Securing devices and endpoints in a remote working world

→ Tom Waller | Architect

Secure Digital Transformation

Kocho

BECOME GREATER

After the workshop, you'll…

✓ Improve your knowledge of cloud-based device management using Microsoft solutions

✓ Have a better understanding of Microsoft Endpoint Manager capabilities

✓ Accelerate your endpoint management and protection journey with Kocho and Microsoft

✓ Have defined next steps based on your needs and objectives

Market trends

The cloud is everywhere

90 percent
of enterprises anticipate higher cloud usage than before COVID-19

Endpoint threats are increasing

24 percent
of enterprise mobile endpoints were exposed to device threats in 2019

Continuous updates keep you moving forward

1–4 times/month
is the typical update cycle, ensuring both security and your ability to work seamlessly

Cybersecurity breaches are getting smarter

36 billion
records were exposed through cybercrime in 2020

BYOD is now standard

59 percent
of organizations let employees use their own devices for work

Today's workplace is evolving

4.3 million
people in the US work from home at least half the time

Top endpoint management challenges

Distributed workers

Remote and hybrid work environments

Endpoint diversity

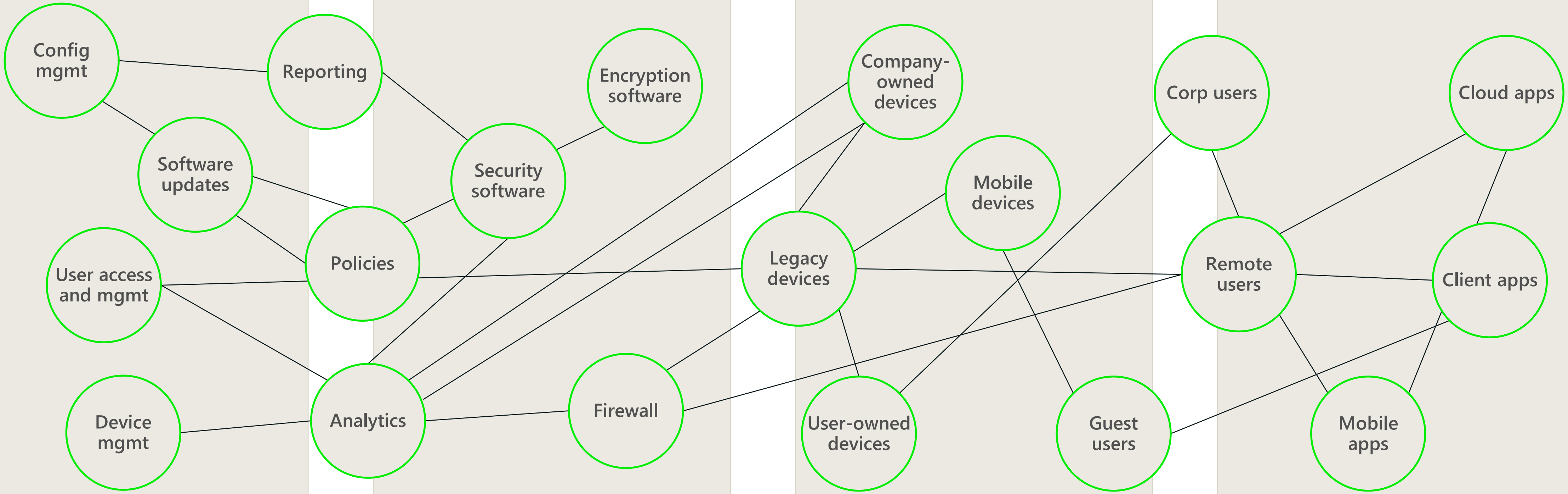
Multiple devices and app platforms

Employee satisfaction

Easy, fast access to company resources

Cybersecurity

Mitigating risk and vulnerabilities



The challenges of endpoint management

Distributed workers

Remote and hybrid work environments

49 million

Remote workers report it takes days—and even weeks—to get issues fixed.

Endpoint diversity

Multiple devices and app platforms

48 percent

IT leaders say ensuring data security is their top challenge in supporting end-user productivity.

Employee satisfaction

Easy, fast access to company resources

44 percent

Remote workers say they have access, but not to everything they need.

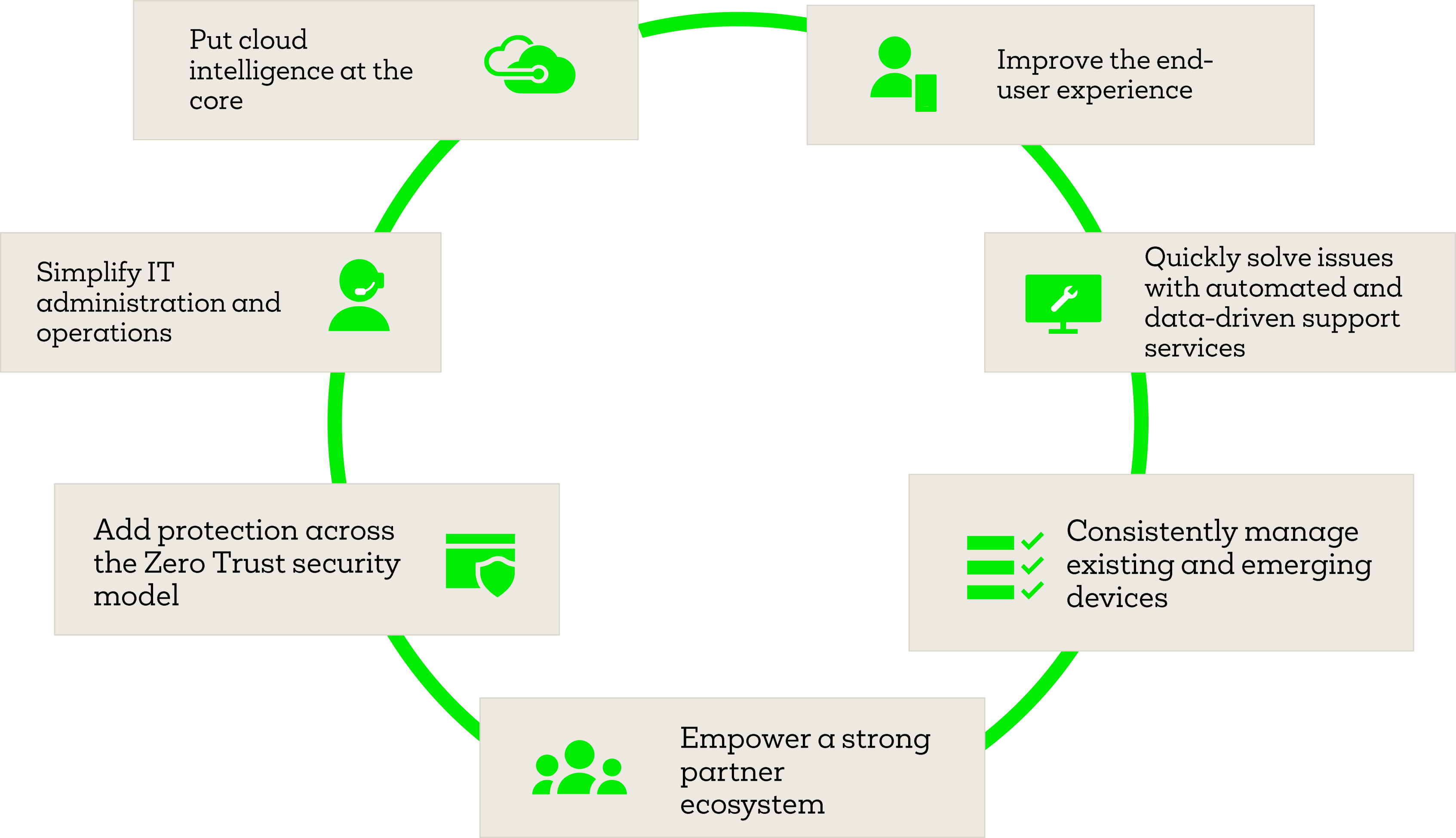
Cybersecurity

Mitigating risk and vulnerabilities

65 percent

Enterprises need to ensure security and compliance across multiple device types.

What do we mean by Modern Management?



Put cloud intelligence at the core

Improve the end-user experience

Quickly solve issues with automated and data-driven support services

Consistently manage existing and emerging devices

Empower a strong partner ecosystem

Add protection across the Zero Trust security model

Simplify IT administration and operations

Technology needs are evolving in the modern workplace

Old world versus new world

Single corporate-owned device	⇋	Multiple BYOD devices and IoT devices
Business owned	⇋	User and business owned
Corporate network and legacy apps	⇋	Cloud managed and SaaS apps
Manual and reactive	⇋	Automated and proactive
Corporate network and firewall	⇋	Expanding perimeters
Employees	⇋	Employees, partners, customers, bots
Mostly onsite employees	⇋	Remote and hybrid environment

People are working in more places, with more flexibility and more devices

How do you secure your endpoint estate?

How do you reduce complexity of IT workloads?

How do you ensure protection, while enabling workforce flexibility and productivity?

Technology must keep us connected and productive while reinforcing our security posture in an increasingly sophisticated and complex world.

Microsoft Endpoint Manager

Endpoint Manager combines the **Microsoft Intune** and **Configuration Manager** solutions to provide modern management of endpoints with the protection of a Zero Trust strategy.

- Protect apps and devices for a resilient workforce
- Maximize digital investment with co-management
- Get integrated Conditional Access controls
- Use simplified management workflows
- Secure managed and unmanaged devices and apps

Unified management

Apps, device controls, and insights are brought together in one cloud-based endpoint management platform.

Built-in protection

IT is empowered to apply the controls needed for a Zero Trust security model and protect their digital estate without getting in the way of user productivity.

Comprehensive scalability

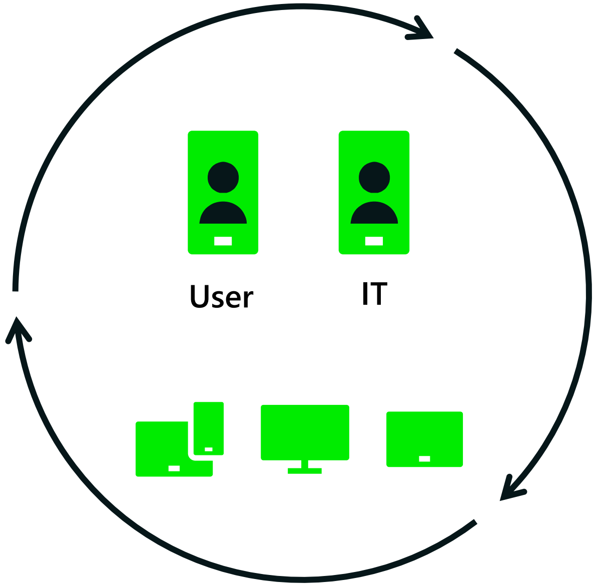
Intuitive management controls, workflows, and analytics ensure healthy and compliant device and app deployments.

Reduced total cost of ownership (TCO)

Device lifecycle with Microsoft Endpoint Manager

Enroll

- Provide specific enrollment methods for iOS/iPadOS, Android, Windows, and macOS
- Provide a self-service company portal for users to enroll BYOD devices
- Deliver custom terms and conditions at enrollment
- Zero-touch provisioning with automated enrollment options for corporate devices



Configure

- Deploy certificates, email, VPN, and Wi-Fi profiles
- Deploy device security policy settings
- Install mandatory apps
- Deploy device restriction policies
- Deploy device feature settings

Support and retire

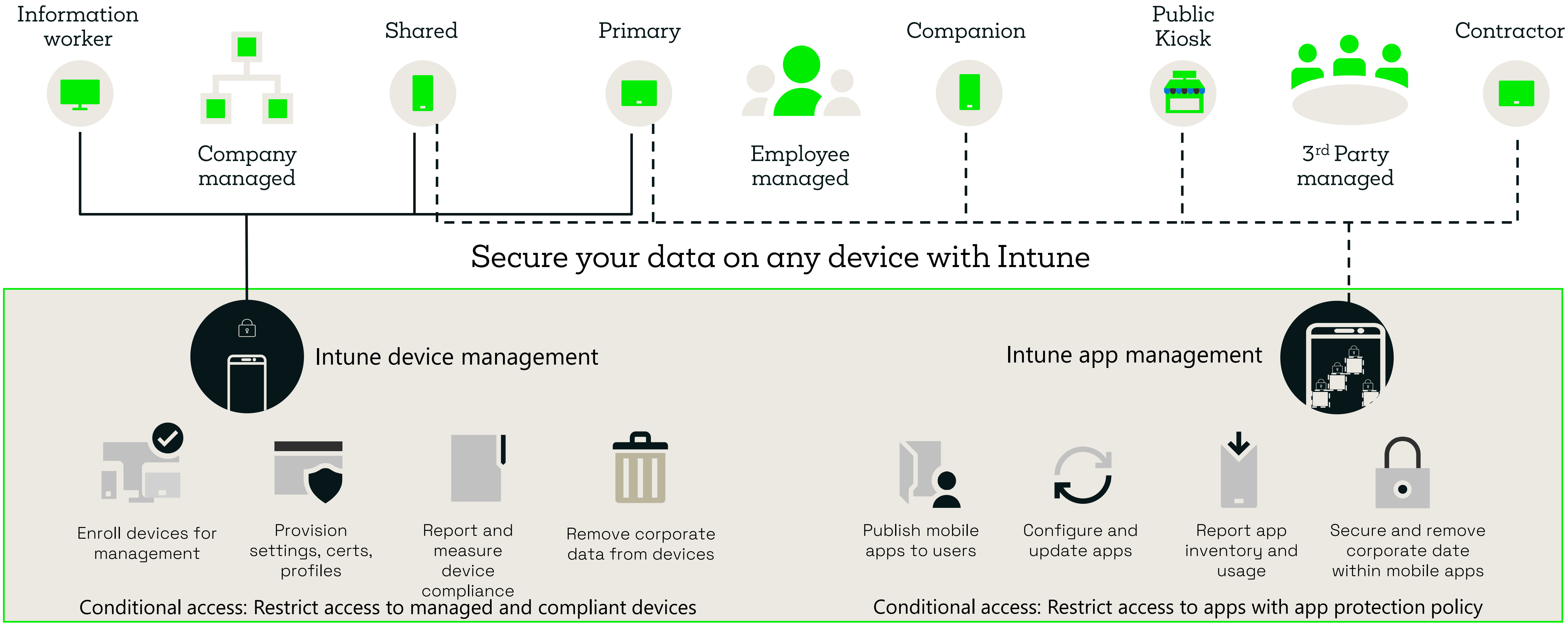
- Revoke access to corporate resources
- Perform selective wipe
- Audit lost and stolen devices
- Retire device
- Provide remote assistance

Protect

- Restrict access to corporate resources if policies are violated (e.g., jailbroken device)
- Protect corporate data by restricting actions such as copy/cut/paste/save outside of managed app ecosystem
- Report on device and app compliance

Enroll

In a complex device landscape, you need choices



Information worker

Company managed

Shared

Primary

Employee managed

Companion

Public Kiosk

3rd Party managed

Contractor

Secure your data on any device with Intune

Intune device management

Enroll devices for management

Provision settings, certs, profiles

Report and measure device compliance

Remove corporate data from devices

Conditional access: Restrict access to managed and compliant devices

Intune app management

Publish mobile apps to users

Configure and update apps

Report app inventory and usage

Secure and remove corporate date within mobile apps

Conditional access: Restrict access to apps with app protection policy

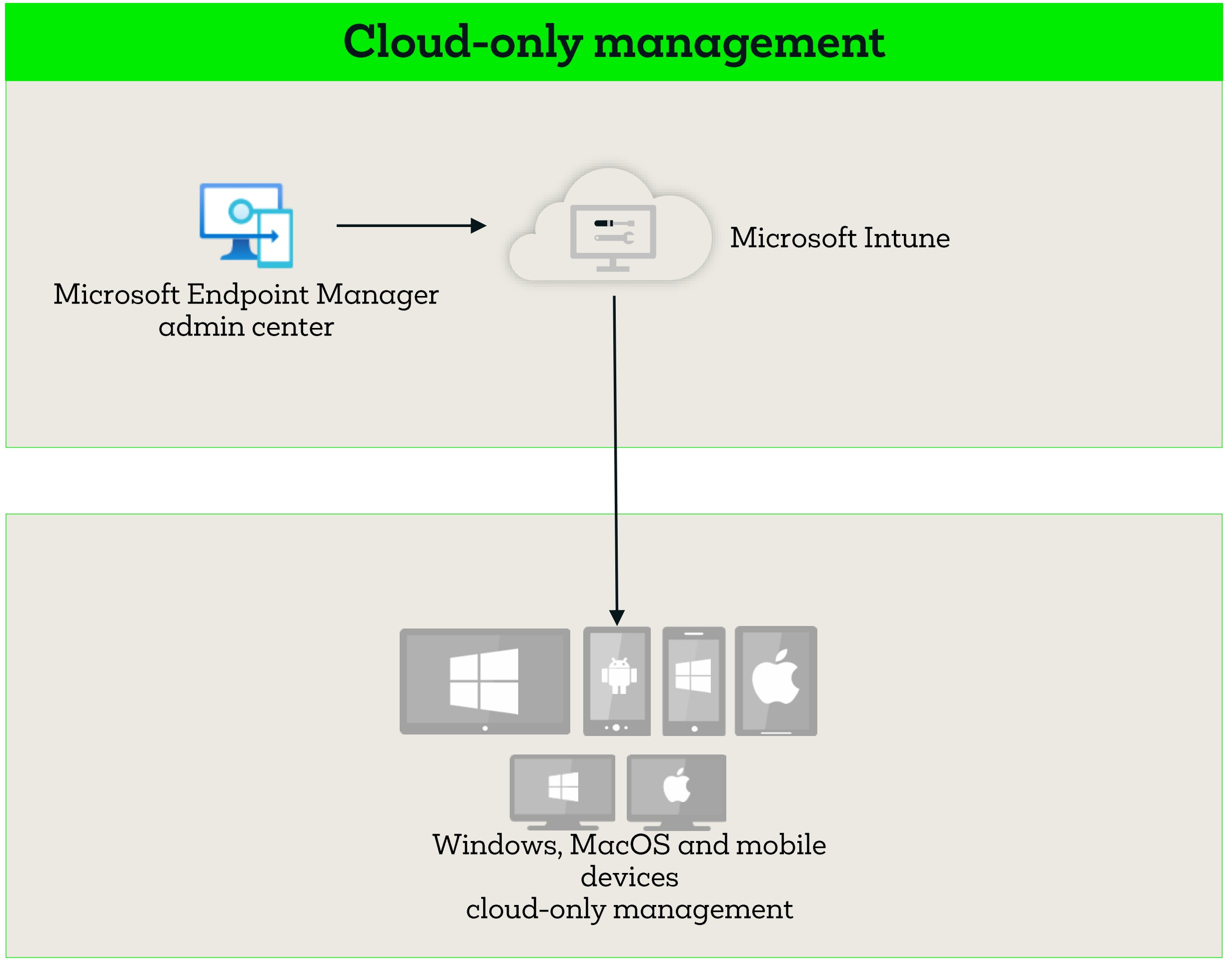
Dependencies for Microsoft Intune standalone (Cloud-only)

Manage and protect

- → No existing infrastructure necessary
- → No existing Microsoft Endpoint Configuration Manager deployment required
- → Simplified policy control
- → Simple web-based administration console
- → Faster cadence of updates
- → Always up-to-date

Device enrollment supported

- → Windows
- → iOS/iPadOS
- → Android
- → macOS


Cloud-only management
Microsoft Endpoint Manager admin center
Microsoft Intune
Windows, MacOS and mobile devices
cloud-only management

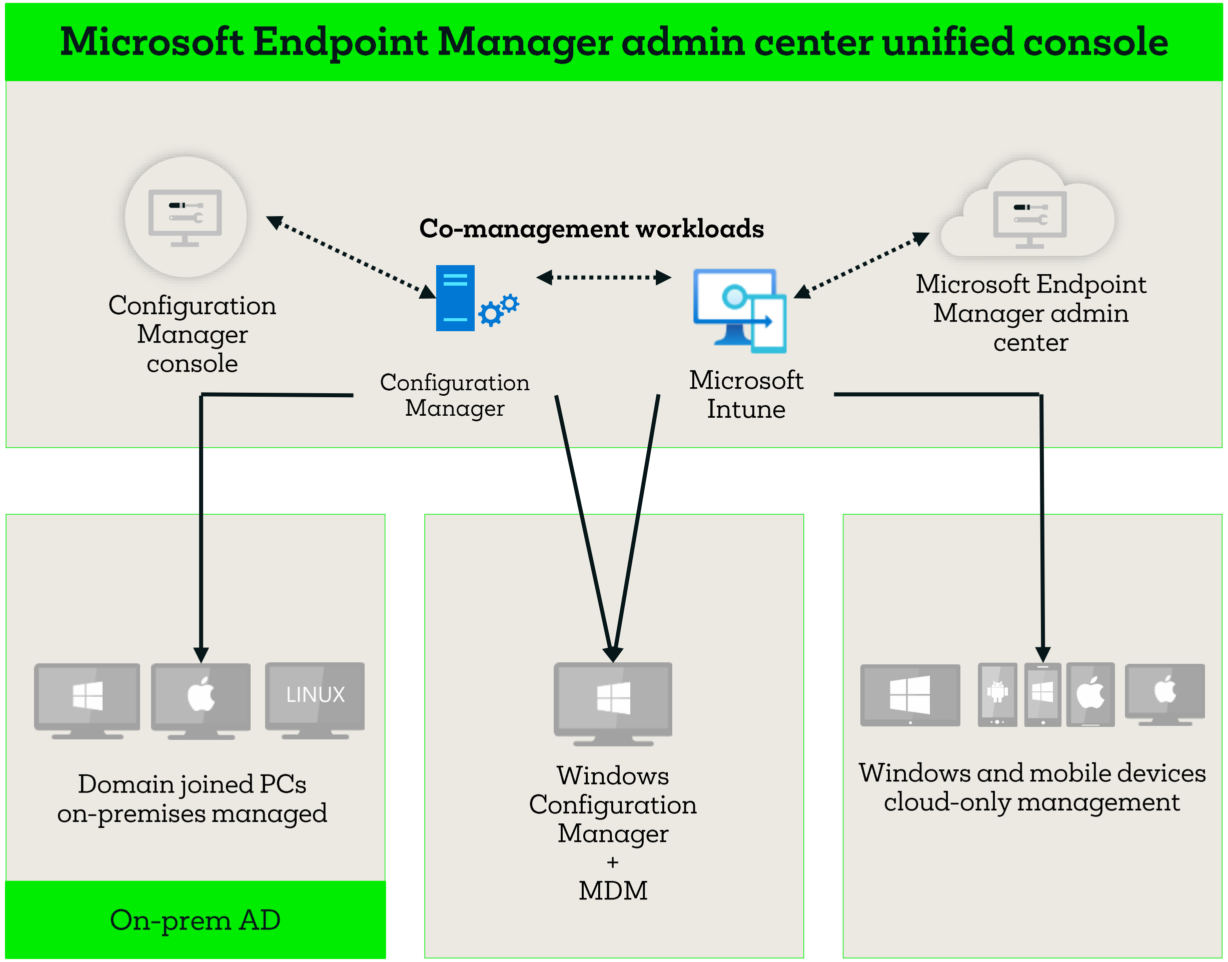
Dependencies for co-management

Microsoft Endpoint Configuration Manager with Microsoft Intune

- → Attach your existing Configuration Manager (version 1710 or later) deployment to Microsoft 365 cloud
- → Co-managed device has a Configuration Manager agent and is enrolled in Intune
- → Single pane of glass for device management
- → Conditional Access with device compliance
- → Intune-based remote actions
- → Modern provisioning with Windows Autopilot
- → Link users, devices, and apps with Azure Active Directory (Azure AD)

Devices Supported (in addition to mobile devices)

- → Windows PCs (x86/64, Intel SoC)
- → Windows Server
- → Linux/UNIX server
- → macOS


Microsoft Endpoint Manager admin center unified console
Configuration Manager console
Co-management workloads
Configuration Manager
Microsoft Intune
Microsoft Endpoint Manager admin center
LINUX
Domain joined PCs on-premises managed
On-prem AD
Windows Configuration Manager + MDM
Windows and mobile devices cloud-only management

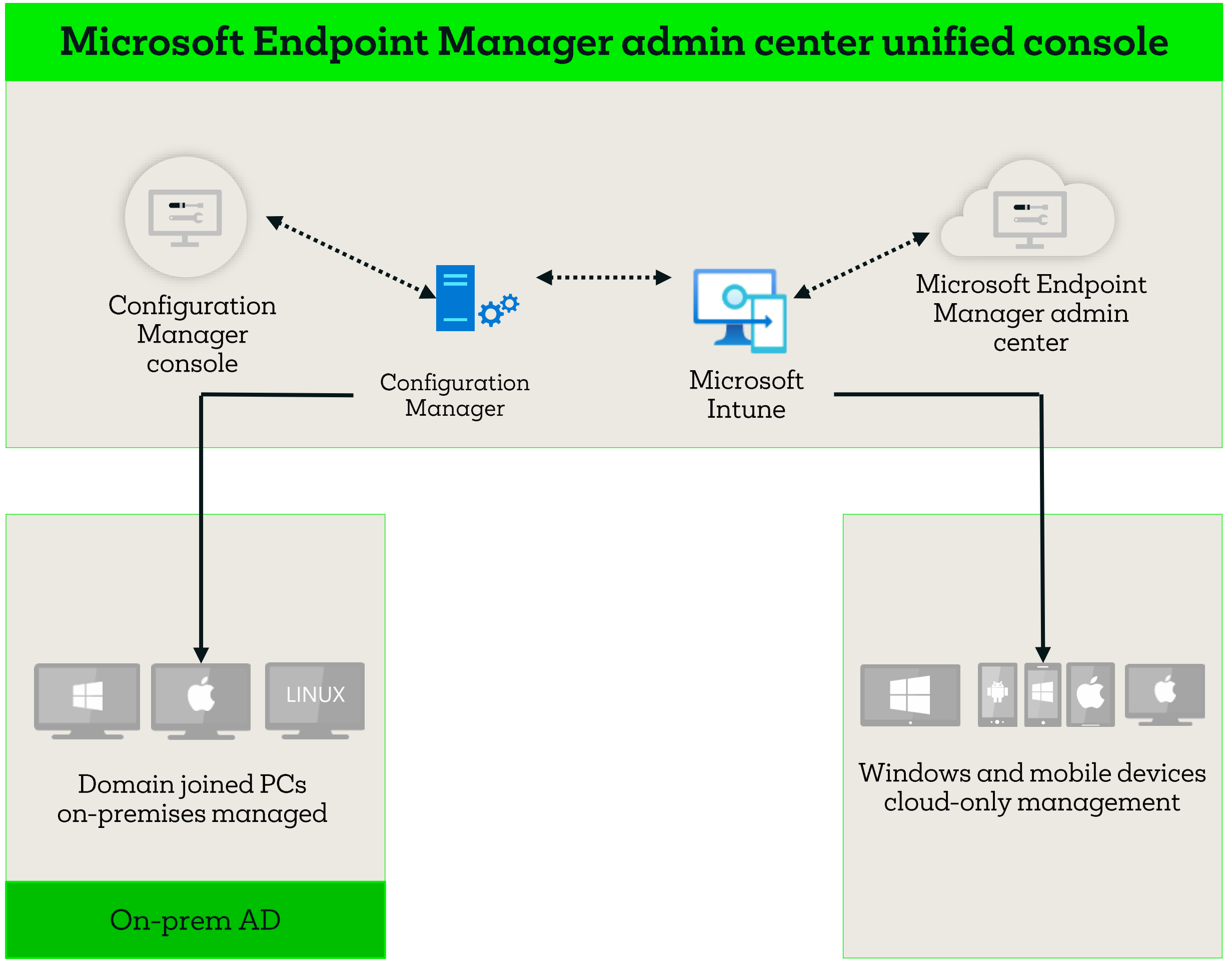
Dependencies tenant attach

Attach Microsoft Endpoint Configuration Manager to Microsoft Intune

- → Attach your existing Configuration Manager (version 2002 or later) deployment to Microsoft 365 cloud
- → Synchronise Configuration Manager agents to Intune without enrolling in Intune
- → Single pane of glass for device management in the cloud
- → Defender for Endpoint integration
- → Helpdesk
- → Desktop Analytics
- → User Experience Analytics

Devices Supported (in addition to mobile devices)

- → Windows PCs (x86/64, Intel SoC)
- → Windows Server
- → Linux/UNIX server
- → macOS


Microsoft Endpoint Manager admin center unified console
Configuration Manager console
Configuration Manager
Microsoft Intune
Microsoft Endpoint Manager admin center
LINUX
Domain joined PCs on-premises managed
On-prem AD
Windows and mobile devices cloud-only management

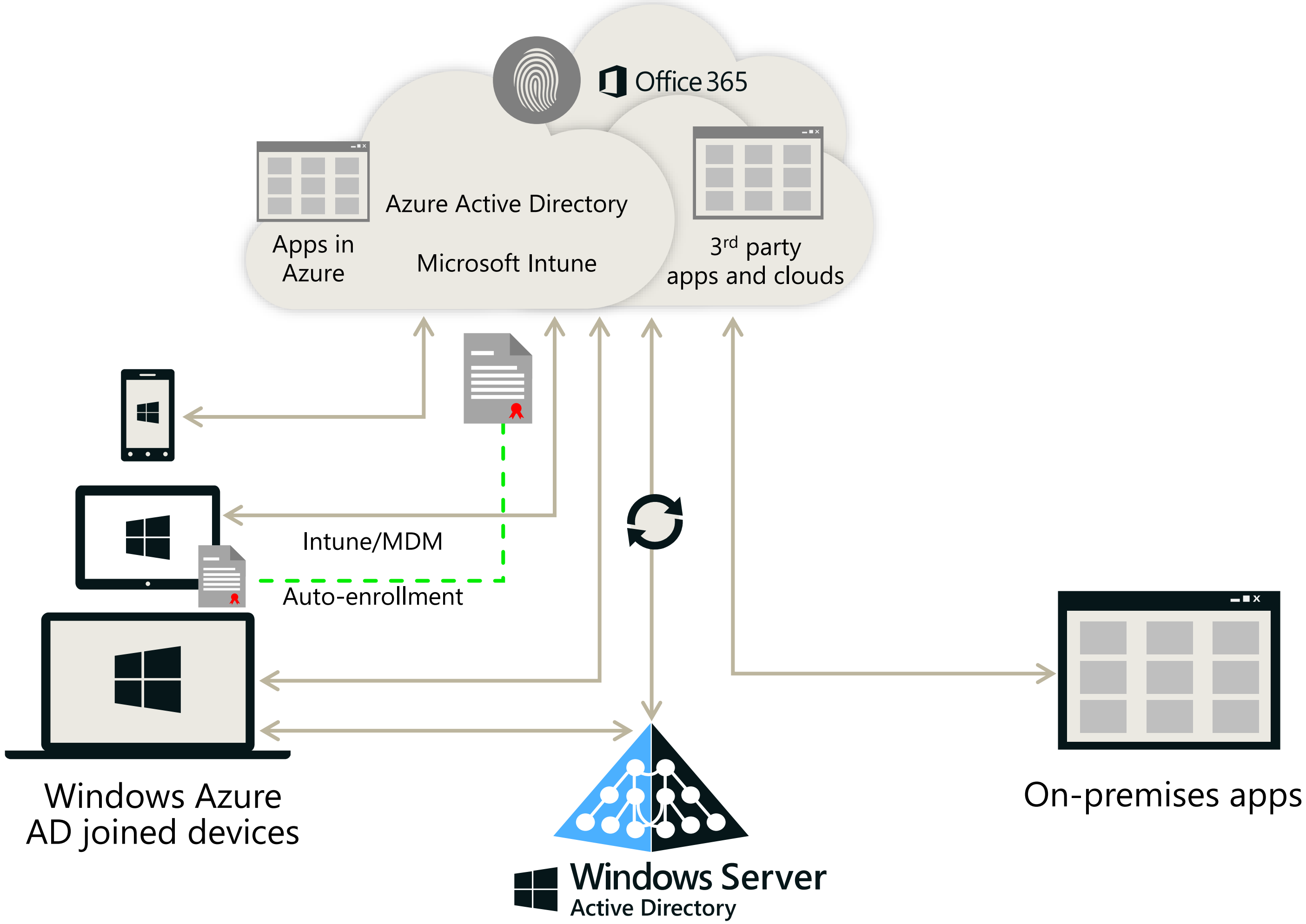
Auto-enrol Windows devices

Azure AD Join makes it possible to connect work-owned Windows devices to your company's Azure Active Directory.

With Azure AD Join, you can auto-enroll devices in Microsoft Intune for management.

Benefits:

- Intune auto-enrollment
- Enterprise-compliant services
- Single sign-on from the desktop to cloud and on-premises applications with no VPN
- Support for hybrid environments



Windows Autopilot

OEM-optimized Windows

+ Software

+ Settings

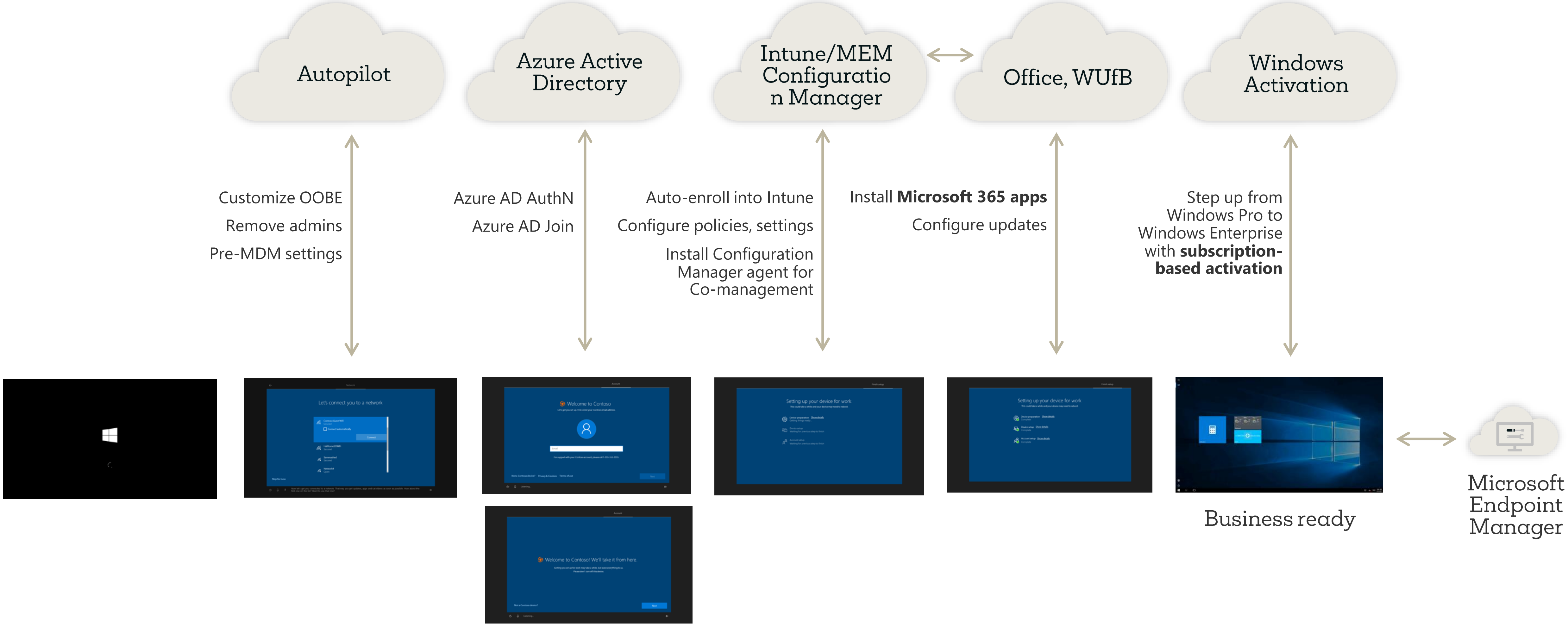
+ Updates

+ Features

+ User data

Ready for productive use

Windows 10 Modern Provisioning



Autopilot

- Customize OOBE
- Remove admins
- Pre-MDM settings

Azure Active Directory

- Azure AD AuthN
- Azure AD Join

Intune/MEM Configuratio n Manager

- Auto-enroll into Intune
- Configure policies, settings
- Install Configuration Manager agent for Co-management

Office, WUfB

- Install **Microsoft 365 apps**
- Configure updates

Windows Activation

- Step up from Windows Pro to Windows Enterprise with **subscription-based activation**

Let's connect you to a network

Welcome to Contoso

Welcome to Contoso! 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.

Setting up your device for work

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

Self-driven deployment

Business ready

Microsoft Endpoint Manager

Windows Autopilot / User-Driven deployment with Azure AD Join

Prerequisites:

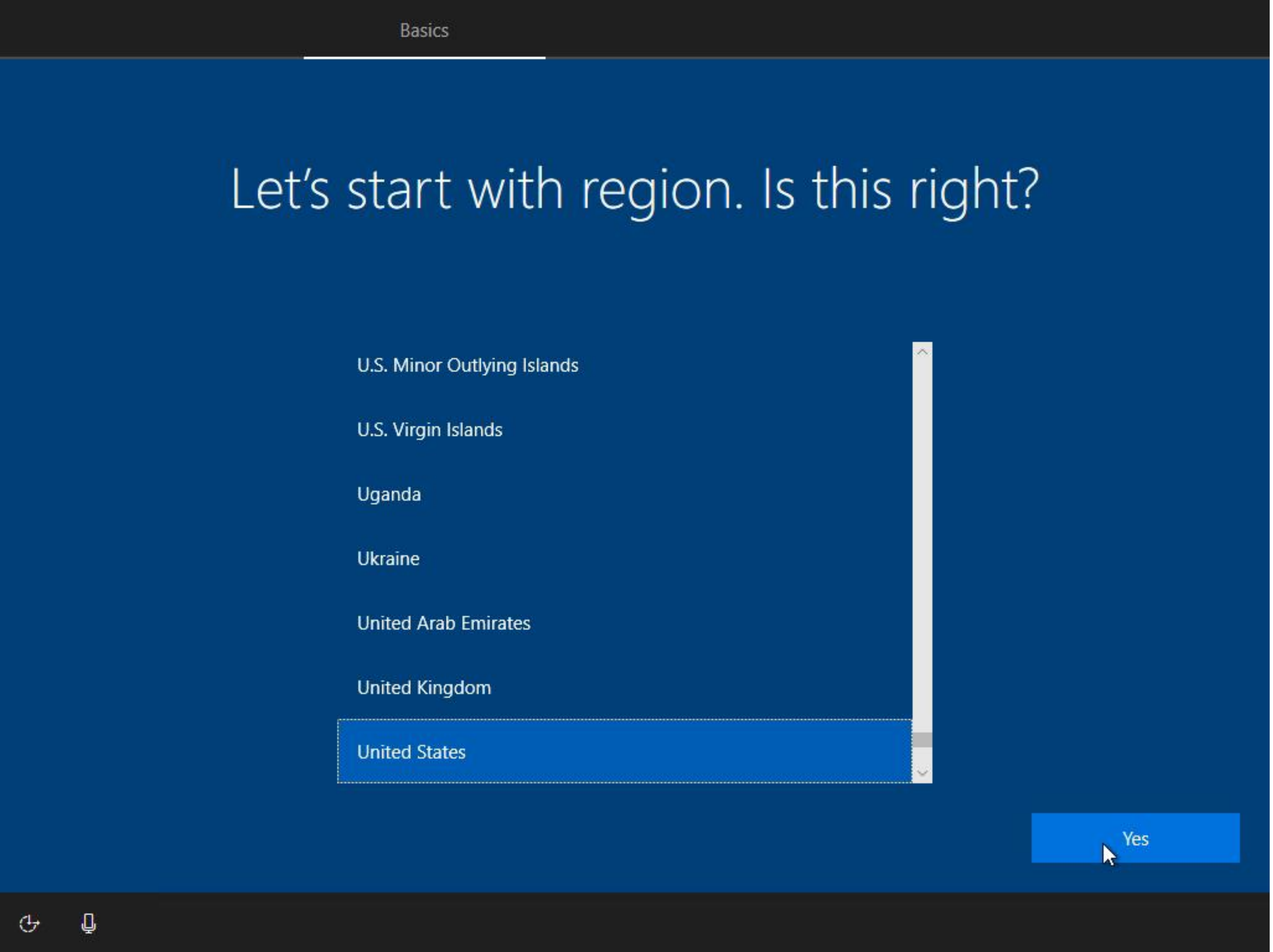
Windows 10 version 1703

Azure Active Directory Premium

Microsoft Intune

Steps:

1. Device connected to internet network
2. Register device with Windows Autopilot
3. Assign Intune Autopilot Profile configured for Azure AD join
4. Boot device



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

User-Driven Azure AD Join

- Connect to a network
- Authenticate to Azure AD
- Password-less with phone sign-in
- Enroll in Intune
- Track progress with the Enrollment Status Page
  - Policies
    Apps (Win32, MSI, UWP)
    Certificates
    Network, VPN connections
- Integration with ConfigMgr task sequences

Windows Autopilot / User-Driven deployment with Hybrid Azure AD

New

Prerequisites:

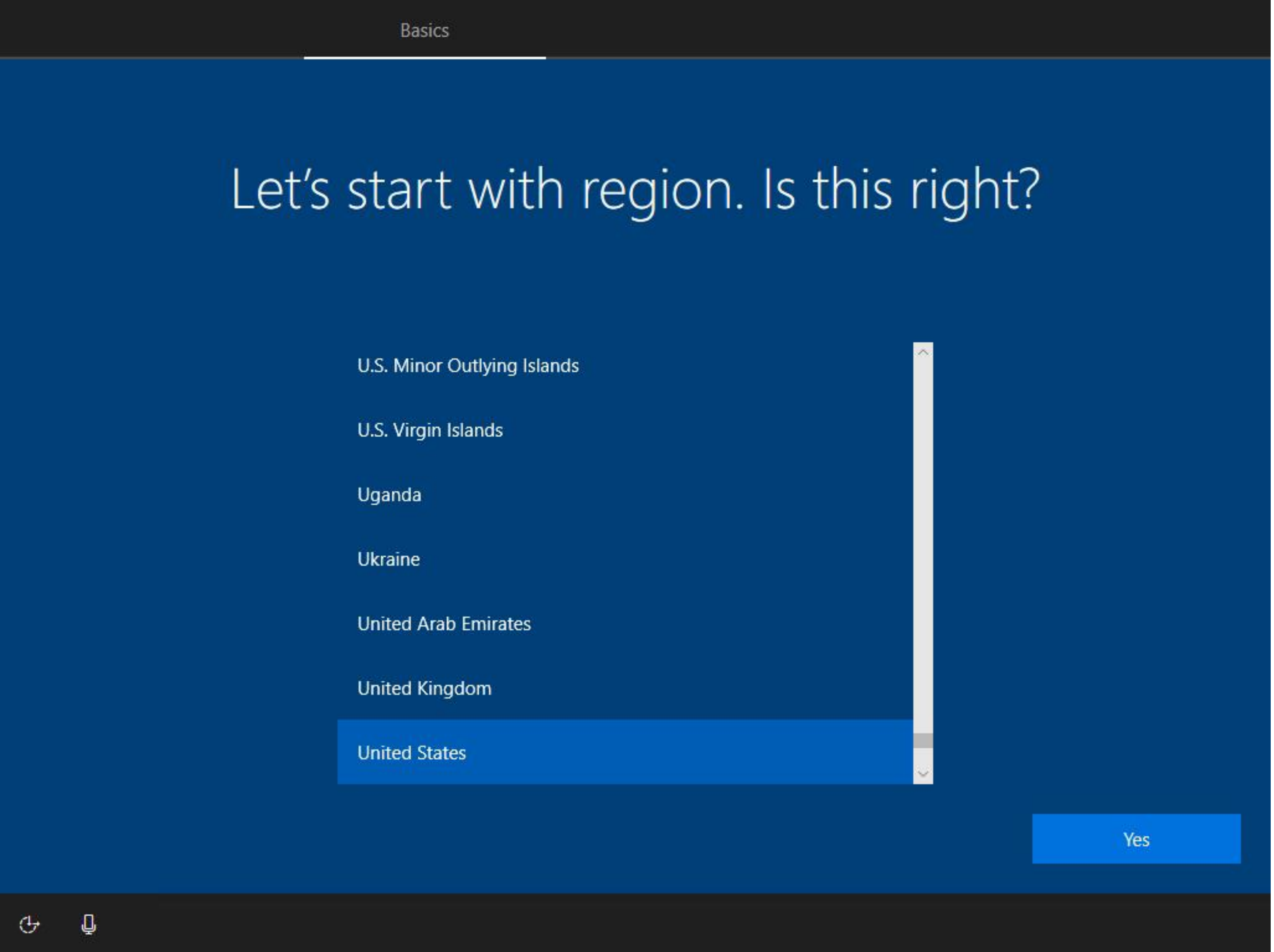
Windows 10 version 1809

Azure Active Directory Premium

Microsoft Intune

Steps:

1. Device connected to corporate network (SBL VPN or client initiated at logon screen)
2. Register device with Windows Autopilot
3. Assign Intune Autopilot Profile configured for Hybrid Azure AD join
4. Boot device



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

New

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 domain join
- VPN support
- Track progress with the Enrollment Status Page
  - Policies
    Apps (Win32, MSI, UWP)
    Certificates
    Network, VPN connections
- Integration with ConfigMgr task sequences

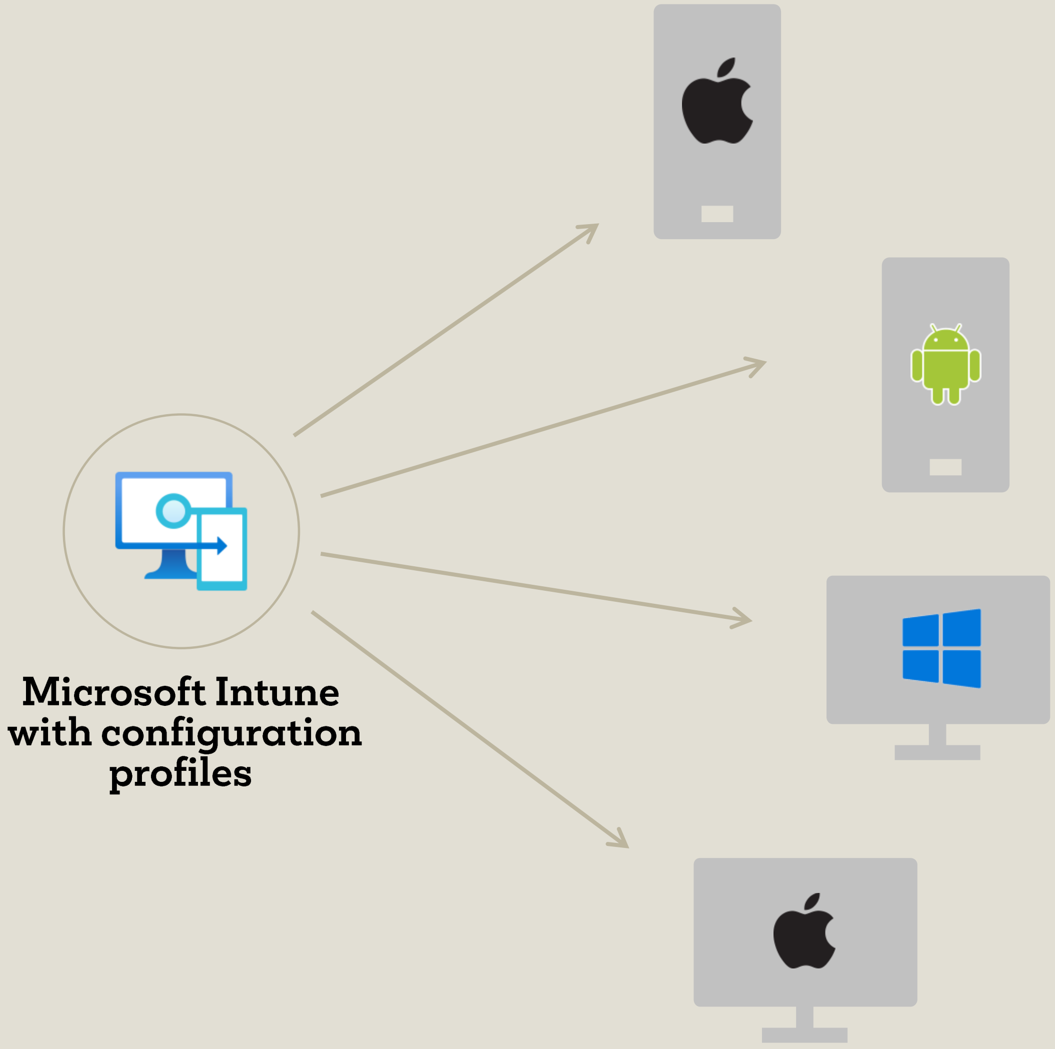
Configure

What are configuration profiles?

Microsoft Intune provides configuration profiles which includes settings and features that can be enabled or disabled on different devices within your organization

Configuration profiles can be applied to:

- → iOS/iPadOS devices
- → Android devices
- → Windows devices
- → macOS devices



What do configuration profiles provide?

Device features

Controls features on the device

Examples: Airprint, notifications and lock screen messages

Device restrictions

Controls security, hardware, data sharing and more settings on the devices

Examples: require a PIN, data encryption, etc

Access configuration

Provide organization's access configuration to the device

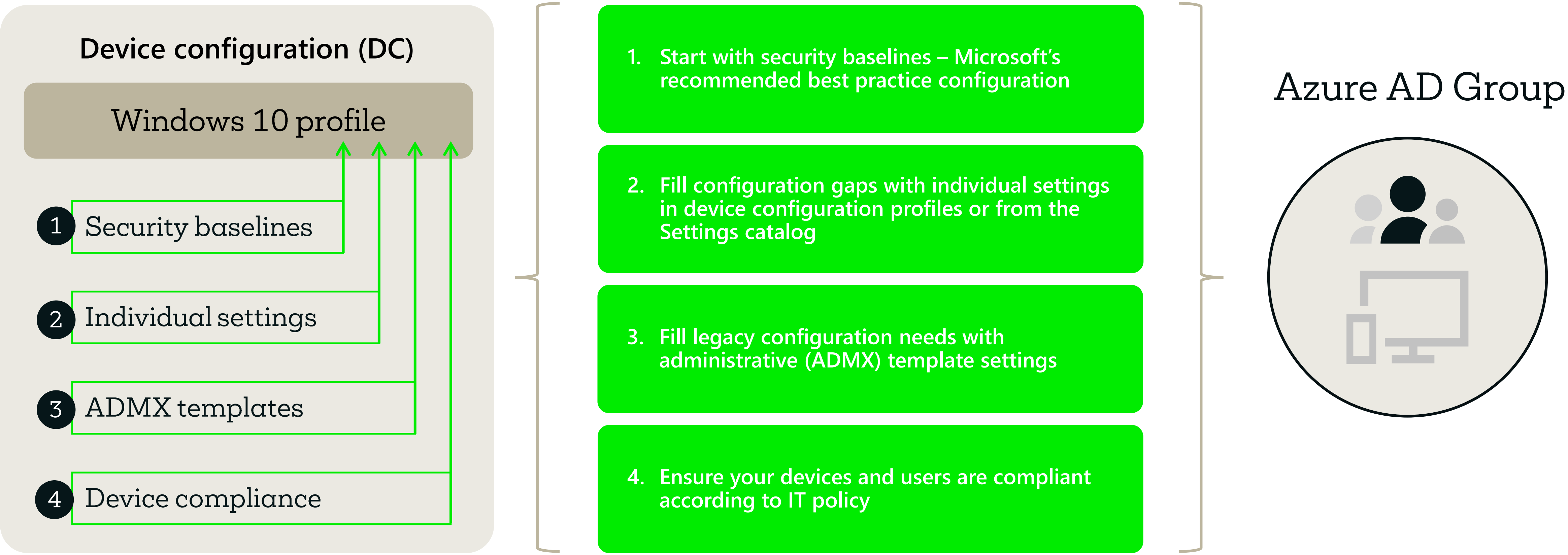
Examples: email profiles, VPN profiles, Wi-Fi settings, certificates, etc

Custom

Set custom configuration or execute custom configuration actions

Examples: set OEM settings, execute PowerShell scripts, etc

Windows 10 recommended device configuration



1. Start with security baselines – Microsoft’s recommended best practice configuration
2. Fill configuration gaps with individual settings in device configuration profiles or from the Settings catalog
3. Fill legacy configuration needs with administrative (ADMX) template settings
4. Ensure your devices and users are compliant according to IT policy

Use security baselines to configure Windows 10 devices

Security baselines are pre-configured groups of **Windows** settings and default values that are recommended by the relevant Microsoft security teams

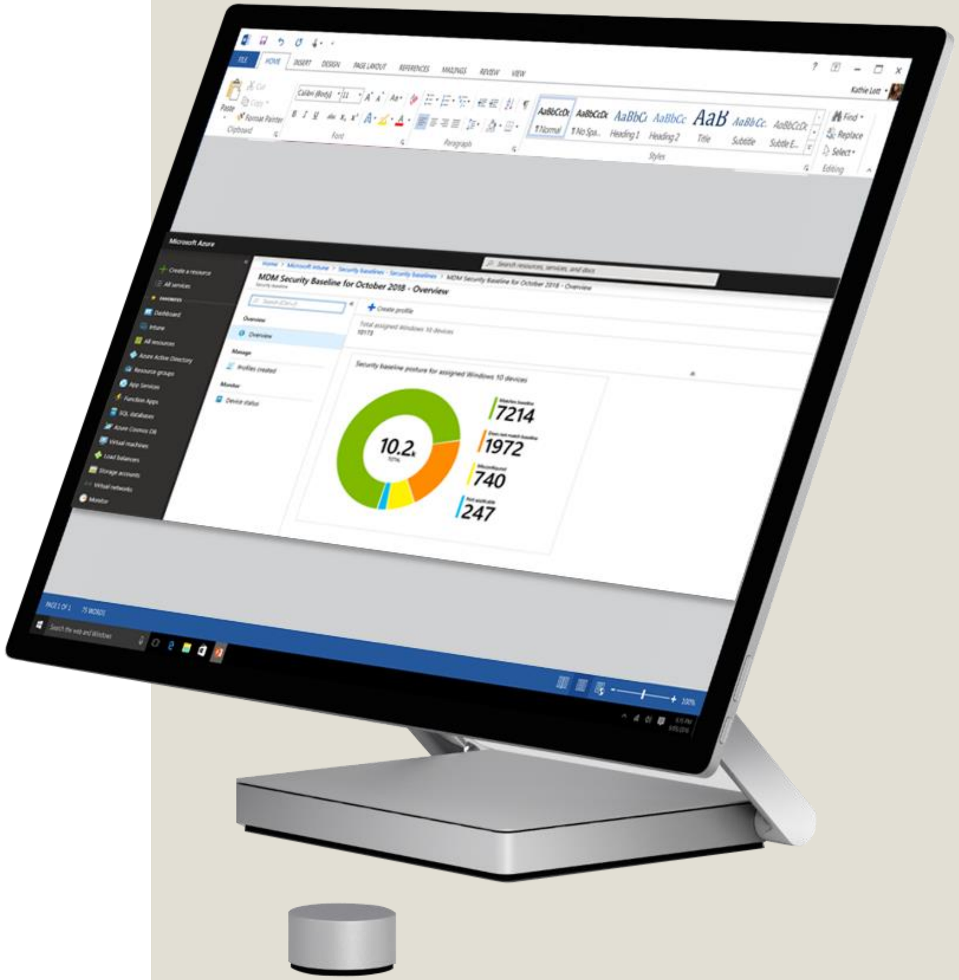
A security baseline profile is a template that consists of multiple **device configuration profiles**

Benefits

Includes the best practices and recommendations on settings that impact security

A good starting point to quickly create and deploy a secure configuration profile

Easier to migrate from group policy to Intune management


Microsoft Azure
MDM Security Baseline for October 2018 - Overview
Security baseline posture for assigned Windows 10 devices
10.2
7214
1972
740
247

Administrative templates

Administrative templates include thousands of settings that control features in Microsoft Edge version 77 and later, Internet Explorer, Microsoft Office programs, remote desktop, OneDrive, passwords, PINs, and more

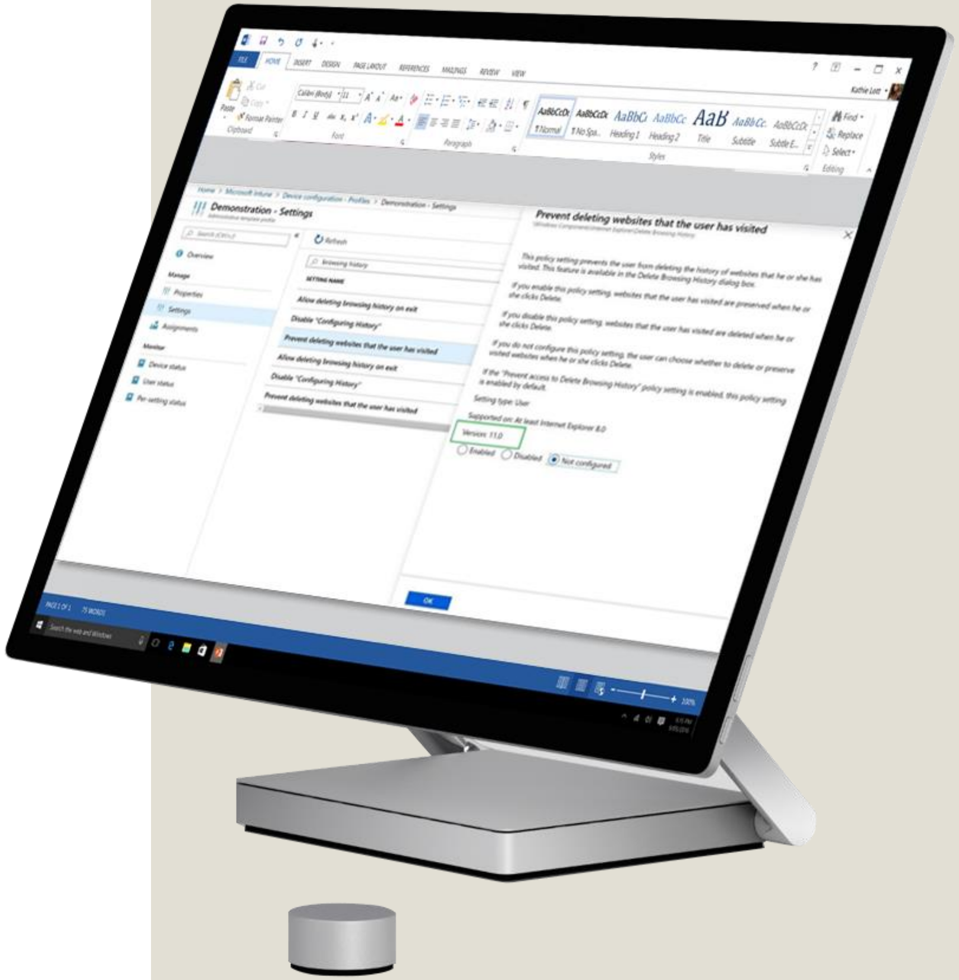
Administrative templates contain ADMX-backed Windows settings that are like group policy settings in Active Directory

Benefits

Administrative templates are built into Intune, and don't require any customizations

The one-stop shop to manage your Windows 10 devices

Easier to migrate from group policy to Intune management



SETTING NAME
- Allow deleting browsing history on exit
- Disable "Configuring History"
- Prevent deleting websites that the user has visited
- Allow deleting browsing history on exit
- Disable "Configuring History"
- Prevent deleting websites that the user has visited

Prevent deleting websites that the user has visited

This policy setting prevents the user from deleting the history of websites that he or she has visited. This feature is available in the Delete Browsing History dialog box.

If you enable this policy setting, websites that the user has visited are preserved when he or she clicks Delete.

If you disable this policy setting, websites that the user has visited are deleted when he or she clicks Delete.

If you do not configure this policy setting, the user can choose whether to delete or preserve visited websites when he or she clicks Delete.

If the "Prevent access to Delete Browsing History" policy setting is enabled, this policy setting is enabled by default.

Setting type: User

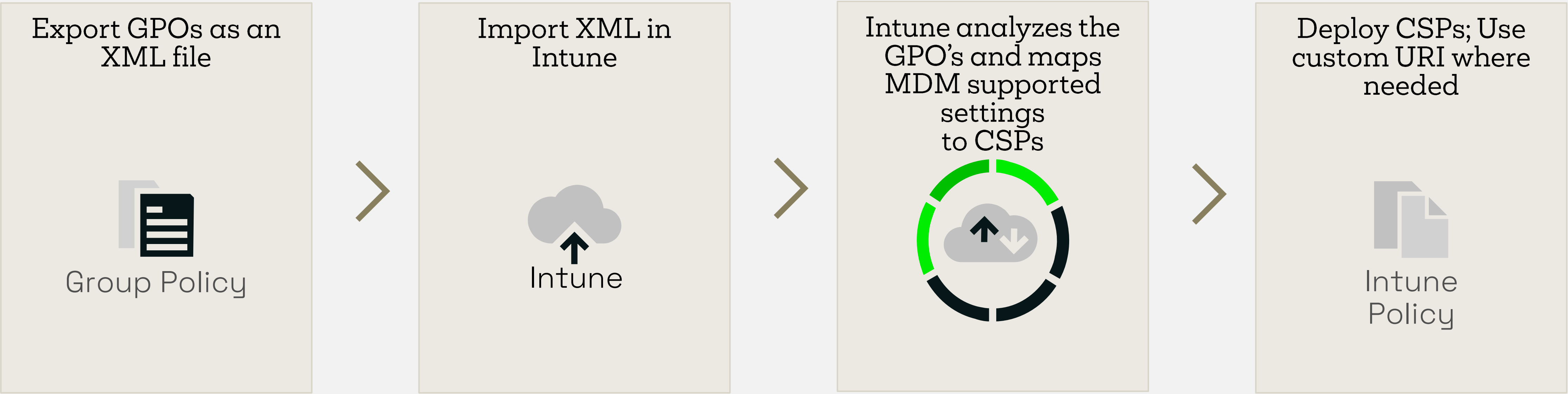
Supported on: At least Internet Explorer 8.0

Version: 11.0

○ Enabled ○ Disabled ● Not configured

Migrate Windows 10 GPOs to Intune CSPs

Group Policy analytics compares GPOs to Intune CSPs



Export GPOs as an XML file

Group Policy

Import XML in Intune

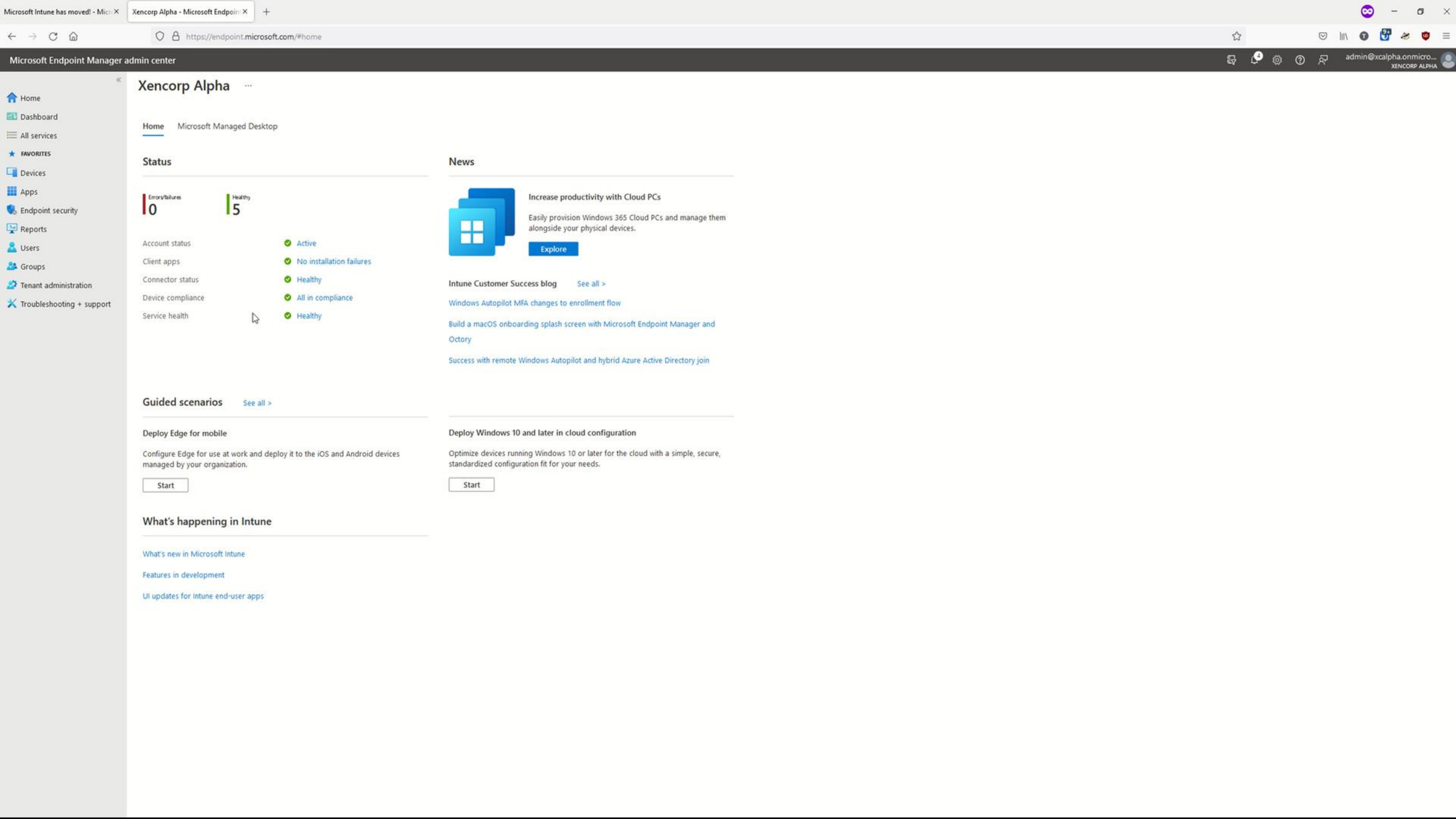
Intune

Intune analyzes the GPO's and maps MDM supported settings to CSPs

Deploy CSPs; Use custom URI where needed

Intune Policy

Review the Group Policy Migration Readiness report to see the number of settings in your GPO that are available in a device configuration profile, if they can be in a custom profile, aren't supported, or are deprecated.


Microsoft Intune has moved! - Micr
Xencorp Alpha - Microsoft Endpoin
https://endpoint.microsoft.com/#home
Microsoft Endpoint Manager admin center
admin@xcalpha.onmicro...
XENCORP ALPHA
Home
Dashboard
All services
FAVORITES
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support

Xencorp Alpha

Home | Microsoft Managed Desktop

Status

Errors/failures	Healthy
0	5

Account status	Active
Client apps	No installation failures
Connector status	Healthy
Device compliance	All in compliance
Service health	Healthy

News

Increase productivity with Cloud PCs

Easily provision Windows 365 Cloud PCs and manage them alongside your physical devices.

Intune Customer Success blog — See all >

Windows Autopilot MFA changes to enrollment flow

Build a macOS onboarding splash screen with Microsoft Endpoint Manager and Octory

Success with remote Windows Autopilot and hybrid Azure Active Directory join

Guided scenarios

See all >

Deploy Edge for mobile

Configure Edge for use at work and deploy it to the iOS and Android devices managed by your organization.

Deploy Windows 10 and later in cloud configuration

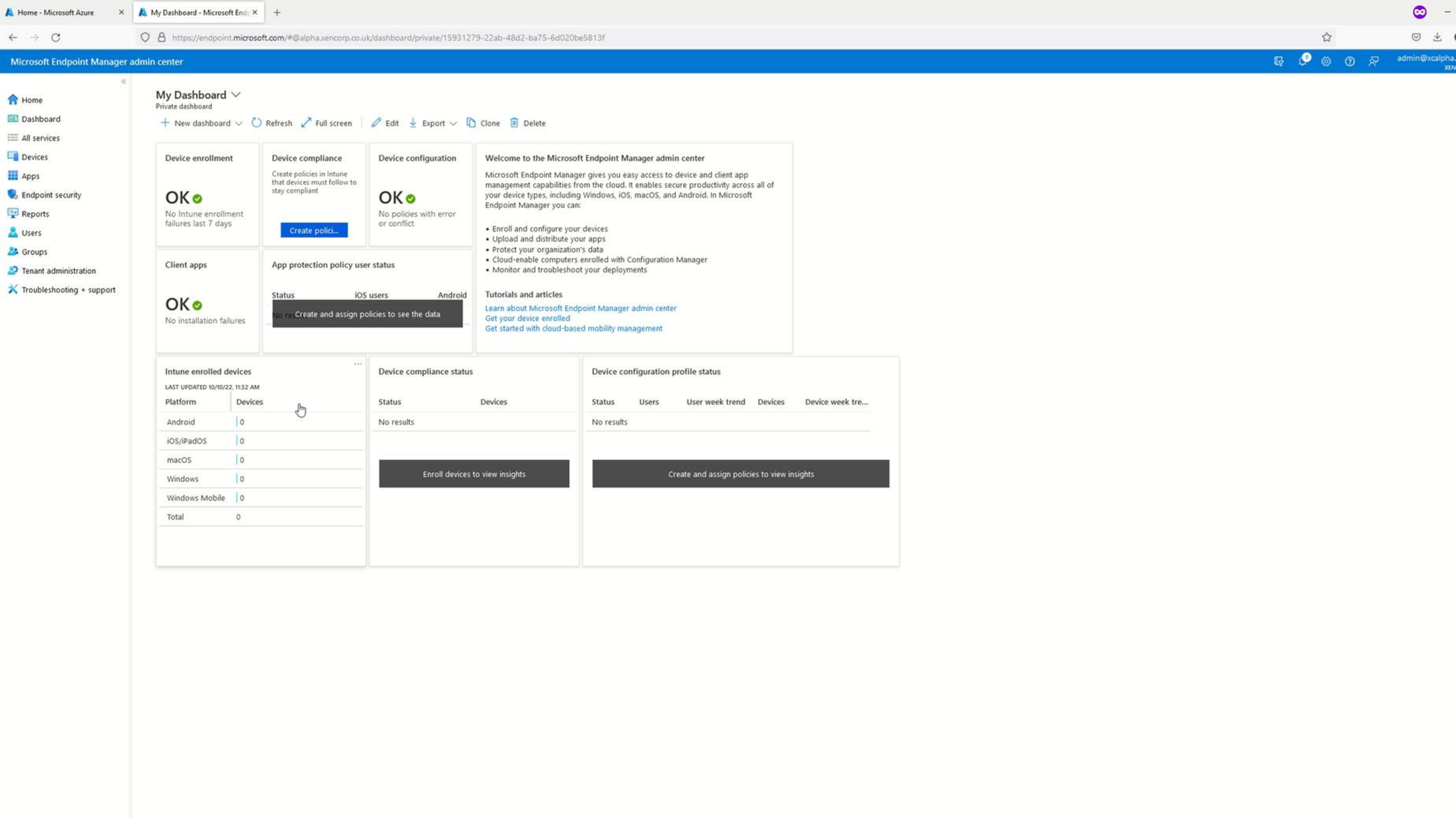
Optimize devices running Windows 10 or later for the cloud with a simple, secure, standardized configuration fit for your needs.

What's happening in Intune

What's new in Microsoft Intune

Features in development

UI updates for Intune end-user apps


Home - Microsoft Azure
My Dashboard - Microsoft End
https://endpoint.microsoft.com/#@alpha.xencorp.co.uk/dashboard/private/15931279-22ab-48d2-ba75-6d020be5813f
Microsoft Endpoint Manager admin center
admin@xcalpha.
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
New dashboard
Refresh
Full screen
Edit
Export
Clone
Delete

My Dashboard

Private dashboard

Device enrollment

OK ✓

No Intune enrollment failures last 7 days

Device compliance

Create policies in Intune that devices must follow to stay compliant

Create polici...

Device configuration

OK ✓

No policies with error or conflict

Welcome to the Microsoft Endpoint Manager admin center

Microsoft Endpoint Manager gives you easy access to device and client app management capabilities from the cloud. It enables secure productivity across all of your device types, including Windows, iOS, macOS, and Android. In Microsoft Endpoint Manager you can:

- Enroll and configure your devices
- Upload and distribute your apps
- Protect your organization's data
- Cloud-enable computers enrolled with Configuration Manager
- Monitor and troubleshoot your deployments

Tutorials and articles

Learn about Microsoft Endpoint Manager admin center
Get your device enrolled
Get started with cloud-based mobility management

Client apps

OK ✓

No installation failures

App protection policy user status

Status	iOS users	Android

Create and assign policies to see the data

Intune enrolled devices

LAST UPDATED 10/10/22, 11:32 AM

Platform	Devices
Android	0
iOS/iPadOS	0
macOS	0
Windows	0
Windows Mobile	0
Total	0

Device compliance status

Status	Devices
No results	

Enroll devices to view insights

Device configuration profile status

Status	Users	User week trend	Devices	Device week tre...
No results				

Create and assign policies to view insights

Windows 10 configuration approaches

	Windows 10 in cloud configuration	Customized Windows 10 management
What a device with this looks like	• Basic productivity apps (Microsoft Teams, Microsoft Edge, Microsoft 365) • Essential line-of-business apps only • Only built-in agents • Cloud enrollment, infrastructure and storage	• Today's typical corporate PC • Lots of apps, agents, and settings • Lots of drivers and devices • On-premise or cloud management and infrastructure
What this means for endpoint management	• Works for a subset of people • Works for targeted scenarios • Every PC has a standard configuration • Simpler end-user experience • Simpler to manage and operate	• Works on any persona • Works for any scenario • PCs have many varying configurations • More complex to operate and manage

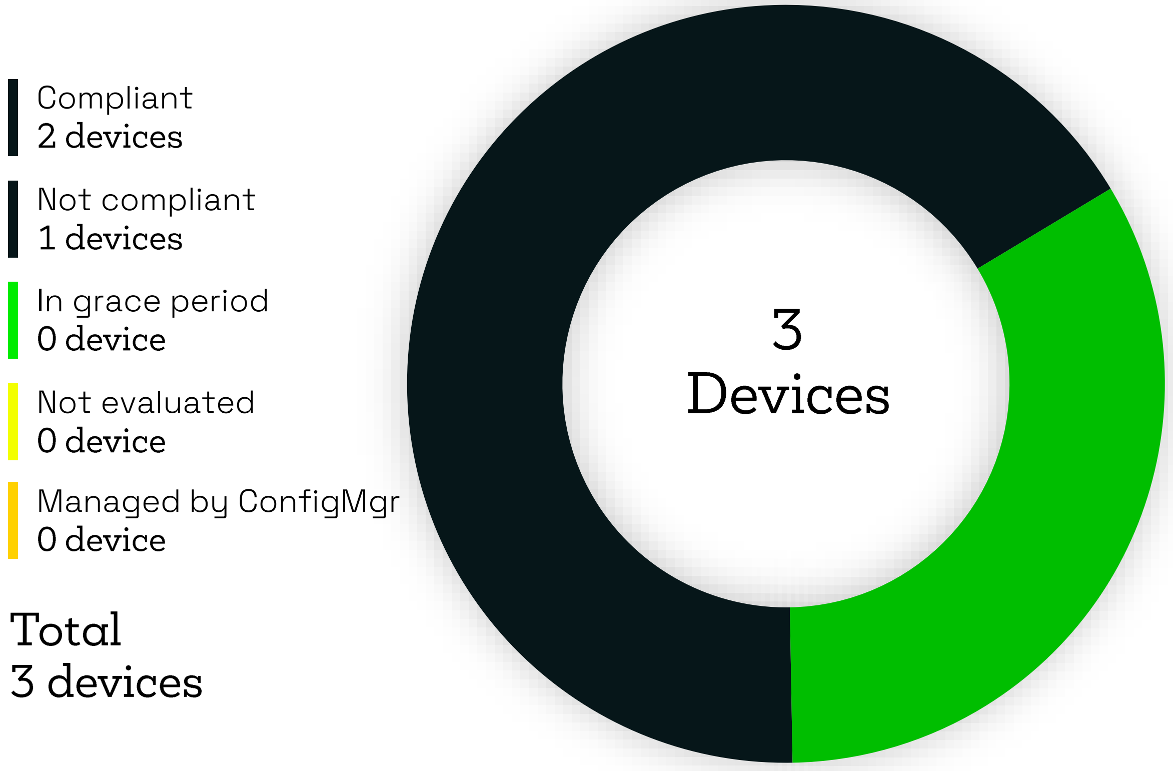
Protect

Microsoft Endpoint Manager compliance policies

Microsoft Endpoint Manager (MEM) provides **compliance policies**, which are **device-level rules** that determine whether a device is compliant with organisation’s “secure device” definition.

Compliance policies can be applied to

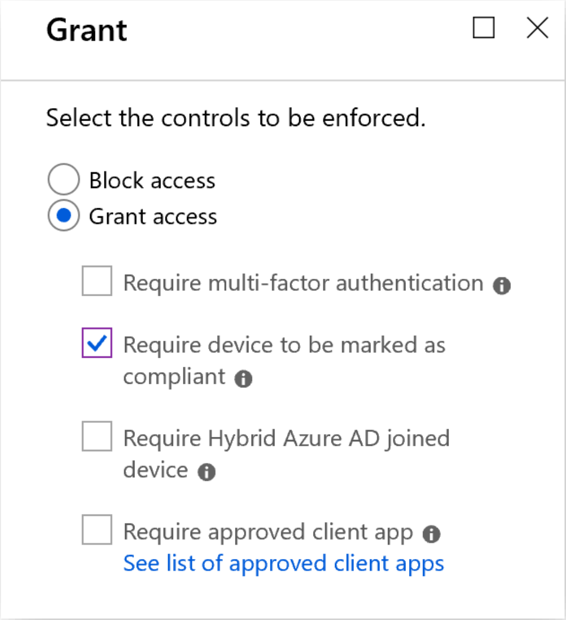
- **iOS/iPadOS** devices (iPhones, iPads, iPods)
- **Android** devices
- **Windows** devices
- **macOS** devices



Use of device compliance

Conditional access

Conditional access policies can use device compliance to grant or block access to organisational resources.



Grant

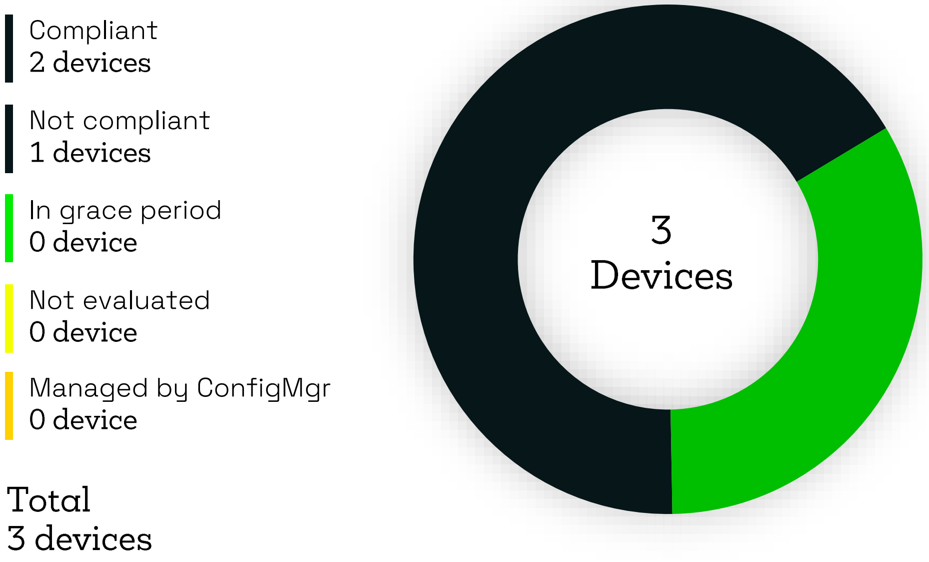
Select the controls to be enforced.

○ Block access
● Grant access

□ Require multi-factor authentication
☑ Require device to be marked as compliant
□ Require Hybrid Azure AD joined device
□ Require approved client app
See list of approved client apps

Monitoring

Organisation-wide device compliance



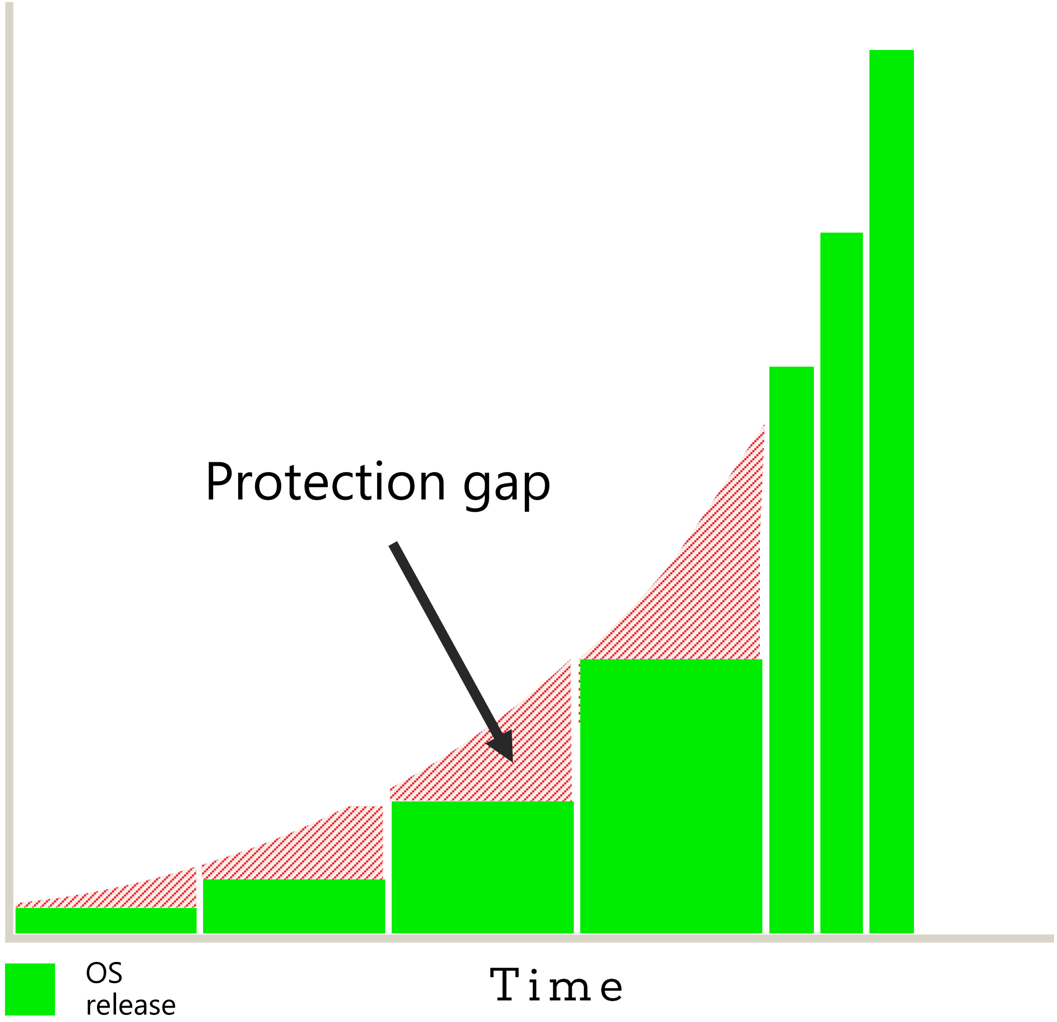
Staying secure during OS updates

Attackers take advantage of periods between OS releases

Stay ahead of the attackers with continual improvements

Continual evolution of features to:

- → Secure data and devices
- → Secure user identities
- → Detect and respond quickly to attacks



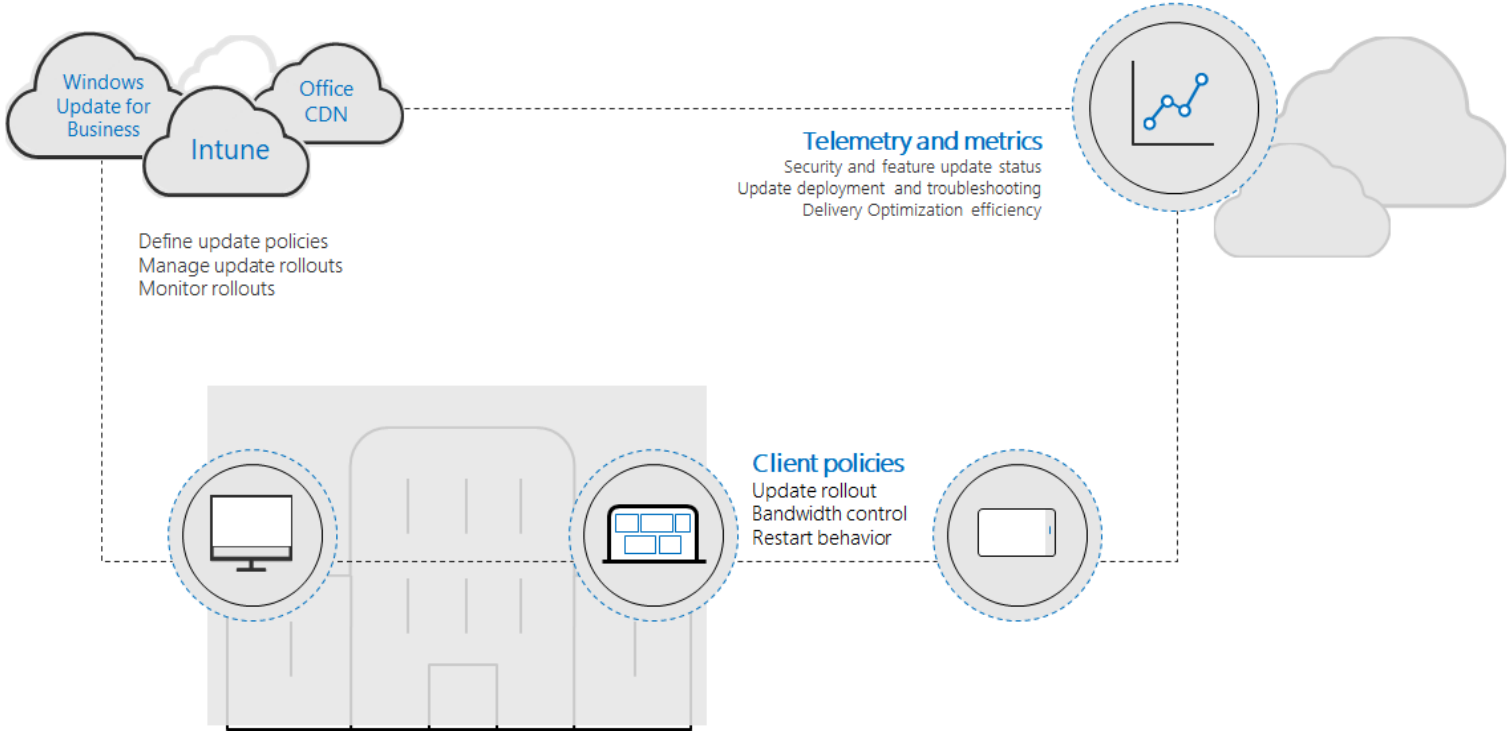
Keeping Windows up-to-date with Microsoft Endpoint Manager and Windows Update for Business

Microsoft Endpoint Manager

Provides OS update policies for Windows to enrolled devices

Windows Update for Business

Provides actual OS update to devices



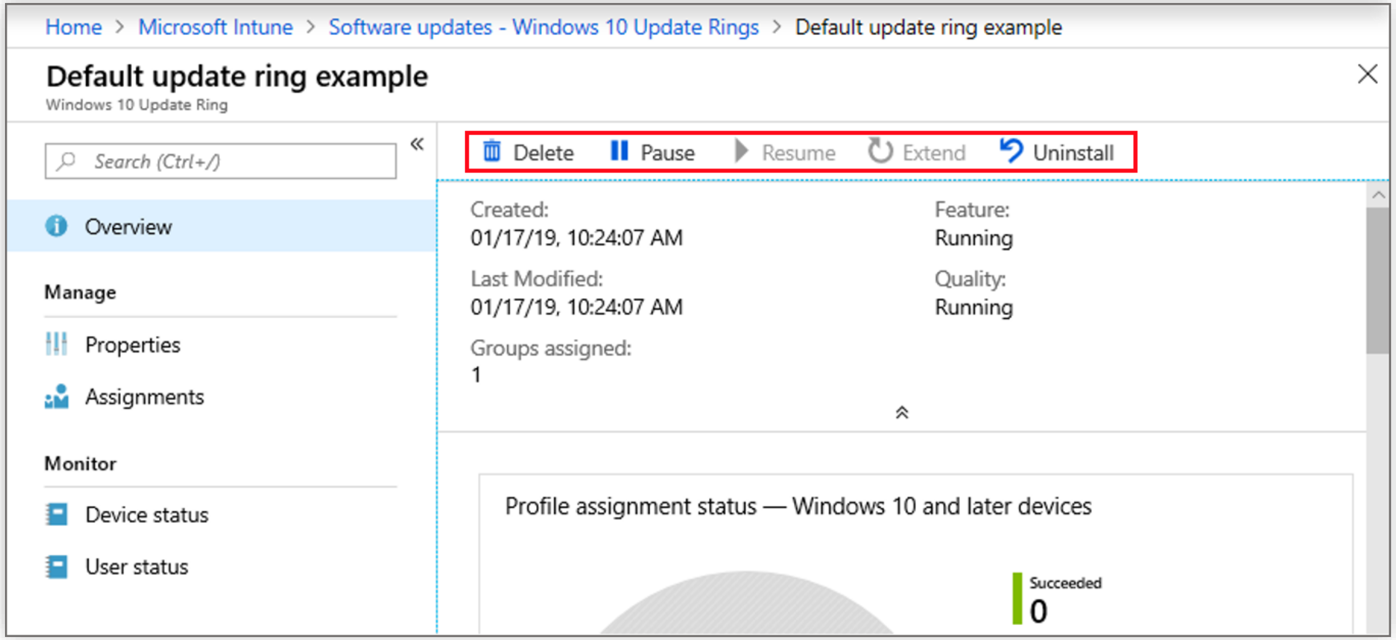
Managing updates from the cloud

Reduce on-premises infrastructure and simplify management

Windows 10 OS updates

Windows 10 update rings in Microsoft Endpoint Manager provide ability to Configure update settings

- → Windows 10 Servicing Branch
- → Restart options
- → Defer installations of updates
- → Set deadlines for applying updates



Home > Microsoft Intune > Software updates - Windows 10 Update Rings > Default update ring example

Default update ring example

Windows 10 Update Ring

Created:
01/17/19, 10:24:07 AM

Last Modified:
01/17/19, 10:24:07 AM

Groups assigned:
1

Feature:
Running

Quality:
Running

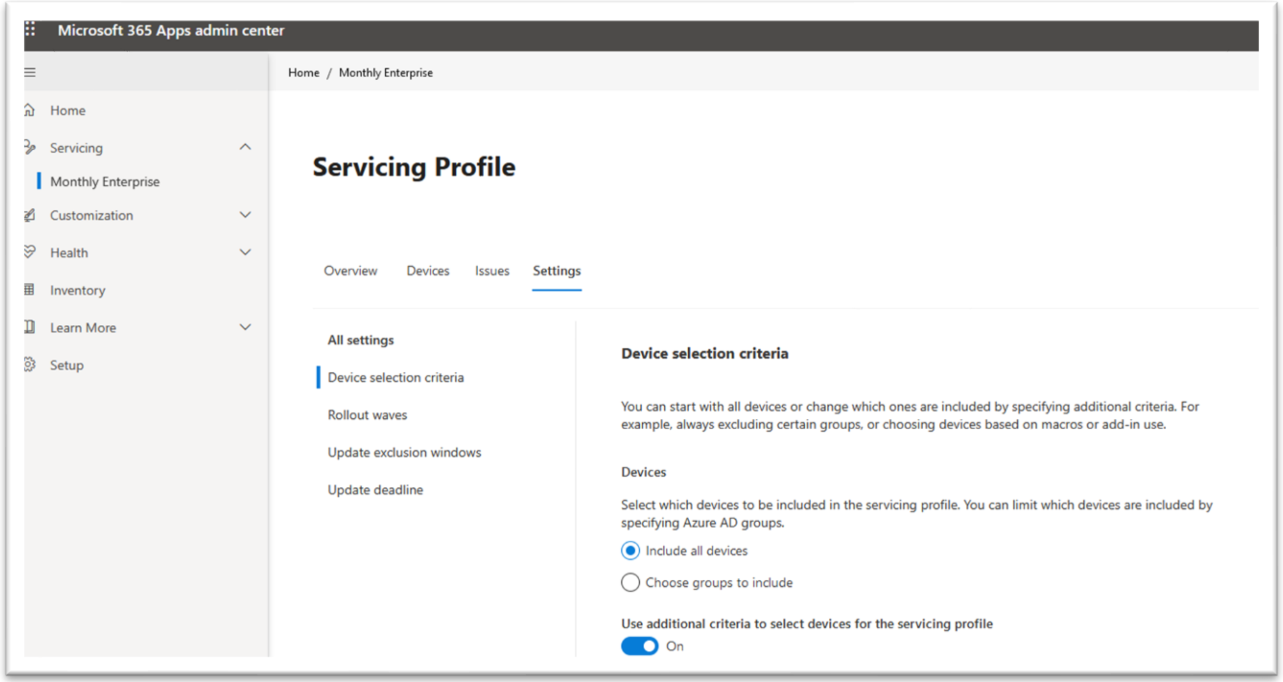
Profile assignment status — Windows 10 and later devices

Succeeded
0

Office 365 updates

Microsoft O365 Apps admin center

- → Manage updates to Office 365 apps using Servicing Profiles
- → On-board clients into Monthly Enterprise channel
- → Create ‘waves’ for deployment
- → Defer if needed
- → Rollback device groups



Servicing Profile

Device selection criteria

You can start with all devices or change which ones are included by specifying additional criteria. For example, always excluding certain groups, or choosing devices based on macros or add-in use.

Devices

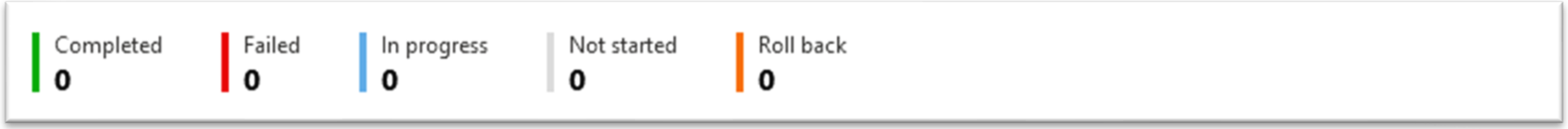
Select which devices to be included in the servicing profile. You can limit which devices are included by specifying Azure AD groups.

● Include all devices

○ Choose groups to include

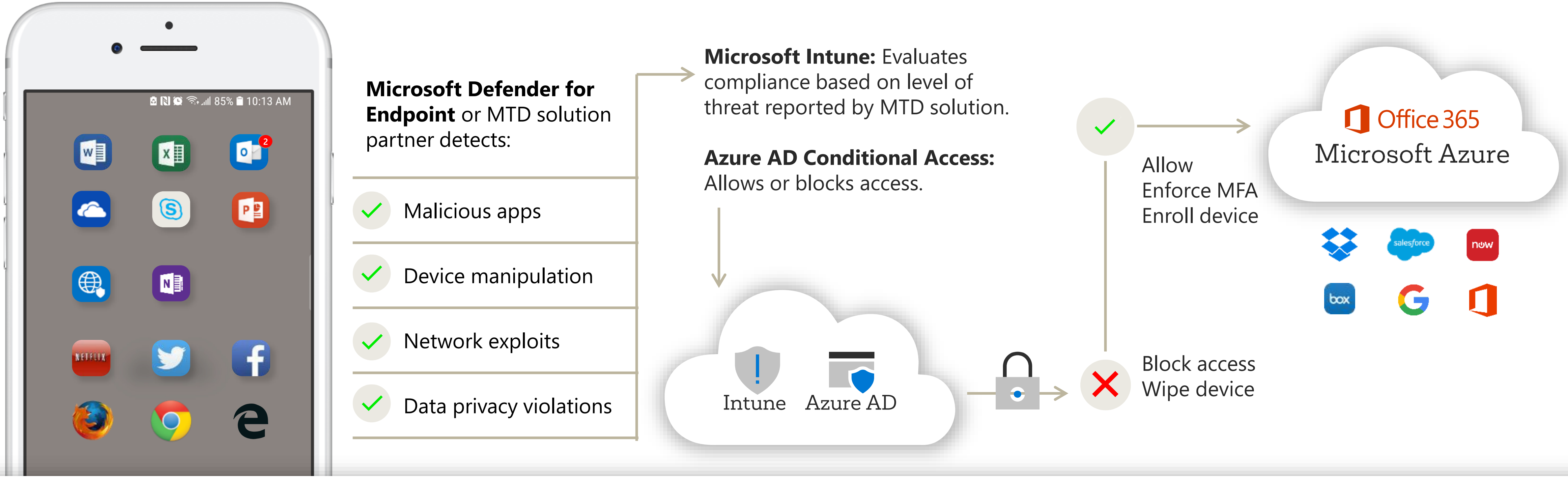
Use additional criteria to select devices for the servicing profile

On



Completed	Failed	In progress	Not started	Roll back
0	0	0	0	0

Mobile Threat Defense (MTD) for device risk-based conditional access



Microsoft Defender for Endpoint or MTD solution partner detects:

- ✓ Malicious apps
- ✓ Device manipulation
- ✓ Network exploits
- ✓ Data privacy violations

Microsoft Intune: Evaluates compliance based on level of threat reported by MTD solution.

Azure AD Conditional Access: Allows or blocks access.

✓ Allow
Enforce MFA
Enroll device

✗ Block access
Wipe device

Microsoft Defender for Endpoint

Mobile Threat Defense partners on iOS and Android

Microsoft

Lookout

Symantec.

ZIMPERIUM.

pradeo

Google Play
Protect

Check Point
SOFTWARE TECHNOLOGIES LTD

Microsoft Defender for Endpoint (Android)

Web Protection

Anti-phishing

Block unsafe network connections

Custom indicators: allow/block URLs

Malware Scan

Alerts for malware, PUA

Files scan

Storage and memory peripheral scans

Single Pane of Glass Reporting

Alerts for phishing

Alerts for malicious apps

Auto-connection for reporting in Microsoft Defender Security Center

Conditional Access

Block risky devices

Mark devices non-compliant

Supported Configurations

Device Administrator

Android Enterprise (Work Profile)

Licensed by Microsoft

Included in per user licenses that offer Microsoft Defender for Endpoint

Part of the 5 qualified devices for eligible licensed users

Reach out to your account team or CSP

Microsoft Defender for Endpoint (iOS)

Web Protection

Anti-phishing

Block unsafe network connections

Custom indicators: allow/block URLs

Single Pane of Glass Reporting

Alerts for phishing

Auto connection for reporting in Microsoft Defender Security Center

Supported Configurations

Supervised

Unsupervised

Licensed by Microsoft

Included in per user licenses that offer Microsoft Defender for Endpoint

Part of the 5 qualified devices for eligible licensed users

Reach out to your account team or CSP

Support and Retire

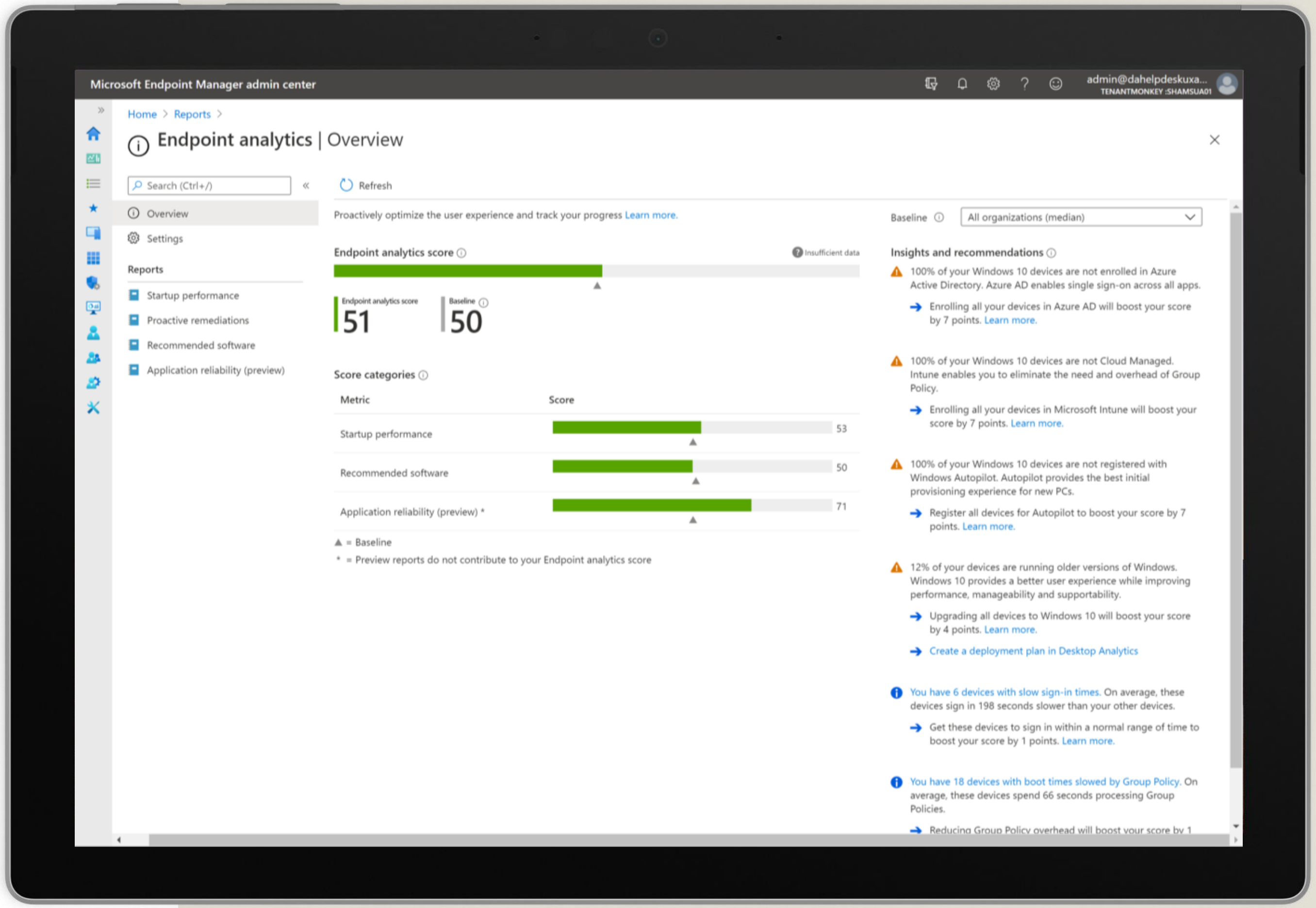
Endpoint analytics is an important part of the Microsoft Productivity Score

Address end-user pain points – including ones that go unreported

Proactively detect and remediate common support issues before end-users know there's a problem

Improve corporate access for remote users with recommended software

Identify and troubleshoot reliability issues with desktop applications (preview)



Endpoint analytics | Overview

Proactively optimize the user experience and track your progress Learn more.

Endpoint analytics score

Endpoint analytics score 51

Baseline 50

Score categories

Metric	Score
Startup performance	53
Recommended software	50
Application reliability (preview) *	71

▲ = Baseline

* = Preview reports do not contribute to your Endpoint analytics score

Insights and recommendations

⚠ 100% of your Windows 10 devices are not enrolled in Azure Active Directory. Azure AD enables single sign-on across all apps.

→ Enrolling all your devices in Azure AD will boost your score by 7 points. Learn more.

⚠ 100% of your Windows 10 devices are not Cloud Managed. Intune enables you to eliminate the need and overhead of Group Policy.

→ Enrolling all your devices in Microsoft Intune will boost your score by 7 points. Learn more.

⚠ 100% of your Windows 10 devices are not registered with Windows Autopilot. Autopilot provides the best initial provisioning experience for new PCs.

→ Register all devices for Autopilot to boost your score by 7 points. Learn more.

⚠ 12% of your devices are running older versions of Windows. Windows 10 provides a better user experience while improving performance, manageability and supportability.

→ Upgrading all devices to Windows 10 will boost your score by 4 points. Learn more.

→ Create a deployment plan in Desktop Analytics

ⓘ You have 6 devices with slow sign-in times. On average, these devices sign in 198 seconds slower than your other devices.

→ Get these devices to sign in within a normal range of time to boost your score by 1 points. Learn more.

ⓘ You have 18 devices with boot times slowed by Group Policy. On average, these devices spend 66 seconds processing Group Policies.

→ Reducing Group Policy overhead will boost your score by 1

Endpoint analytics requirements

Enroll devices via **Configuration Manager** with **Tenant Attach** feature or with **Intune**

Windows 10 devices must be **Azure AD joined** or **hybrid Azure AD joined**

Supported licenses

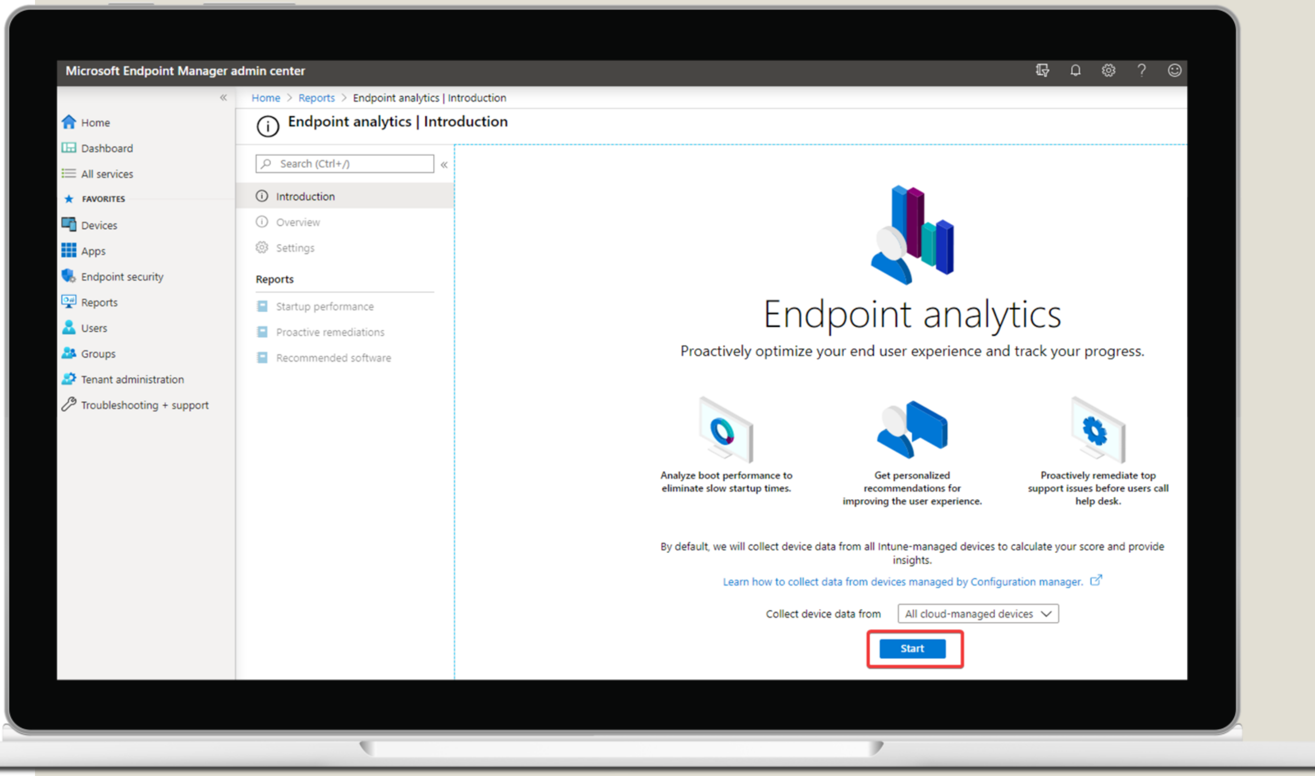
- Enterprise Mobility + Security E3 or higher
- Microsoft 365 Enterprise E3 or higher

Startup performance

Windows 1903 Enterprise/Education or higher

Proactive remediations also require one of the following licenses for the managed devices:

- Windows 10 Enterprise E3 or E5 (included in Microsoft 365 F3, E3, or E5)
- Windows 10 Education A3 or A5 (included in Microsoft 365 A3 or A5)
- Windows Virtual Desktop Access E3 or E5



Endpoint analytics | Introduction

Endpoint analytics

Proactively optimize your end user experience and track your progress.

Analyze boot performance to eliminate slow startup times.

Get personalized recommendations for improving the user experience.

Proactively remediate top support issues before users call help desk.

By default, we will collect device data from all Intune-managed devices to calculate your score and provide insights.

Learn how to collect data from devices managed by Configuration manager.

Collect device data from: All cloud-managed devices

Startup performance

Monitor your scores (0 to 100)

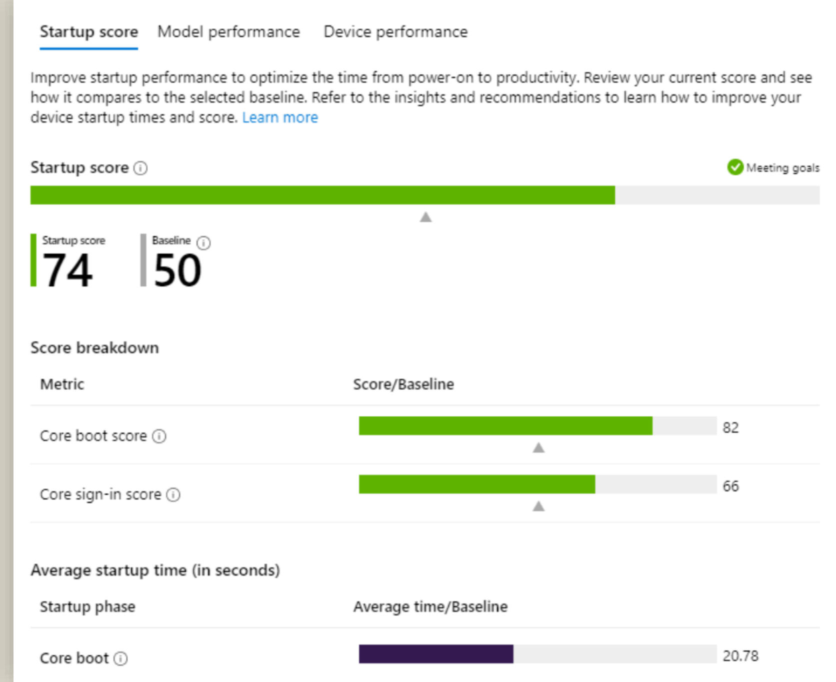
Boot score

Sign-In score

Check Insights and recommendations as

Slow boots and sign-in times

GPO impact during the startup



Improve startup performance to optimize the time from power-on to productivity. Review your current score and see how it compares to the selected baseline. Refer to the insights and recommendations to learn how to improve your device startup times and score. Learn more

Startup score ⓘ ✓ Meeting goals

Startup score 74

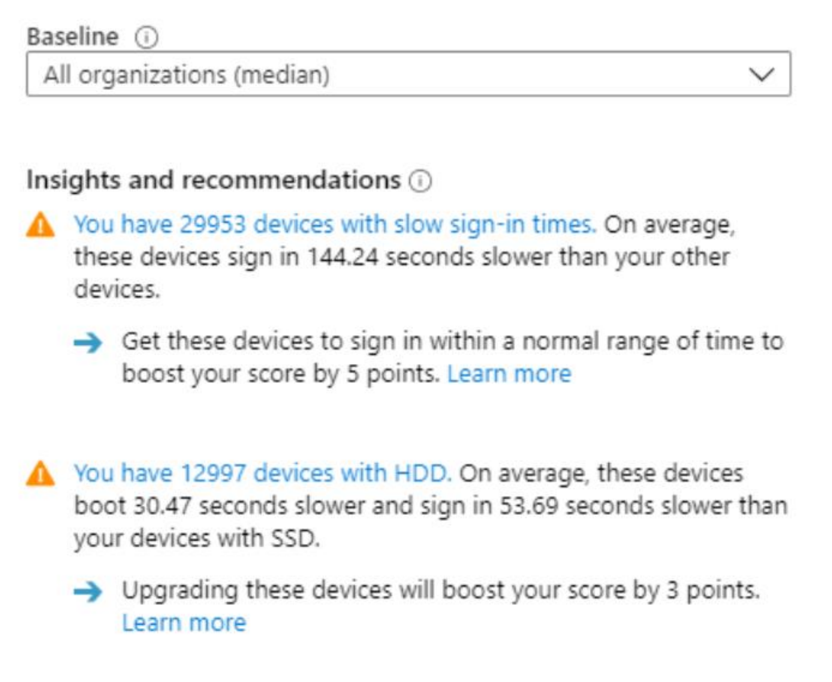
Baseline ⓘ 50

Score breakdown

Metric	Score/Baseline
Core boot score ⓘ	82
Core sign-in score ⓘ	66

Average startup time (in seconds)

Startup phase	Average time/Baseline
Core boot ⓘ	20.78



Baseline ⓘ

All organizations (median)

Insights and recommendations ⓘ

⚠ You have 29953 devices with slow sign-in times. On average, these devices sign in 144.24 seconds slower than your other devices.

→ Get these devices to sign in within a normal range of time to boost your score by 5 points. Learn more

⚠ You have 12997 devices with HDD. On average, these devices boot 30.47 seconds slower and sign in 53.69 seconds slower than your devices with SSD.

→ Upgrading these devices will boost your score by 3 points. Learn more

Proactive remediations

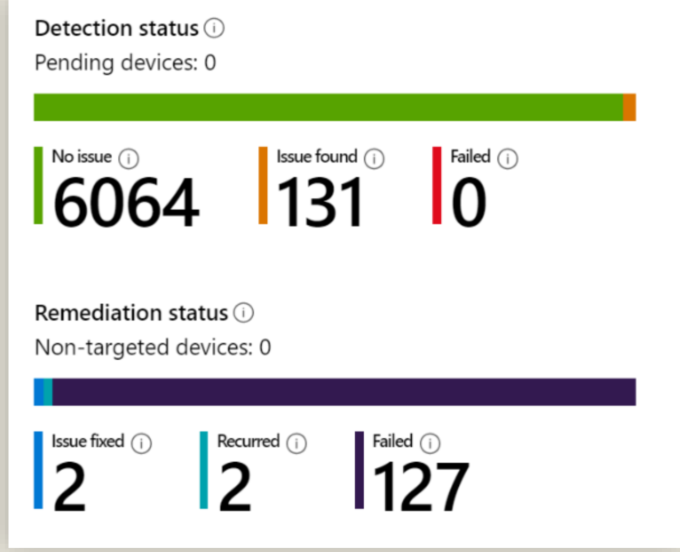
Proactive remediations are **script packages that can detect and fix common support issues** on a user's device before they even realize there's a problem

Two scripts, **one for detection and another one for remediation**

These remediations can help to **reduce support calls**

Check out remediation scripts ready to be used

https://docs.microsoft.com/en-us/mem/analytics/powershell-scripts



Detection status ⓘ

Pending devices: 0

No issue ⓘ 6064

Issue found ⓘ 131

Failed ⓘ 0

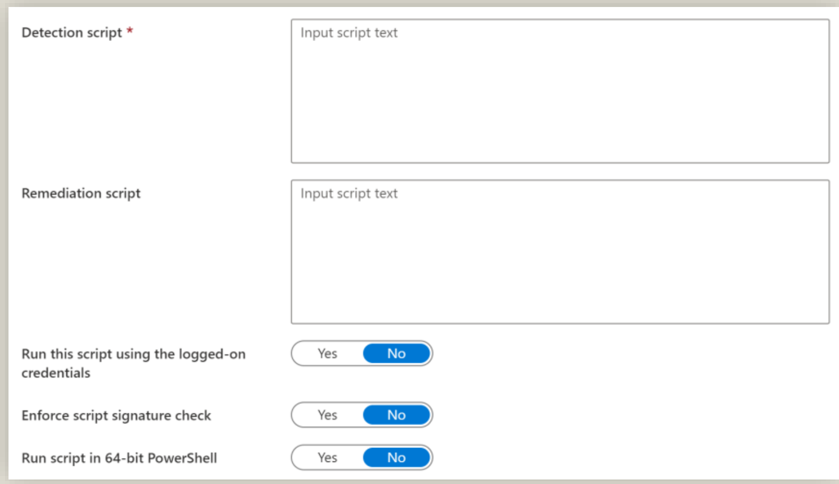
Remediation status ⓘ

Non-targeted devices: 0

Issue fixed ⓘ 2

Recurred ⓘ 2

Failed ⓘ 127



Detection script *

Input script text

Remediation script

Input script text

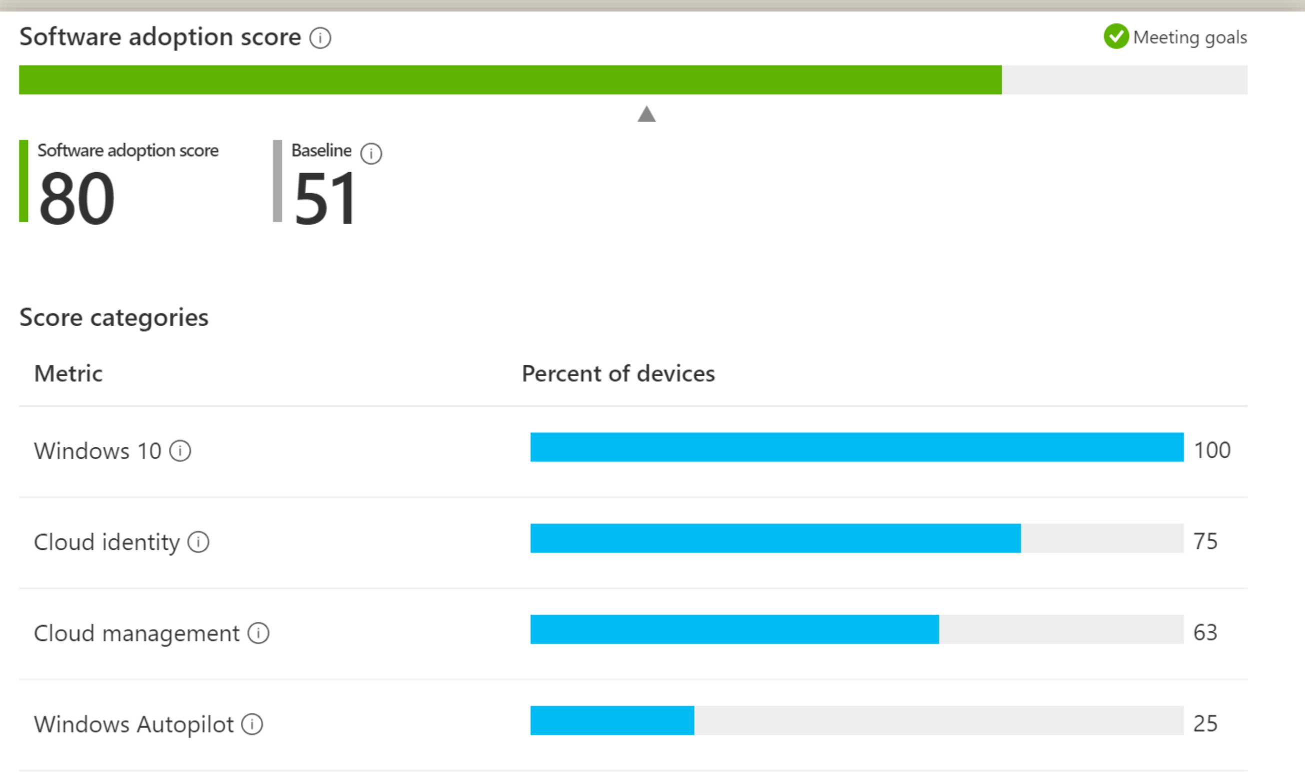
Run this script using the logged-on credentials: Yes [✓ No]

Enforce script signature check: Yes [✓ No]

Run script in 64-bit PowerShell: Yes [✓ No]

Recommended software

The **Software adoption score** represents a weighted average of the percent of devices that have deployed **various recommended software** like Windows 10 Deployment, Azure Identity, Autopilot Device or Device Enrolled in Intune



Software adoption score ⓘ

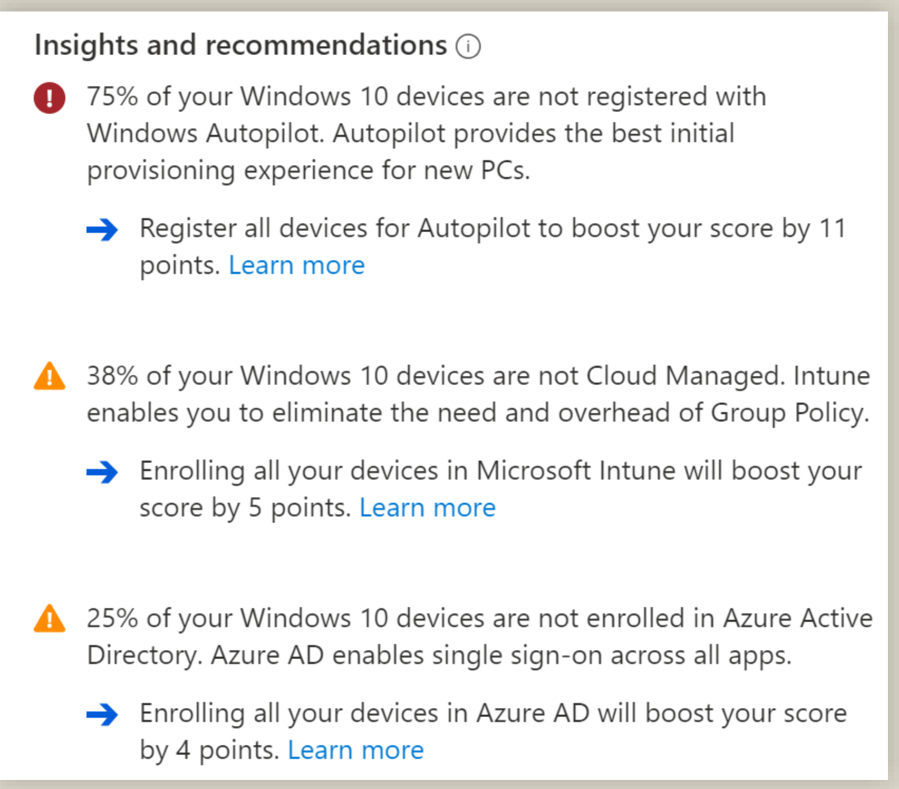
✓ Meeting goals

Software adoption score
80

Baseline ⓘ
51

Score categories

Metric	Percent of devices
Windows 10 ⓘ	100
Cloud identity ⓘ	75
Cloud management ⓘ	63
Windows Autopilot ⓘ	25



Insights and recommendations ⓘ

! 75% of your Windows 10 devices are not registered with Windows Autopilot. Autopilot provides the best initial provisioning experience for new PCs.

→ Register all devices for Autopilot to boost your score by 11 points. Learn more

⚠ 38% of your Windows 10 devices are not Cloud Managed. Intune enables you to eliminate the need and overhead of Group Policy.

→ Enrolling all your devices in Microsoft Intune will boost your score by 5 points. Learn more

⚠ 25% of your Windows 10 devices are not enrolled in Azure Active Directory. Azure AD enables single sign-on across all apps.

→ Enrolling all your devices in Azure AD will boost your score by 4 points. Learn more

Wipe vs Retire

Wipe	Retire
Restore the device to its factory defaults	Removes managed app data, settings, and email profiles that were assigned by using Intune but leaves the user's personal data on the device
Removes all company and user data and settings	Removes the device from Intune management **next time when the device checks in**
Can be performed on Windows, iOS/iPadOS and Android devices	Use the **Delete** action instead if you want **to remove the device immediately**

Common scenarios	Suggested action
Lost device	**Remote lock** whilst looking for device, **Wipe** if the device cannot be found
Stolen device	Wipe
Retire device	Wipe
Forgotten passcode	Passcode reset
User leaving company, personal device enrolled to Intune	Retire

Retire impact across supported platforms

Content type	Windows 10	iOS/iPadOS	macOS	Android DA	Samsung KNOX	Android Enterprise
Company Apps/Data installed by Microsoft Intune	Apps are uninstalled and sideloading keys are removed	Apps uninstalled Company app data removed App data from MS apps that use mobile app management is removed The app is not removed	Not supported	Apps and data remain installed App data from mobile app management apps is removed The app is not removed	Apps uninstalled App data from mobile app management apps is removed The app is not removed	Apps uninstalled. Company app data removed App data from MS apps that use mobile app management is removed
Settings	Configurations that were set by Intune policy are no longer enforced Users can change the settings	Configurations that were set by Intune policy are no longer enforced Users can change the settings	Configurations that were set by Intune policy are no longer enforced Users can change the settings	Configurations that were set by Intune policy are no longer enforced Users can change the settings	Configurations that were set by Intune policy are no longer enforced Users can change the settings	Configurations that were set by Intune policy are no longer enforced Users can change the settings
Wi-Fi & VPN profiles	Removed	Removed	Removed	Removed	Removed	Removed

Kocho

BECOME GREATER

Thank you

→ Any questions?

About Kocho

Kocho
BECOME GREATER

At Kocho, we believe greatness lies in everyone. That's why we exist, to help ambitious companies realise their potential.

By combining the power of Microsoft cloud technology with world-class identity, cyber security and our team of talented people, we take our clients on a journey of secure cloud transformation.

And we're with you every step of the way. Because the path to greatness isn't walked alone. We help you adopt and embrace the right technology solutions at the right time.

The result? Sustainable and secure growth that amplifies your business success.

Kocho. Become Greater.

Award-winning solutions

Eight-time winner of the Microsoft Partner of the Year Award for Identity Management, Enterprise Mobility, and Security and Compliance.

Microsoft Partner
Microsoft

- Gold Security
- Gold Datacenter
- Gold Cloud Platform
- Gold Cloud Productivity
- Gold Application Developer
- Gold Windows and Devices
- Gold Enterprise Mobility Management
- Gold Small and Midmarket Cloud Solutions

hello@kocho.co.uk

0800 044 5009