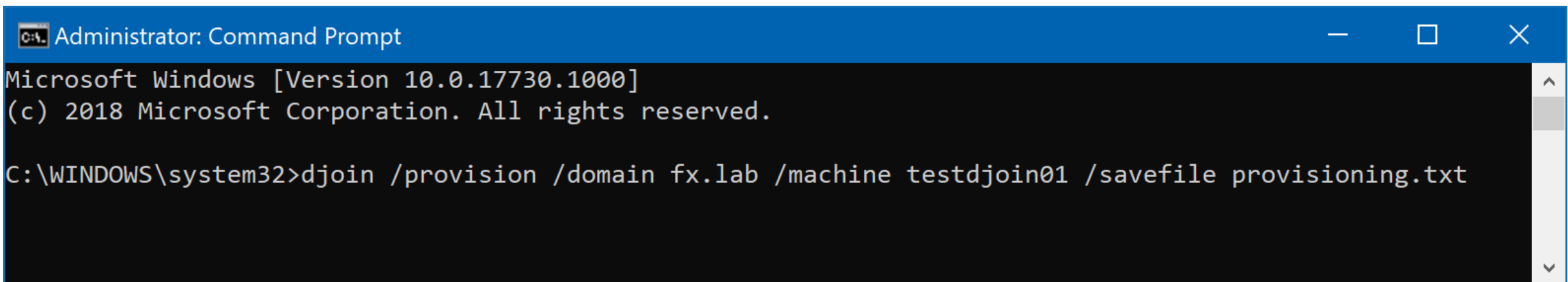
Booting your device and connecting to corpnet

Let's talk about ODJ blobs

Stands for an **O**ffline **D**omain **J**oin blob

At the center of the Hybrid Autopilot flow

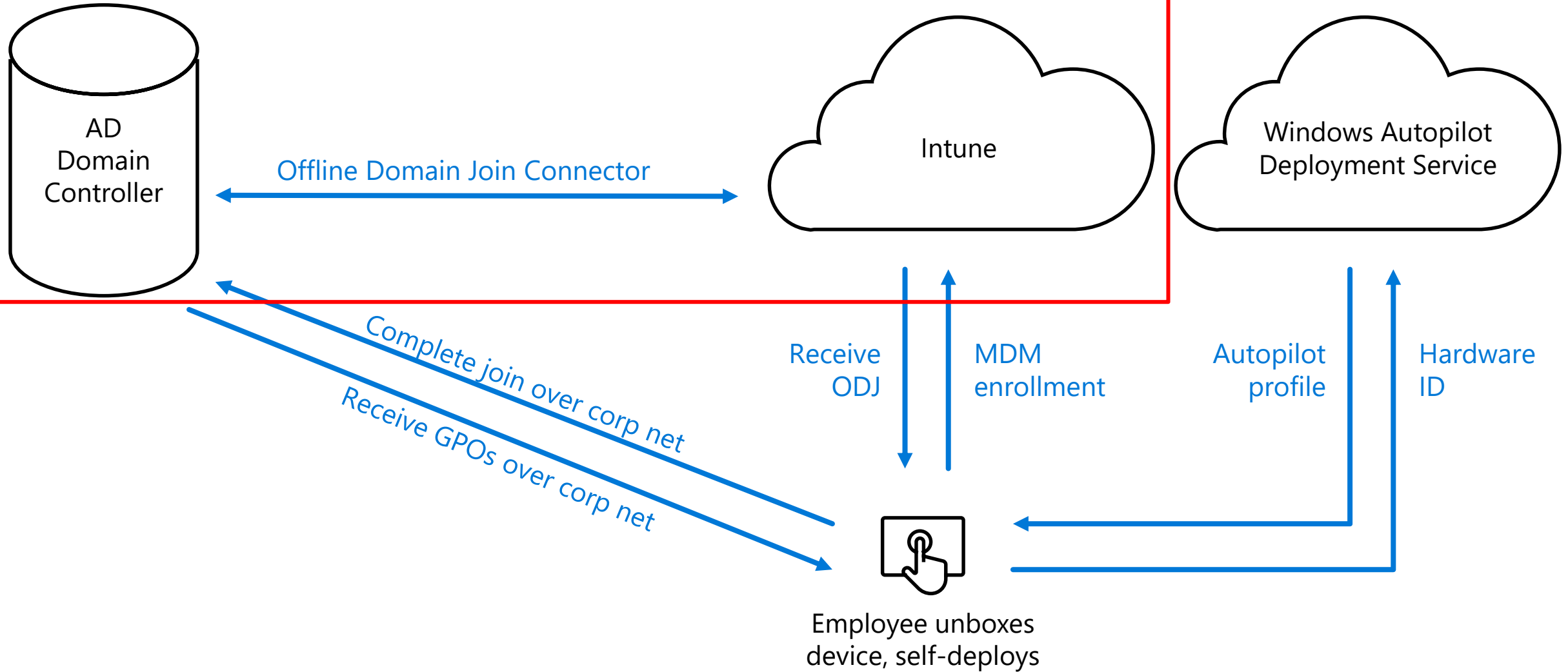
You can generate your own blob from any domain joined machine if you have rights to join

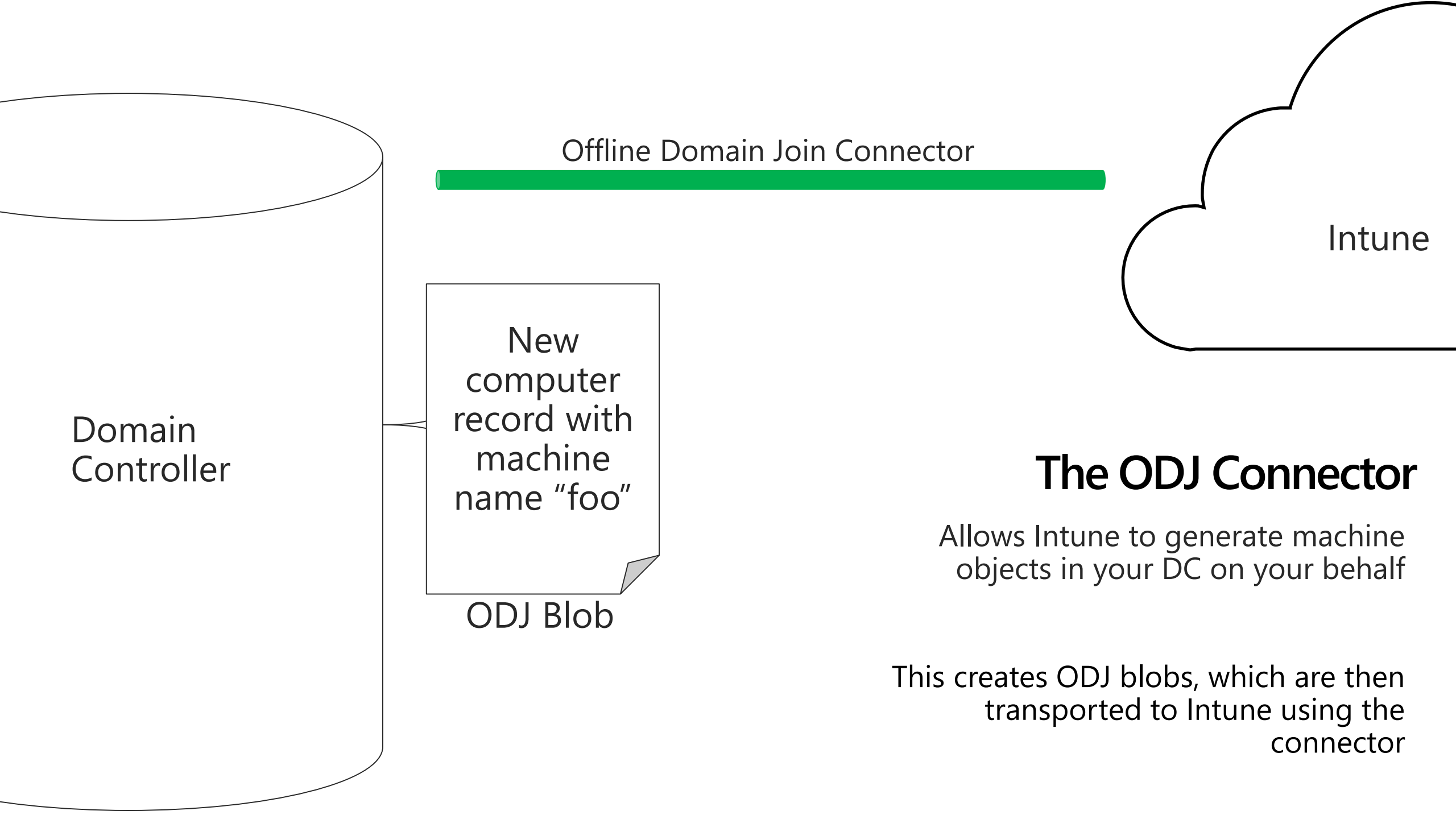


```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17730.1000]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>djoin /provision /domain fx.lab /machine testdjoin01 /savefile provisioning.txt
```

Hybrid Azure AD Join through Windows Autopilot





Offline Domain Join Connector

Intune

Domain
Controller

New
computer
record with
machine
name "foo"

ODJ Blob

The ODJ Connector

Allows Intune to generate machine objects in your DC on your behalf

This creates ODJ blobs, which are then transported to Intune using the connector

Demo: Hybrid Azure AD Join

- Create a resource
- All services
- FAVORITES
- Azure Active Directory
- Intune
- Dashboard
- All resources
- Resource groups
- App Services
- SQL databases
- Azure Cosmos DB
- Virtual machines
- Load balancers
- Storage accounts
- Virtual networks
- Security Center
- Cost Management + Billing
- Help + support
- Monitor
- Advisor

Windows Autopilot deployment profiles

Windows enrollment

+ Create profile

Windows Autopilot deployment profiles lets you customize the out-of-box experience for your devices. [Learn More.](#)

NAME	DESCRIPTION	JOIN TYPE	ASSIGNED
User Driven Profile		Azure AD joined	Yes
Kiosk		Azure AD joined	Yes

Create profile

Windows Autopilot deployment profiles

* Name
Hybrid Azure AD Join ✓

Description
Deployment profile for Hybrid Azure AD Join

* Deployment mode ⓘ
User-Driven

* Join to Azure AD as ⓘ
Hybrid Azure AD joined

Out-of-box experience (OOBE)
Defaults configured >

Create

Let's start with region. Is this right?

United Arab Emirates

United Kingdom

United States

Uruguay

Uzbekistan

Vanuatu

Vatican City

Yes



Listening...



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

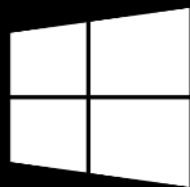
United Kingdom

United States

Yes



We'll continue setting up your device after this
reboot





Just a moment...



Please wait while we set up your device...



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

We're getting everything ready for you.

Don't turn off your PC



Recycle Bin



Microsoft
Edge



Type here to search



3:46 PM
9/20/2018



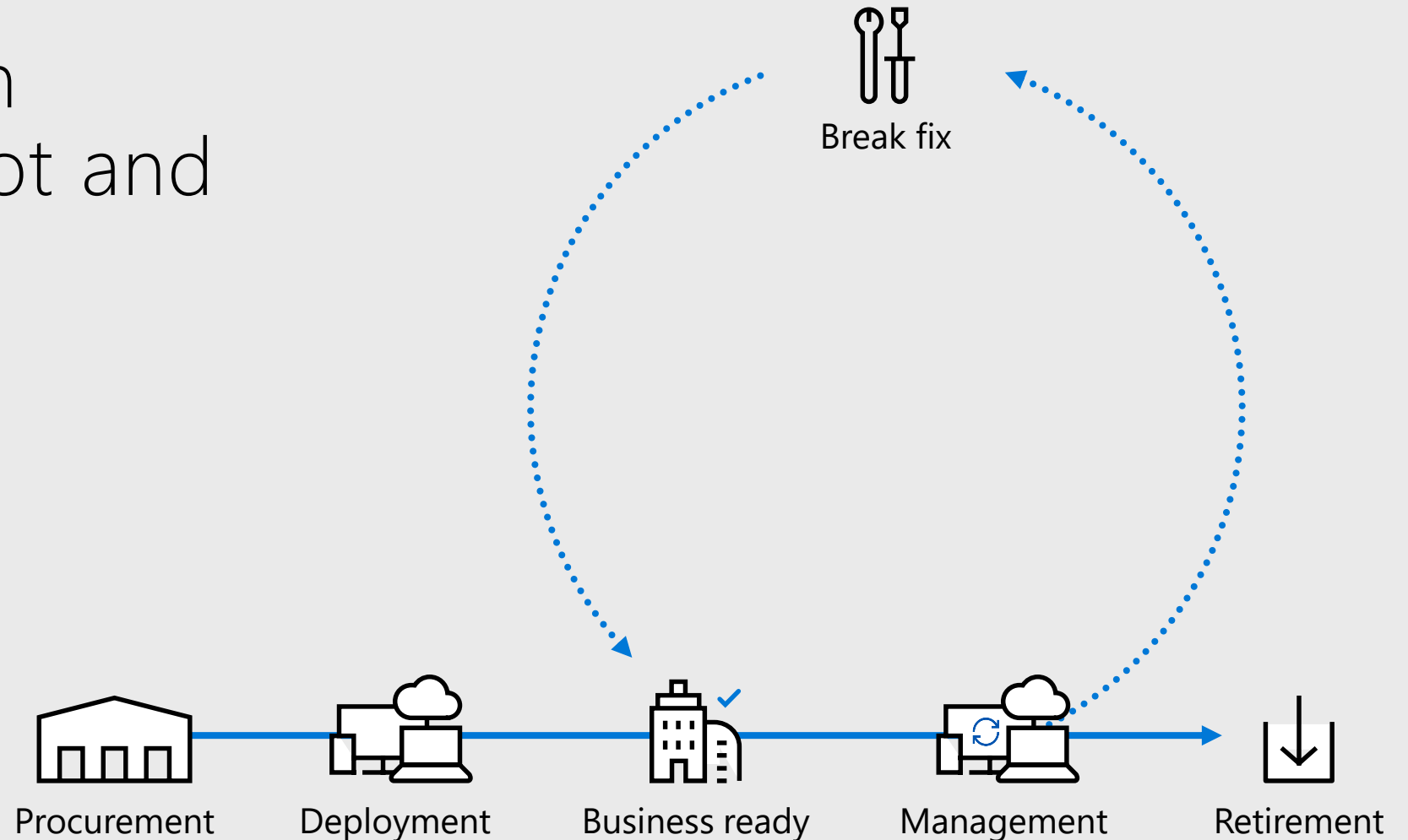
Windows Autopilot scenarios

AVAILABLE	AVAILABLE	AVAILABLE in 1809	AVAILABLE in 1809	AVAILABLE in 1809	AVAILABLE in 1809
User-driven mode	Windows Autopilot reset - local	Windows Autopilot reset - remote	Self-deploying mode	Hybrid Azure AD Join	Autopilot for existing devices
Windows 10 1703 and above	Windows 10 1709 and above	Windows 10 1809 and above	Windows 10 1809 and above	Windows 10 1809 and above	Windows 10 1809 and above
Join device to AAD, enroll in Intune/MDM	Join device to AAD, enroll in Intune/MDM	Execute a device reset via Intune and maintain AAD join and MDM enrollment	No need to provide credentials, automatically joins AAD	Join device to AD, enroll in Intune/MDM	Windows 7 to Windows 10 ConfigMgr task sequence, followed by Windows Autopilot user-driven mode

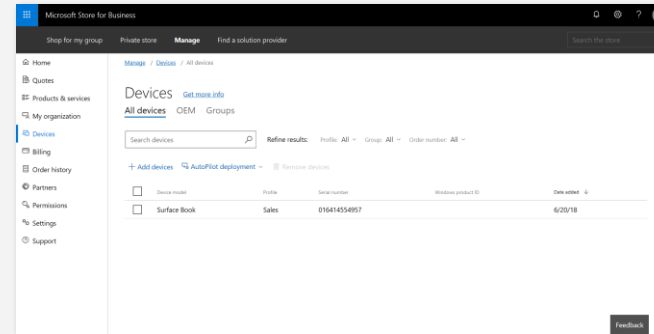
Device lifecycle management with Windows Autopilot and Intune

Key Benefits:

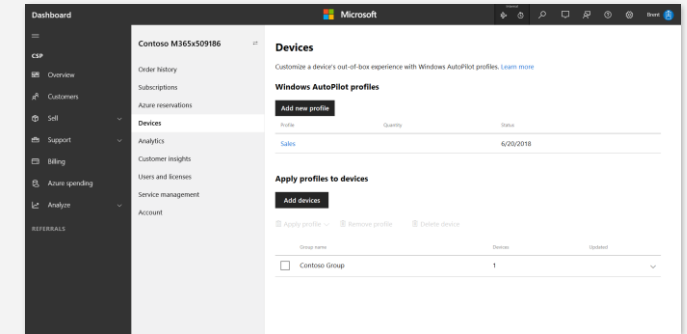
- No more maintenance of images and drivers
- No need for IT to touch the devices
- Simple process for users and IT
- Integration in the device supply chain
- Reset device back to a business ready state



Administering Windows Autopilot

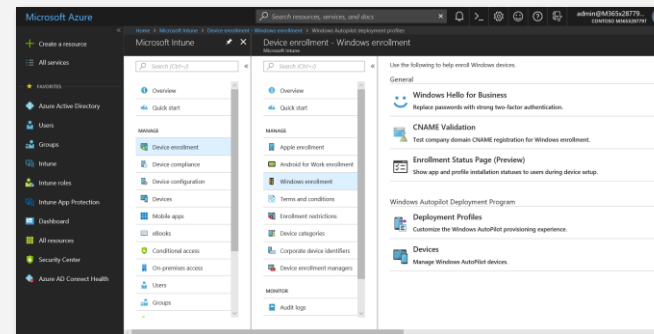


Microsoft Store for Business

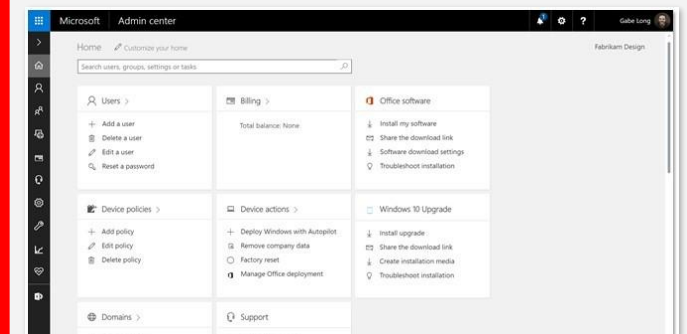


Partner Center

The only portal enterprises should use



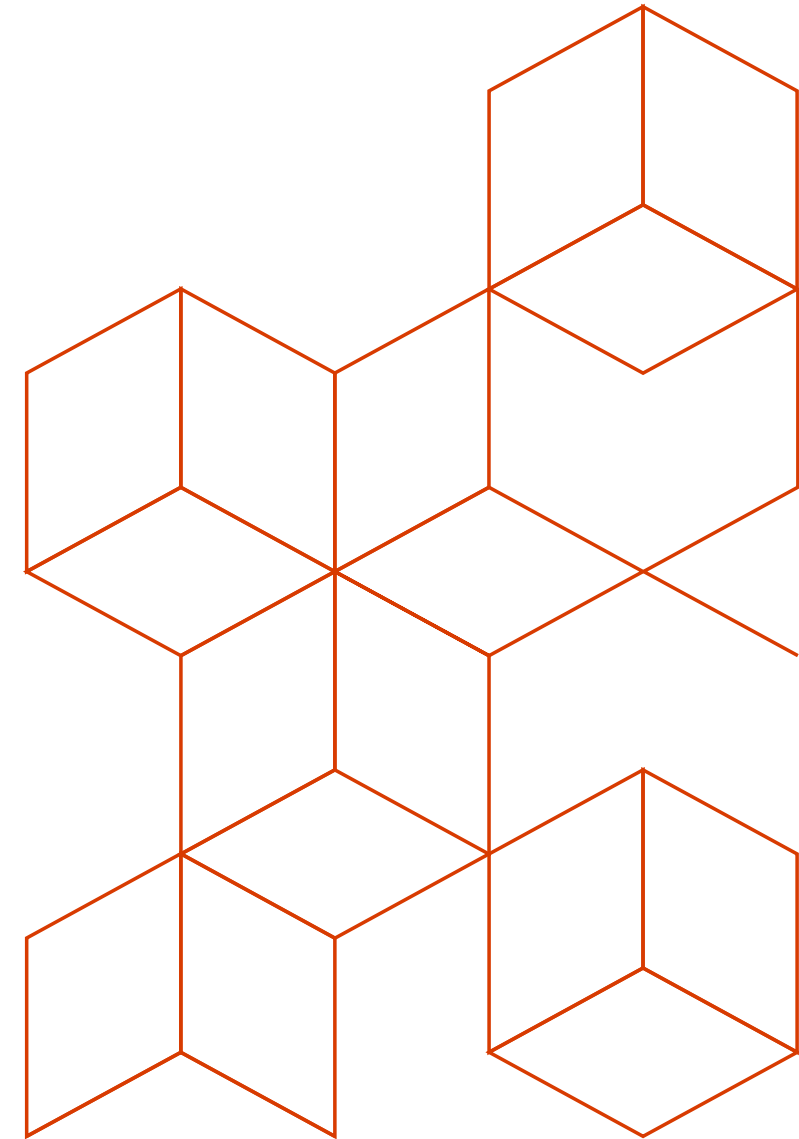
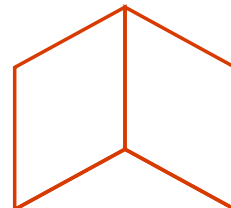
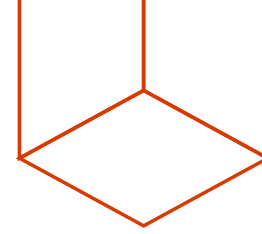
Microsoft Intune



Microsoft 365 Business

Windows Autopilot

Step 1. Registering devices



Participant device manufacturers

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.



DELL



HP



LENOVO



SURFACE

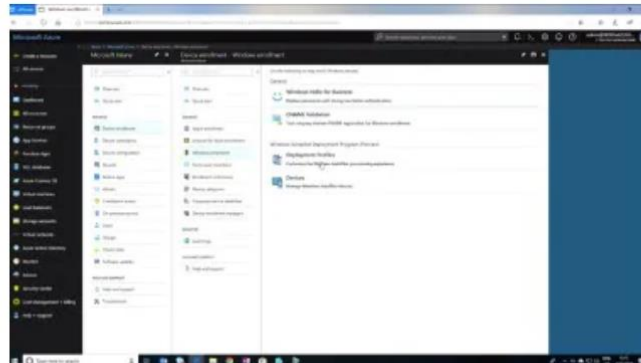


TOSHIBA

Device manufacturers coming soon



Additional Resources



Registering new devices

Supply chain integration

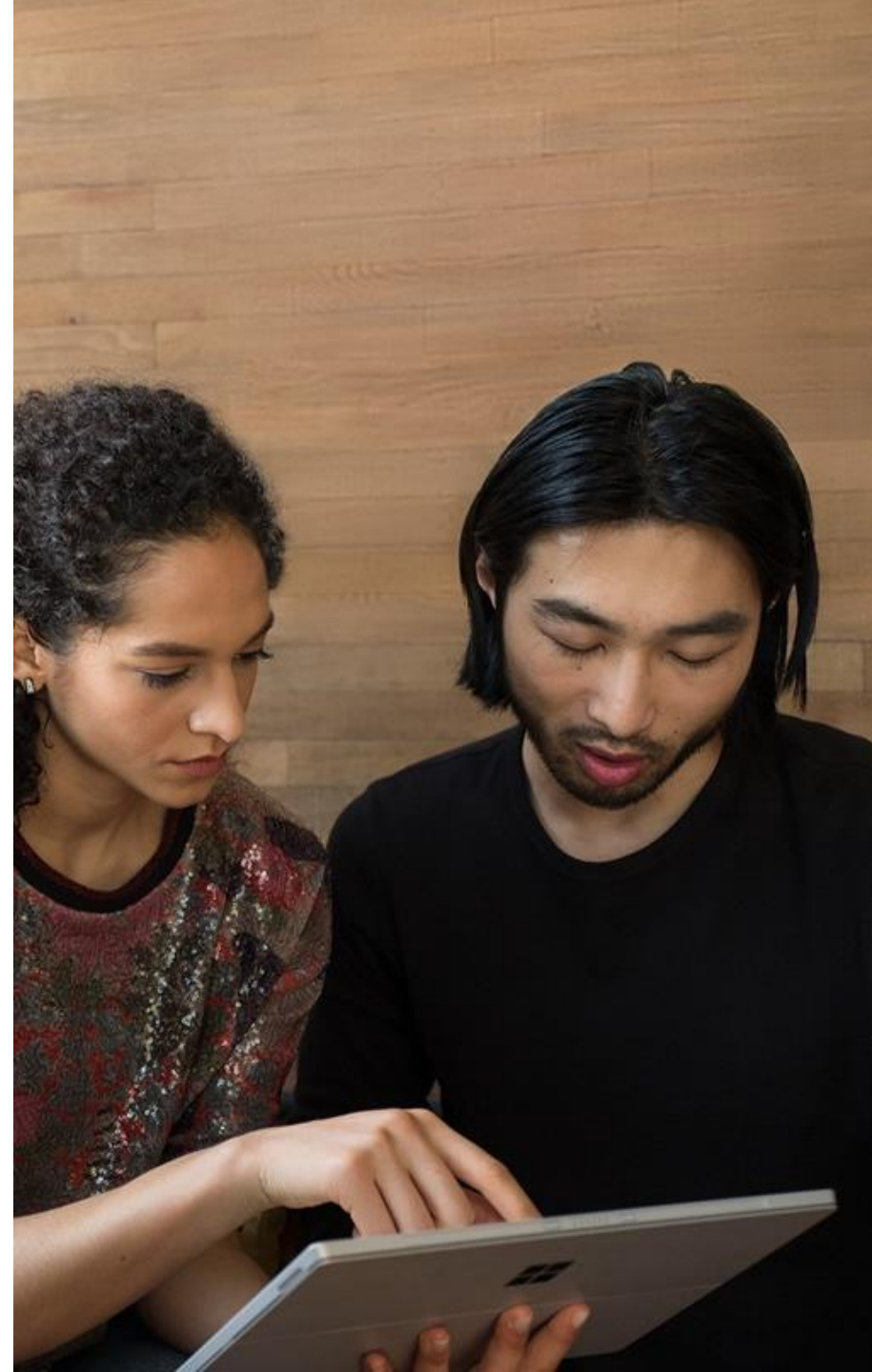
OEMs, distributors, and resellers make the process easy:

- Automatically add new devices to Azure tenant at time of shipment
- Associate devices to customer's purchase order for easy device grouping
- Tag devices with a customer specified label
- Provide an preinstalled image that is ready for configuration*

For a list of those supporting Windows Autopilot supply chain integration please visit:

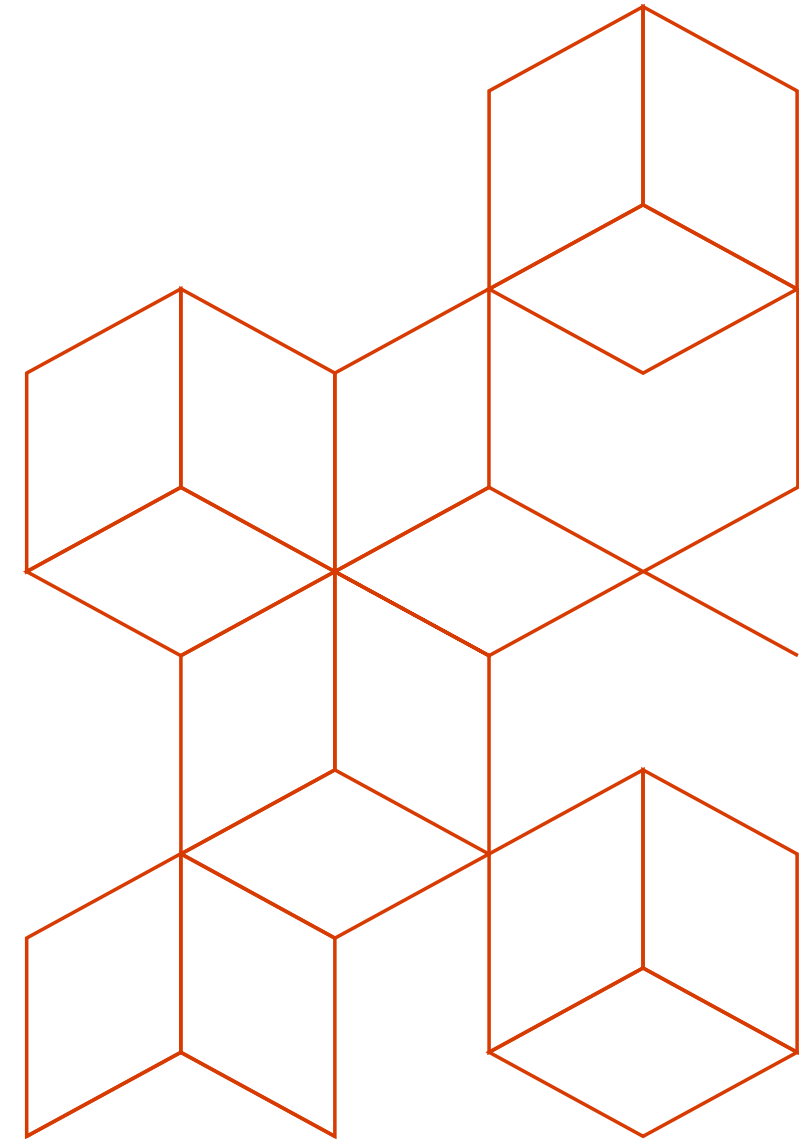
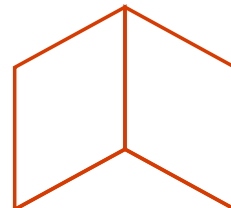
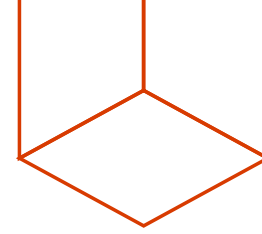
<https://aka.ms/WindowsAutopilot>

*Subject to OEM. Check with your vendor for availability.



Windows Autopilot

Step 2. Assign profile



Creating an Autopilot profile

Configure important details:

- Deployment mode
- Specific settings required for the deployment mode
 - New! BitLocker encryption even for non-admin users (requires Windows 10 1809)
- Out-of-box experience (OOBE) settings
 - New! Hide change account options (requires Windows 10 1809)
- New! Device naming pattern, supporting variable substitution (requires Windows 10 1809):
 - %SERIAL%
 - %RAND:x% (where X is the number of digits)

The image shows two side-by-side windows from the Windows Autopilot configuration tool. The left window is titled 'Create profile' and contains the following fields:

- Name:** A text input field with the placeholder 'Enter the name'.
- Description:** A text area with the placeholder 'Optional'.
- Deployment mode:** A dropdown menu currently set to 'User-Driven'.
- Join to Azure AD as:** A dropdown menu with the placeholder 'Select directory service devices will join'.
- Out-of-box experience (OOBE):** A section with the text 'Defaults configured' and a right-pointing arrow.

The right window is titled 'Out-of-box experience (OOBE)' and contains the following settings:

- Configure your AutoPilot devices using the settings below.**
- The following options are automatically enabled for AutoPilot profiles:**
 - Skip Work or Home usage selection
 - Skip OEM registration and OneDrive configuration
 - Skip user authentication in OOBE
- End user license agreement (EULA):** A toggle switch currently set to 'Hide'.
- What does it mean to skip the EULA?** A help link with an information icon and an external link icon.
- Privacy Settings:** A toggle switch currently set to 'Hide'.
- Hide change account options (Windows Insider only):** A toggle switch currently set to 'Hide'.
- User account type:** A dropdown menu currently set to 'Administrator'.
- Apply computer name template (Windows Insider only):** A toggle switch currently set to 'Yes'.
- Create a unique name for your devices.** A text input field with the placeholder 'My Company-%RAND:4%'.

Assigning an Autopilot profile

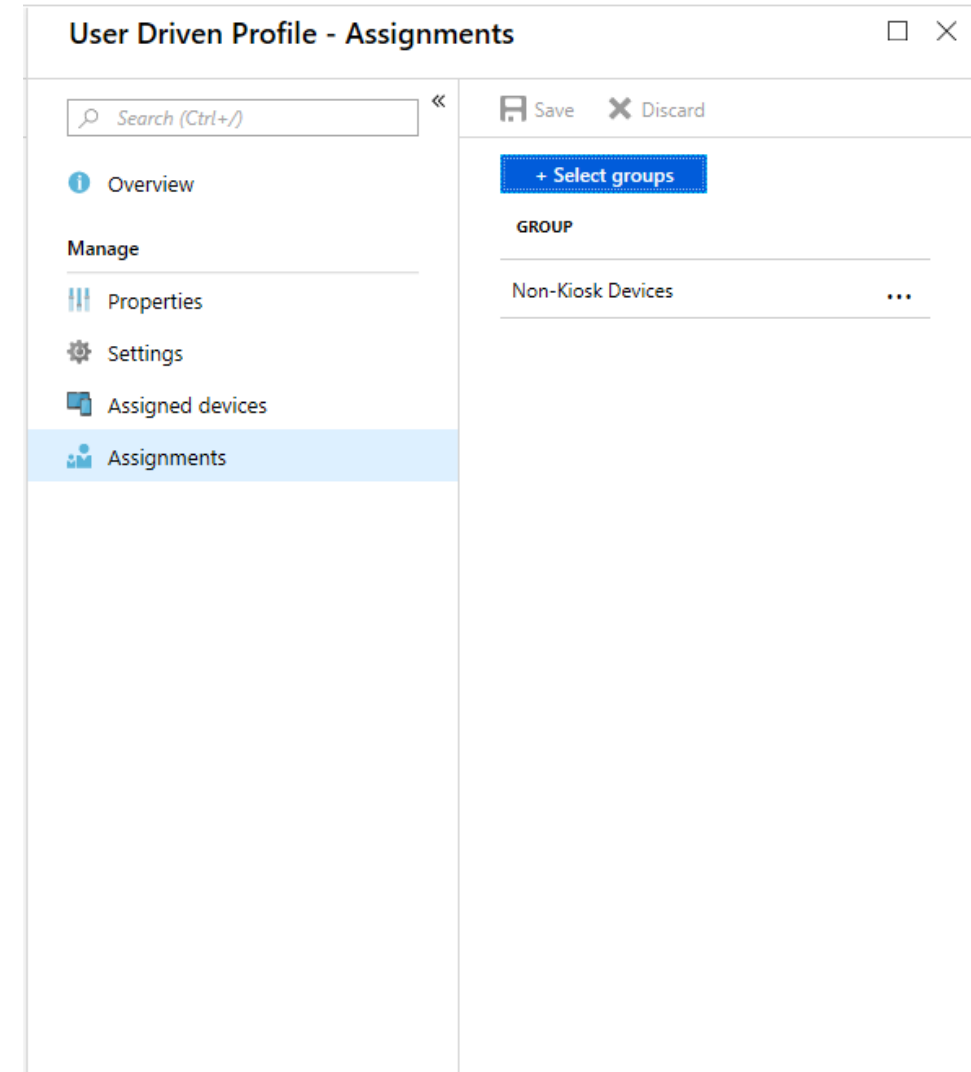
Automated using groups

If you have existing Windows 10 devices:

- An Azure AD device object is automatically created for each imported Autopilot device
- Create one or more Azure AD groups
- Assign an Autopilot profile to the Azure AD group
- Intune will automatically assign the profile to all members of the assigned group

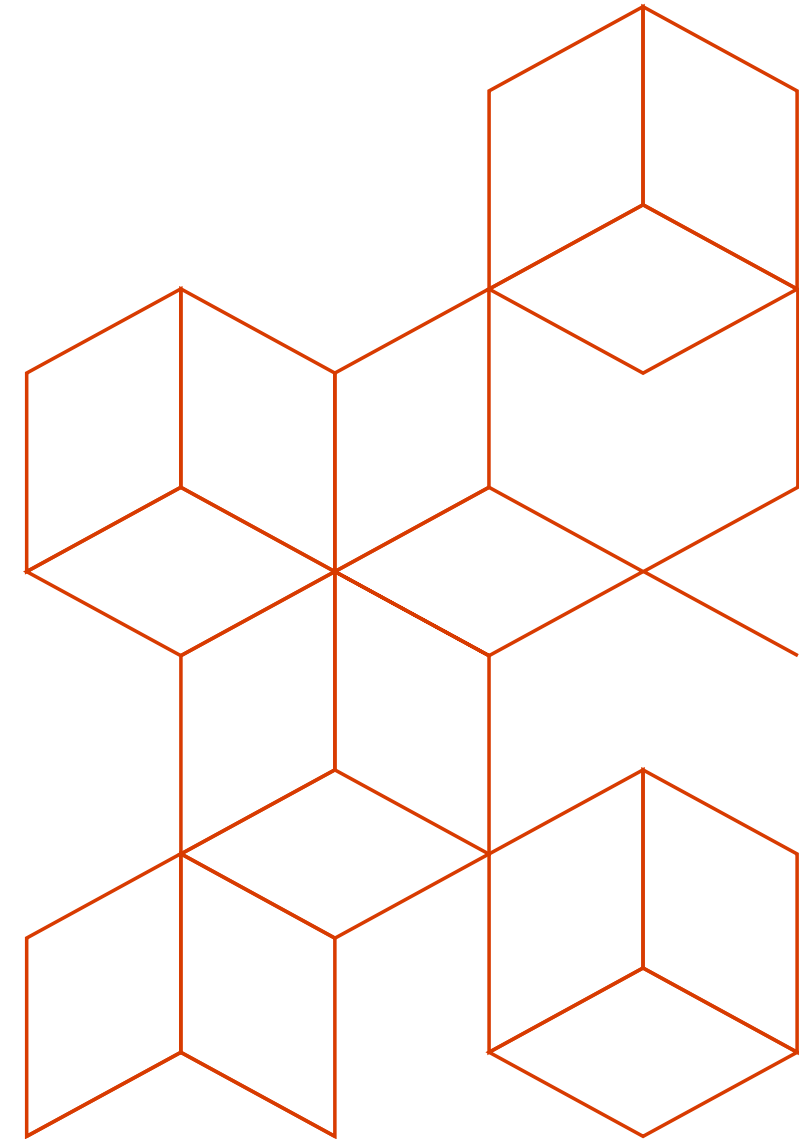
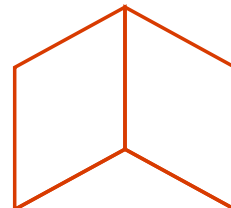
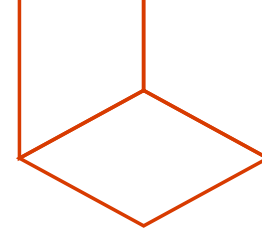
Options for grouping:

- Dynamic group with all Autopilot devices
- Dynamic group based on purchase order ID
- Dynamic group based on device tag (orderId)
- Manual



Windows Autopilot

Step 3. Deploy!



Windows Autopilot

Pre-requisites

Windows 10 version 1703 or higher

- Specific capabilities require higher versions

One of the following, to provide needed Azure Active Directory (automatic MDM enrollment and company branding features) and MDM functionality:

- Microsoft 365 Business subscriptions
- Microsoft 365 F1 subscriptions
- Microsoft 365 Enterprise E3 or E5 subscriptions, which include all Windows 10, Office 365, and EM+S features (Azure AD and Intune)
- Enterprise Mobility + Security E3 or E5 subscriptions, which include all needed Azure AD and Intune features
- Azure Active Directory Premium P1 or P2 and Intune subscriptions (or an alternative MDM service)

See <https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/windows-autopilot-requirements-licensing> for more information

Windows Autopilot

One-time configuration tasks

Azure Active Directory

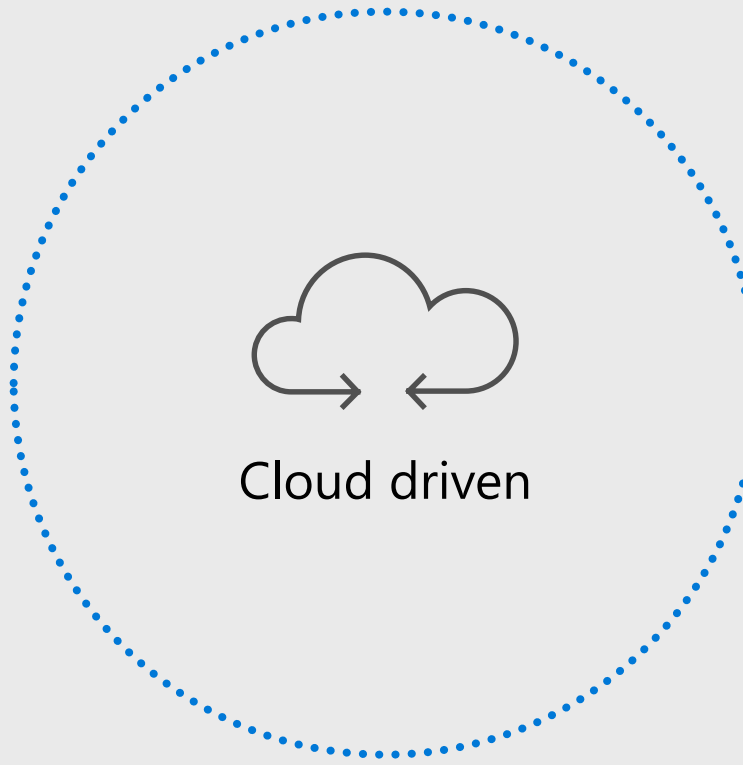
- Configure automatic MDM enrollment. See <https://docs.microsoft.com/en-us/intune/windows-enroll#enable-windows-10-automatic-enrollment>.
- Configure company branding. See <https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/customize-branding>.
- Enable Windows Subscription Activation 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
- (Optional) New! Set up enrollment restrictions so only Autopilot-registered devices can enroll

See <https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/windows-autopilot-requirements-configuration> for more information

Windows Autopilot deployment



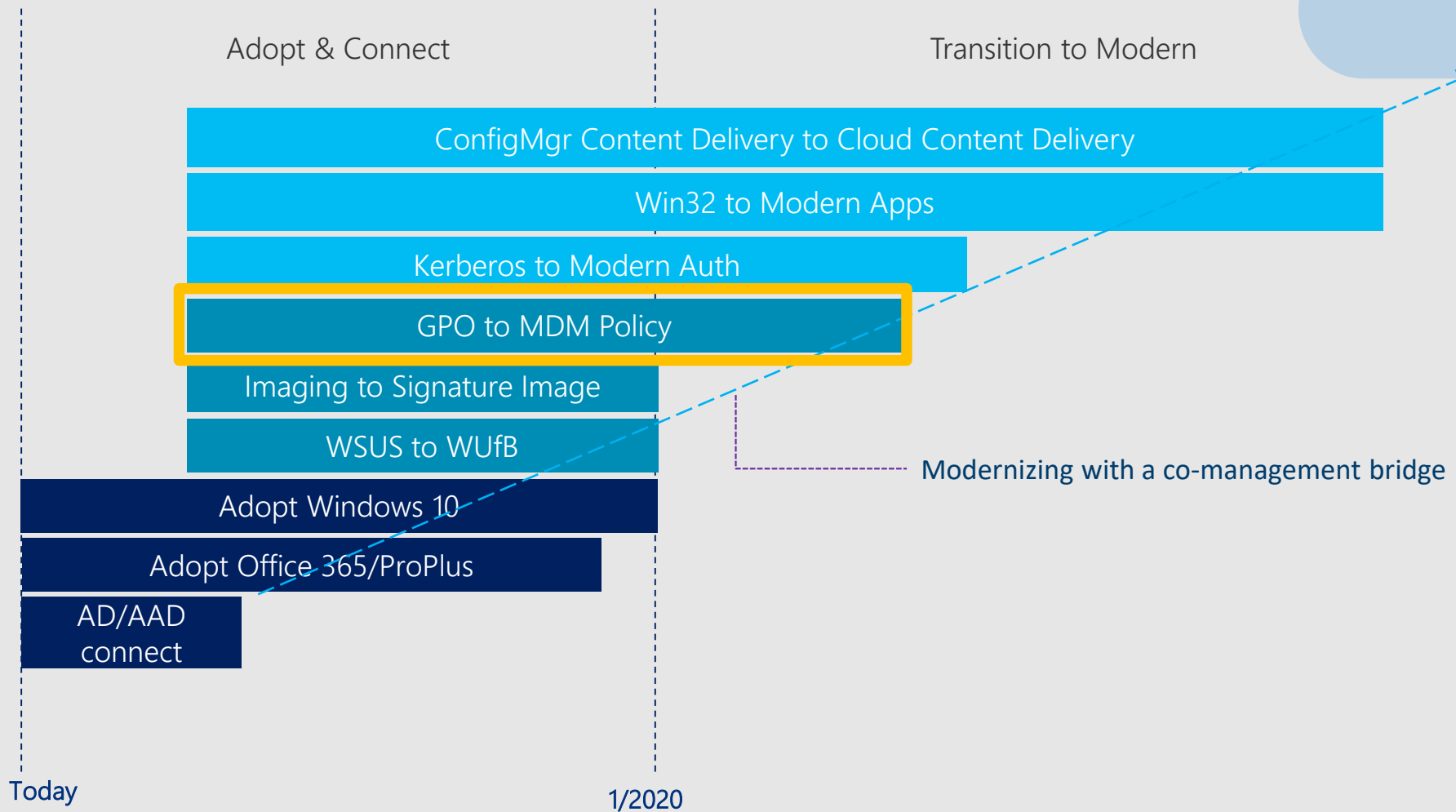
Three simple steps

Register devices

Create an Autopilot profile and
assign to a group

Ship the device to the user

Bridging to Modern Management



MDM Migration Analysis Tool for IT Admins

- An easy-to-use tool which quickly shows you MDM support for the Group Policies your organization uses today.

The screenshot shows a Windows PowerShell terminal window on the left and a web browser window on the right. The terminal window displays the execution of the MMAT tool, including the command to set execution policy to unrestricted, the execution of the analysis tool, and the resulting directory listing of files generated by the tool.

```
TECH-WAD-HOL210: Using MMAT to accel
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.
PS C:\Users\Administrator> cd c:\mmat
PS C:\mmat> Set-ExecutionPolicy Unrestricted -Scope Process

Execution Policy Change
The execution policy helps protect you from scripts that you do not trust. Changing the
you to the security risks described in the about_Execution_Policies help topic at
http://go.microsoft.com/fwlink/?LinkID=135170. Do you want to change the execution policy
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"):
PS C:\mmat> $VerbosePreference="Continue"
PS C:\mmat> .\Invoke-MdmMigrationAnalysisTool.ps1 -collectGPOReports -runAnalysisTool
VERBOSE: Starting analysis tool: <C:\mmat\Invoke-MdmMigrationAnalysisTool.ps1\..\MdmMigr
MDM Migration Analysis Tool. Copyright (c) Microsoft 2016.
Completed MDM Migration Analysis Tool
VERBOSE: Completed running analysis tool
PS C:\mmat> dir

Directory: C:\mmat

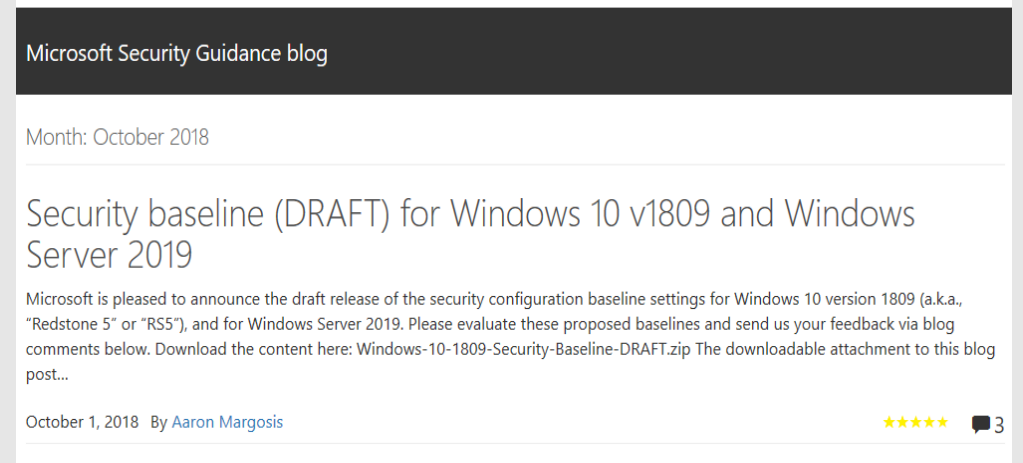
Mode                LastWriteTime         Length Name
----                -
d-----          7/6/2017 10:24 AM             collectGPOReports
d-----          6/8/2017 11:43 AM             sampleOutput
-a-----          7/6/2017 10:27 AM           12381 GPOResult-31B2F340-016D-11D2-945F-00C0
-a-----          7/6/2017 10:27 AM           24148 GPOResult-6AC1786C-016F-11D2-945F-00C0
-a-----         1/27/2017  8:03 AM           19195 Invoke-MdmMigrationAnalysisTool.ps1
-a-----          7/6/2017 10:27 AM           12378 MachineRsop.log
-a-----         1/27/2017  8:03 AM          748435 MDM Migration Analysis Tool Instruction
-a-----          7/6/2017 10:32 AM           16823 MDMMigrationAnalysis.html
-a-----          7/6/2017 10:32 AM          139723 MDMMigrationAnalysis.xml
-a-----          7/6/2017 10:27 AM            385 MDMMigrationAnalysisReportInformation.x
-a-----          7/6/2017 10:32 AM           1624 MdmMigrationAnalysisTool-PS1-Invocatio
-a-----         1/27/2017  8:03 AM          192512 MdmMigrationAnalysisTool.exe
-a-----          7/6/2017 10:32 AM            564 MdmMigrationAnalysisTool.log
-a-----         1/27/2017  8:03 AM          611840 MdmMigrationAnalysisTool.pdb
-a-----         1/27/2017  8:03 AM          33657 MDMMigrationAnalysisXmlToHtml.xslt
-a-----         1/27/2017  8:03 AM          99768 MDMPolicyMapping.xml
-a-----         1/27/2017  8:03 AM            1064 MIT_License.txt
-a-----         1/27/2017  8:03 AM            370 PartiallySupportedPolicyStrings.xml
-a-----         1/27/2017  8:03 AM            120 README.md
-a-----         1/27/2017  8:03 AM           2099 RegistryFilterList.xml
-a-----          7/6/2017 10:27 AM            2178 UserRsop.log
```

The web browser window displays the MDM Migration Analysis Tool (MMAT) User Manual. The page title is "MDM Migration Analysis Tool (MMAT) User Manual". The page content includes an "Executive Summary" section with the heading "What is this thing called MMAT?". The summary text states: "More and more organizations want to move to mobile device management (MDM) to manage their devices including PC. For Windows 10 Creators Update, Microsoft is adding functionality to the Operating System itself to make transitioning to MDM easier. See additional documentation for more background." It also mentions that transitioning from Group Policy to MDM can be challenging and that MMAT will determine which Group Policies have been set for a target user/computer and cross-reference against its built-in list of supported MDM policies.

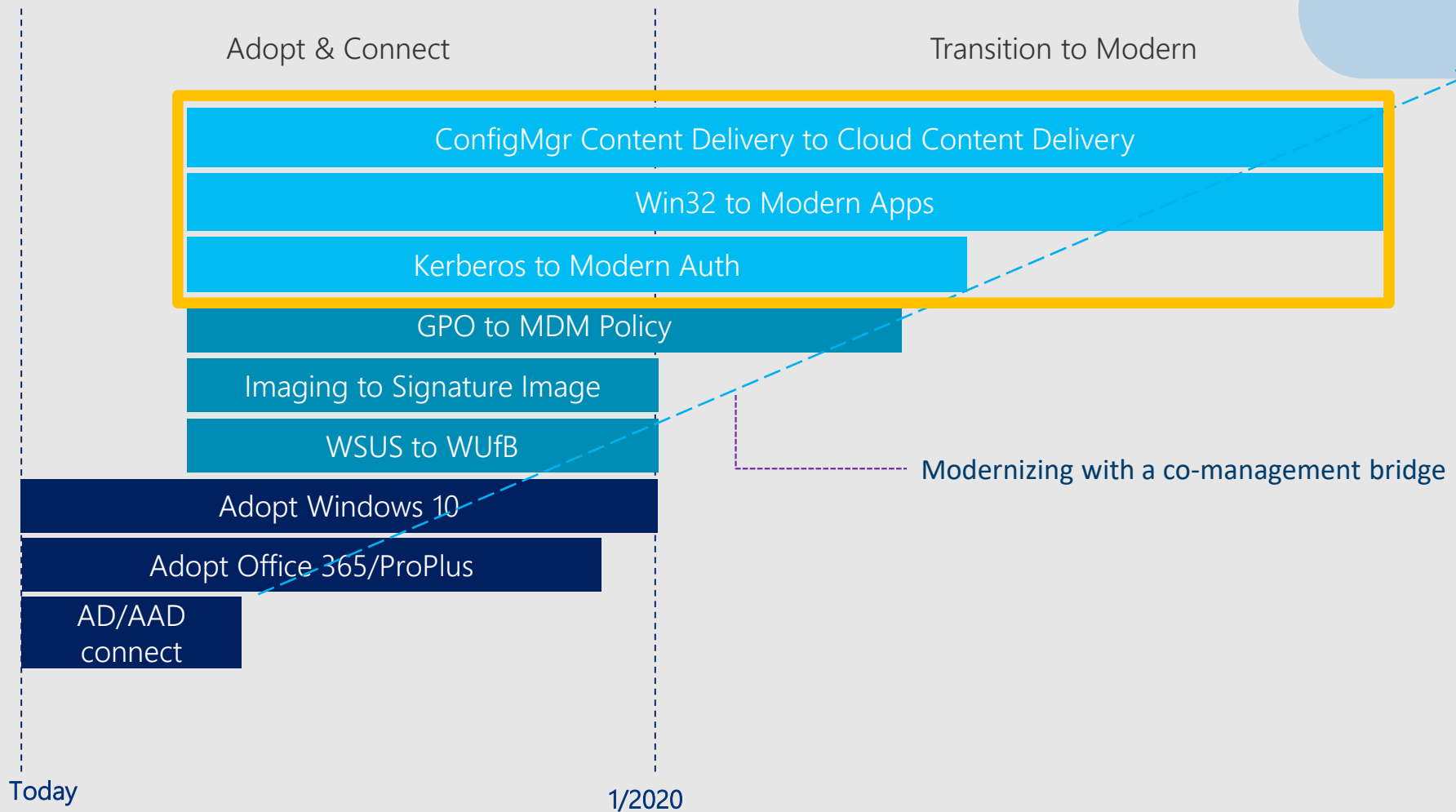
Windows Security Baselines

MDM security baseline includes policies that cover the following:

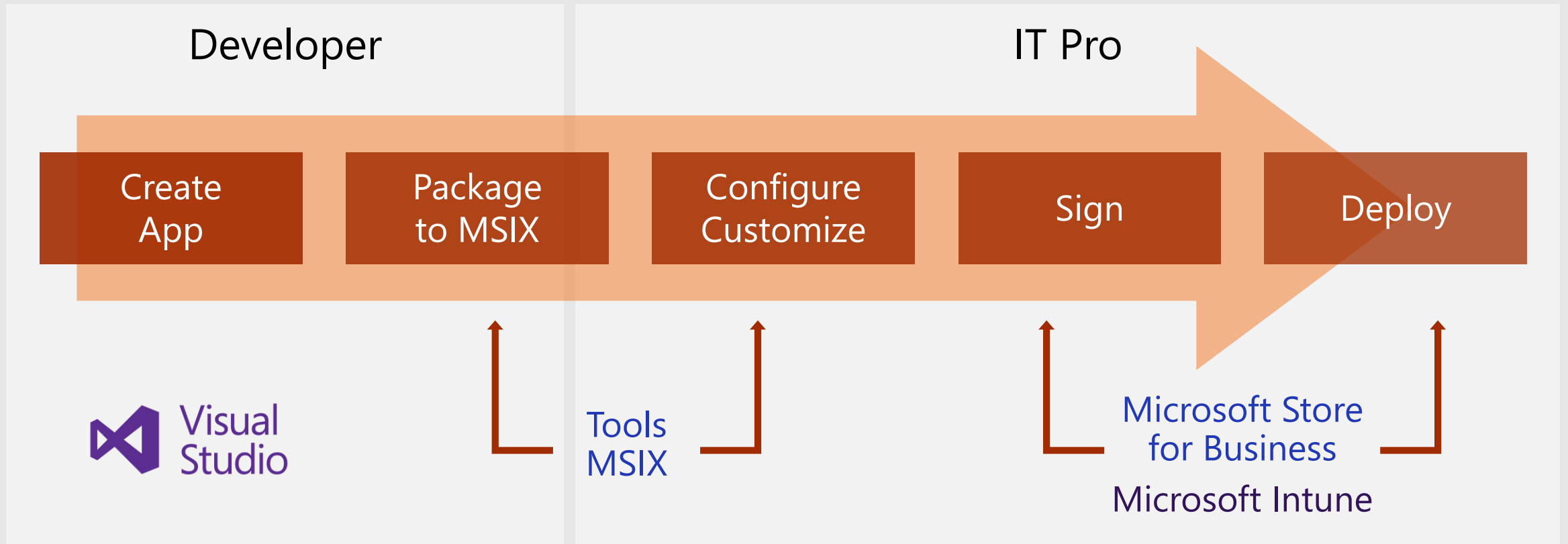
- Microsoft inbox security technology (not deprecated) such as Bitlocker, Smartscreen, and DeviceGuard (virtual-based security), ExploitGuard, Defender, and Firewall
- Restricting remote access to devices
- Setting credential requirements for passwords and PINs
- Restricting use of legacy technology
- Legacy technology policies that offer alternative solutions with modern technology
- And much more



Bridging to Modern Management



Modern IT: Application Lifecycle



MSIX Packaging Tool

Interactive UI

Command line support

Supports modification packages

No source code required!

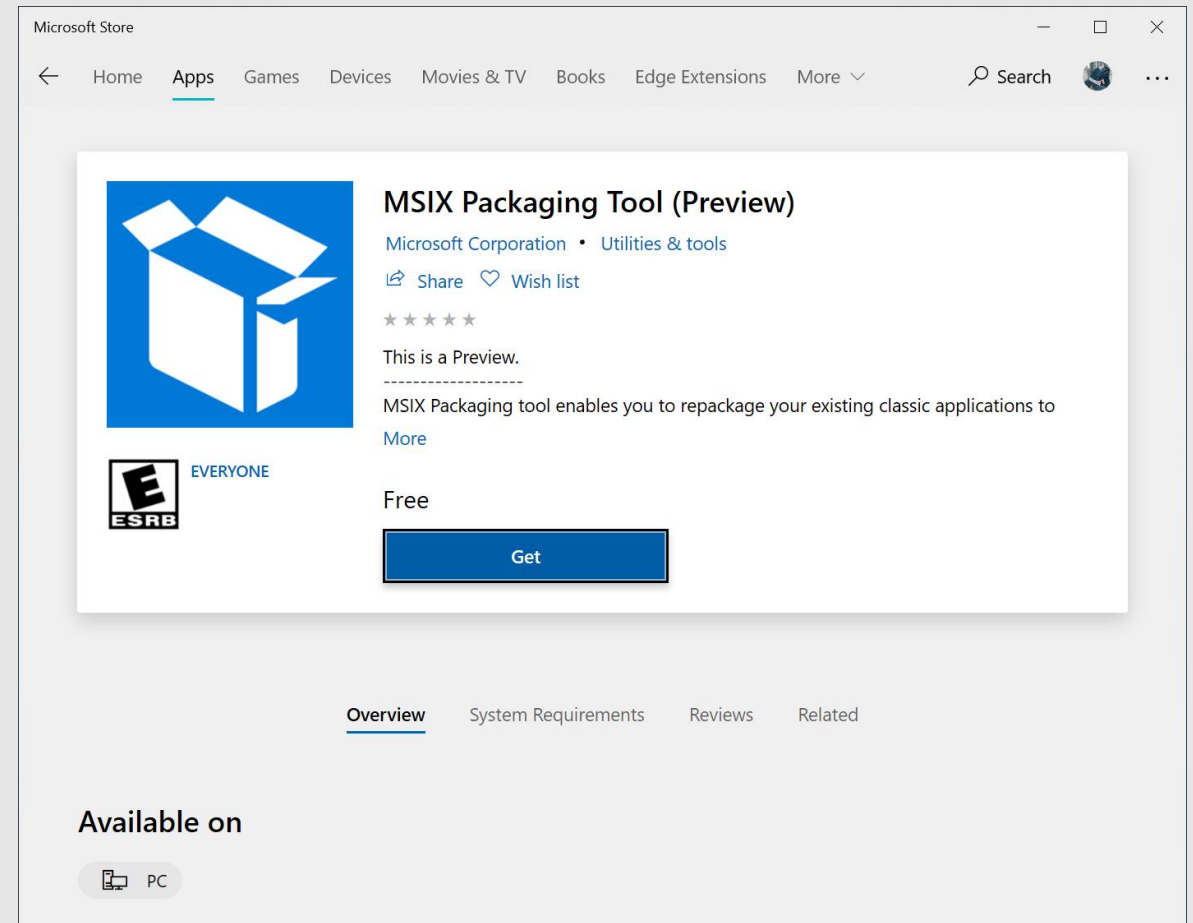
MSI

Setup.exe

ClickOnce

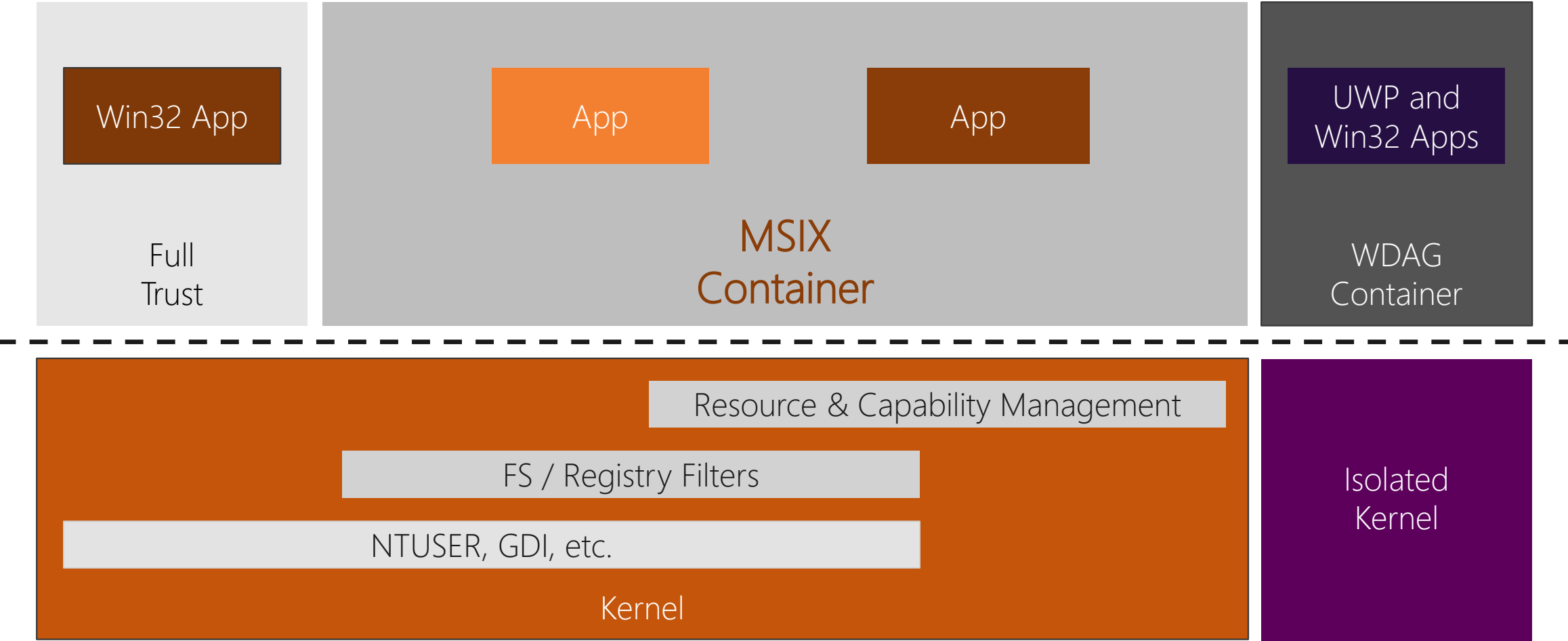
App-V

Scripts



The screenshot shows the Microsoft Store interface for the MSIX Packaging Tool (Preview). The page features a blue icon of an open box, the Microsoft Corporation logo, and the category 'Utilities & tools'. It includes a 'Share' button, a 'Wish list' button, and a five-star rating. A note states 'This is a Preview.' Below this, a description reads: 'MSIX Packaging tool enables you to repackage your existing classic applications to More'. The price is listed as 'Free', and there is a prominent blue 'Get' button. The ESRB rating is 'EVERYONE'. At the bottom, there are tabs for 'Overview', 'System Requirements', 'Reviews', and 'Related'. A section titled 'Available on' shows a 'PC' icon.

Container continuum



MSIX

MSIX provides an enterprise ready deployment platform

- You can use it today
- Just putting your app into an MSIX makes your app run faster
- Your install will be reliable and fast
- Windows 7 support releases to github today
- Package Support Framework allows for all code to move to MSIX

Partners are already supporting MSIX

- Tools
- Package Support Framework



Roadmap for Modern IT

- Intune security baselines
- Easy management of specialized devices with per-device licenses
- ConfigMgr Integration with Desktop Analytics
- ConfigMgr compliance policies as part of compliance assessment in Intune
 - Existing rules
 - New rule: Required apps
- AutoPilot “white glove”

Modern IT

Take action today *when you get home*

1

Modern Desktop POC Kit

Self-Service POC Kit with 80 labs

[Aka.ms/POCKit](https://aka.ms/POCKit)

[Forrester Study: Modernize Your Device Management Practices with the Cloud](#)

2

FastTrack

FastTrack Manager or FastTrack Ready Partner

Support deployment of Azure AD & Intune

[FastTrack.microsoft.com](https://fasttrack.microsoft.com)

3

AutoPilot

Determine the best scenarios for your organization

Contact your OEM



Begin your journey with
Windows 10 today