Introduction to Modern Device Management

May 2025

@directorcia

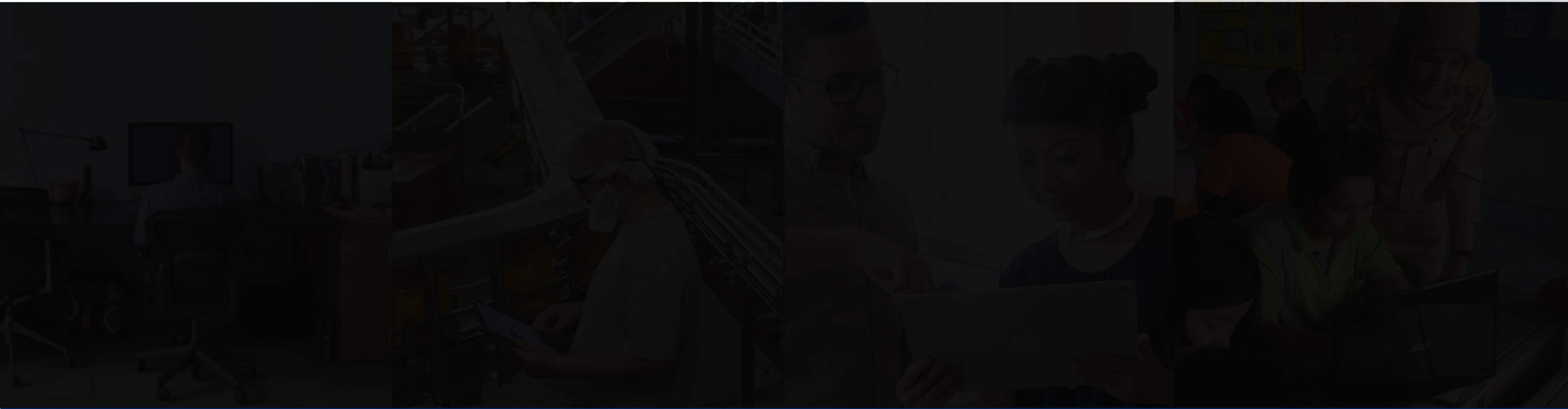
http://about.me/ciaops

Why manage devices?

- PCs no longer dominate
- Devices provide access to corporate information
- Devices do not generally remain in one location
- Devices typically contain personal and corporate data
- Device are now being targeted by attackers (aka Flubot)
- Device are at more risk (stolen, unauthorised access, shared, etc)

M365 Flexible Device Management for all Organizations & Users

Enterprise		Small Business	School
Knowledge Workers	Firstline Workers	SMB Employee	Teachers / Students
Productive on company-owned and personal devices	Productive on shared/Kiosk devices	Productive personal devices Simplified admin experience in	Productive on lab or school devices Grouped based on classes/labs/carts Customized console, policies for EDU
Intune and ConfigManager in Microsoft 365 Enterprise	Intune in Microsoft 365 F1	Microsoft 365 Business powered by Intune	Intune for Education in Microsoft 365 Education



Cloud powered endpoint management

Config Mgr Attached

OR

Cloud Only

Risk-based Control

Endpoint Compliance and Risk

Conditional Access

App Protection Policy

Third party risk and compliance signaling

Zero Touch Provisioning

Windows Autopilot

Android Enterprise ZTD

Apple DEP

Samsung Knox Mobile Enrollment

Intelligent Security

Secure Score

Advanced Threat Protection

BitLocker management

Security Baselines

Windows Hello, Attestation

Advanced Analytics

Technology Experience Score

Desktop Analytics

Log Analytics

Real time advanced threat detection

Dynamic user risk assessment

Unified Management

Mobility and PC Management

M365 Admin Center

Guided Deployments

Office 365 Pro Plus

Edge

Full stack integration

Role Based Admin

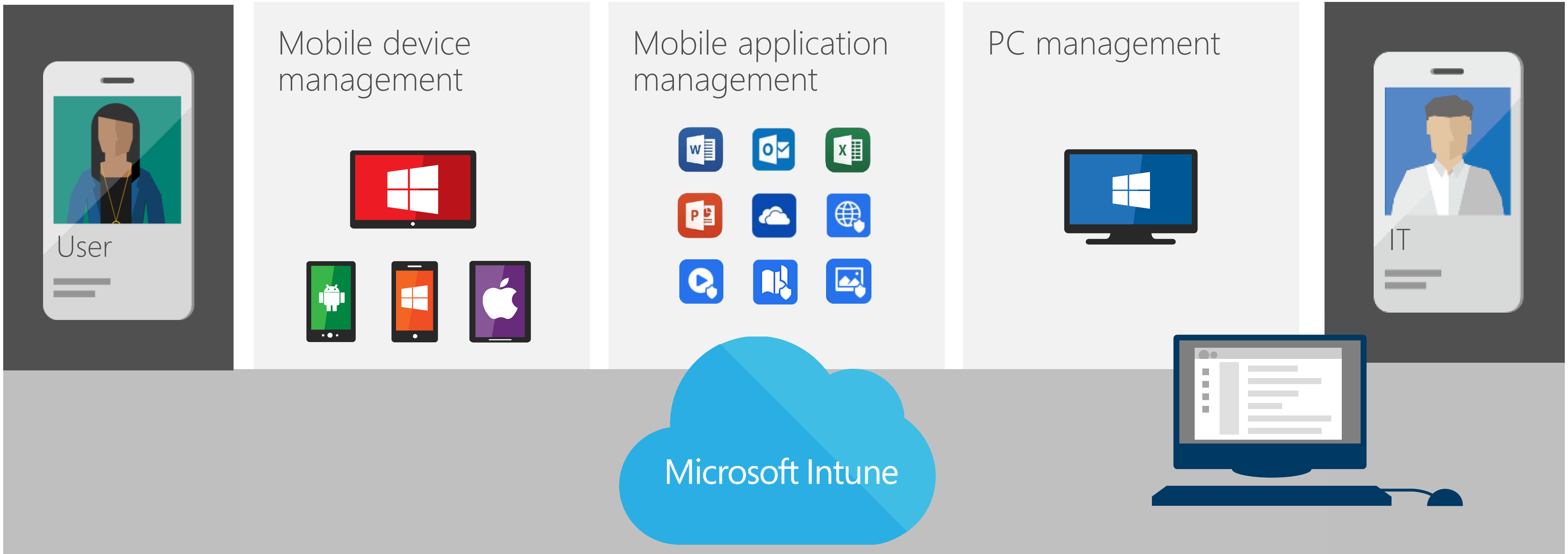
Graph API

PowerShell

Audit

Cloud content optimization

Enterprise mobility management with Intune



User

Mobile device management

Mobile application management

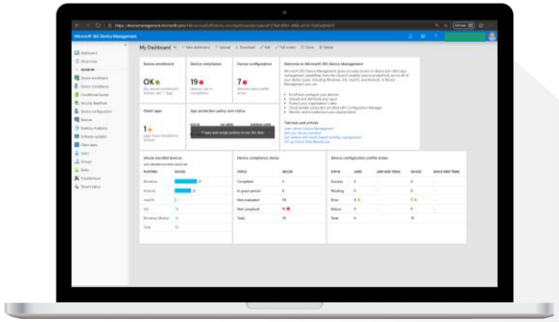
PC management

IT

Microsoft Intune

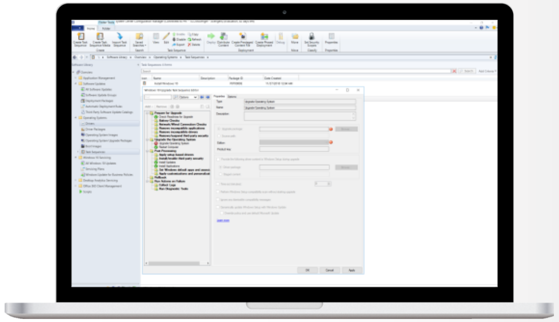
Intune helps organizations provide their employees with access to corporate applications, data, and resources from virtually anywhere on almost any device, while helping to keep corporate information secure.

Microsoft Intune



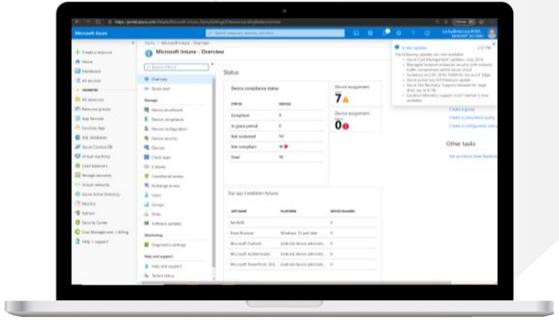
Cloud infrastructure
Mobility Management
PC management
Security Admin

Configuration Manager



Intelligent edge for cloud infra
On premises infrastructure
PC Management

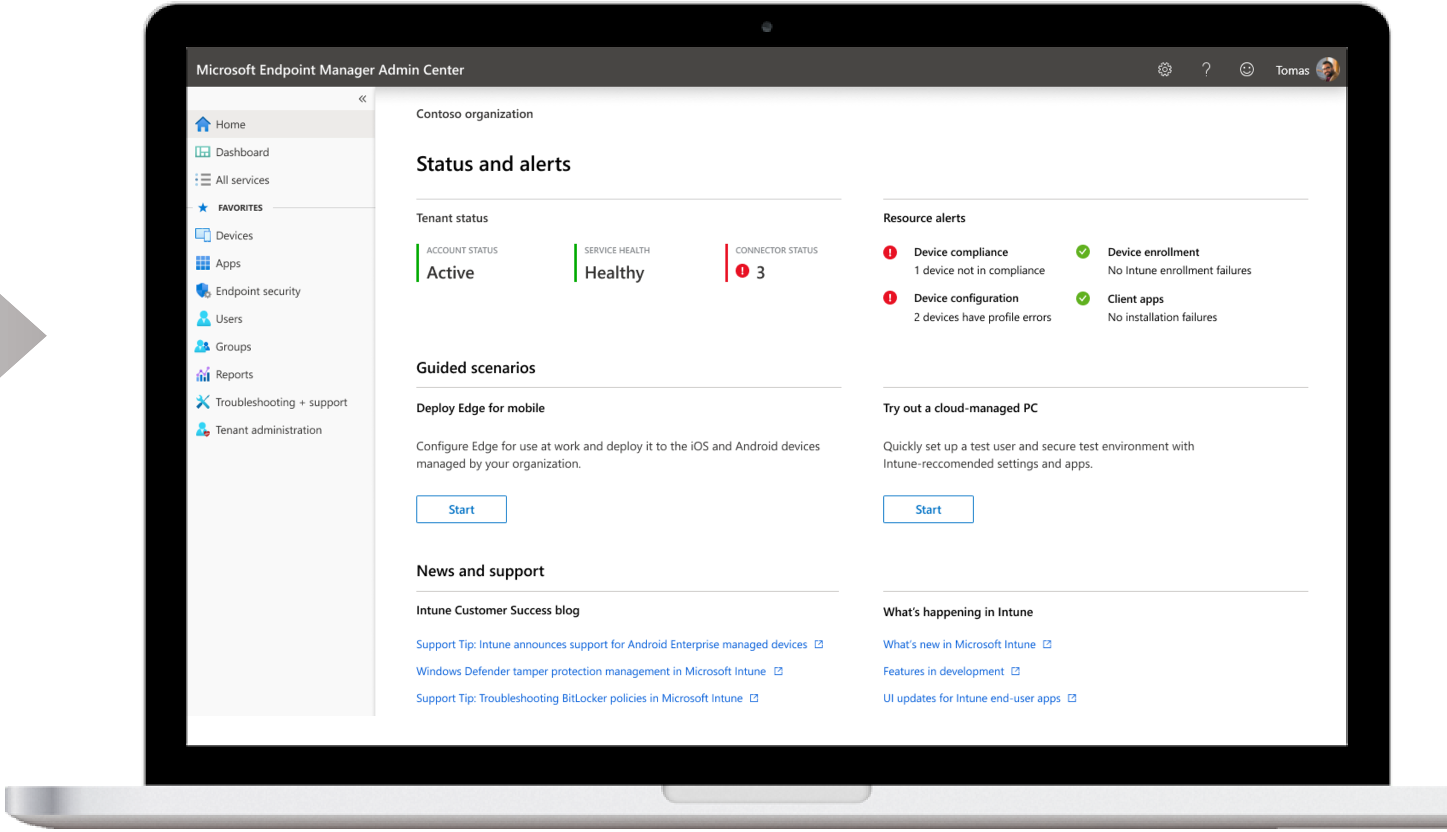
Other Endpoint Management Tools



Desktop Analytics
Autopilot
and more

Integrated solution for IT admins to understand and take action across all endpoints in their estate

Microsoft Endpoint Manager



Microsoft Endpoint Manager Admin Center

Tomas

- Home
- Dashboard
- All services
- FAVORITES
- Devices
- Apps
- Endpoint security
- Users
- Groups
- Reports
- Troubleshooting + support
- Tenant administration

Contoso organization

Status and alerts

Tenant status

ACCOUNT STATUS	SERVICE HEALTH	CONNECTOR STATUS
Active	Healthy	3

Resource alerts

Device compliance
1 device not in compliance

Device enrollment
No Intune enrollment failures

Device configuration
2 devices have profile errors

Client apps
No installation failures

Guided scenarios

Deploy Edge for mobile

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

Start

Try out a cloud-managed PC

Quickly set up a test user and secure test environment with Intune-reccomended settings and apps.

Start

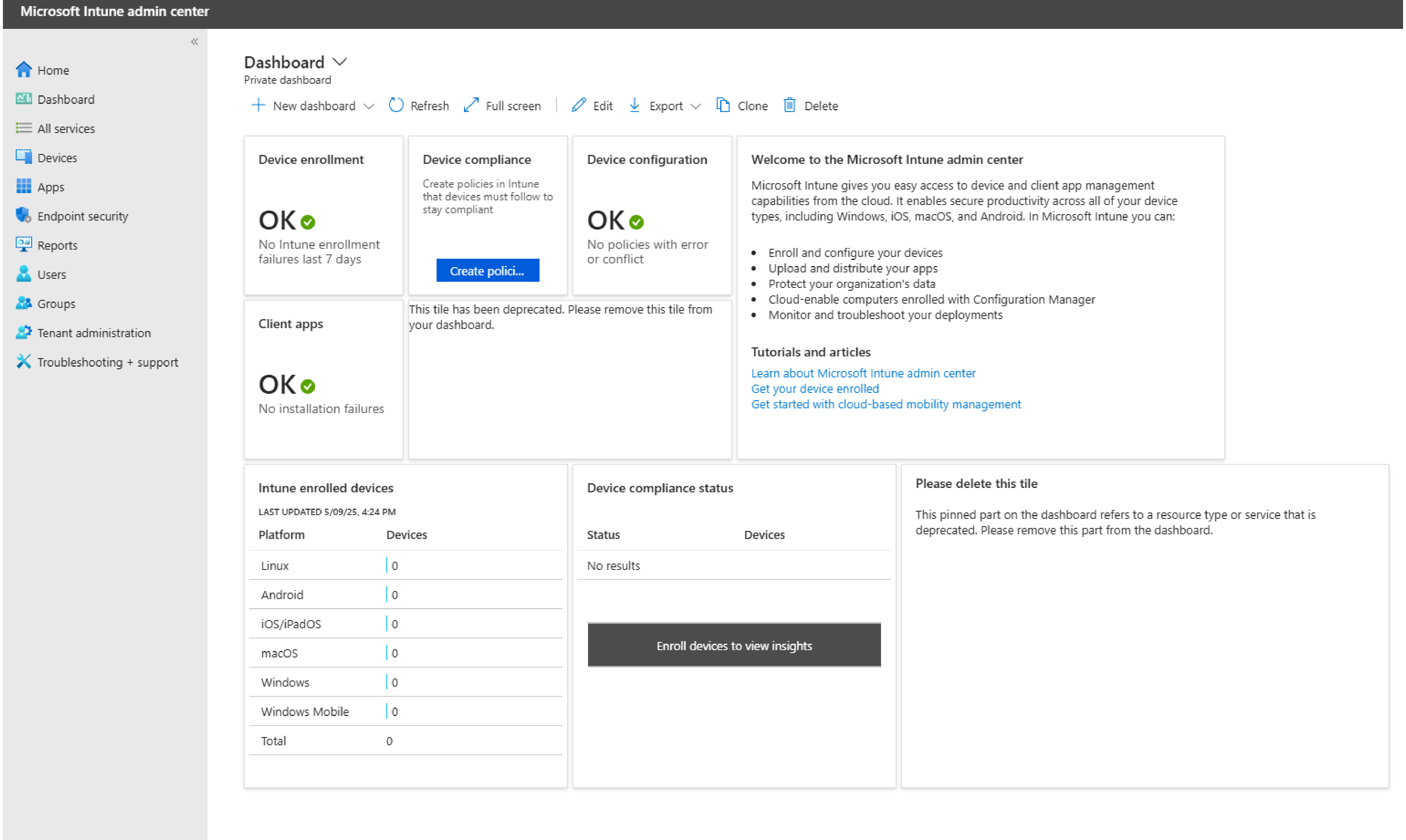
News and support

Intune Customer Success blog

- Support Tip: Intune announces support for Android Enterprise managed devices
- Windows Defender tamper protection management in Microsoft Intune
- Support Tip: Troubleshooting BitLocker policies in Microsoft Intune

What's happening in Intune

- What's new in Microsoft Intune
- Features in development
- UI updates for Intune end-user apps



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

Device configuration

OK ✓

No policies with error or conflict

Welcome to the Microsoft Intune admin center

Microsoft Intune 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 Intune 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 Intune admin center

Get your device enrolled

Get started with cloud-based mobility management

Client apps

OK ✓

No installation failures

This tile has been deprecated. Please remove this tile from your dashboard.

Intune enrolled devices

LAST UPDATED 5/09/25, 4:24 PM

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

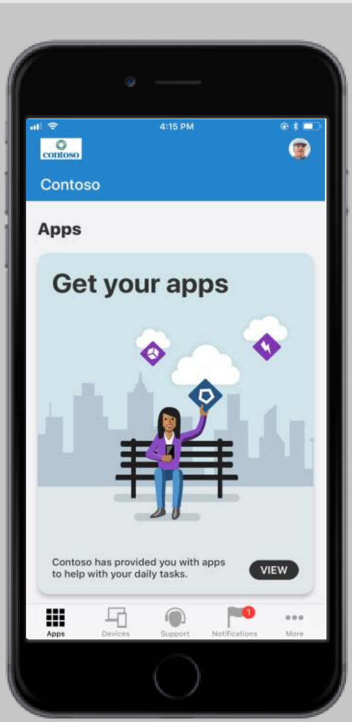
Device compliance status

Status	Devices
No results	

Please delete this tile

This pinned part on the dashboard refers to a resource type or service that is deprecated. Please remove this part from the dashboard.

iOS deployment scenarios

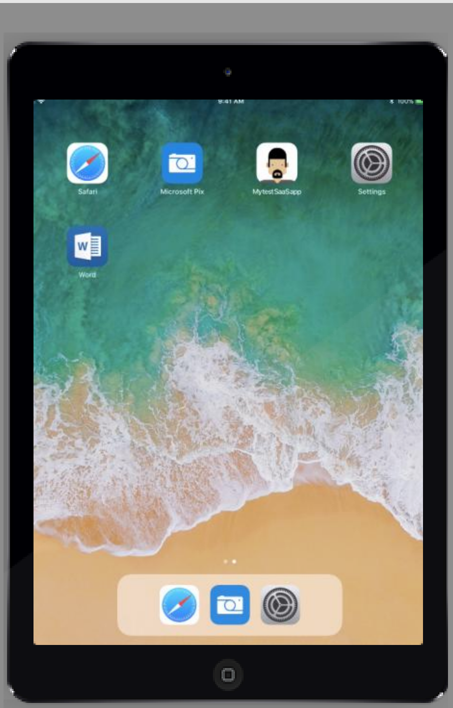


Get your apps

Contoso has provided you with apps to help with your daily tasks.

VIEW

BYOD



CORP OWNED

iOS app managed

- Data protection at the app level
- App protection without full device management

iOS device managed

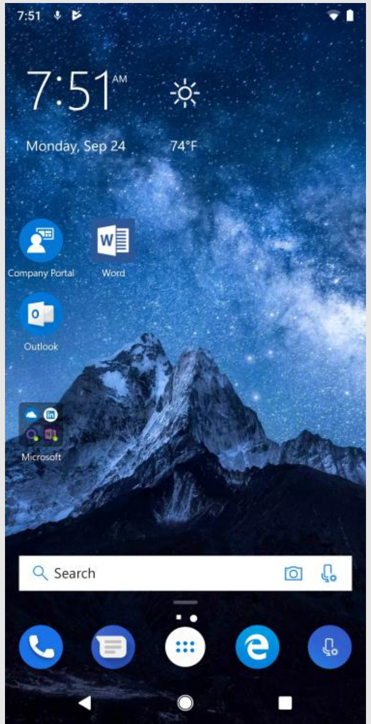
- User-based enrollment via Company Portal
- Push Apps and policies
- Device based Compliance

- Apple Corporate programs like VPP, DEP, ASM
- Supervised mode with for controls
- Secure locked down devices: Kiosk, Classroom
- Lock management profile to a device

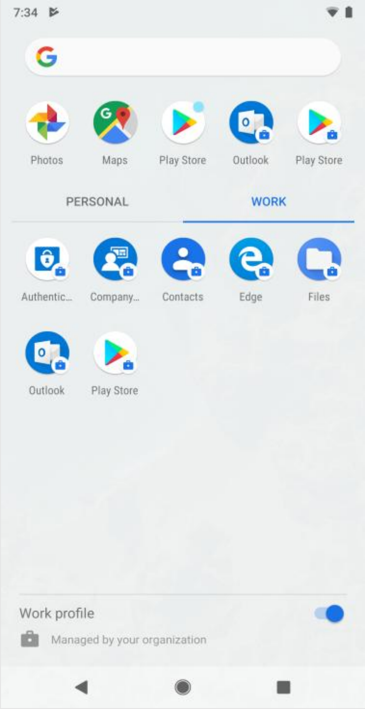
Android deployment scenarios

BYOD

Intune App Protection Without Enrollment

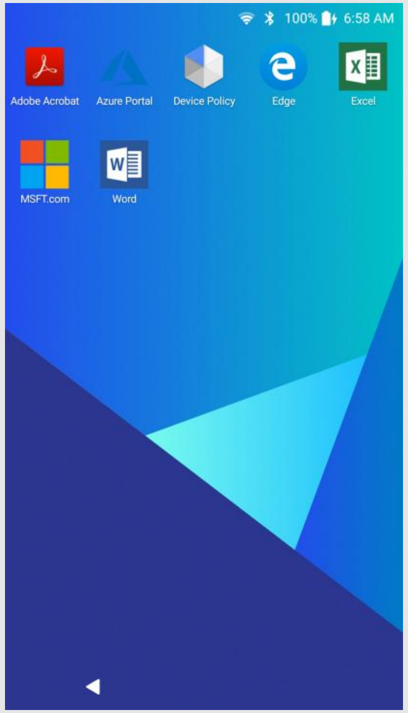


AE Work Profile

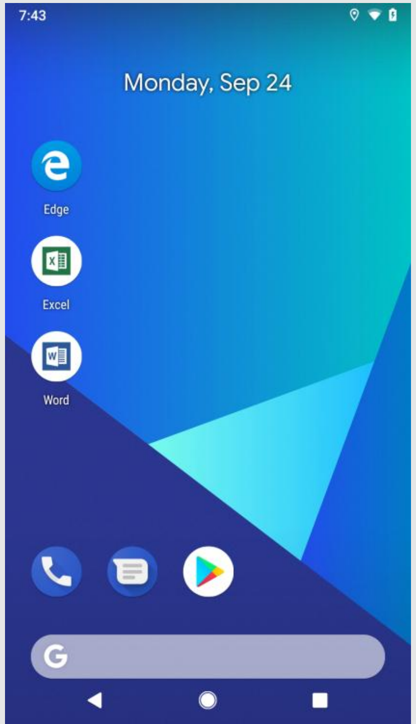


Corp Owned

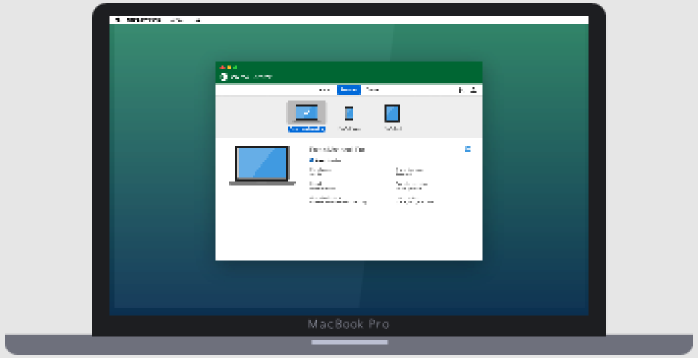
AE Dedicated (kiosk)



AE Fully managed



macOS deployment scenarios



Intune managed

Basic platform MDM management. Ideal for:

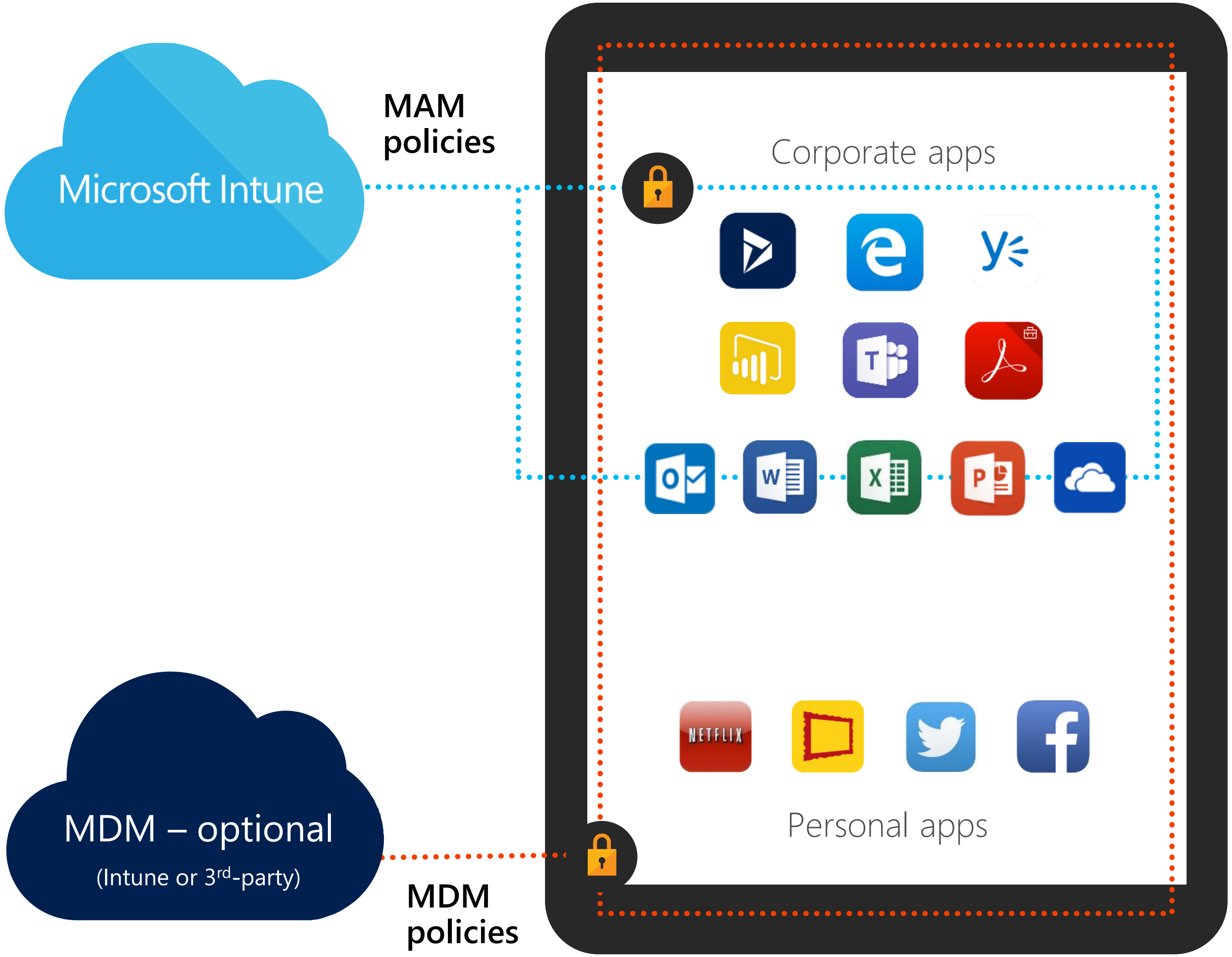
- Scoped/modern management needs for corp owned devices
- Deploying certs, pw configuration, apps
- Limiting access to compliant Macs
- Protection with device wipe, encryption

Jamf managed, Intune compliant

Advanced MDM management. Ideal for:

- Extensive inventory
- Depth of security controls
- Self Service app catalog & End user controls
- Limiting access to compliant Macs
- Scripting

Introduction to Intune App Protection Policies (APP)



Familiar Office experience

- Seamless “enrollment” into app management
- Use for personal and corporate accounts

Comprehensive protection

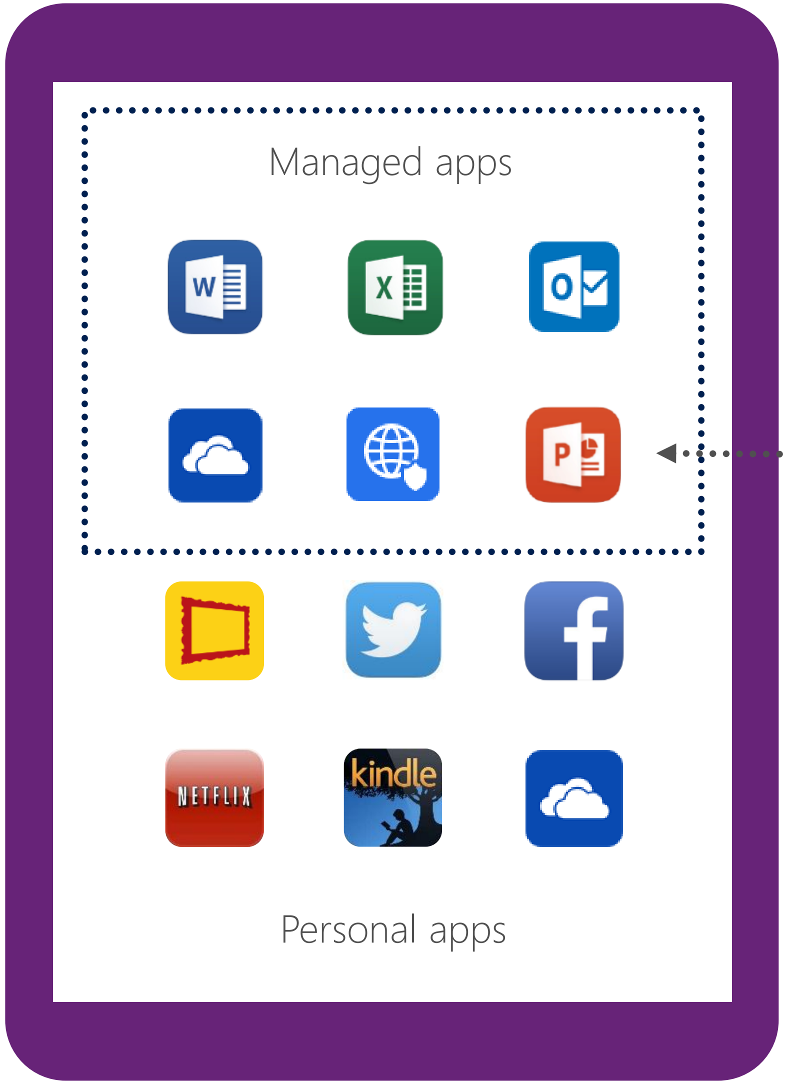
- App encryption at rest
- App access control – PIN or credentials
- Save as/copy/paste restrictions
- App-level selective wipe

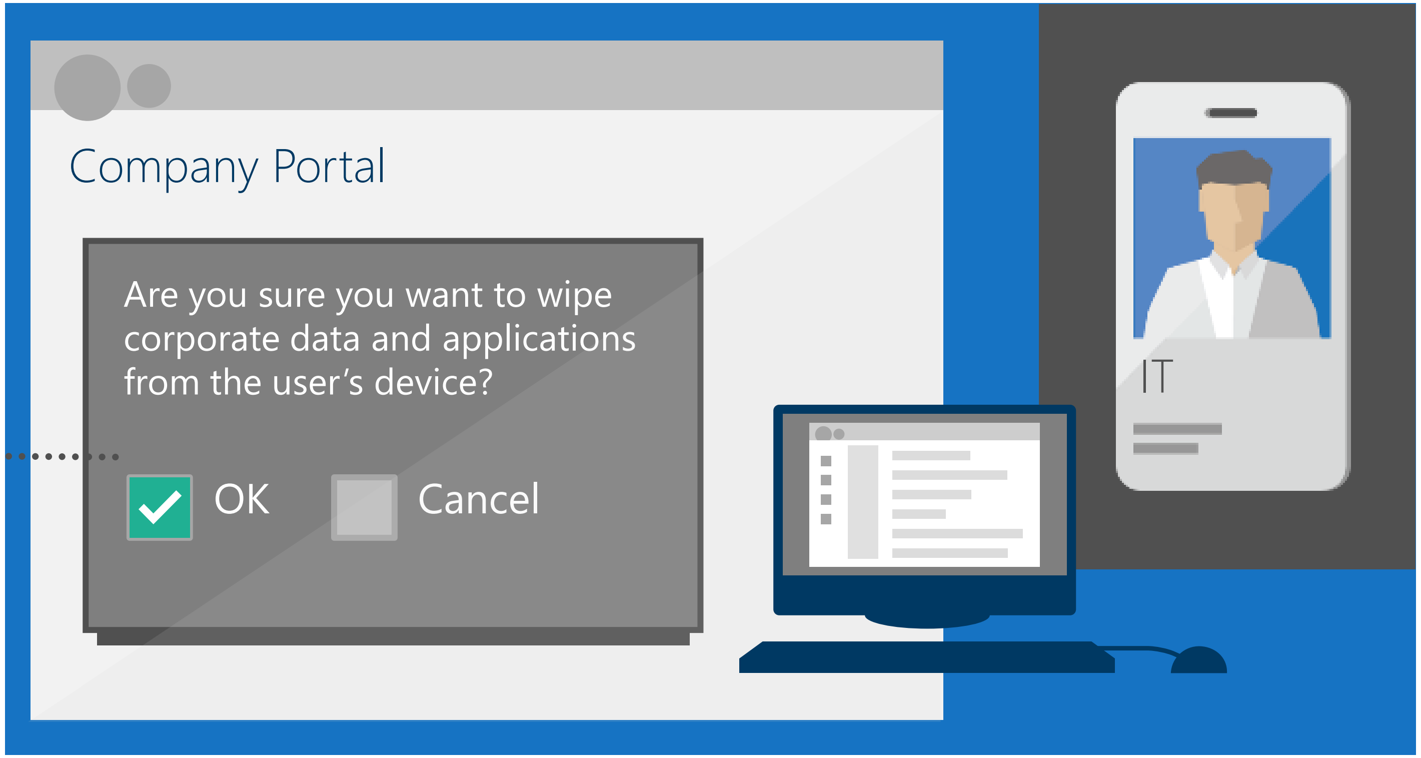
MDM mgmt. by Intune or third-party is optional

Might be a good solution for these scenarios:

- BYOD when MDM is not required
- Extending app access to vendors and partners
- Already have an existing MDM solution

Selective wipe



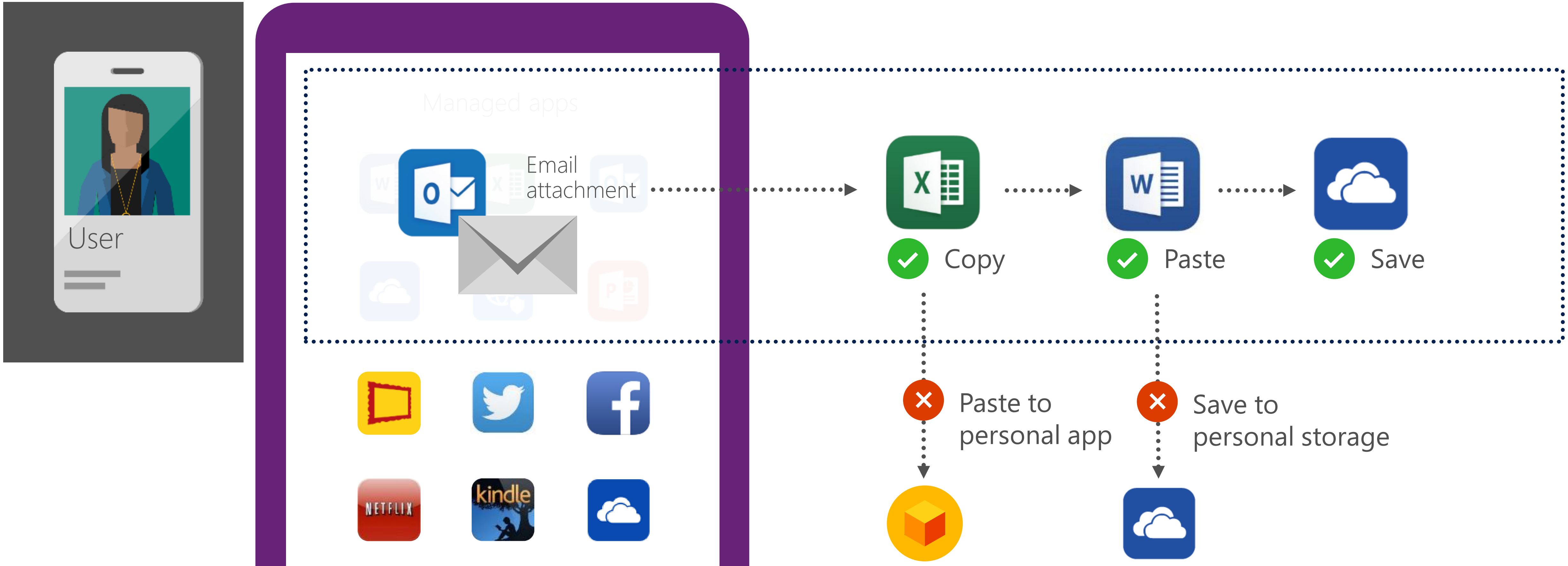

Company Portal

Are you sure you want to wipe corporate data and applications from the user's device?

☑ OK □ Cancel

- Perform selective wipe via self-service company portal or admin console
- Remove managed apps and data
- Keep personal apps and data intact

Mobile application management



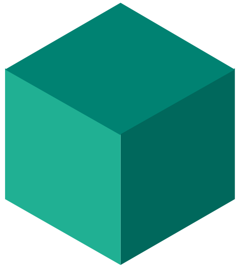
Maximize productivity while preventing leakage of company data by restricting actions such as copy/cut/paste/save in your managed app ecosystem

Mobile application management policies

Enforce corporate data access requirements

Prevent data leakage on the device

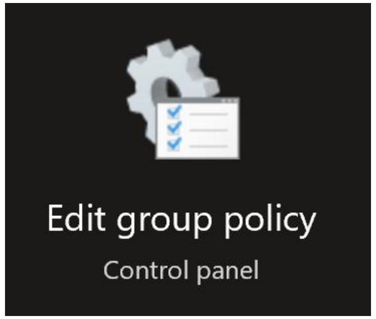
Enforce encryption of app data at rest



App-level selective wipe

Ways to get policies on Windows devices

Local Security Policy
App


Edit group policy
Control panel

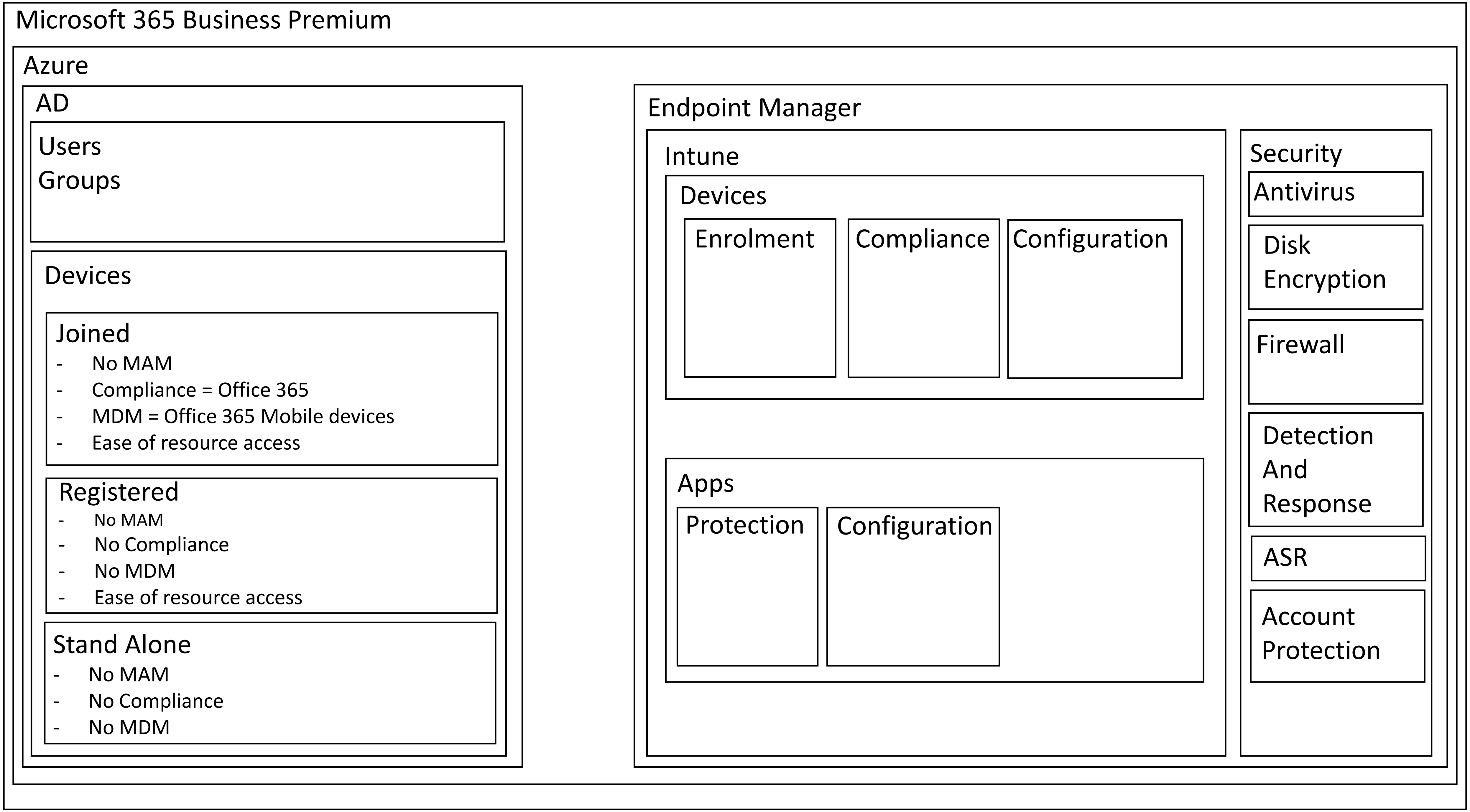
Microsoft® System Center Configuration Manager

Endpoint Manager

Intune

Endpoint Security

Defender for Endpoint



Microsoft 365 Business Premium

Azure

AD

Users
Groups

Devices

Joined

- No MAM
- Compliance = Office 365
- MDM = Office 365 Mobile devices
- Ease of resource access

Registered

- No MAM
- No Compliance
- No MDM
- Ease of resource access

Stand Alone

- No MAM
- No Compliance
- No MDM

Endpoint Manager

Intune

Devices

Enrolment

Compliance

Configuration

Apps

Protection

Configuration

Security

Antivirus

Disk Encryption

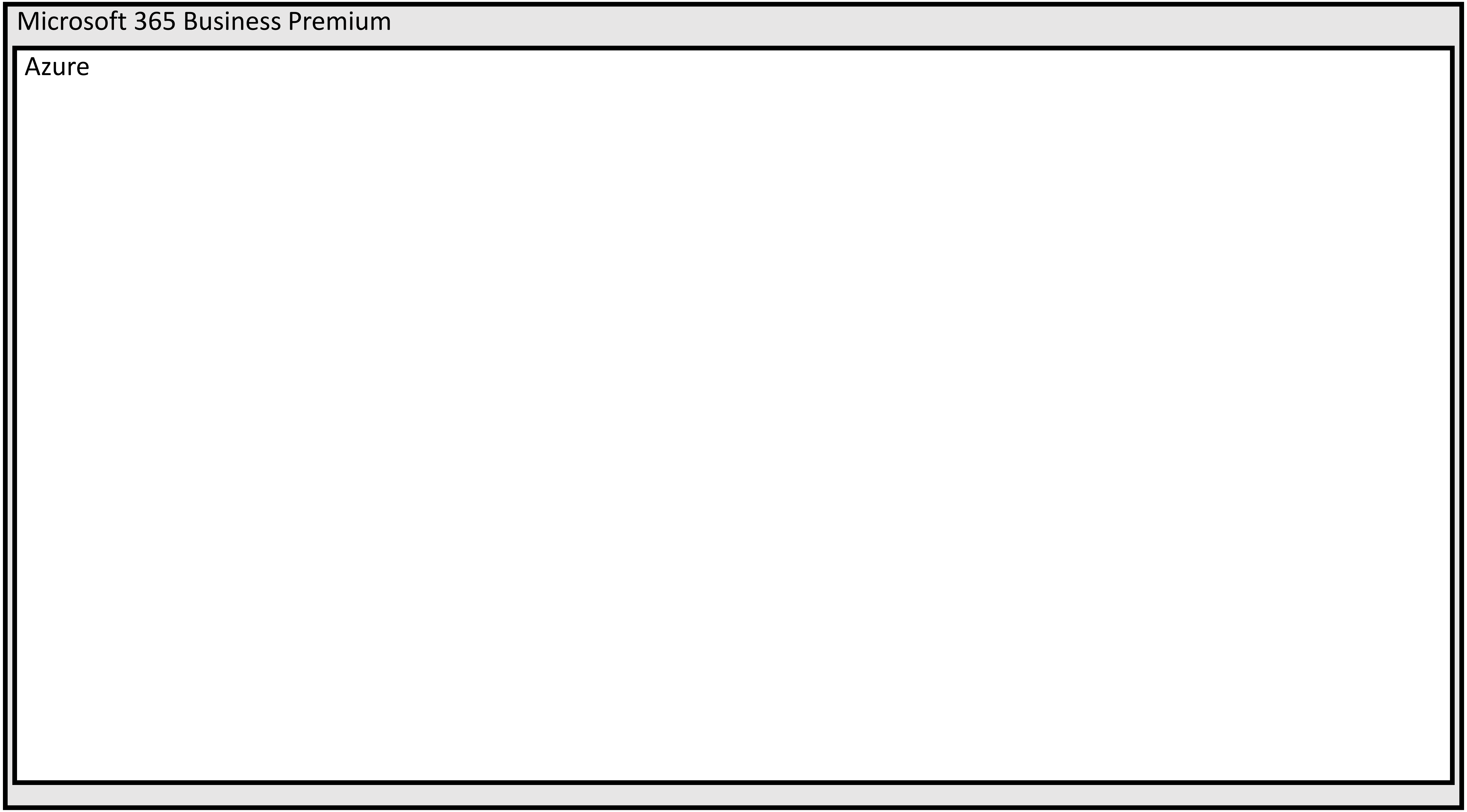
Firewall

Detection And Response

ASR

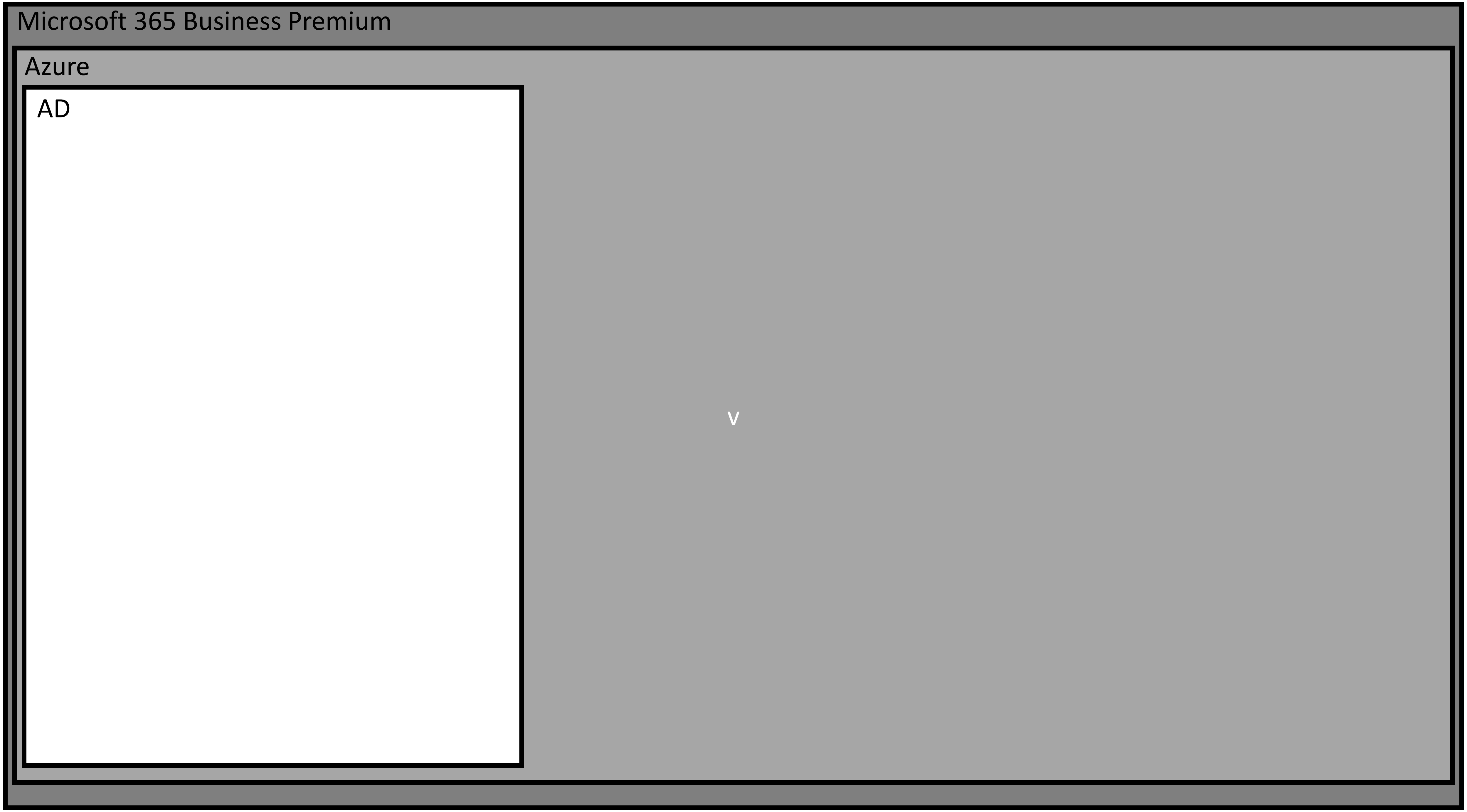
Account Protection

Microsoft 365 Business Premium



Microsoft 365 Business Premium

Azure

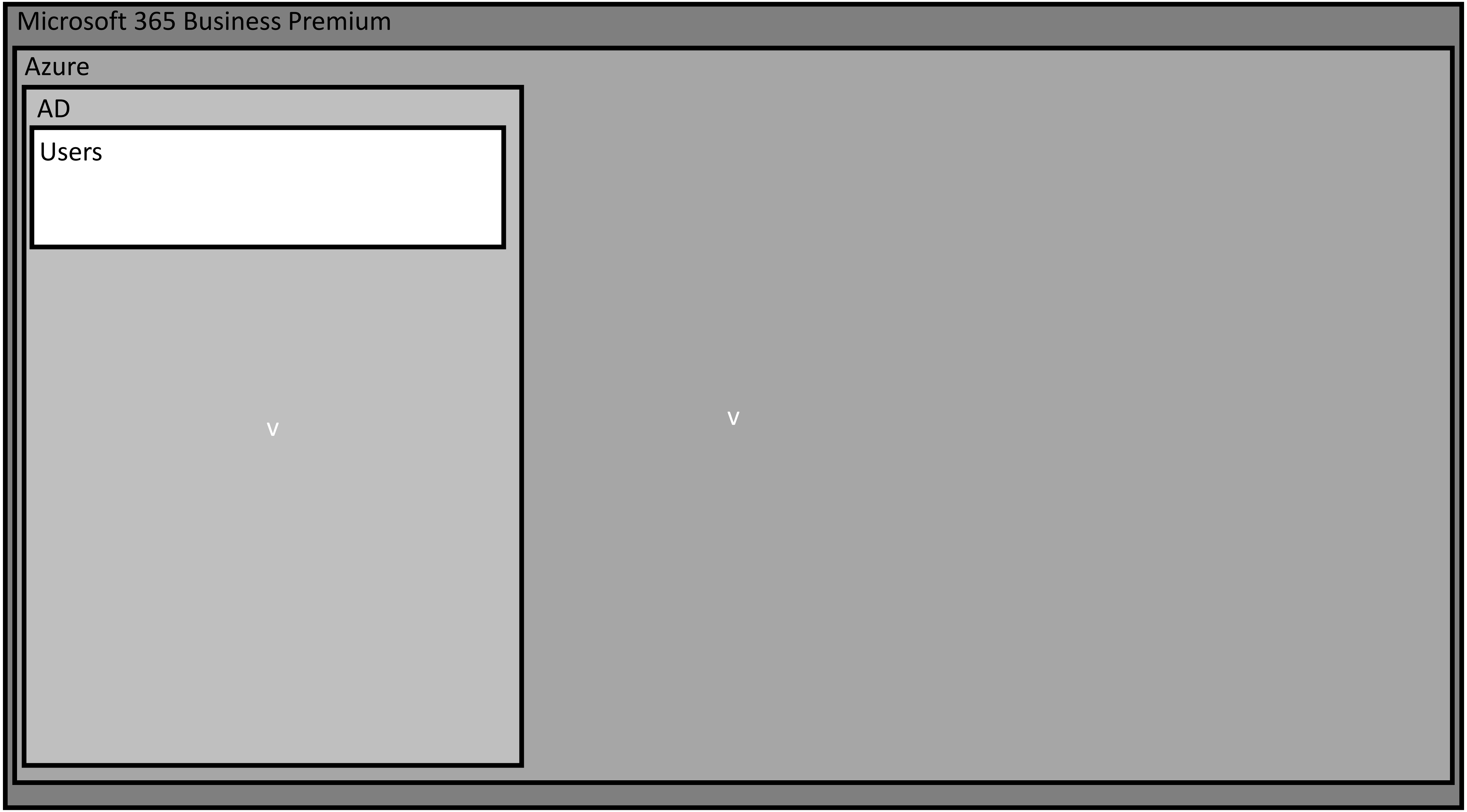


Microsoft 365 Business Premium

Azure

AD

v



Microsoft 365 Business Premium

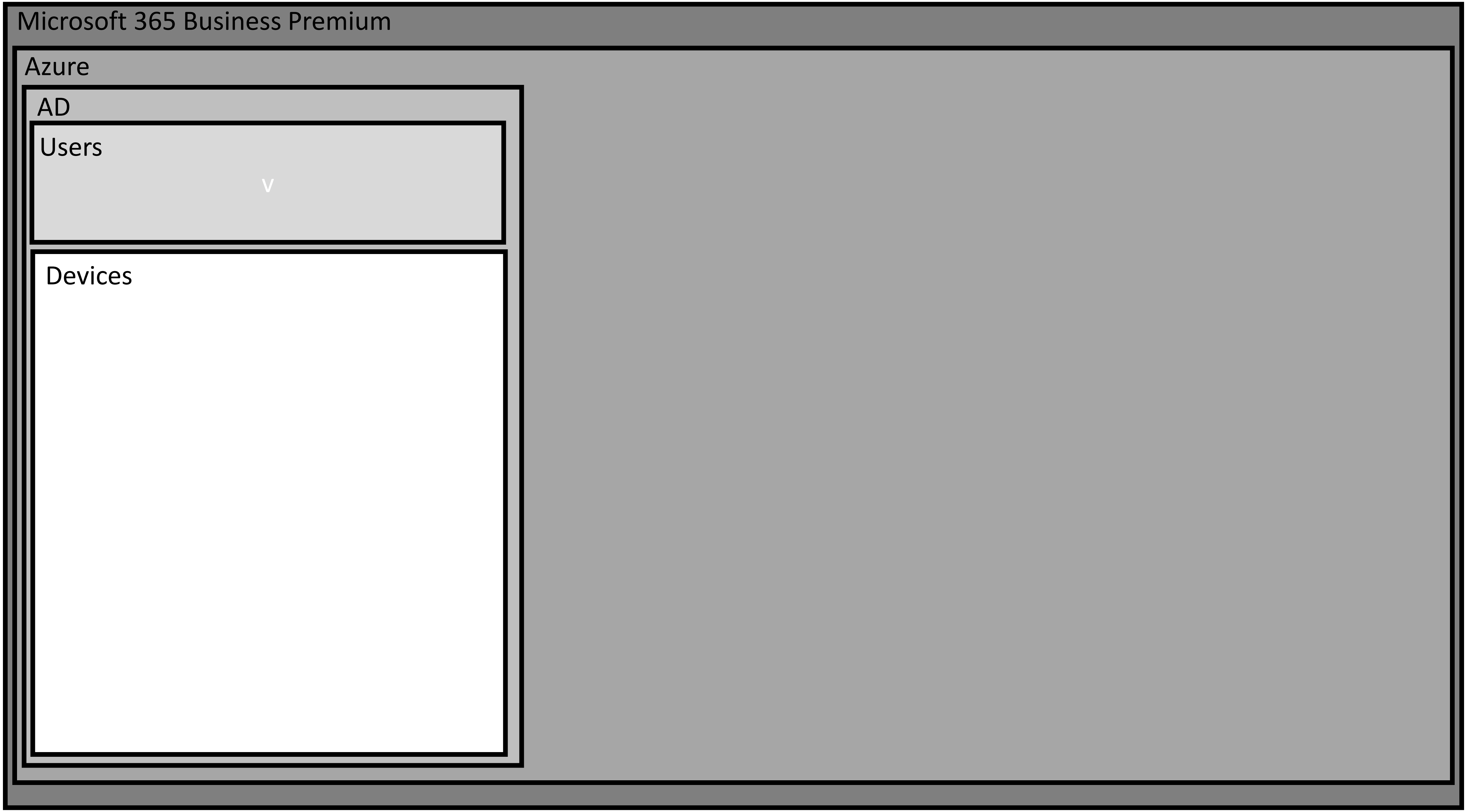
Azure

AD

Users

v

v



Microsoft 365 Business Premium

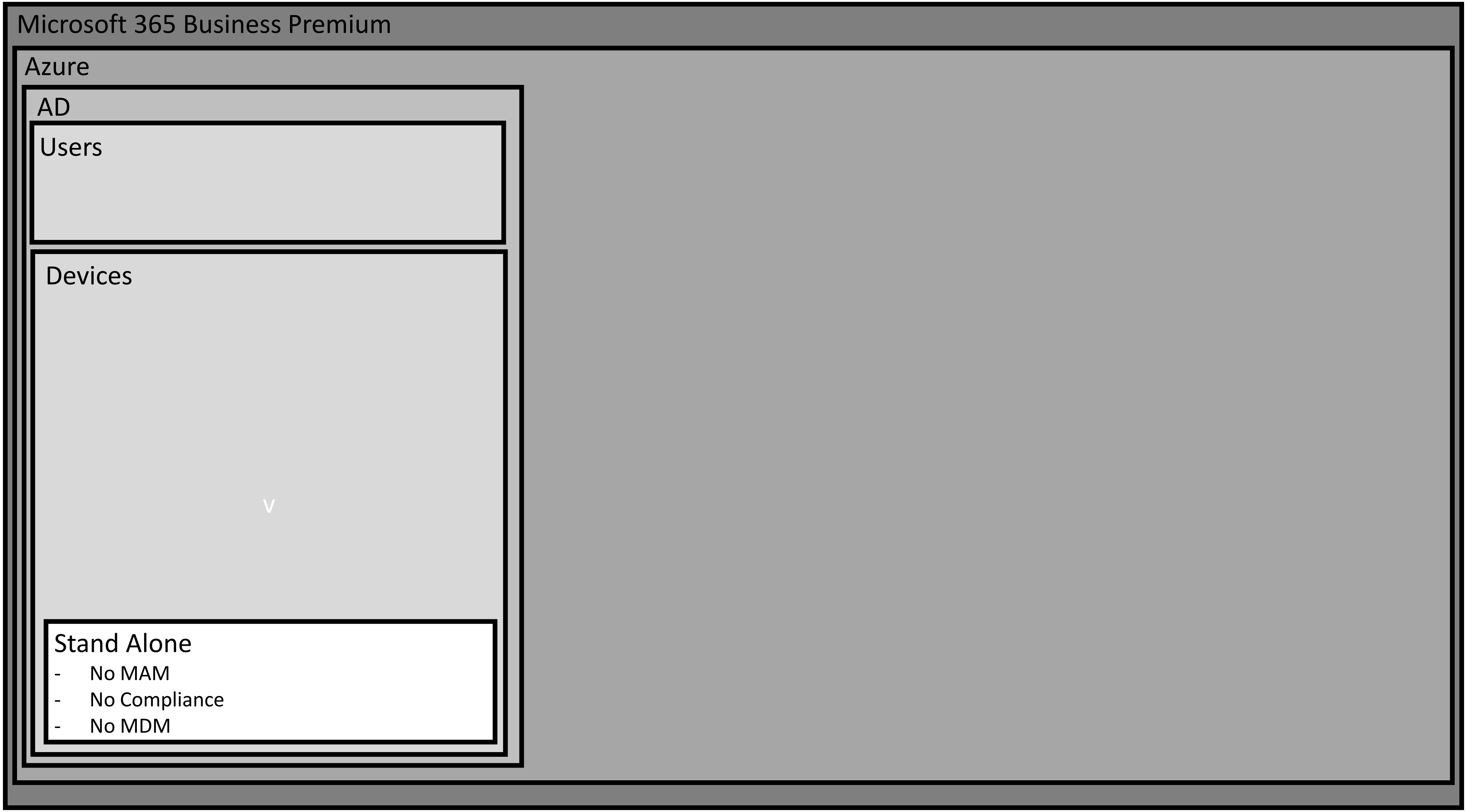
Azure

AD

Users

v

Devices



Microsoft 365 Business Premium

Azure

AD

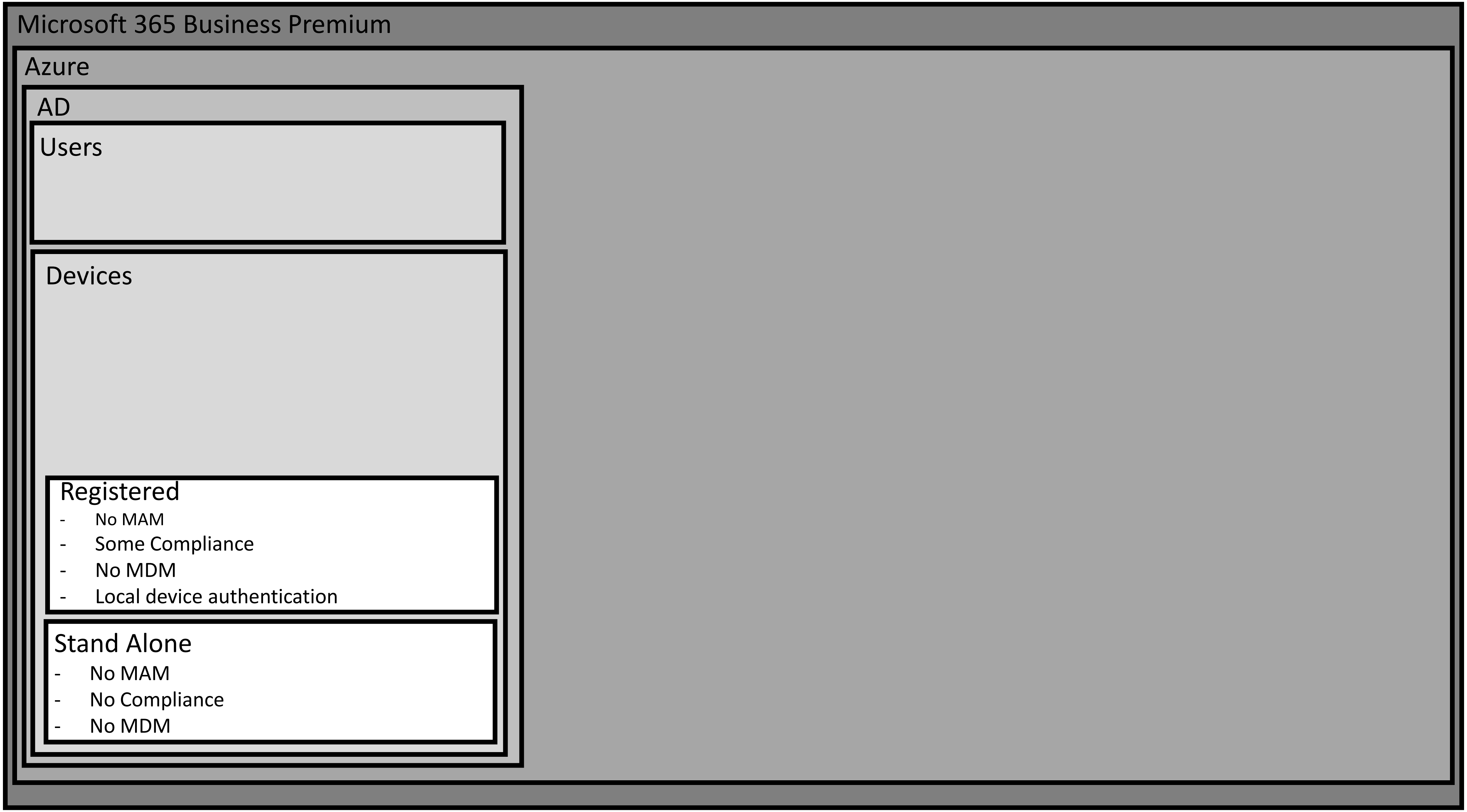
Users

Devices

v

Stand Alone

- No MAM
- No Compliance
- No MDM



Microsoft 365 Business Premium

Azure

AD

Users

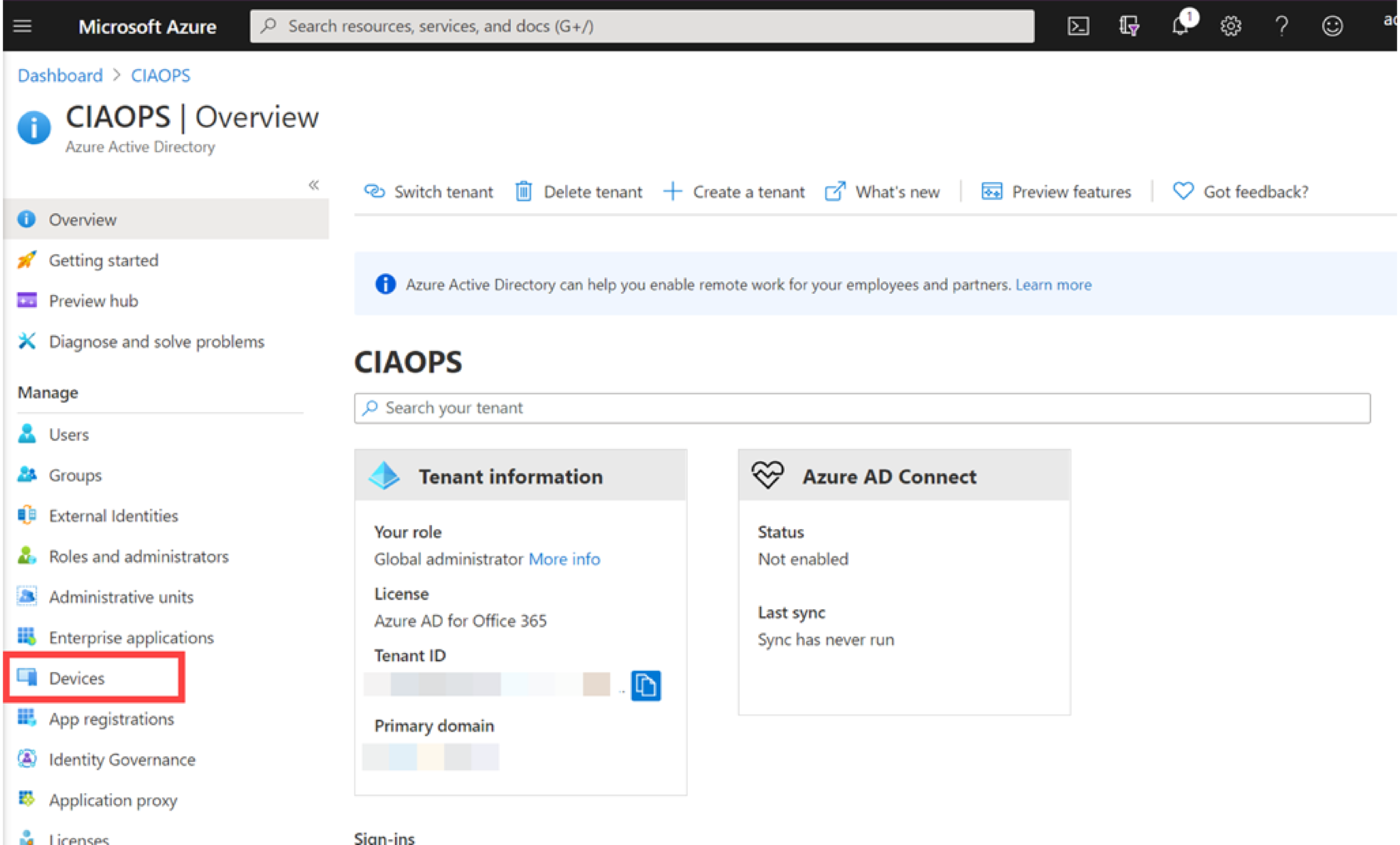
Devices

Registered

- No MAM
- Some Compliance
- No MDM
- Local device authentication

Stand Alone

- No MAM
- No Compliance
- No MDM



Azure Active Directory can help you enable remote work for your employees and partners. Learn more

CIAOPS

Tenant information

Your role
Global administrator More info

License
Azure AD for Office 365

Tenant ID
[redacted]

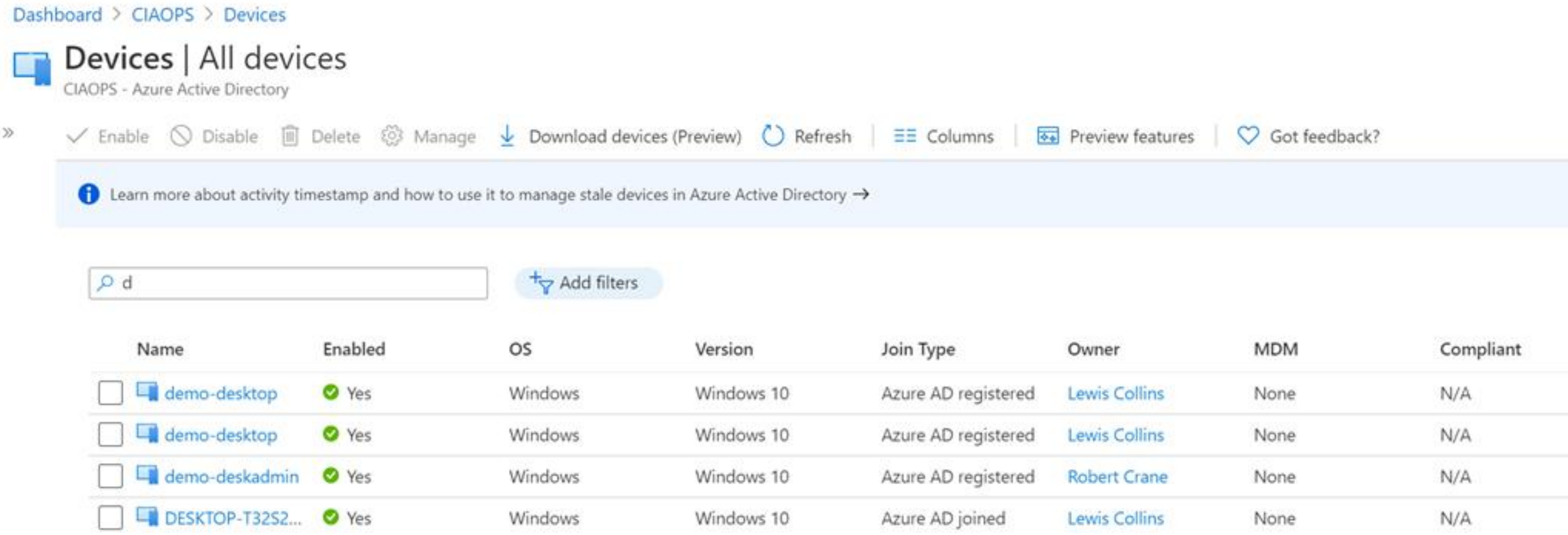
Primary domain
[redacted]

Azure AD Connect

Status
Not enabled

Last sync
Sync has never run

Sign-ins

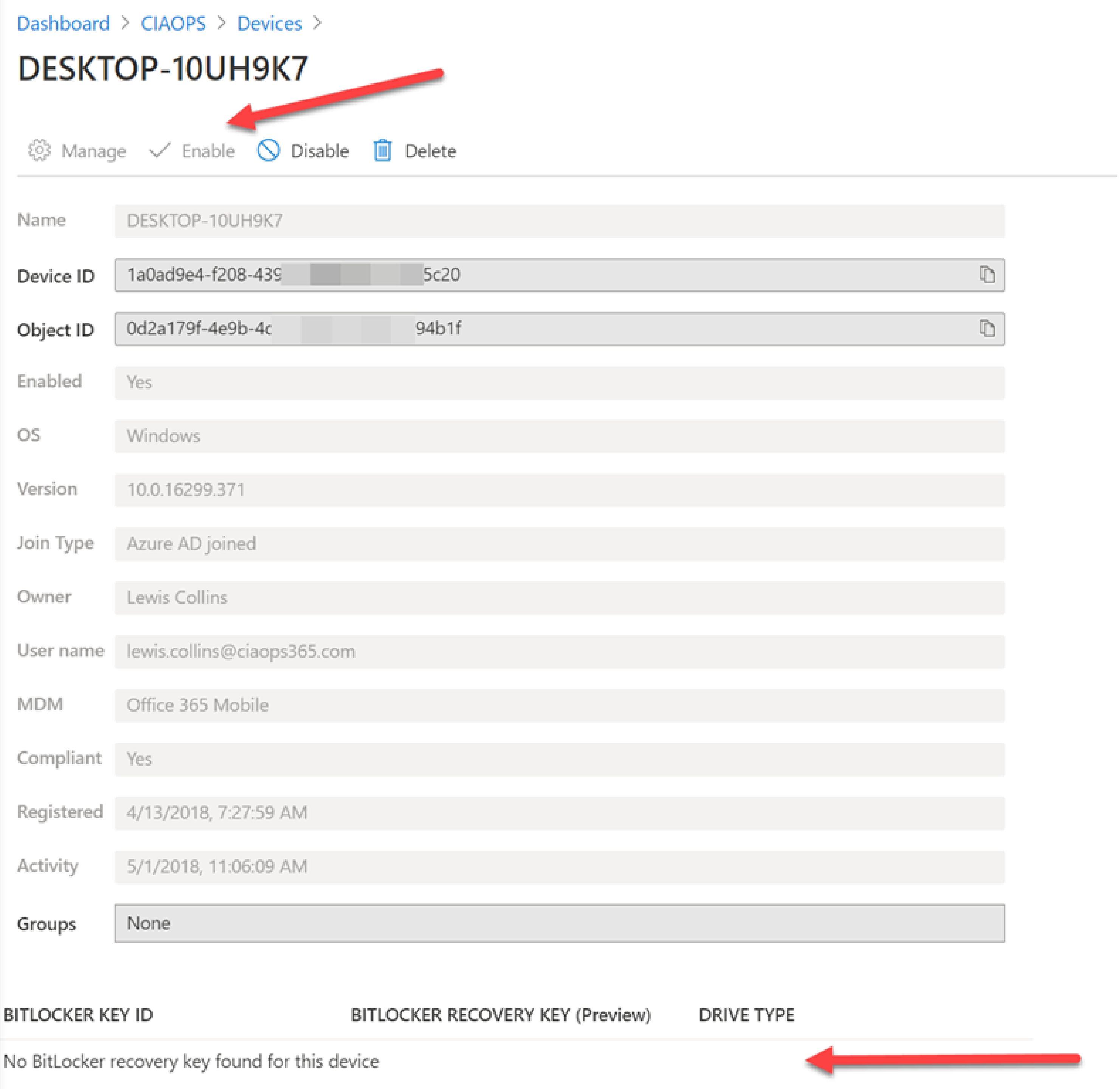


Devices | All devices

CIAOPS - Azure Active Directory

Learn more about activity timestamp and how to use it to manage stale devices in Azure Active Directory →

	Name	Enabled	OS	Version	Join Type	Owner	MDM	Compliant
□	demo-desktop	✓ Yes	Windows	Windows 10	Azure AD registered	Lewis Collins	None	N/A
□	demo-desktop	✓ Yes	Windows	Windows 10	Azure AD registered	Lewis Collins	None	N/A
□	demo-deskadmin	✓ Yes	Windows	Windows 10	Azure AD registered	Robert Crane	None	N/A
□	DESKTOP-T32S2...	✓ Yes	Windows	Windows 10	Azure AD joined	Lewis Collins	None	N/A



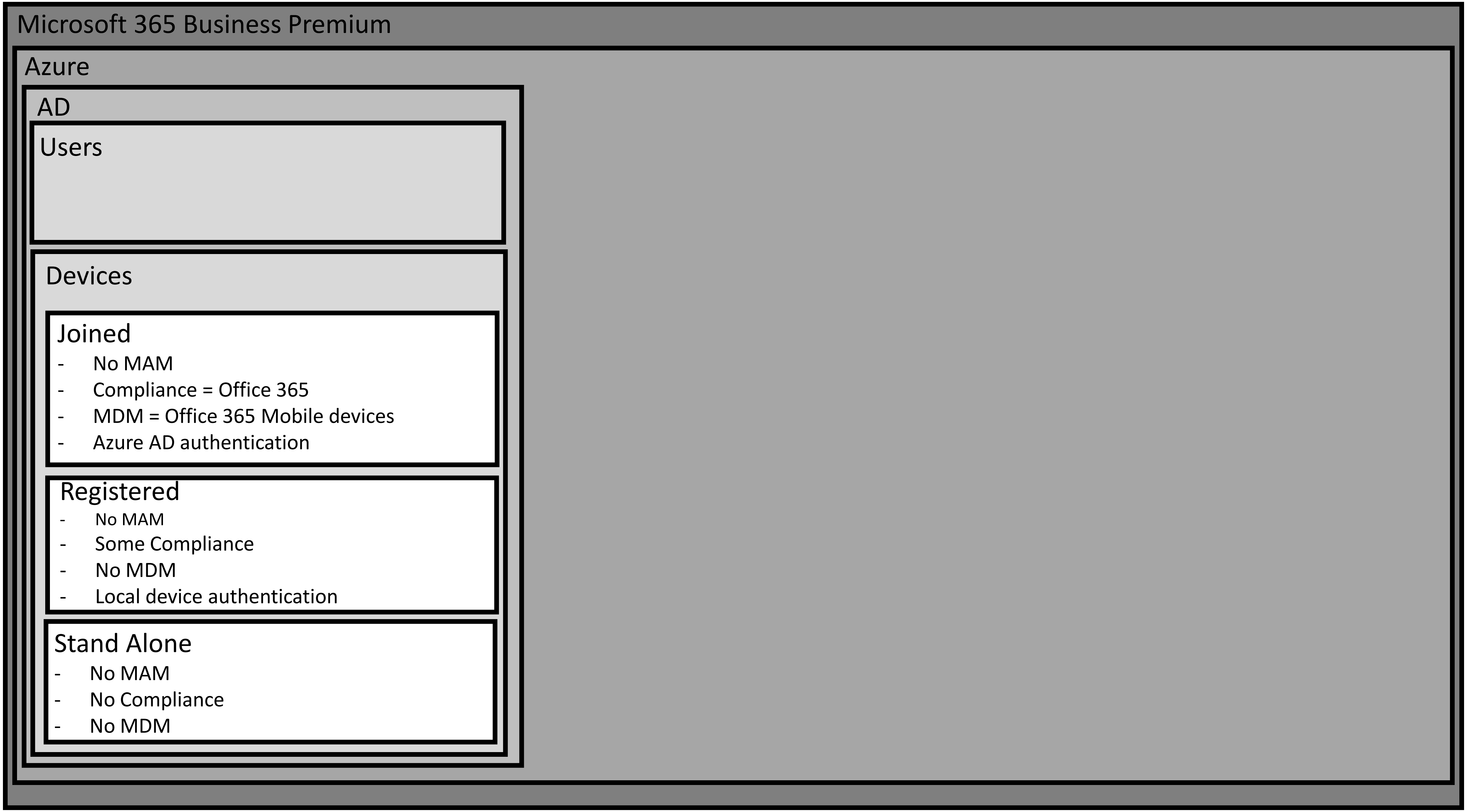
DESKTOP-10UH9K7

Name	DESKTOP-10UH9K7
Device ID	1a0ad9e4-f208-439[redacted]5c20
Object ID	0d2a179f-4e9b-4c[redacted]94b1f
Enabled	Yes
OS	Windows
Version	10.0.16299.371
Join Type	Azure AD joined
Owner	Lewis Collins
User name	lewis.collins@ciaops365.com
MDM	Office 365 Mobile
Compliant	Yes
Registered	4/13/2018, 7:27:59 AM
Activity	5/1/2018, 11:06:09 AM
Groups	None

BITLOCKER KEY ID	BITLOCKER RECOVERY KEY (Preview)	DRIVE TYPE
No BitLocker recovery key found for this device		

Basic Device Management Resources

- Register your personal device on your organization’s network
- Entra registered devices
- Join your work device to your organization’s network
- Entra joined devices
- Set Up Basic Mobility and Security
- Create device security policies in Basic Mobility and Security



Microsoft 365 Business Premium

Azure

AD

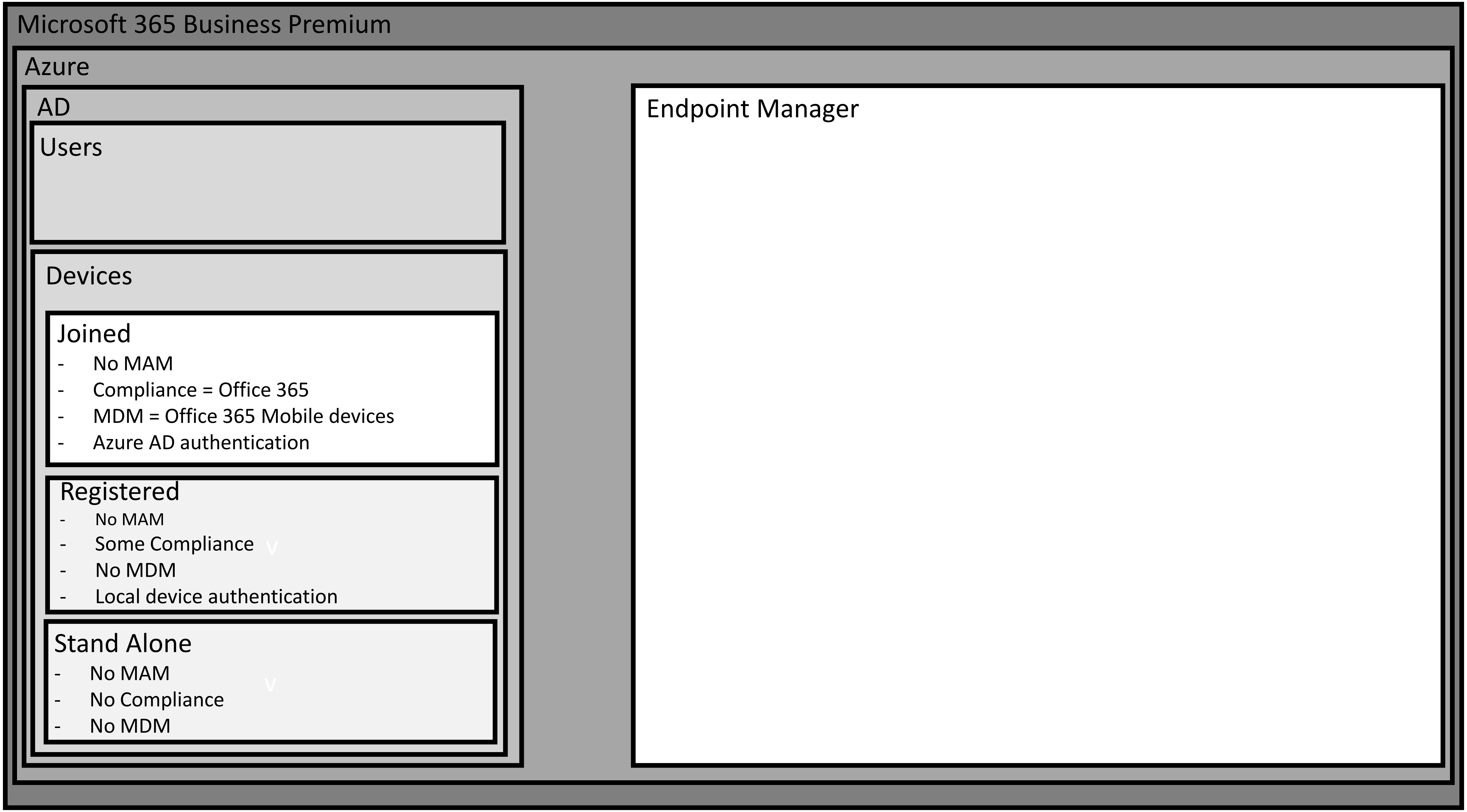
Users

Devices

Joined
- No MAM
- Compliance = Office 365
- MDM = Office 365 Mobile devices
- Azure AD authentication

Registered
- No MAM
- Some Compliance
- No MDM
- Local device authentication

Stand Alone
- No MAM
- No Compliance
- No MDM



Microsoft 365 Business Premium

Azure

AD

Users

Devices

Joined

- No MAM
- Compliance = Office 365
- MDM = Office 365 Mobile devices
- Azure AD authentication

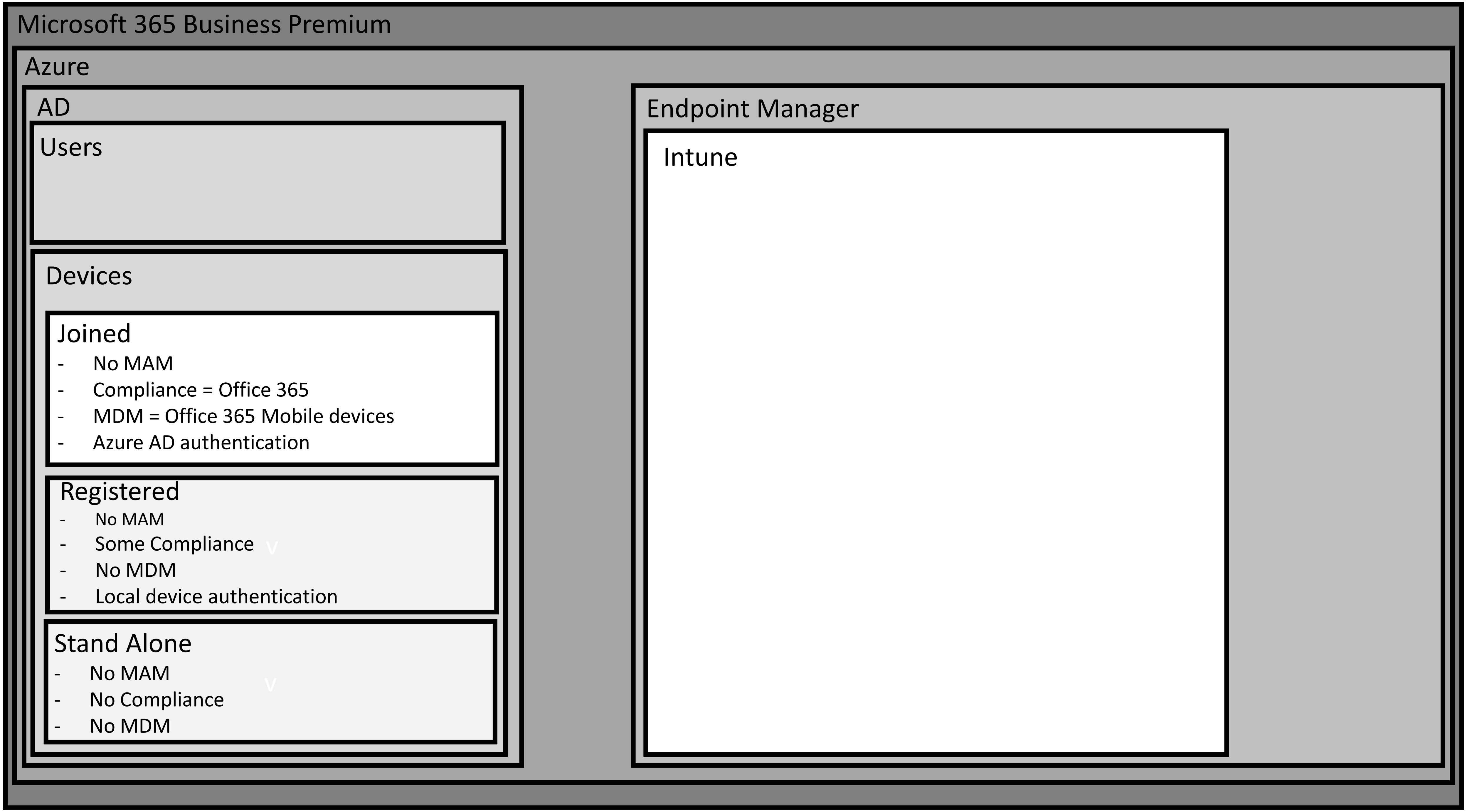
Registered

- No MAM
- Some Compliance
- No MDM
- Local device authentication

Stand Alone

- No MAM
- No Compliance
- No MDM

Endpoint Manager



Microsoft 365 Business Premium

Azure

AD

Users

Devices

Joined

- No MAM
- Compliance = Office 365
- MDM = Office 365 Mobile devices
- Azure AD authentication

Registered

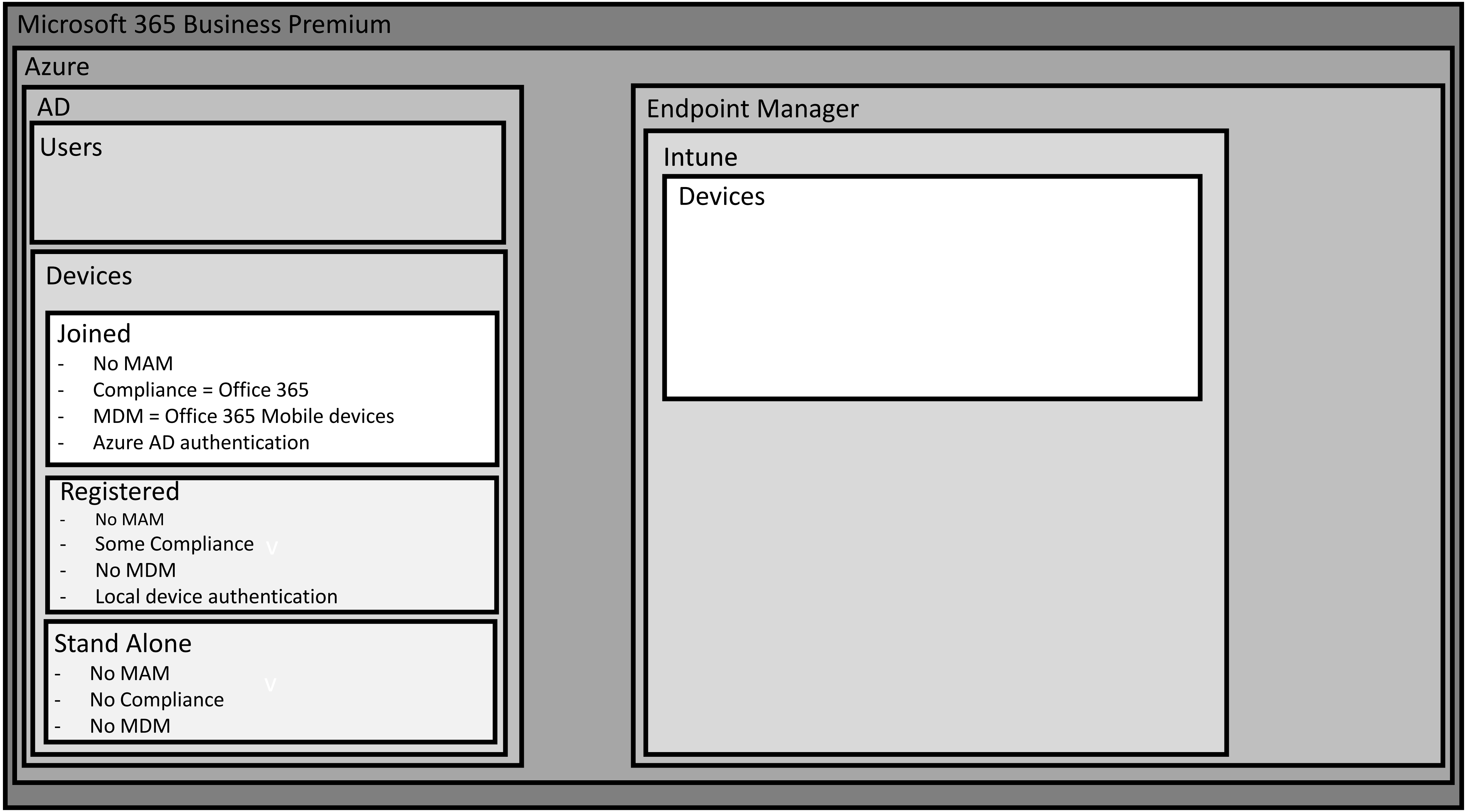
- No MAM
- Some Compliance
- No MDM
- Local device authentication

Stand Alone

- No MAM
- No Compliance
- No MDM

Endpoint Manager

Intune



Microsoft 365 Business Premium

Azure

AD

Users

Devices

Joined

- No MAM
- Compliance = Office 365
- MDM = Office 365 Mobile devices
- Azure AD authentication

Registered

- No MAM
- Some Compliance
- No MDM
- Local device authentication

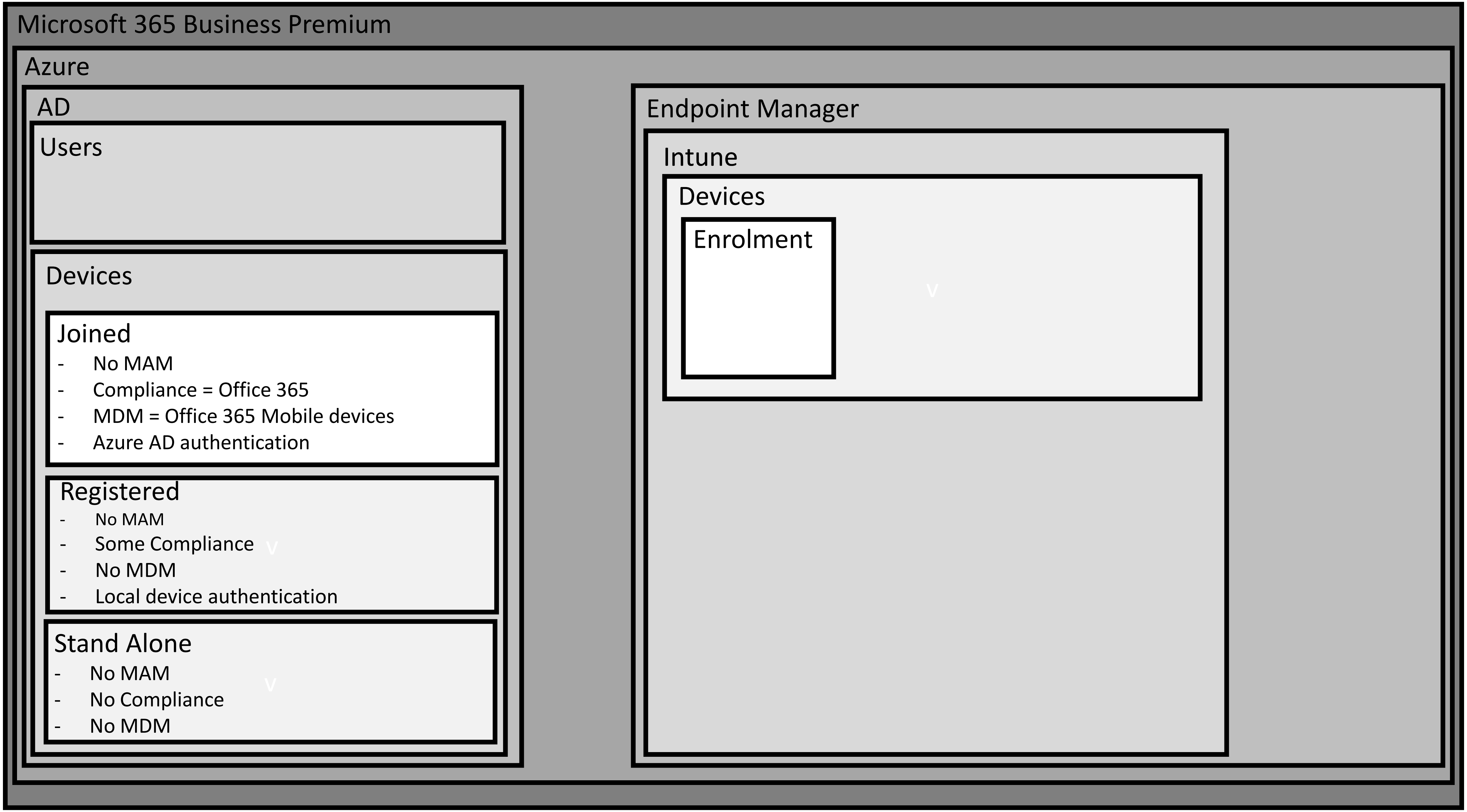
Stand Alone

- No MAM
- No Compliance
- No MDM

Endpoint Manager

Intune

Devices



Microsoft 365 Business Premium

Azure

AD

Users

Devices

Joined

- No MAM
- Compliance = Office 365
- MDM = Office 365 Mobile devices
- Azure AD authentication

Registered

- No MAM
- Some Compliance
- No MDM
- Local device authentication

Stand Alone

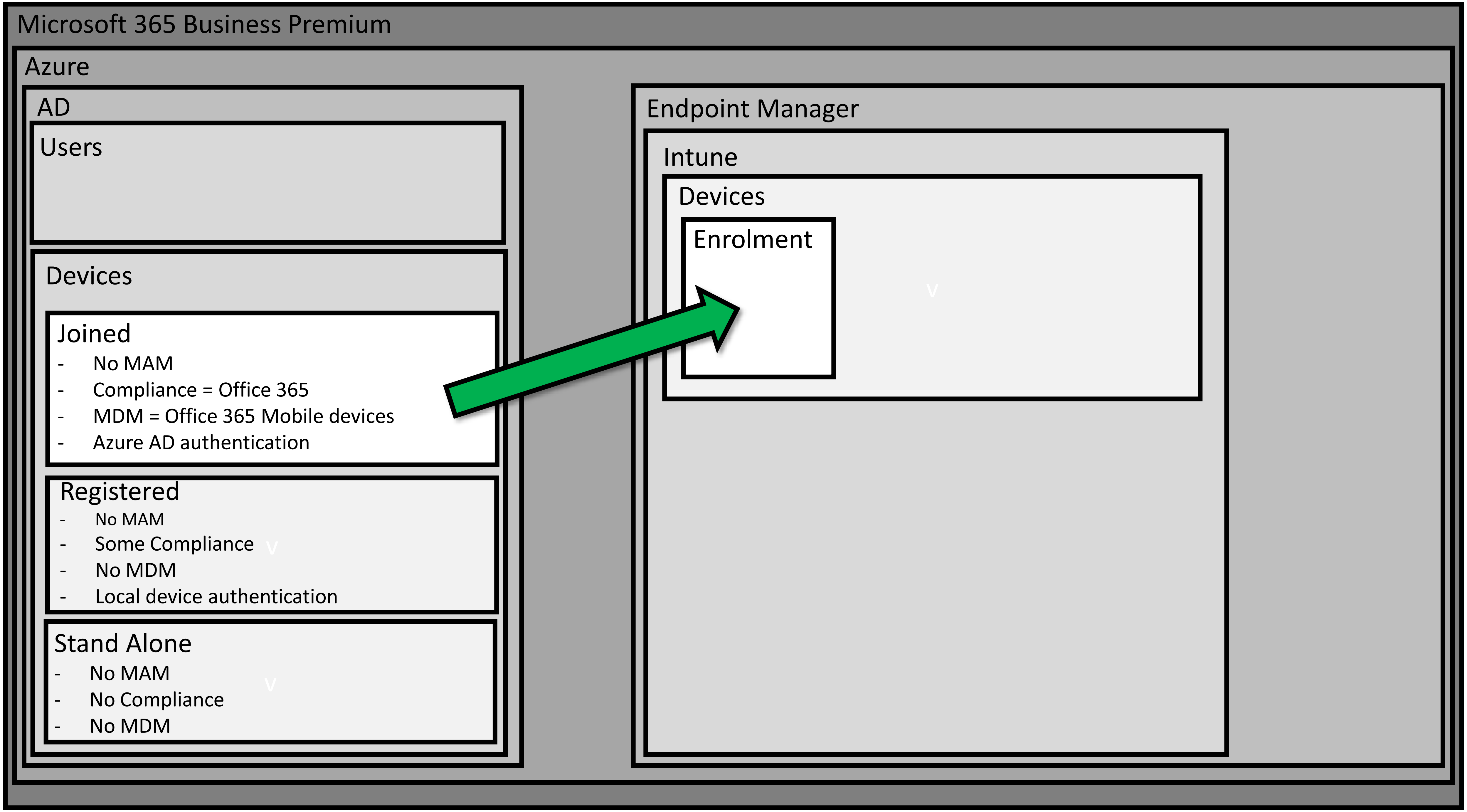
- No MAM
- No Compliance
- No MDM

Endpoint Manager

Intune

Devices

Enrolment



Microsoft 365 Business Premium

Azure

AD

Users

Devices

Joined

- No MAM
- Compliance = Office 365
- MDM = Office 365 Mobile devices
- Azure AD authentication

Registered

- No MAM
- Some Compliance
- No MDM
- Local device authentication

Stand Alone

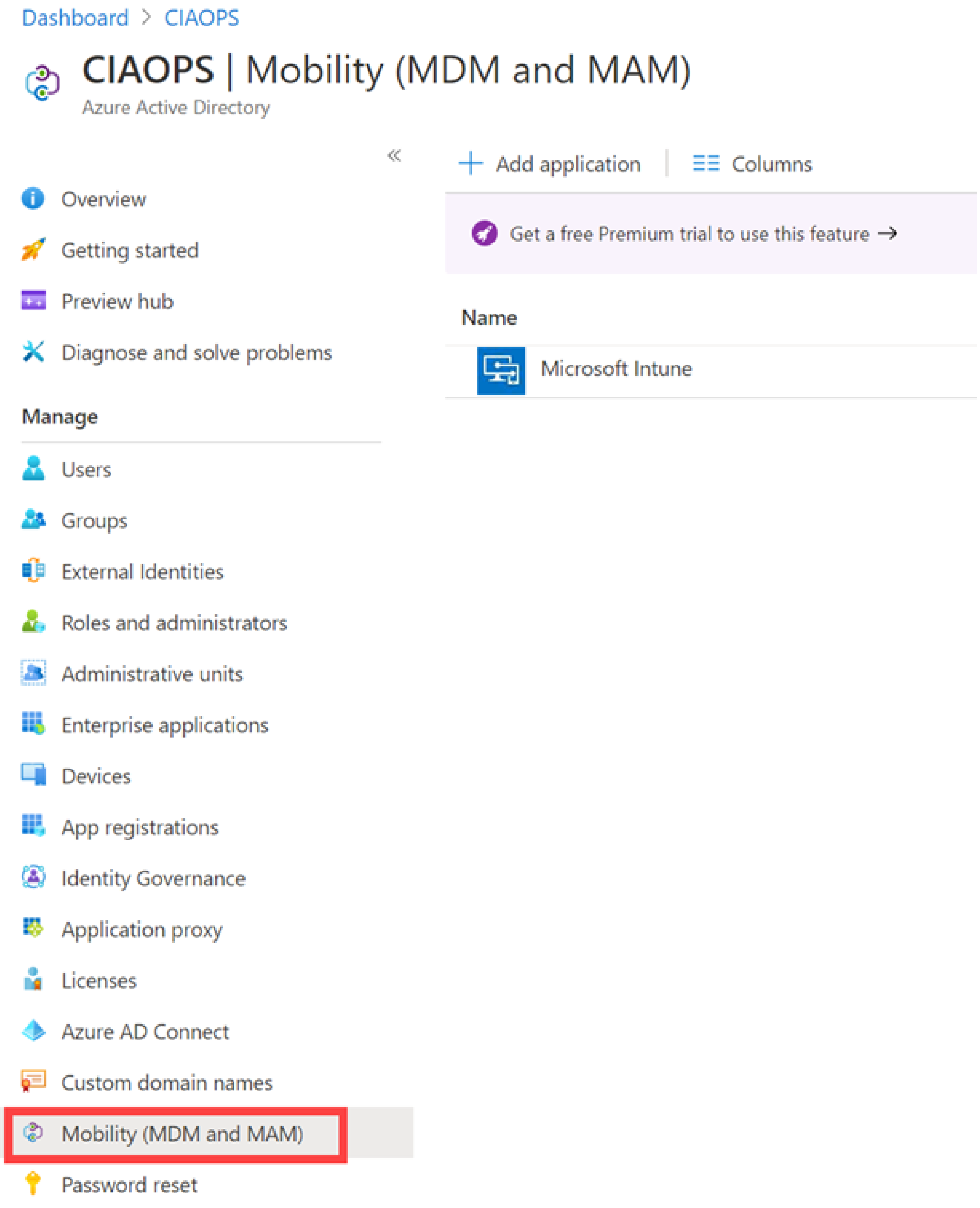
- No MAM
- No Compliance
- No MDM

Endpoint Manager

Intune

Devices

Enrolment



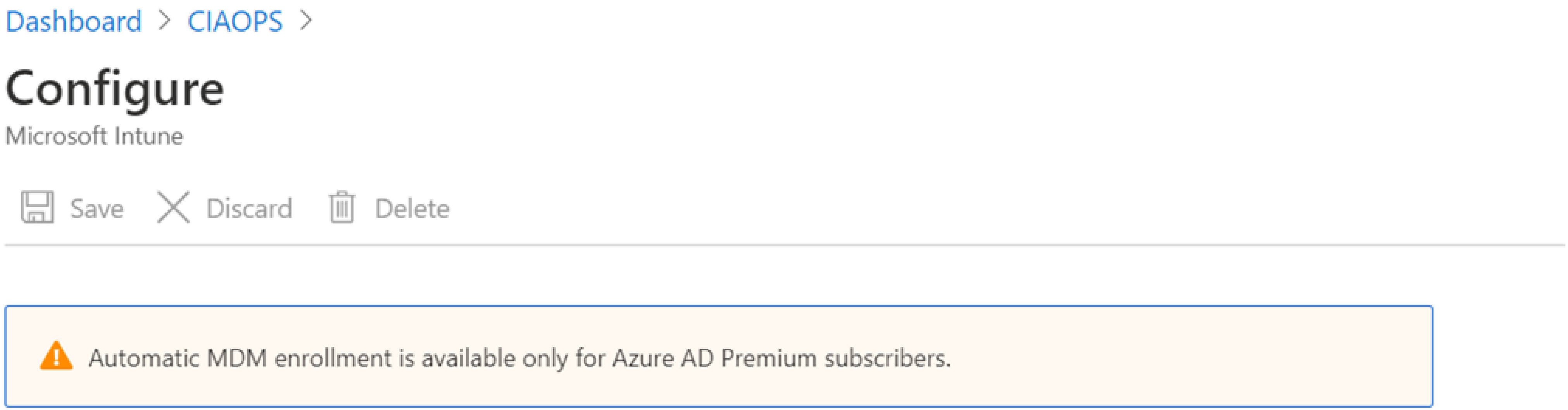
Dashboard > CIAOPS

CIAOPS | Mobility (MDM and MAM)

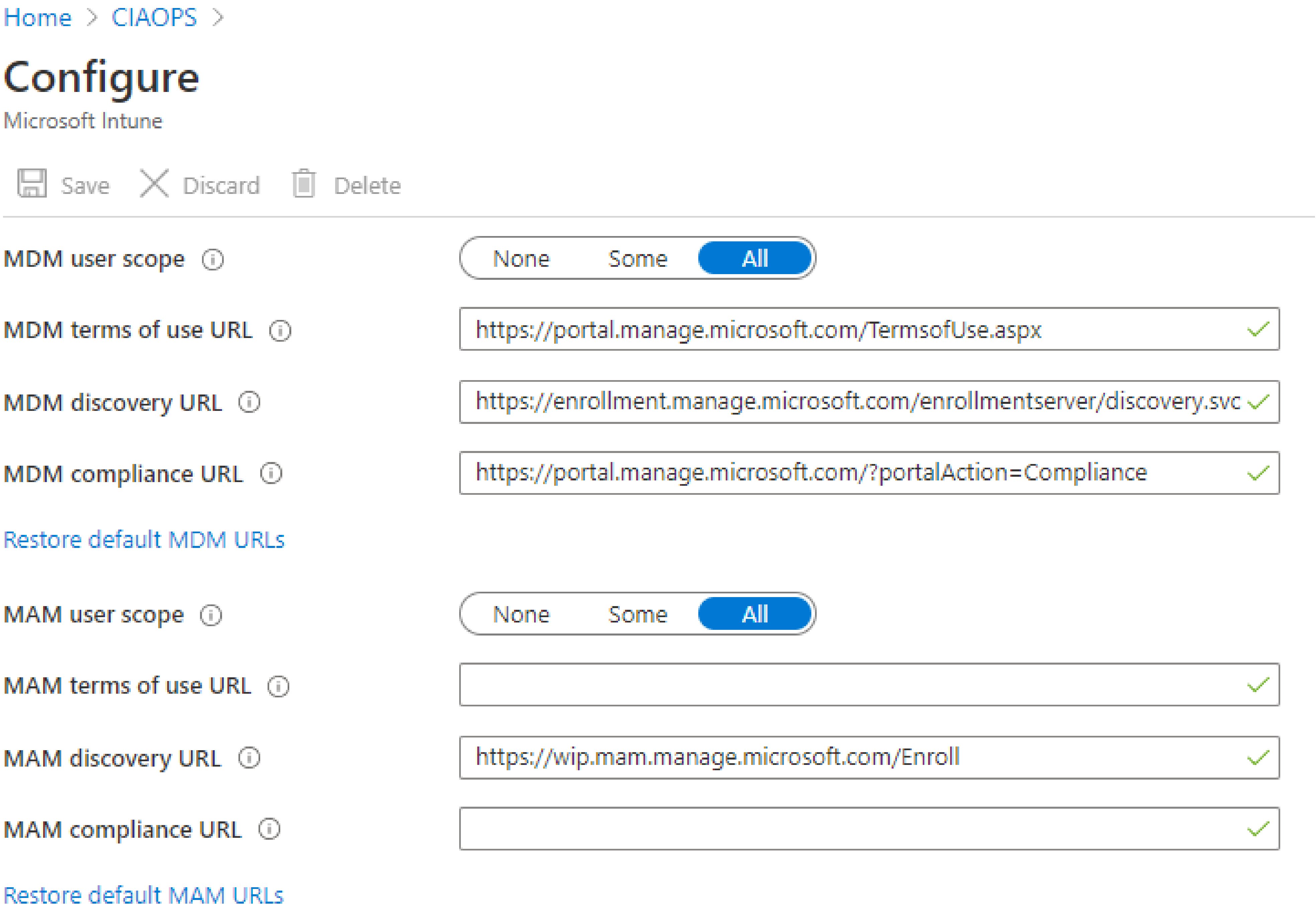
Azure Active Directory

Get a free Premium trial to use this feature →

Name
Microsoft Intune



⚠ Automatic MDM enrollment is available only for Azure AD Premium subscribers.



Configure

Microsoft Intune

MDM user scope ⓘ None Some [✓ All]

MDM terms of use URL ⓘ https://portal.manage.microsoft.com/TermsofUse.aspx ✓

MDM discovery URL ⓘ https://enrollment.manage.microsoft.com/enrollmentserver/discovery.svc ✓

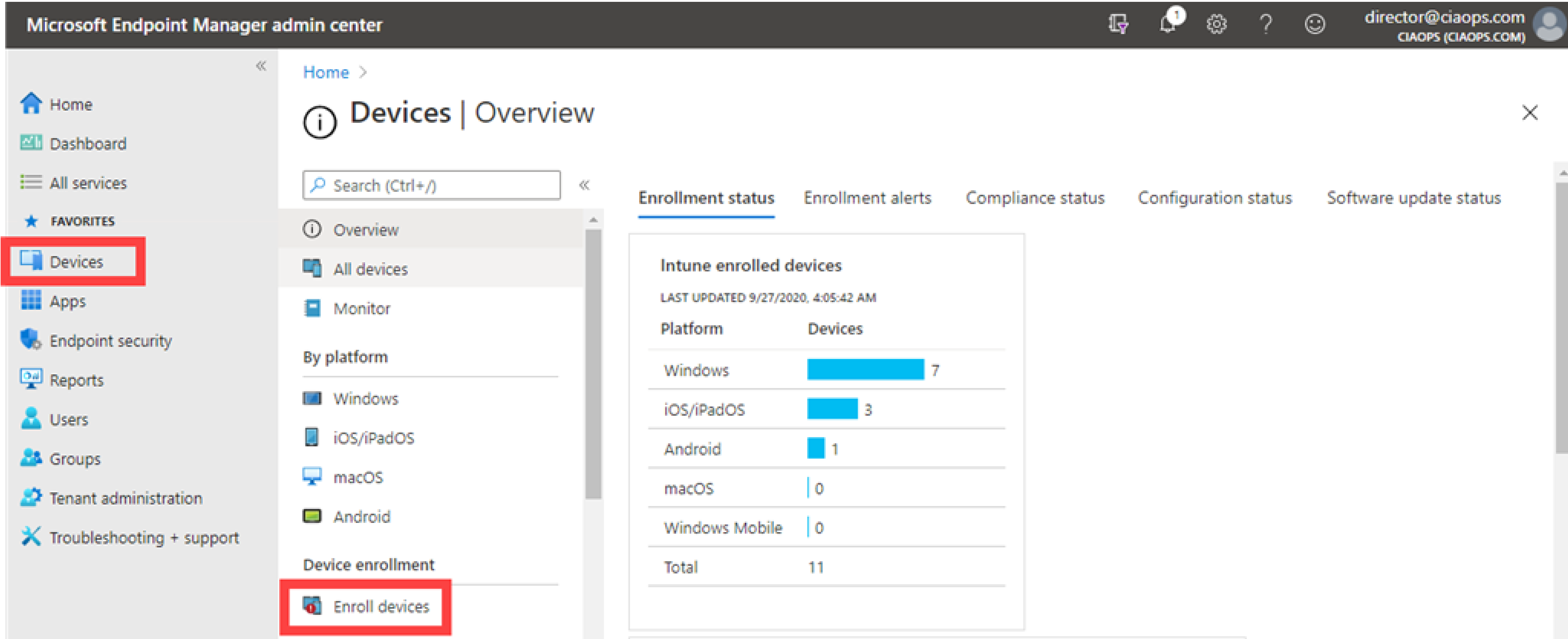
MDM compliance URL ⓘ https://portal.manage.microsoft.com/?portalAction=Compliance ✓

MAM user scope ⓘ None Some [✓ All]

MAM terms of use URL ⓘ ✓

MAM discovery URL ⓘ https://wip.mam.manage.microsoft.com/Enroll ✓

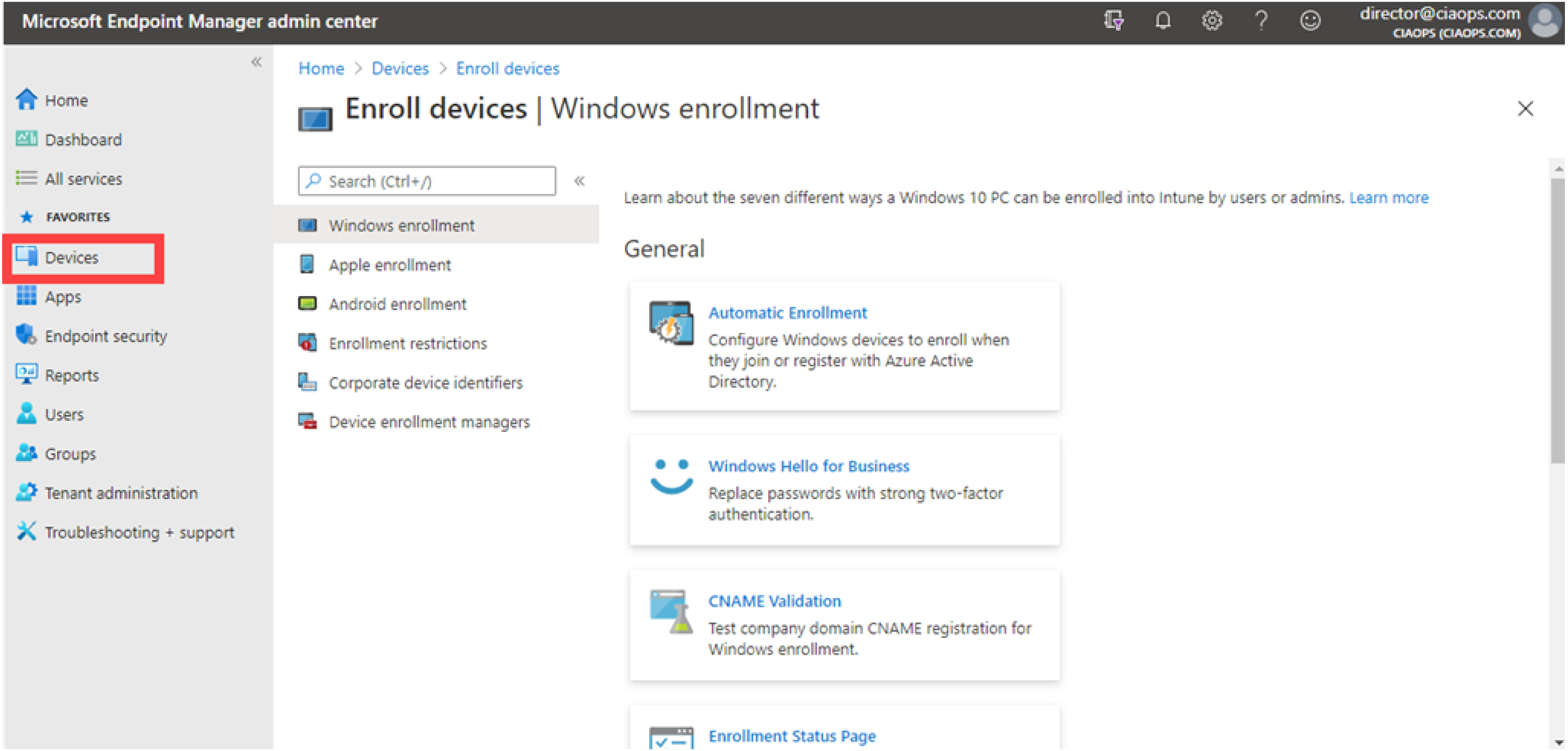
MAM compliance URL ⓘ ✓



Intune enrolled devices

LAST UPDATED 9/27/2020, 4:05:42 AM

Platform	Devices
Windows	7
iOS/iPadOS	3
Android	1
macOS	0
Windows Mobile	0
Total	11



Enroll devices | Windows enrollment

Learn about the seven different ways a Windows 10 PC can be enrolled into Intune by users or admins. Learn more

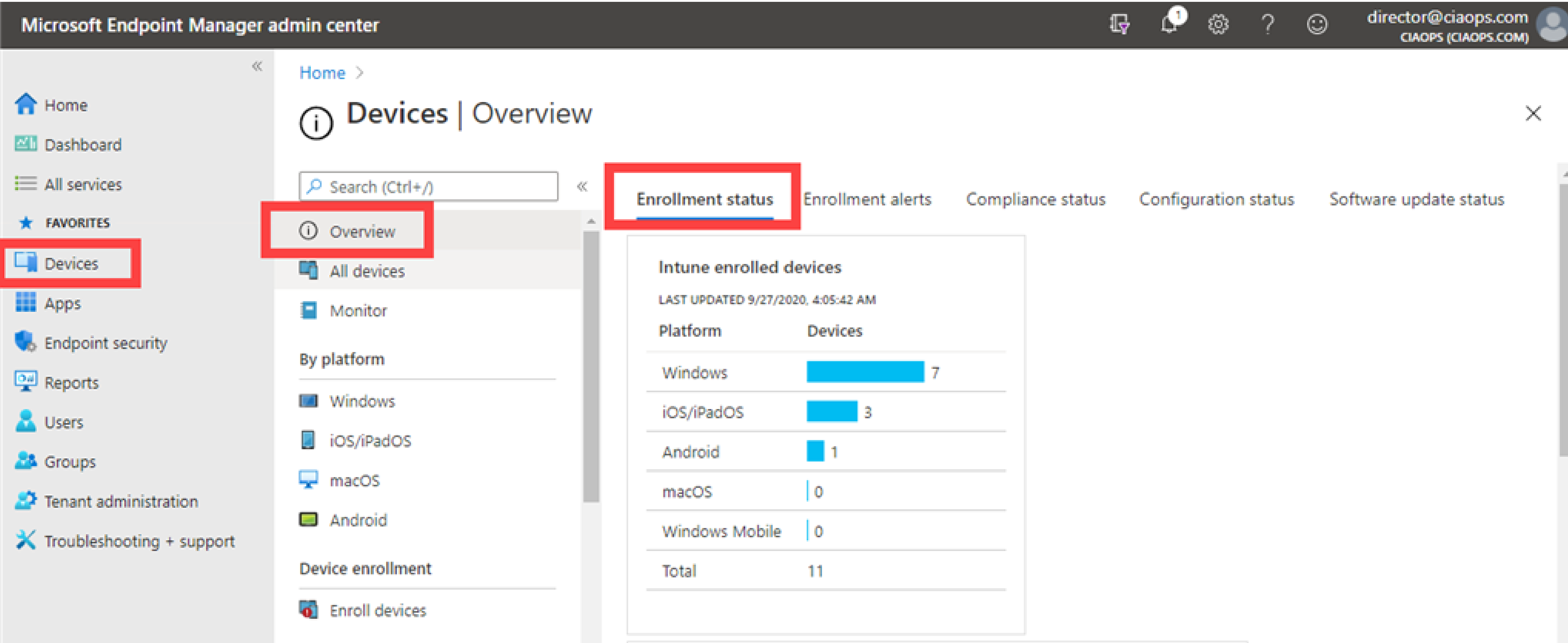
General

Automatic Enrollment
Configure Windows devices to enroll when they join or register with Azure Active Directory.

Windows Hello for Business
Replace passwords with strong two-factor authentication.

CNAME Validation
Test company domain CNAME registration for Windows enrollment.

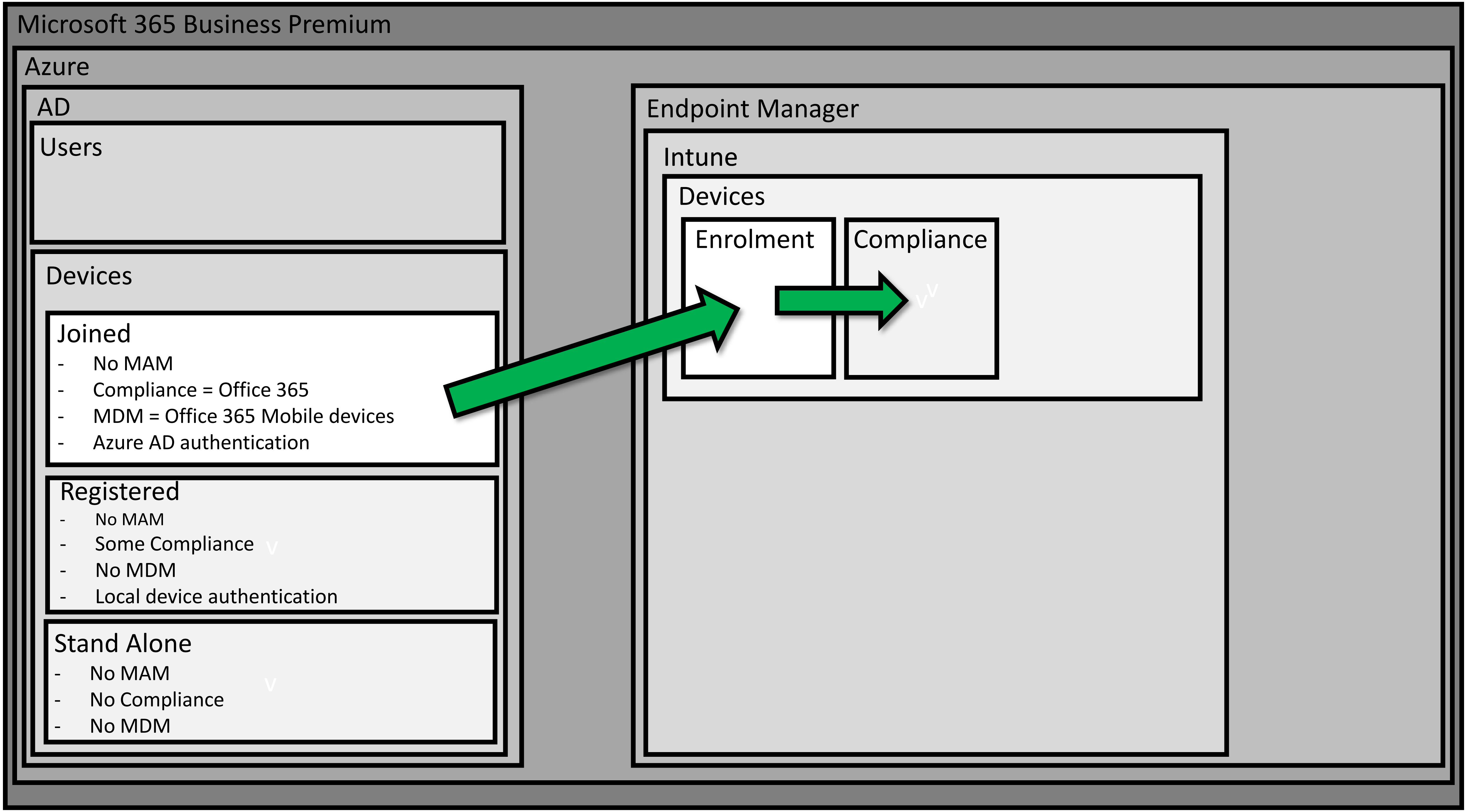
Enrollment Status Page



Intune enrolled devices

LAST UPDATED 9/27/2020, 4:05:42 AM

Platform	Devices
Windows	7
iOS/iPadOS	3
Android	1
macOS	0
Windows Mobile	0
Total	11



Microsoft 365 Business Premium

Azure

AD

Users

Devices

Joined

- No MAM
- Compliance = Office 365
- MDM = Office 365 Mobile devices
- Azure AD authentication

Registered

- No MAM
- Some Compliance
- No MDM
- Local device authentication

Stand Alone

- No MAM
- No Compliance
- No MDM

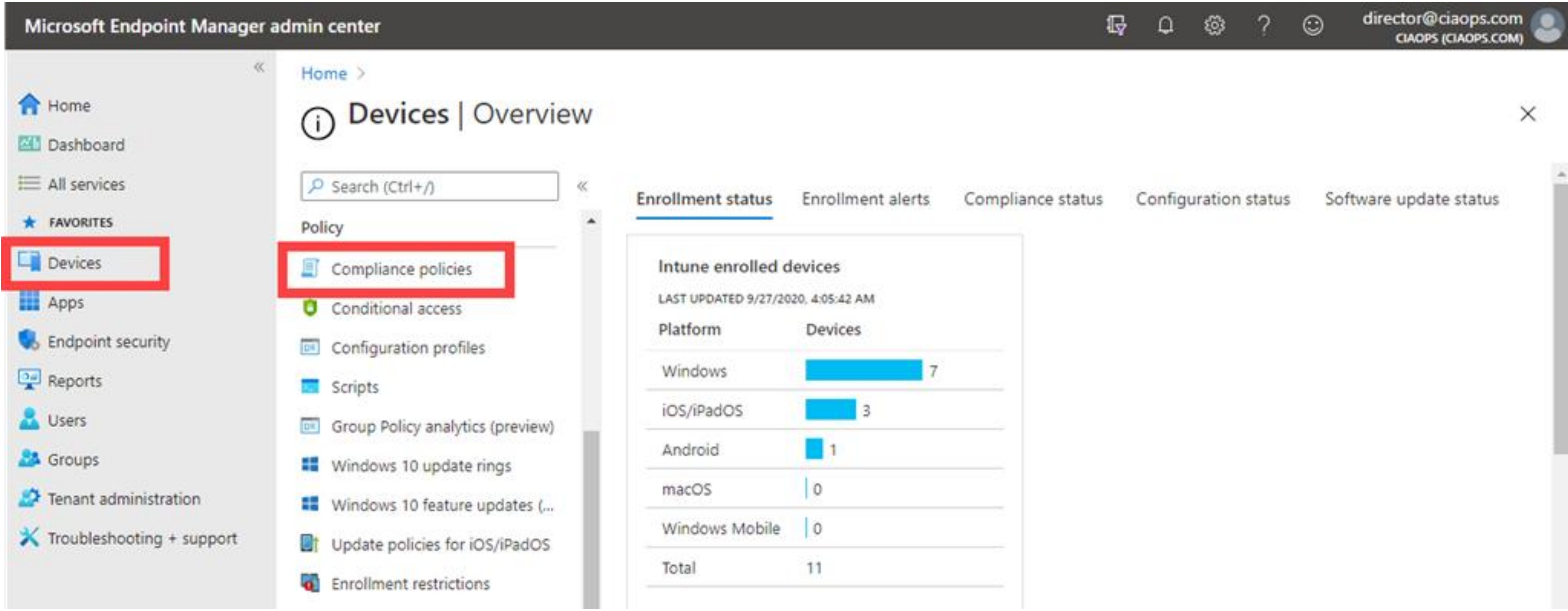
Endpoint Manager

Intune

Devices

Enrolment

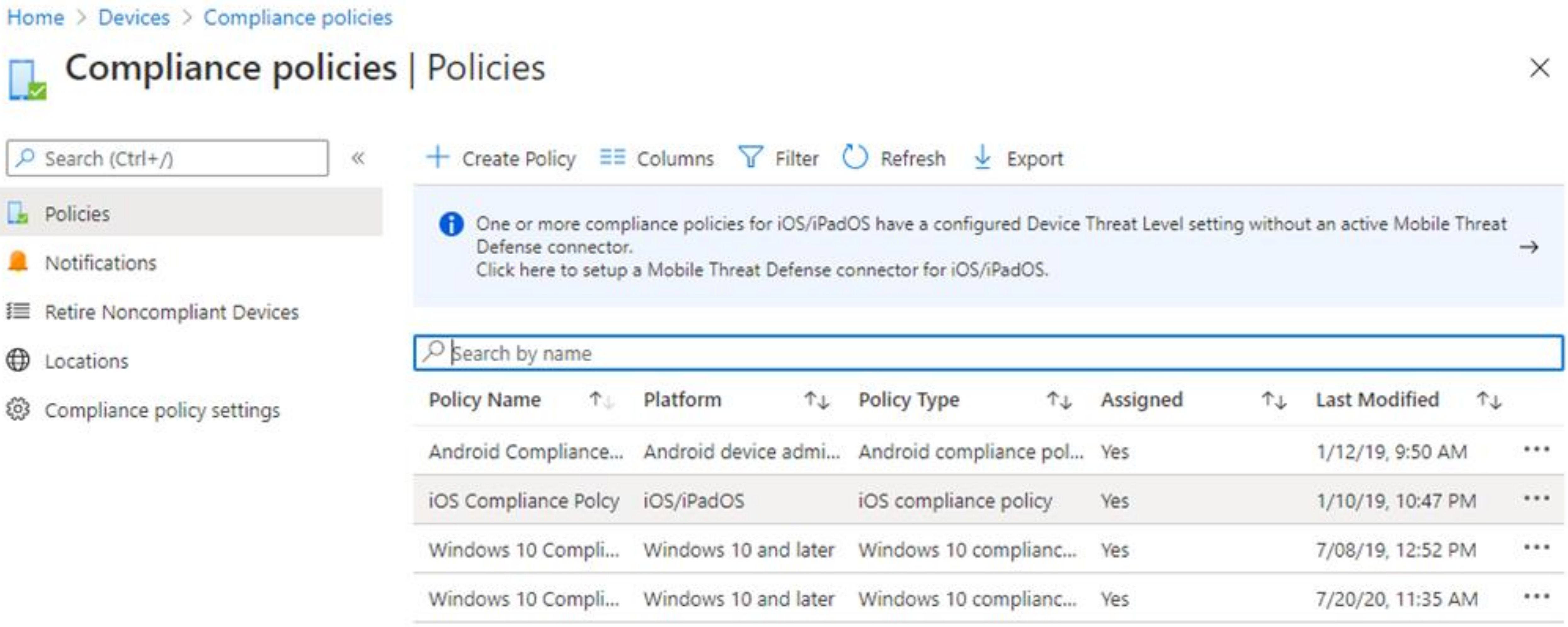
Compliance



Intune enrolled devices

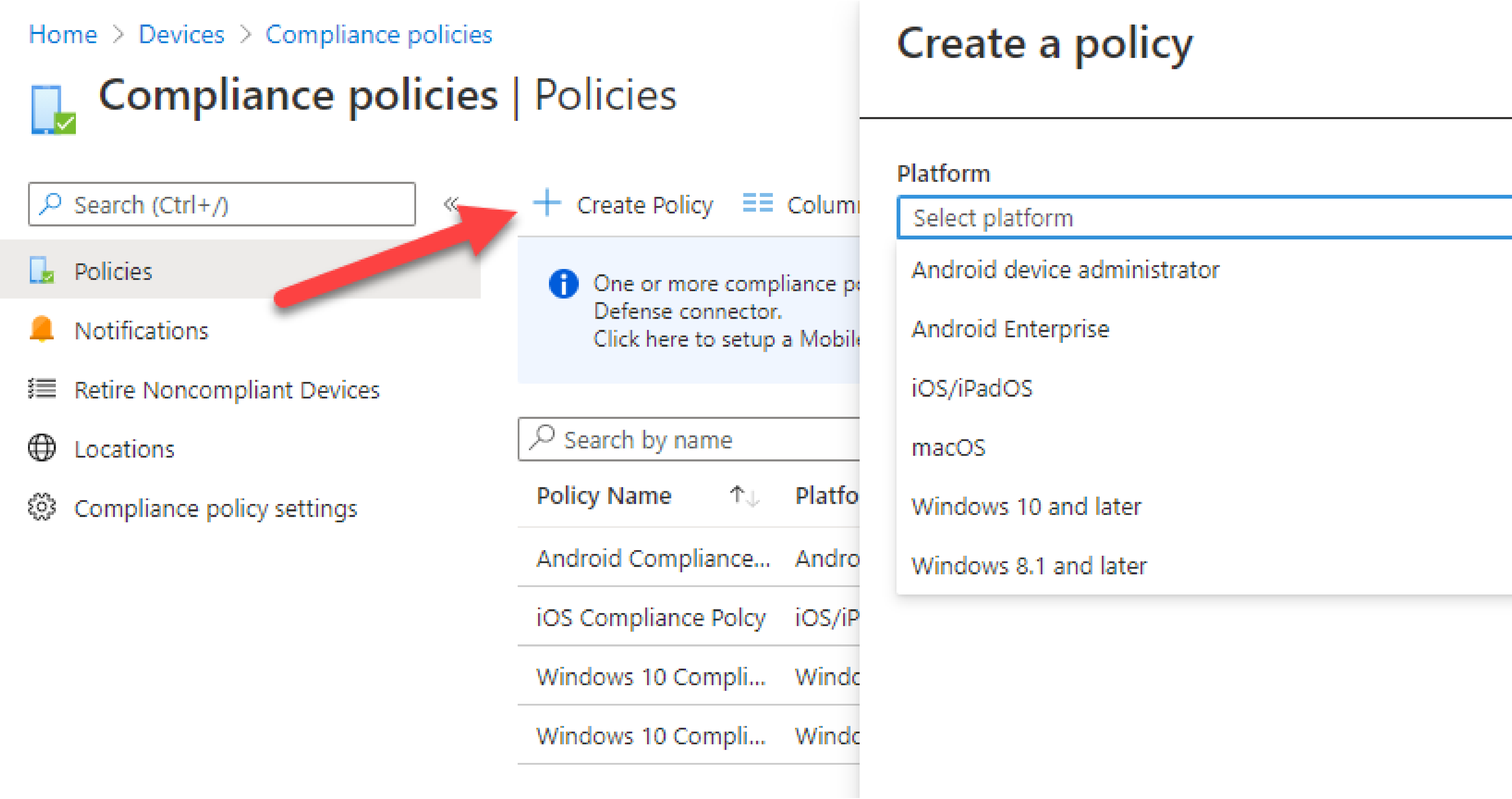
LAST UPDATED 9/27/2020, 4:05:42 AM

Platform	Devices
Windows	7
iOS/iPadOS	3
Android	1
macOS	0
Windows Mobile	0
Total	11


Home > Devices > Compliance policies
Compliance policies | Policies
Search (Ctrl+/)
Policies
Notifications
Retire Noncompliant Devices
Locations
Compliance policy settings
Create Policy
Columns
Filter
Refresh
Export
Search by name

One or more compliance policies for iOS/iPadOS have a configured Device Threat Level setting without an active Mobile Threat Defense connector.
Click here to setup a Mobile Threat Defense connector for iOS/iPadOS.

Policy Name	Platform	Policy Type	Assigned	Last Modified	
Android Compliance...	Android device admi...	Android compliance pol...	Yes	1/12/19, 9:50 AM	•••
iOS Compliance Polcy	iOS/iPadOS	iOS compliance policy	Yes	1/10/19, 10:47 PM	•••
Windows 10 Compli...	Windows 10 and later	Windows 10 complianc...	Yes	7/08/19, 12:52 PM	•••
Windows 10 Compli...	Windows 10 and later	Windows 10 complianc...	Yes	7/20/20, 11:35 AM	•••



Home > Devices > Compliance policies

Compliance policies | Policies

Search (Ctrl+/)

Policies

Notifications

Retire Noncompliant Devices

Locations

Compliance policy settings

+ Create Policy   Colum

One or more compliance p
Defense connector.
Click here to setup a Mobil

Search by name

Policy Name	Platfo
Android Compliance...	Andro
iOS Compliance Polcy	iOS/iP
Windows 10 Compli...	Windo
Windows 10 Compli...	Windo

Create a policy

Platform

Select platform

Android device administrator

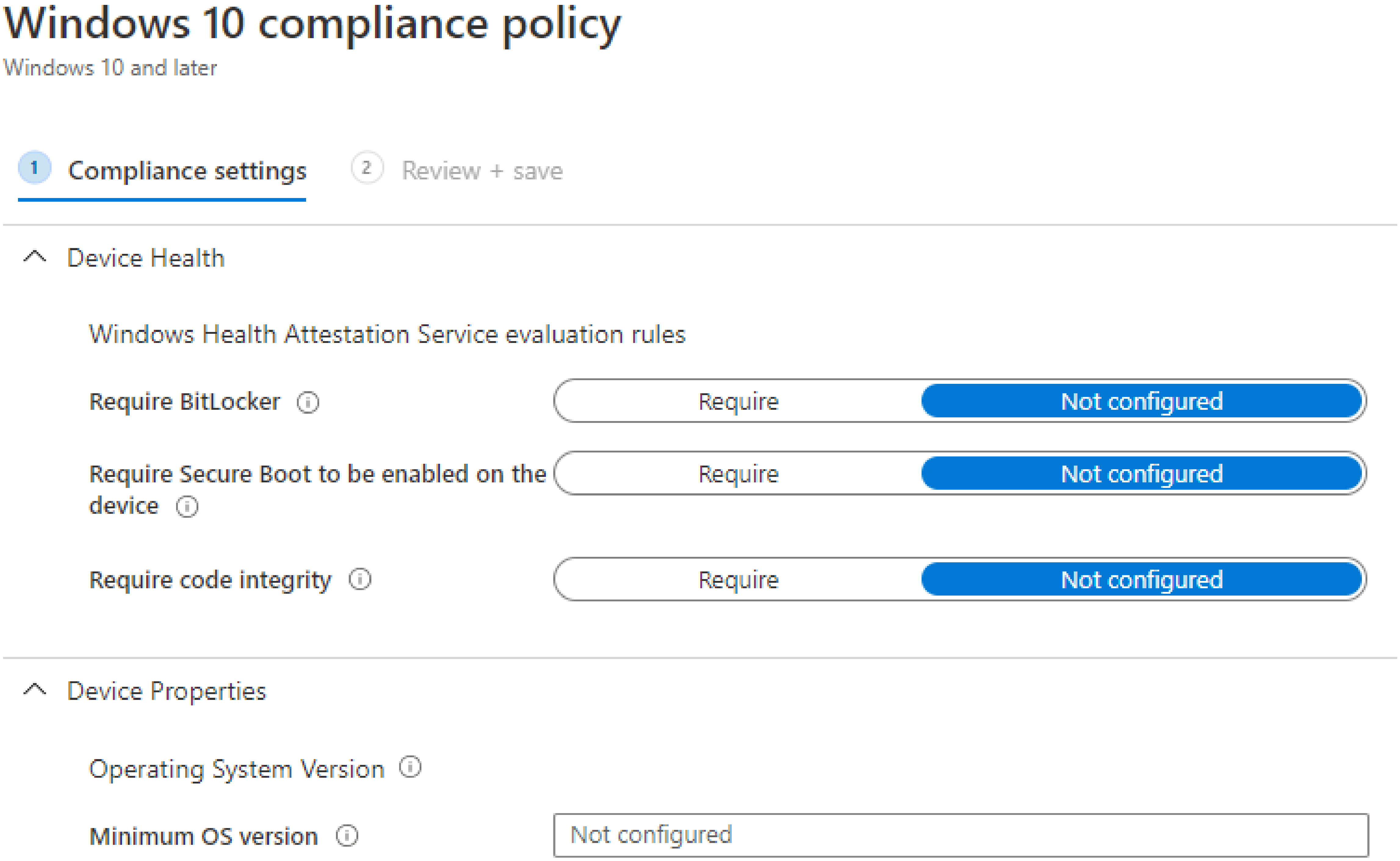
Android Enterprise

iOS/iPadOS

macOS

Windows 10 and later

Windows 8.1 and later



Windows 10 compliance policy

Windows 10 and later

^ Device Health

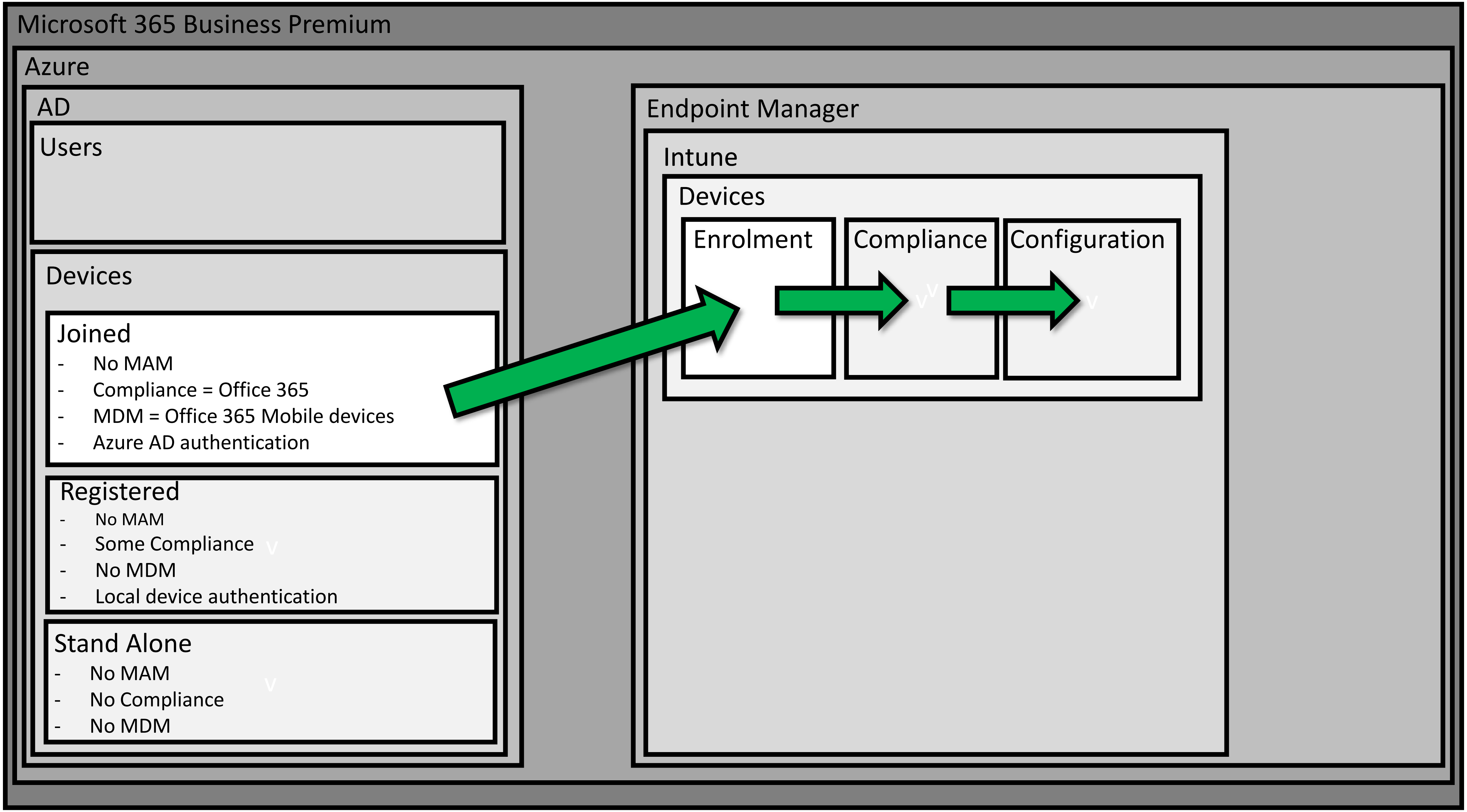
Windows Health Attestation Service evaluation rules

Require BitLocker ⓘ	Require [✓ Not configured]
Require Secure Boot to be enabled on the device ⓘ	Require [✓ Not configured]
Require code integrity ⓘ	Require [✓ Not configured]

^ Device Properties

Operating System Version ⓘ

Minimum OS version ⓘ	Not configured



Microsoft 365 Business Premium

Azure

AD

Users

Devices

Joined

- No MAM
- Compliance = Office 365
- MDM = Office 365 Mobile devices
- Azure AD authentication

Registered

- No MAM
- Some Compliance
- No MDM
- Local device authentication

Stand Alone

- No MAM
- No Compliance
- No MDM

Endpoint Manager

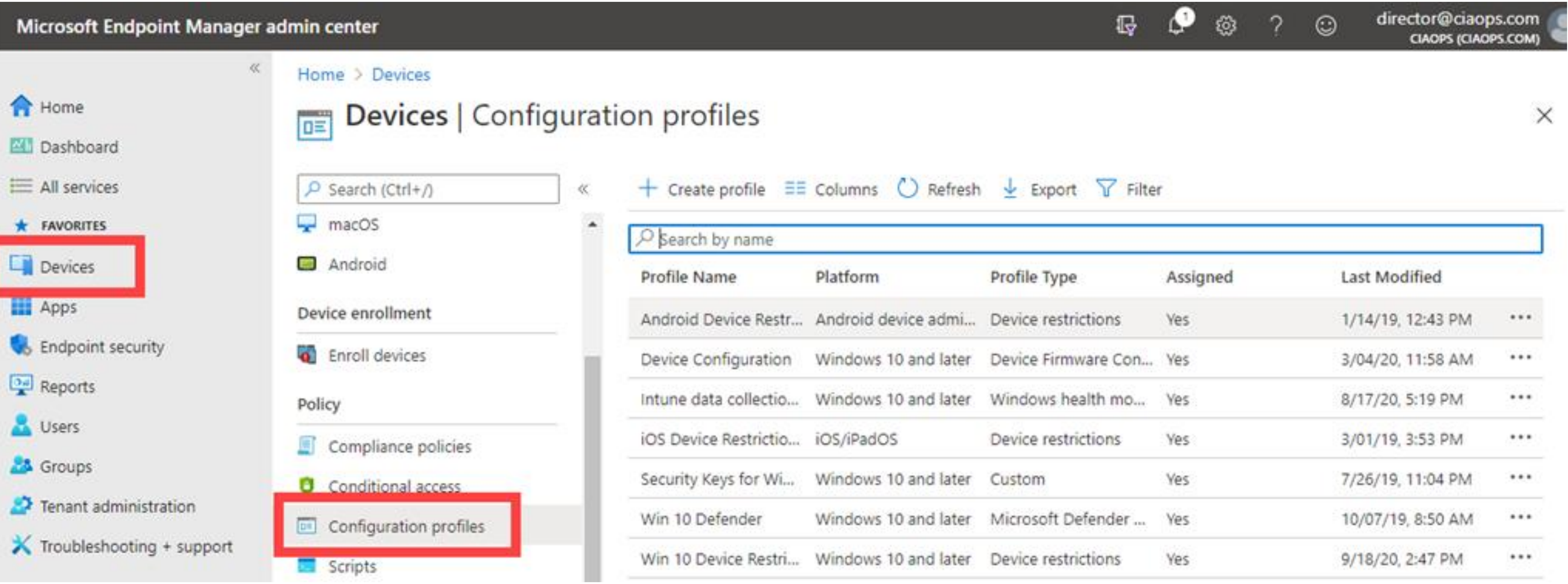
Intune

Devices

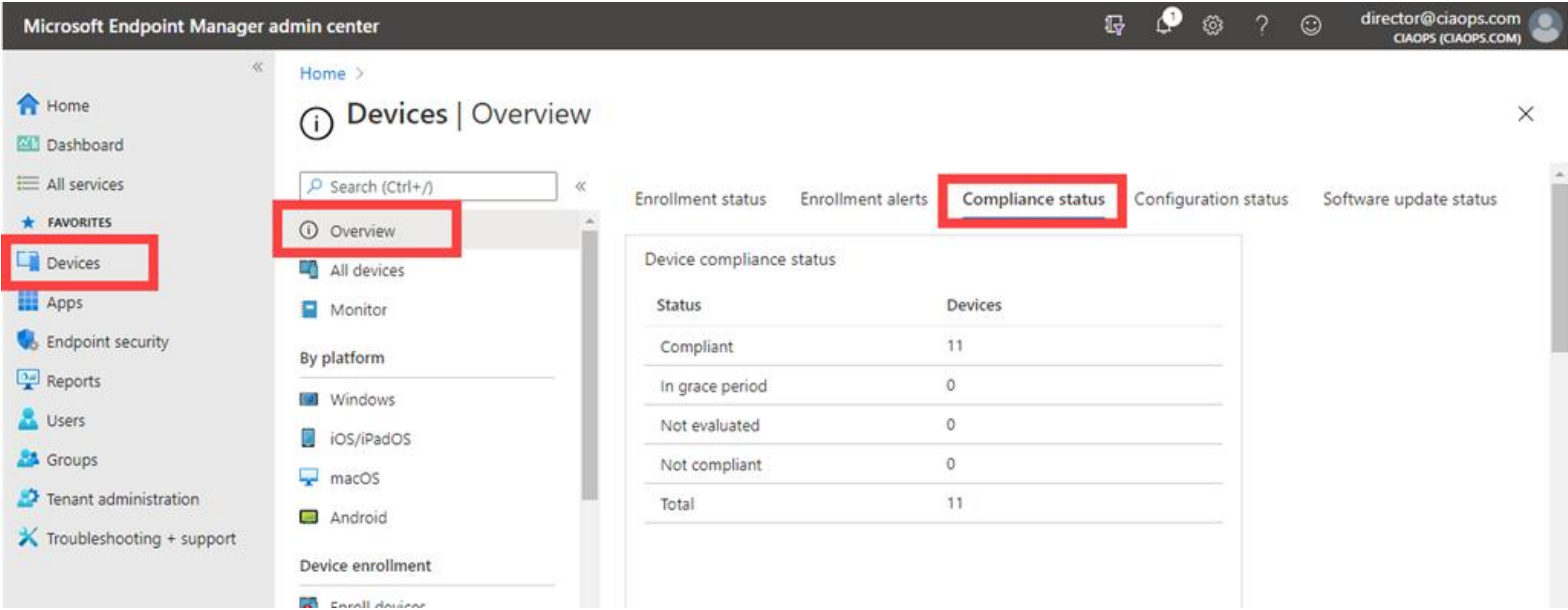
Enrolment

Compliance

Configuration

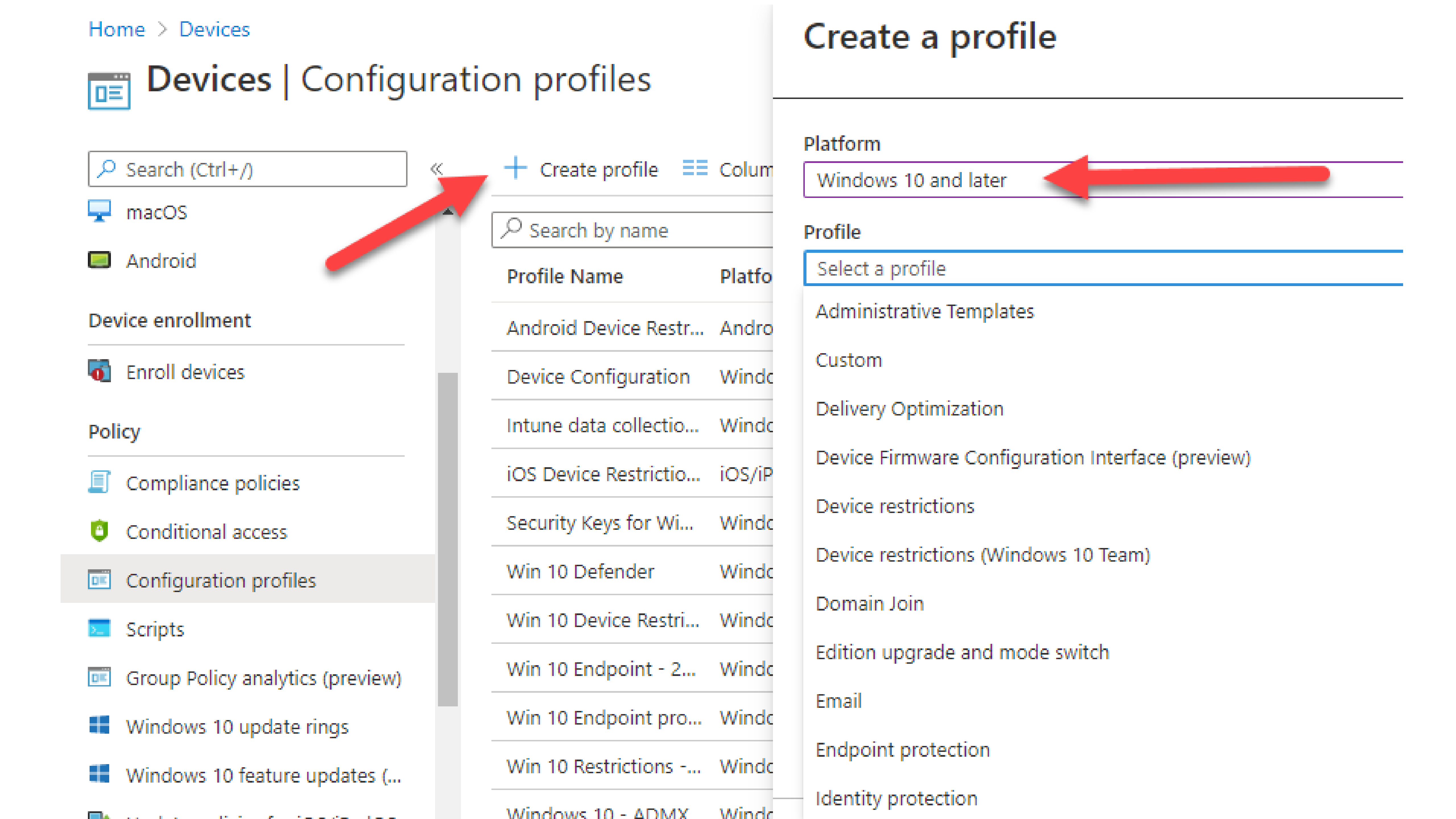


Profile Name	Platform	Profile Type	Assigned	Last Modified	
Android Device Restr...	Android device admi...	Device restrictions	Yes	1/14/19, 12:43 PM	•••
Device Configuration	Windows 10 and later	Device Firmware Con...	Yes	3/04/20, 11:58 AM	•••
Intune data collectio...	Windows 10 and later	Windows health mo...	Yes	8/17/20, 5:19 PM	•••
iOS Device Restrictio...	iOS/iPadOS	Device restrictions	Yes	3/01/19, 3:53 PM	•••
Security Keys for Wi...	Windows 10 and later	Custom	Yes	7/26/19, 11:04 PM	•••
Win 10 Defender	Windows 10 and later	Microsoft Defender ...	Yes	10/07/19, 8:50 AM	•••
Win 10 Device Restri...	Windows 10 and later	Device restrictions	Yes	9/18/20, 2:47 PM	•••



Device compliance status

Status	Devices
Compliant	11
In grace period	0
Not evaluated	0
Not compliant	0
Total	11



Home > Devices

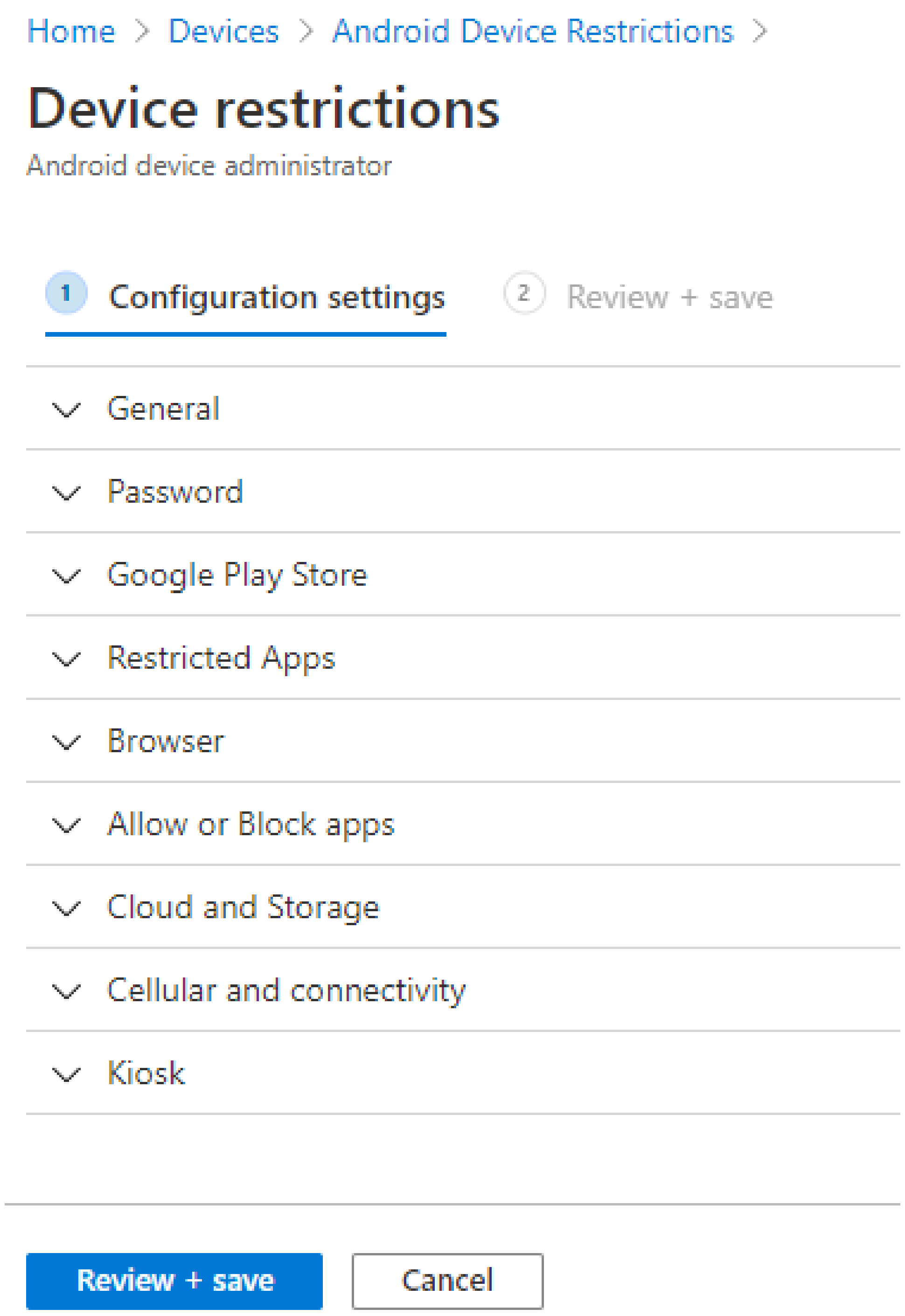
Devices | Configuration profiles

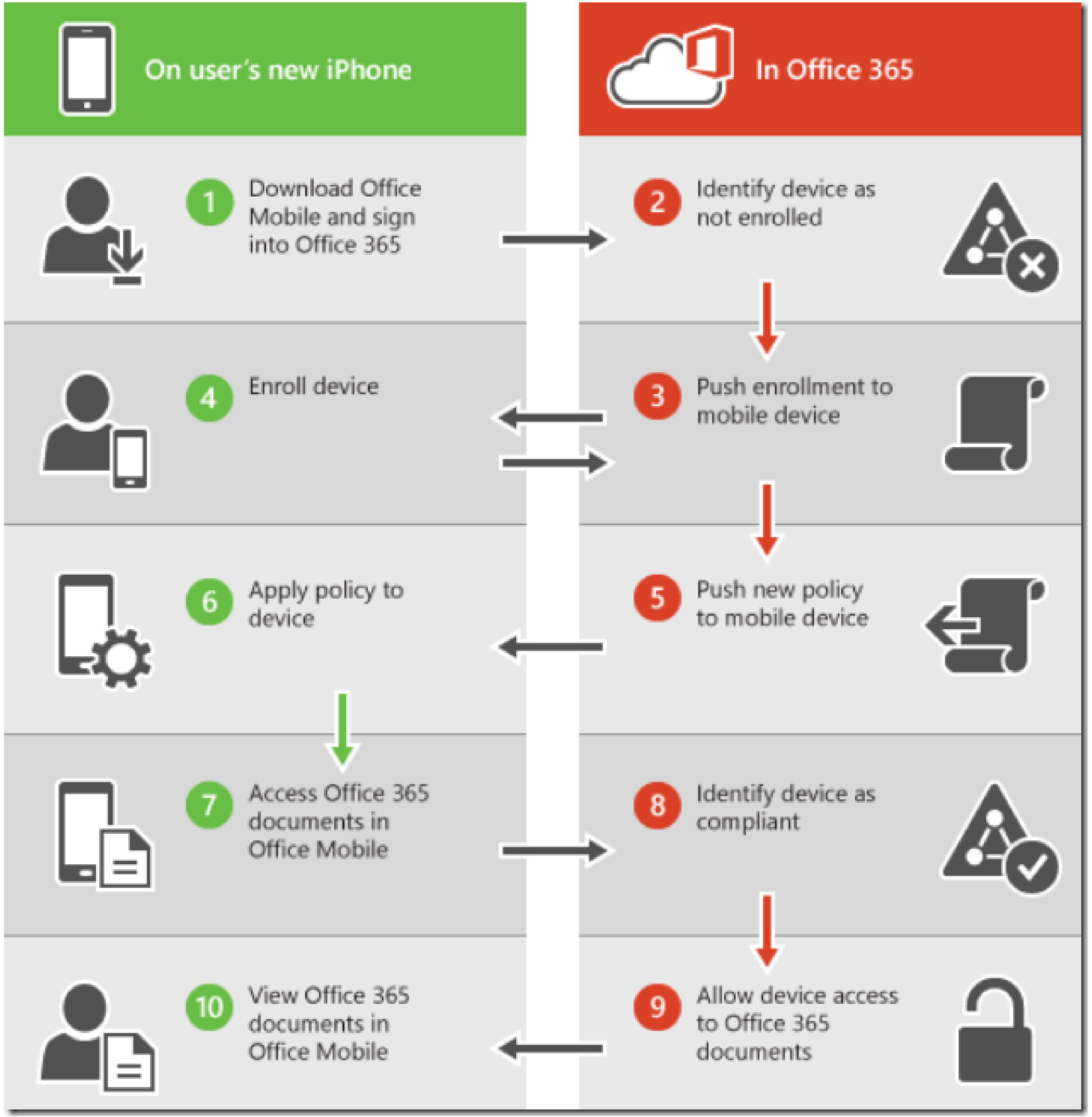
Profile Name	Platfo
Android Device Restr...	Andro
Device Configuration	Windc
Intune data collectio...	Windc
iOS Device Restrictio...	iOS/iP
Security Keys for Wi...	Windc
Win 10 Defender	Windc
Win 10 Device Restri...	Windc
Win 10 Endpoint - 2...	Windc
Win 10 Endpoint pro...	Windc
Win 10 Restrictions -...	Windc
Windows 10 - ADMX	Windc

Create a profile

Platform: Windows 10 and later

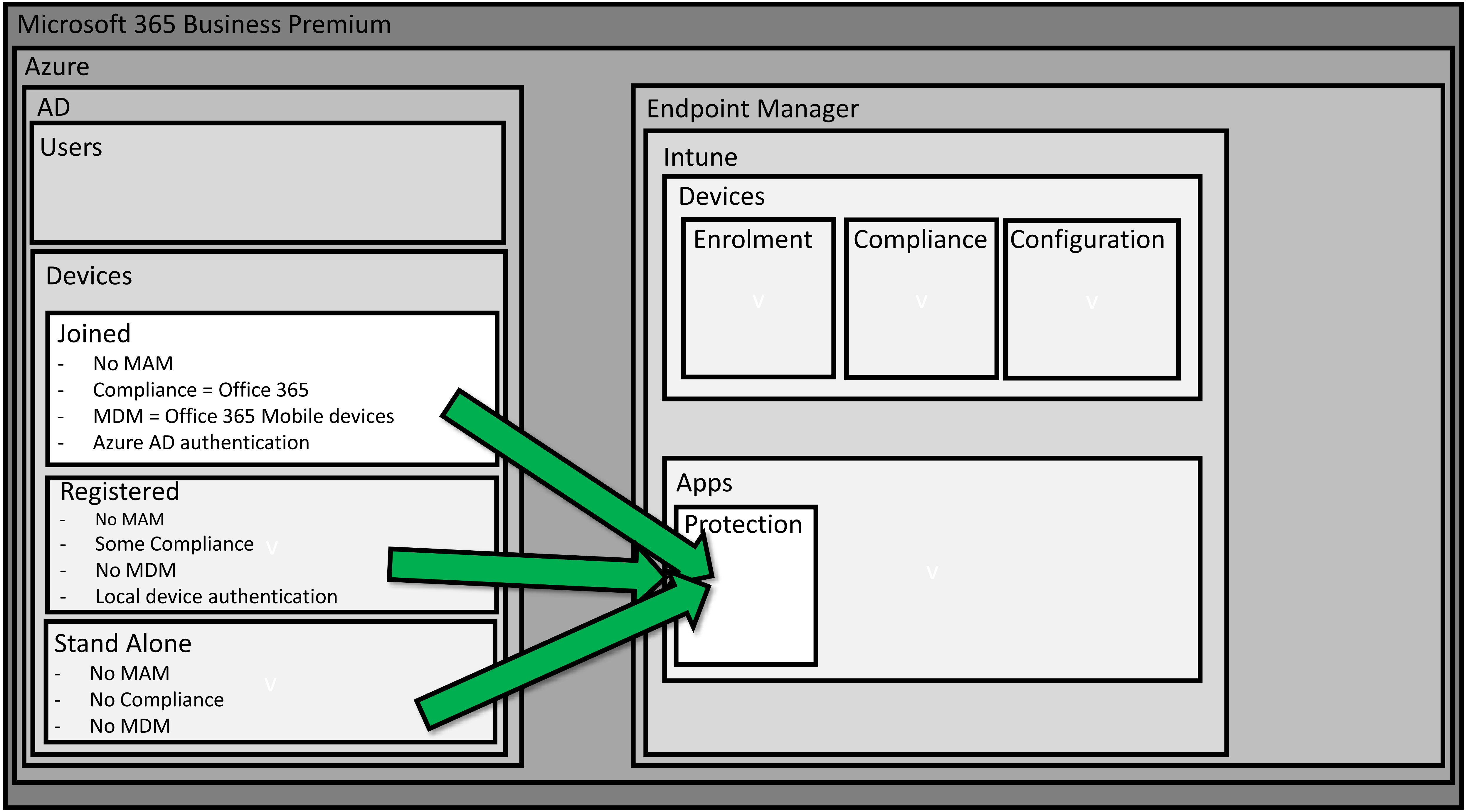
Profile: Select a profile


Home > Devices > Android Device Restrictions >
Device restrictions
Android device administrator
1 Configuration settings
2 Review + save
General
Password
Google Play Store
Restricted Apps
Browser
Allow or Block apps
Cloud and Storage
Cellular and connectivity
Kiosk
Review + save
Cancel


On user's new iPhone
In Office 365
1 Download Office Mobile and sign into Office 365
2 Identify device as not enrolled
3 Push enrollment to mobile device
4 Enroll device
5 Push new policy to mobile device
6 Apply policy to device
7 Access Office 365 documents in Office Mobile
8 Identify device as compliant
9 Allow device access to Office 365 documents
10 View Office 365 documents in Office Mobile

Intune Resources

- Adding an Apple Certificate to Intune
- Use compliance policies to set rules for devices you manage with Intune
- Create a device profile in Microsoft Intune



Microsoft 365 Business Premium

Azure

AD

Users

Devices

Joined

- No MAM
- Compliance = Office 365
- MDM = Office 365 Mobile devices
- Azure AD authentication

Registered

- No MAM
- Some Compliance v
- No MDM
- Local device authentication

Stand Alone

- No MAM v
- No Compliance
- No MDM

Endpoint Manager

Intune

Devices

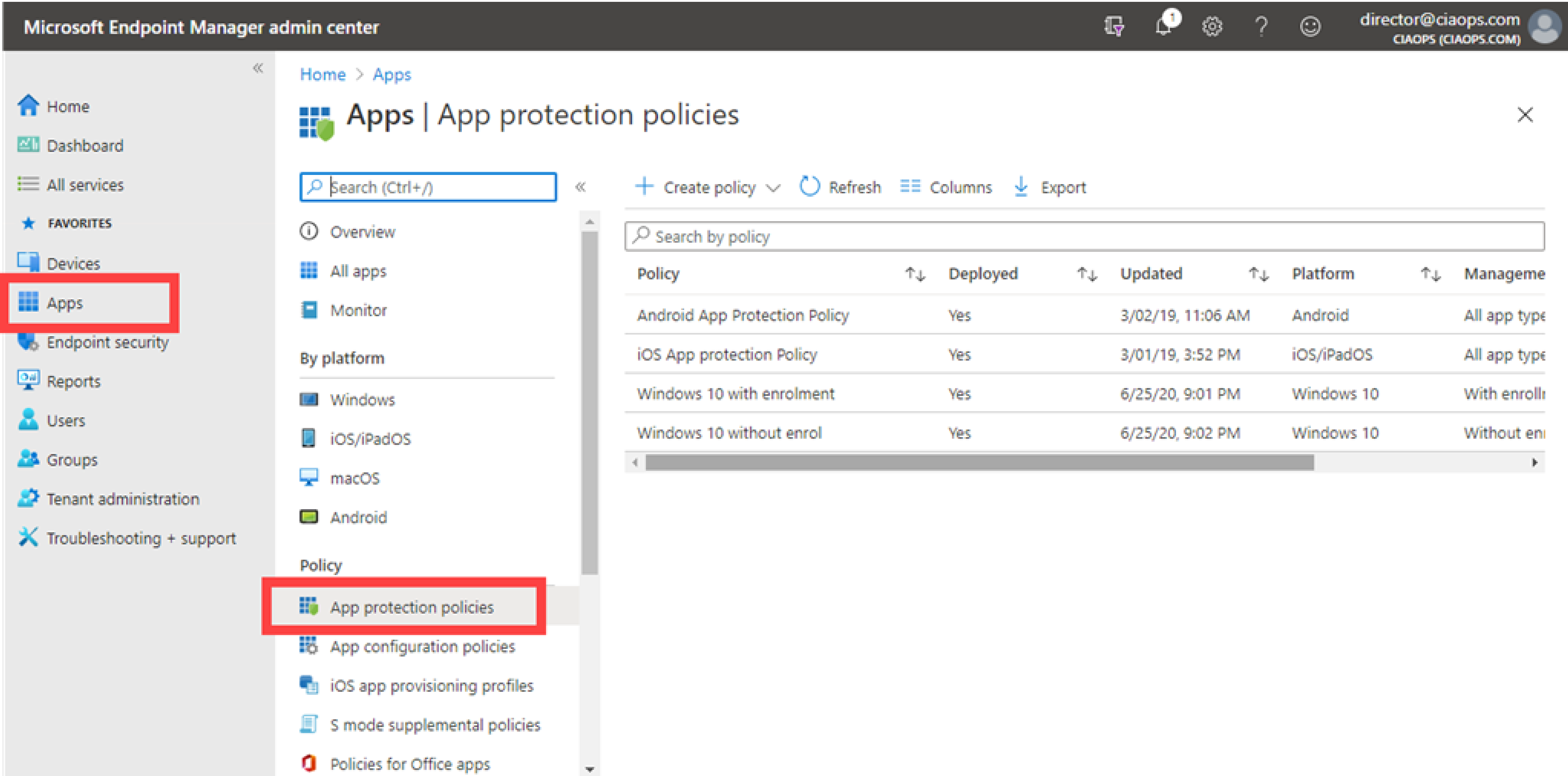
Enrolment v

Compliance v

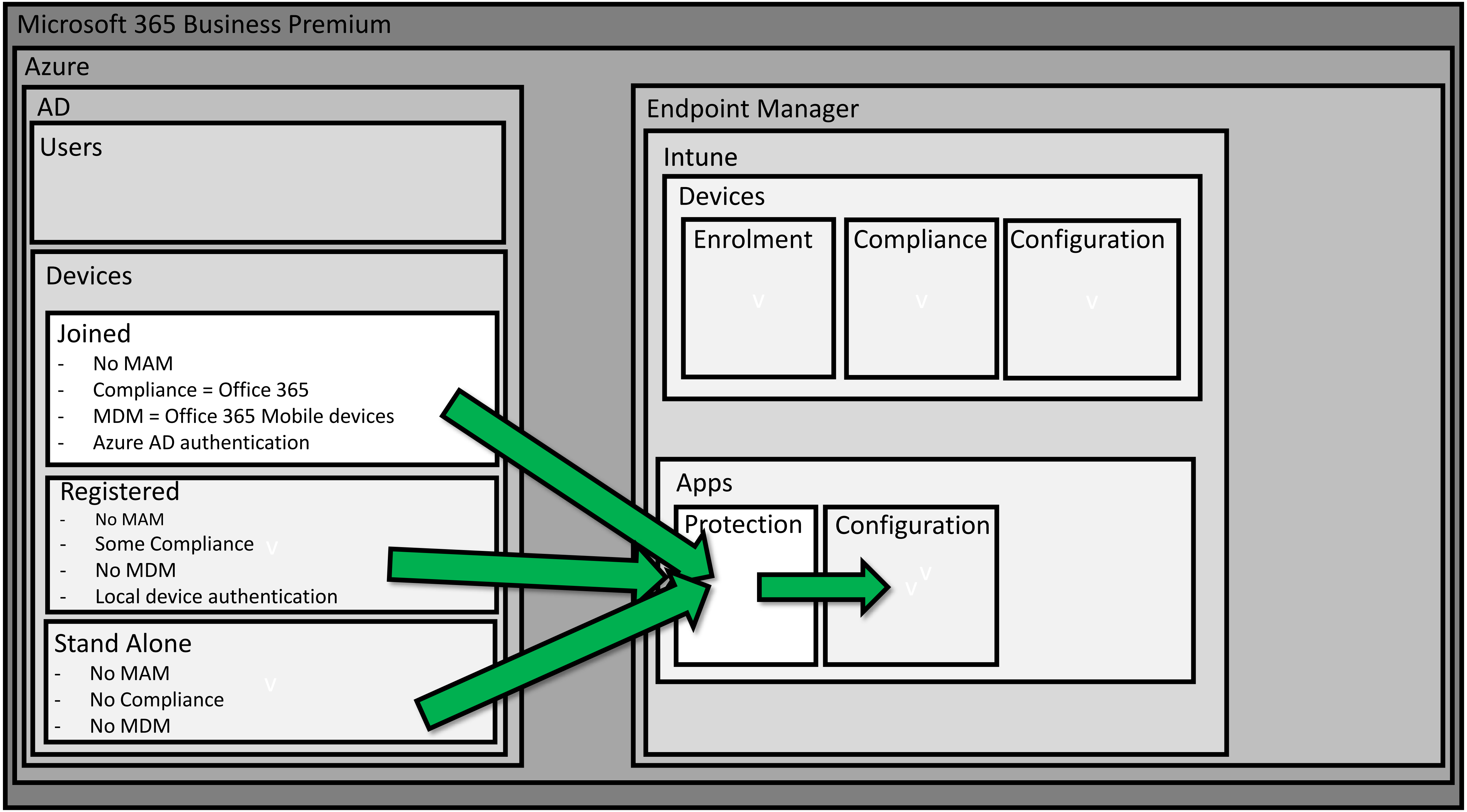
Configuration v

Apps v

Protection



Policy	Deployed	Updated	Platform	Manageme
Android App Protection Policy	Yes	3/02/19, 11:06 AM	Android	All app type
iOS App protection Policy	Yes	3/01/19, 3:52 PM	iOS/iPadOS	All app type
Windows 10 with enrolment	Yes	6/25/20, 9:01 PM	Windows 10	With enrolli
Windows 10 without enrol	Yes	6/25/20, 9:02 PM	Windows 10	Without enr



Microsoft 365 Business Premium

Azure

AD

Users

Devices

Joined
- No MAM
- Compliance = Office 365
- MDM = Office 365 Mobile devices
- Azure AD authentication

Registered
- No MAM
- Some Compliance
- No MDM
- Local device authentication

Stand Alone
- No MAM
- No Compliance
- No MDM

Endpoint Manager

Intune

Devices

Enrolment

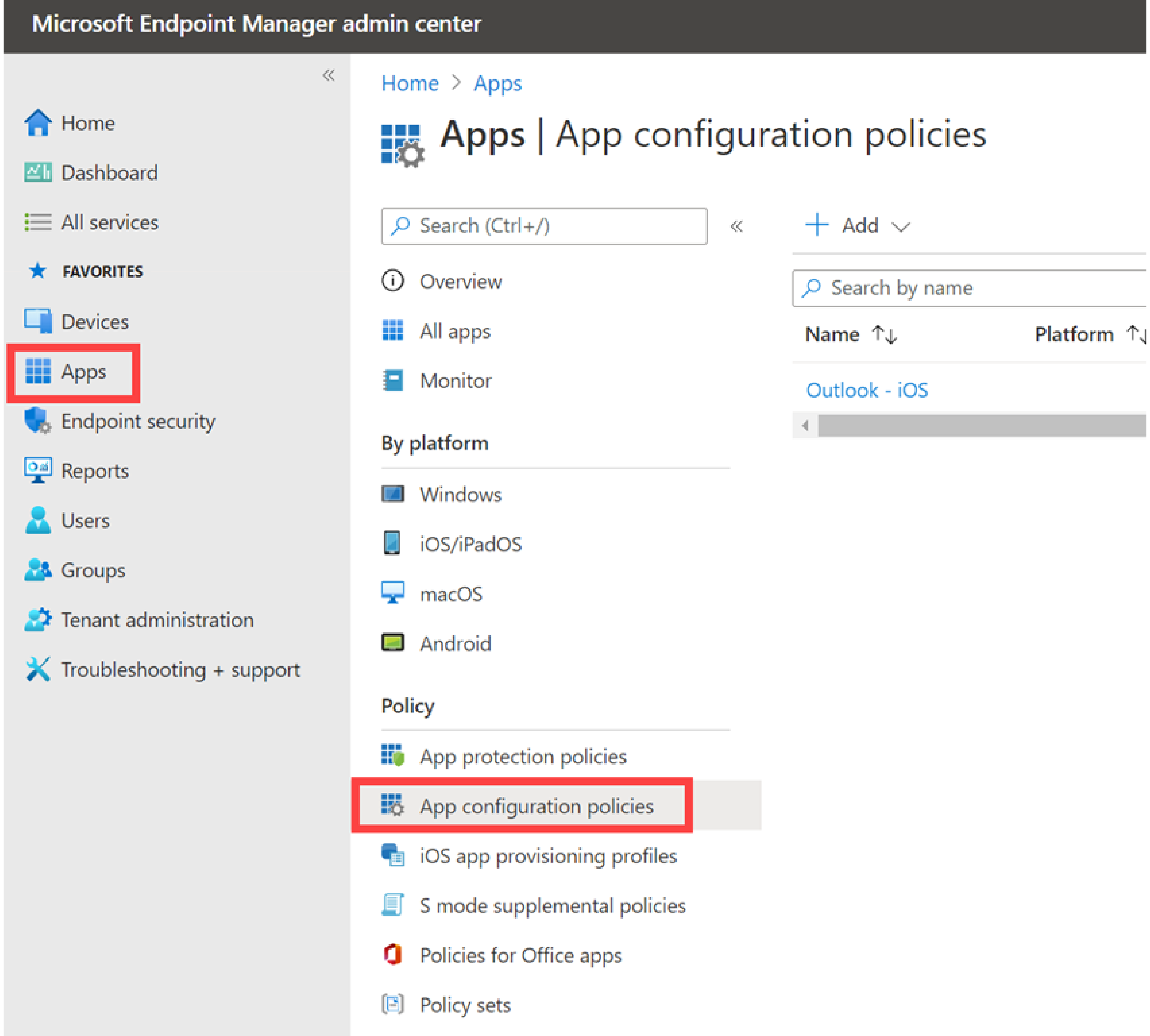
Compliance

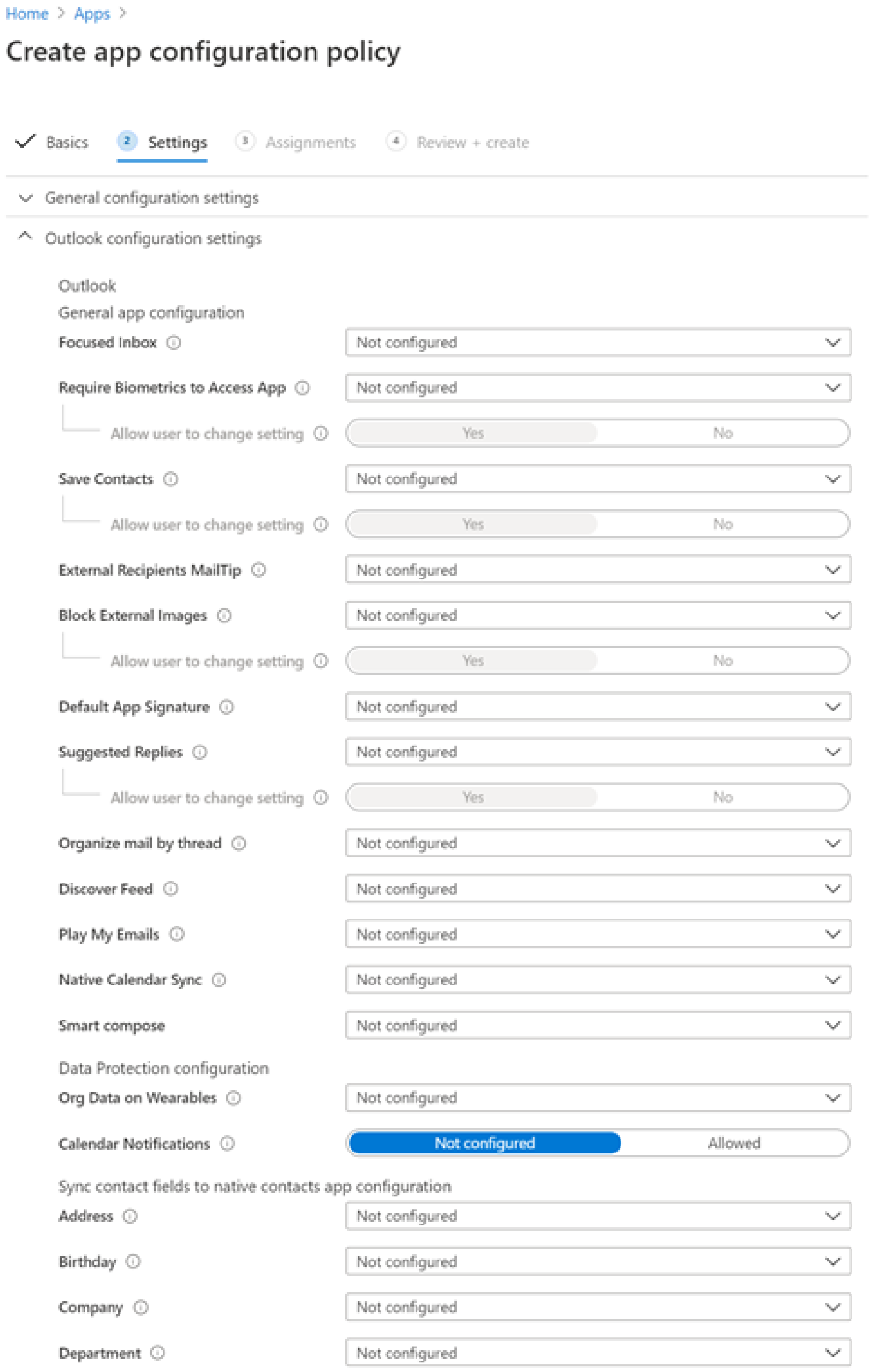
Configuration

Apps

Protection

Configuration


Microsoft Endpoint Manager admin center
Home
Dashboard
All services
FAVORITES
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Apps
Apps | App configuration policies
Search (Ctrl+/)
Overview
All apps
Monitor
By platform
Windows
iOS/iPadOS
macOS
Android
Policy
App protection policies
App configuration policies
iOS app provisioning profiles
S mode supplemental policies
Policies for Office apps
Policy sets
+ Add
Search by name
Name
Platform
Outlook - iOS



Create app configuration policy

General configuration settings
Outlook configuration settings

Outlook

General app configuration

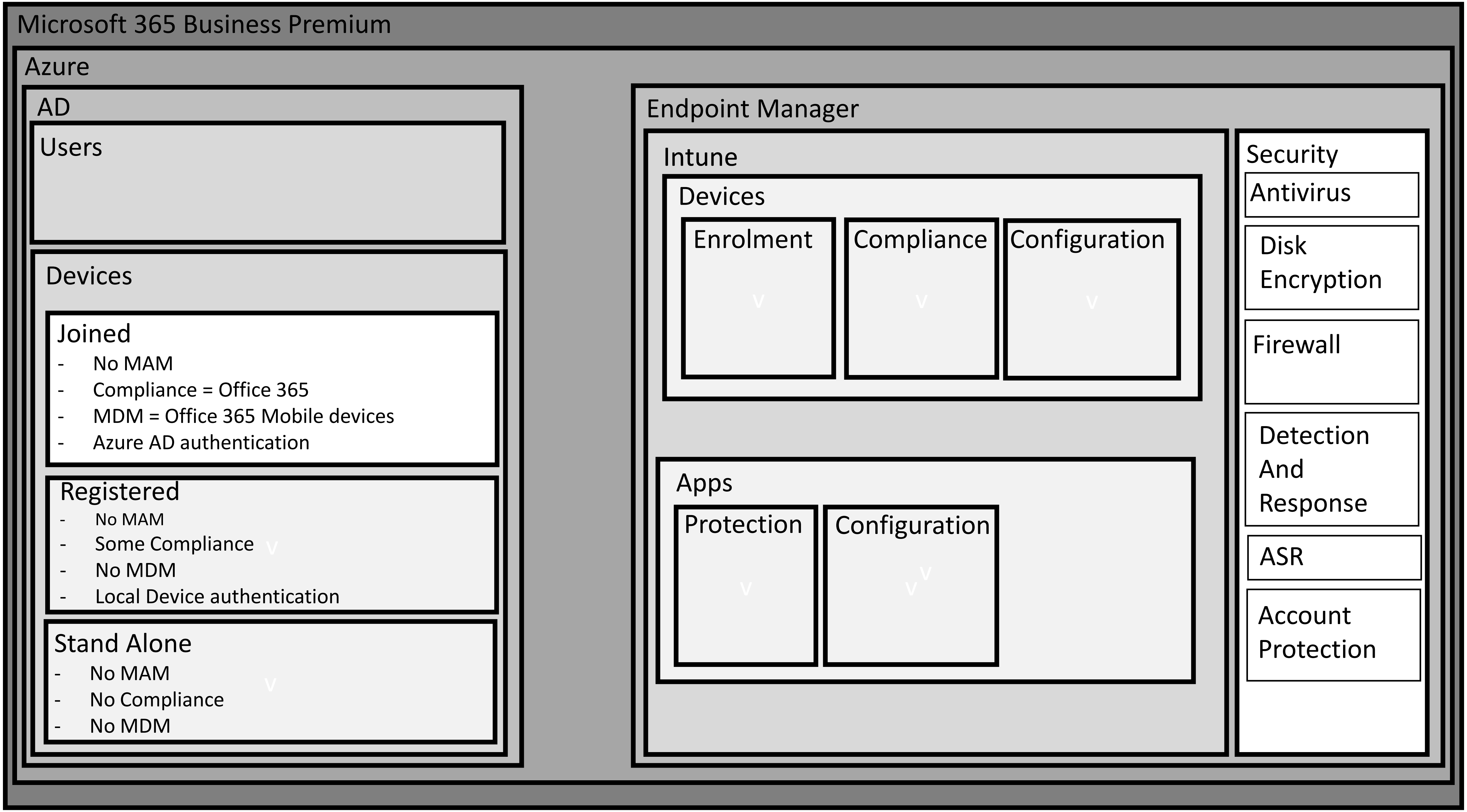
Focused Inbox ⓘ	Not configured
Require Biometrics to Access App ⓘ	Not configured
Allow user to change setting ⓘ	Yes / No
Save Contacts ⓘ	Not configured
Allow user to change setting ⓘ	Yes / No
External Recipients MailTip ⓘ	Not configured
Block External Images ⓘ	Not configured
Allow user to change setting ⓘ	Yes / No
Default App Signature ⓘ	Not configured
Suggested Replies ⓘ	Not configured
Allow user to change setting ⓘ	Yes / No
Organize mail by thread ⓘ	Not configured
Discover Feed ⓘ	Not configured
Play My Emails ⓘ	Not configured
Native Calendar Sync ⓘ	Not configured
Smart compose	Not configured

Data Protection configuration

Org Data on Wearables ⓘ	Not configured
Calendar Notifications ⓘ	[✓ Not configured] Allowed

Sync contact fields to native contacts app configuration

Address ⓘ	Not configured
Birthday ⓘ	Not configured
Company ⓘ	Not configured
Department ⓘ	Not configured



Microsoft 365 Business Premium

Azure

AD

Users

Devices

Joined
- No MAM
- Compliance = Office 365
- MDM = Office 365 Mobile devices
- Azure AD authentication

Registered
- No MAM
- Some Compliance
- No MDM
- Local Device authentication

Stand Alone
- No MAM
- No Compliance
- No MDM

Endpoint Manager

Intune

Devices

Enrolment

Compliance

Configuration

Apps

Protection

Configuration

Security

Antivirus

Disk Encryption

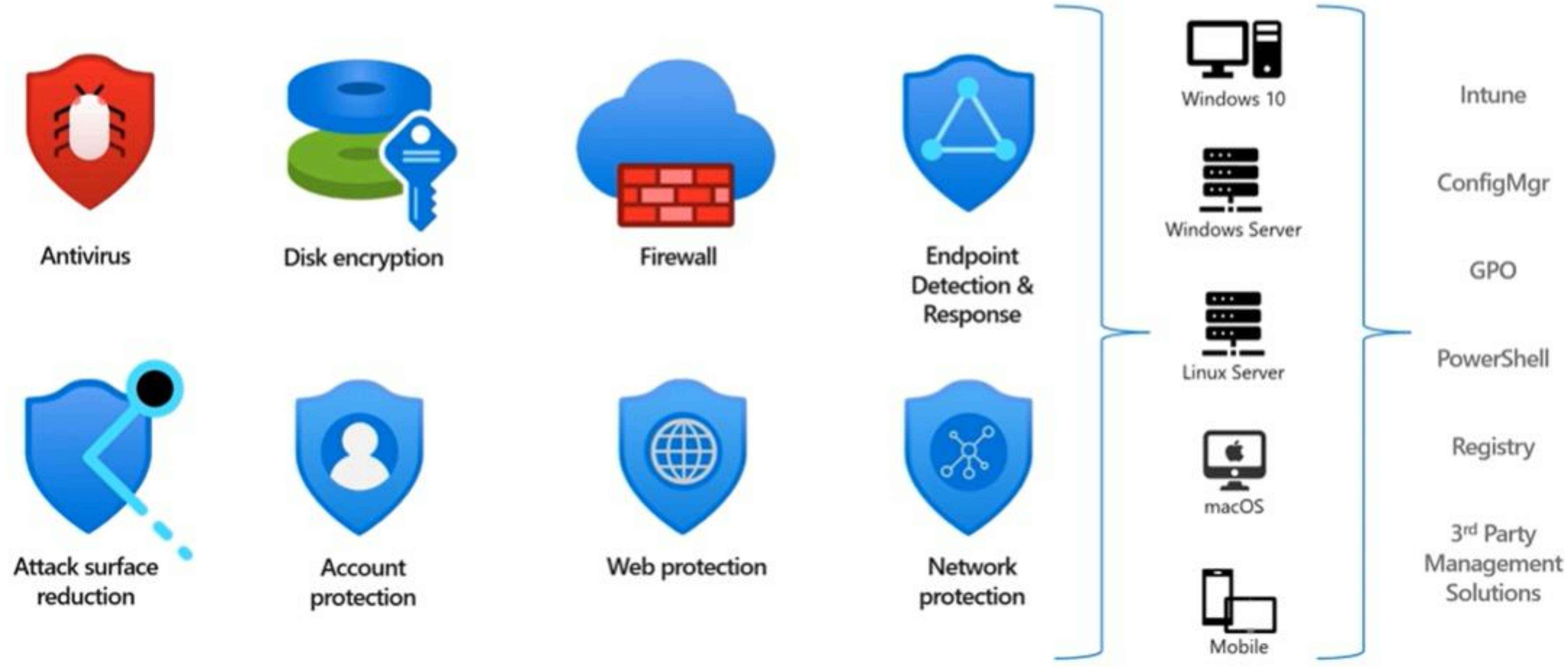
Firewall

Detection And Response

ASR

Account Protection

Endpoint Security at a glance



Antivirus

Disk encryption

Firewall

Endpoint Detection & Response

Attack surface reduction

Account protection

Web protection

Network protection

Windows 10

Windows Server

Linux Server

macOS

Mobile

Intune

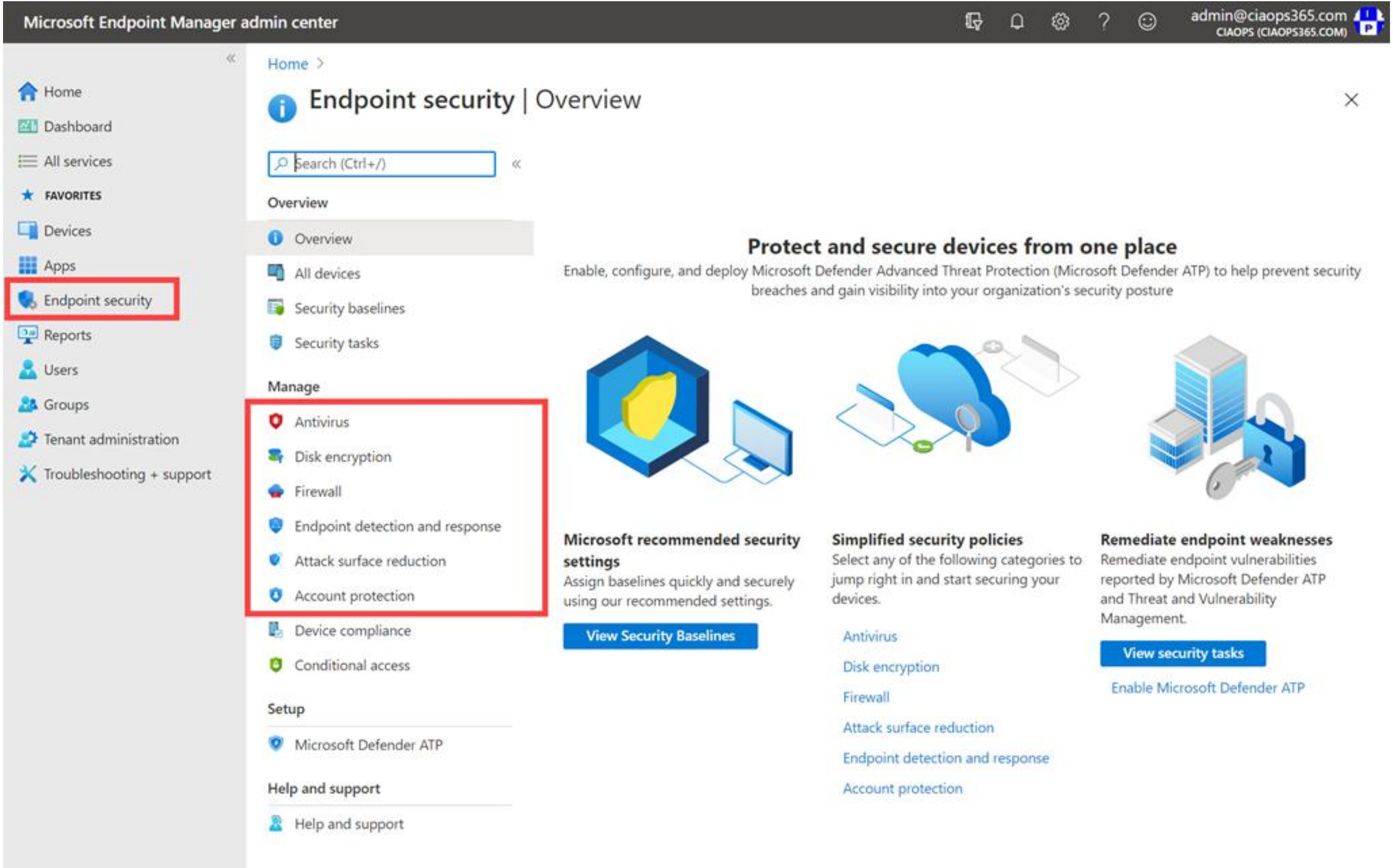
ConfigMgr

GPO

PowerShell

Registry

3rd Party Management Solutions



Endpoint security | Overview

Protect and secure devices from one place

Enable, configure, and deploy Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP) to help prevent security breaches and gain visibility into your organization's security posture

Microsoft recommended security settings

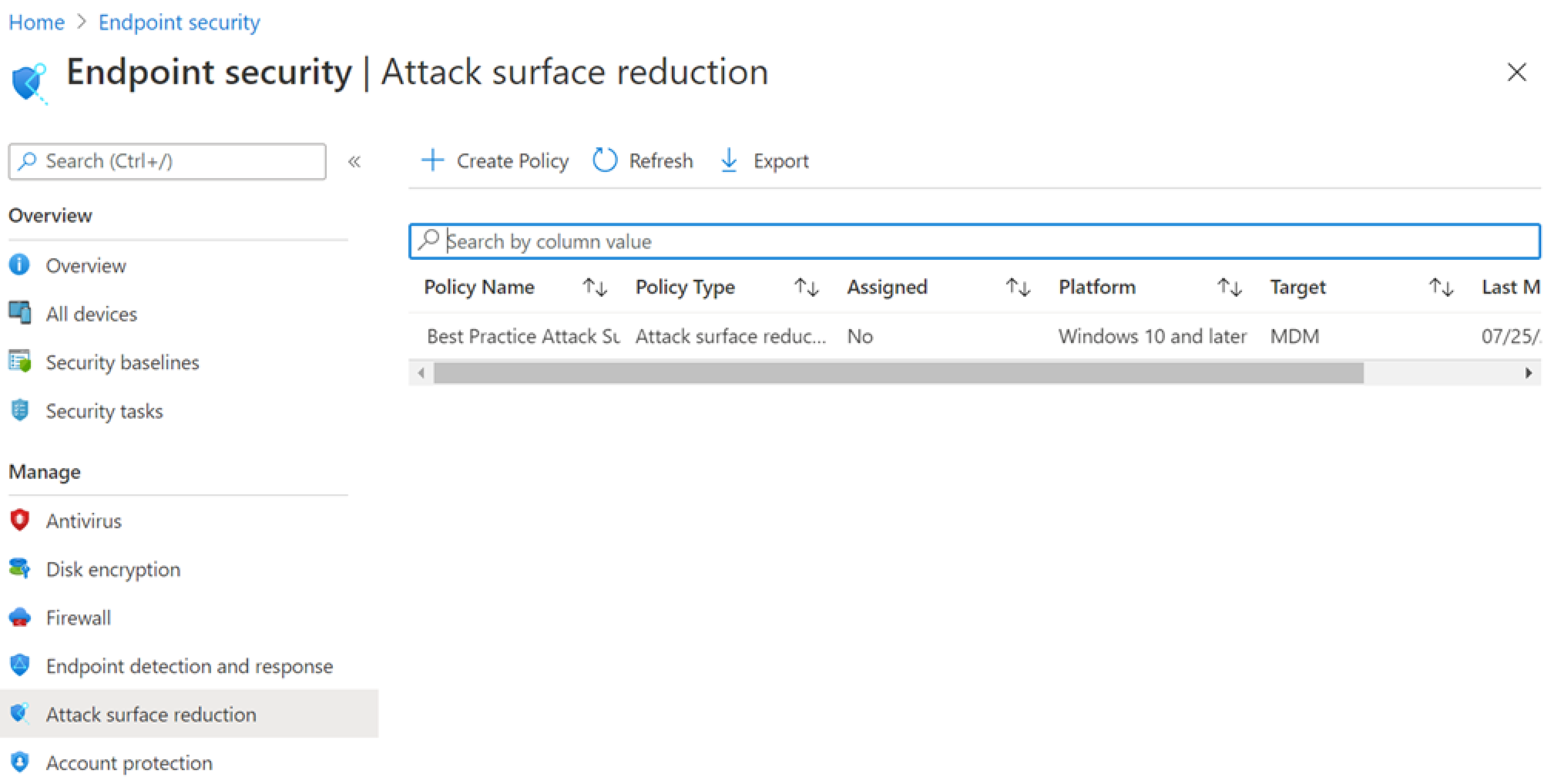
Assign baselines quickly and securely using our recommended settings.

Simplified security policies

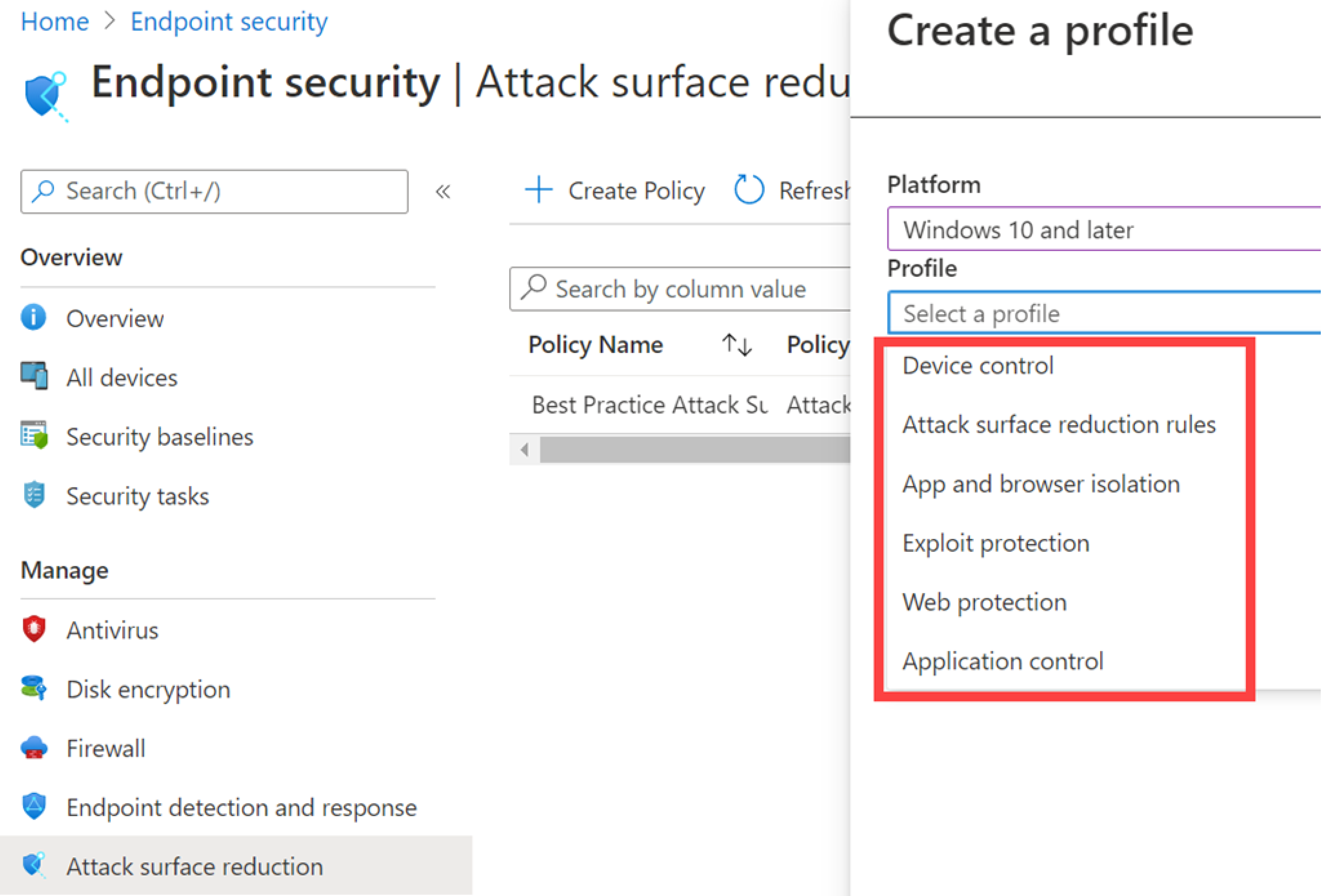
Select any of the following categories to jump right in and start securing your devices.

Remediate endpoint weaknesses

Remediate endpoint vulnerabilities reported by Microsoft Defender ATP and Threat and Vulnerability Management.



Policy Name ↑↓	Policy Type ↑↓	Assigned ↑↓	Platform ↑↓	Target ↑↓	Last M
Best Practice Attack Su	Attack surface reduc...	No	Windows 10 and later	MDM	07/25/



Home > Endpoint security

Endpoint security | Attack surface redu

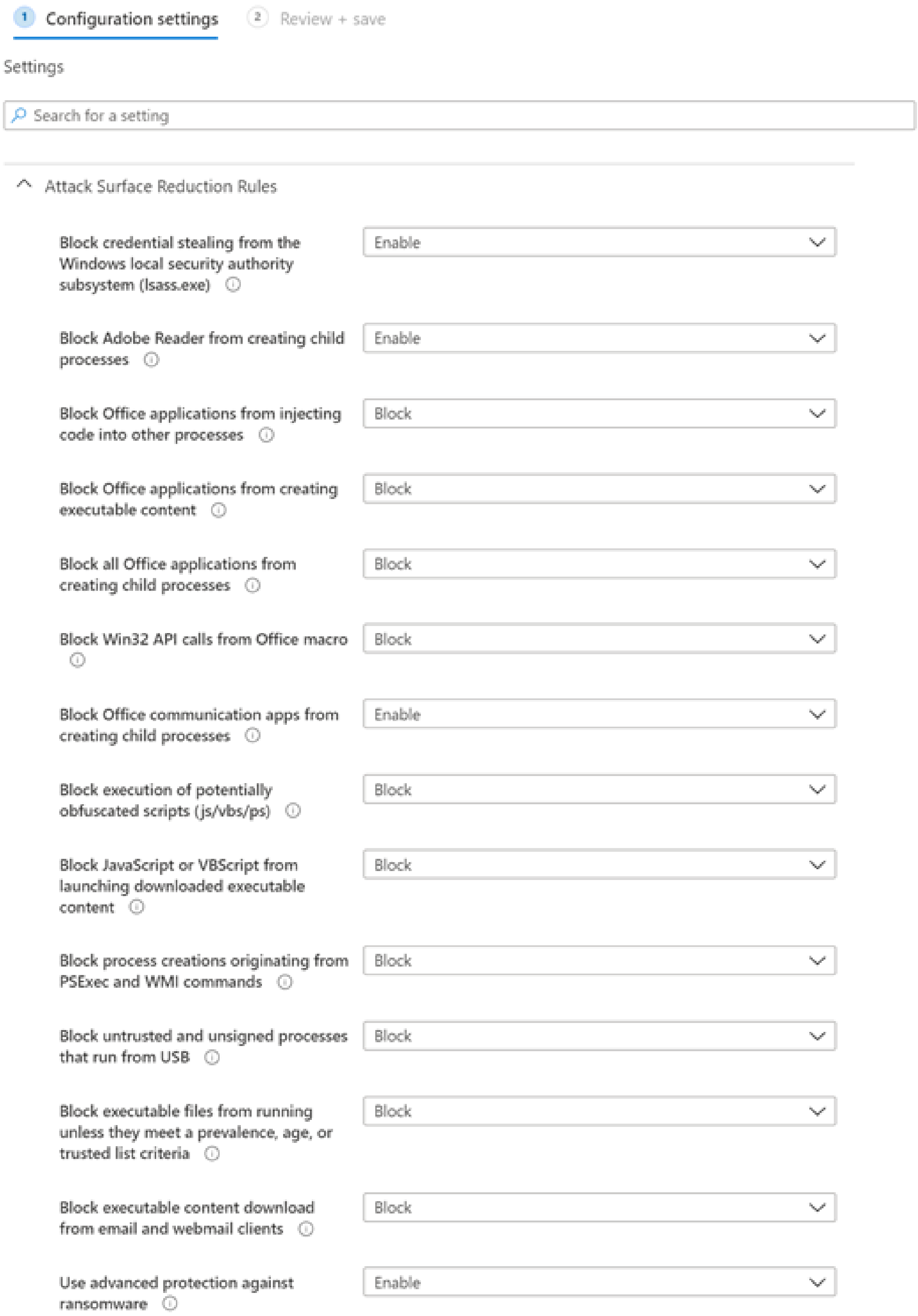
Policy Name	Policy
Best Practice Attack Su	Attack

Create a profile

Platform: Windows 10 and later

Profile: Select a profile

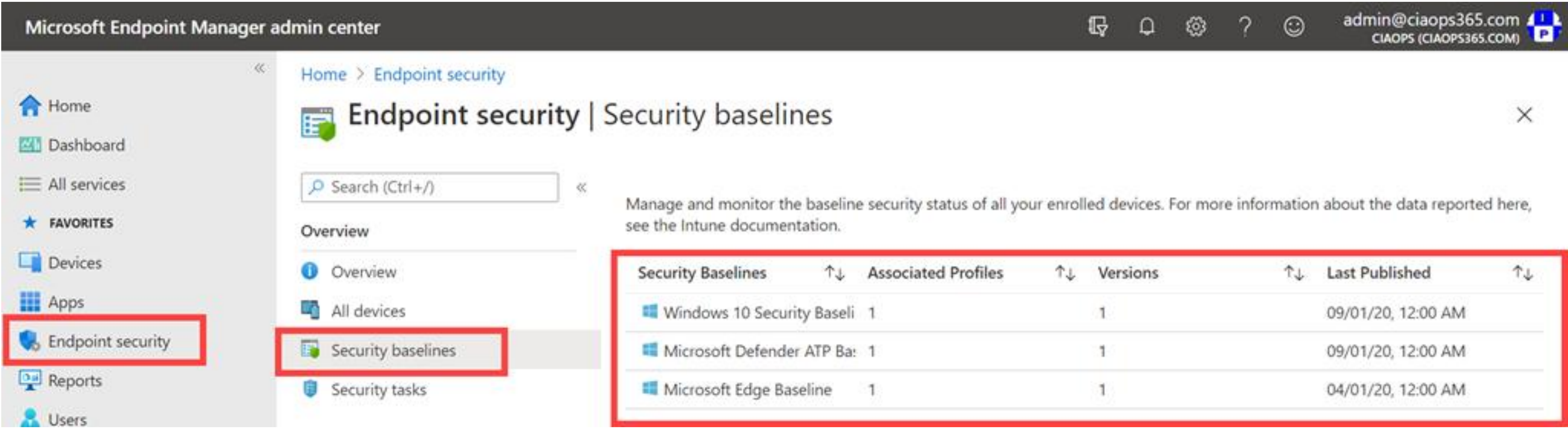
- Device control
- Attack surface reduction rules
- App and browser isolation
- Exploit protection
- Web protection
- Application control



Settings

Attack Surface Reduction Rules

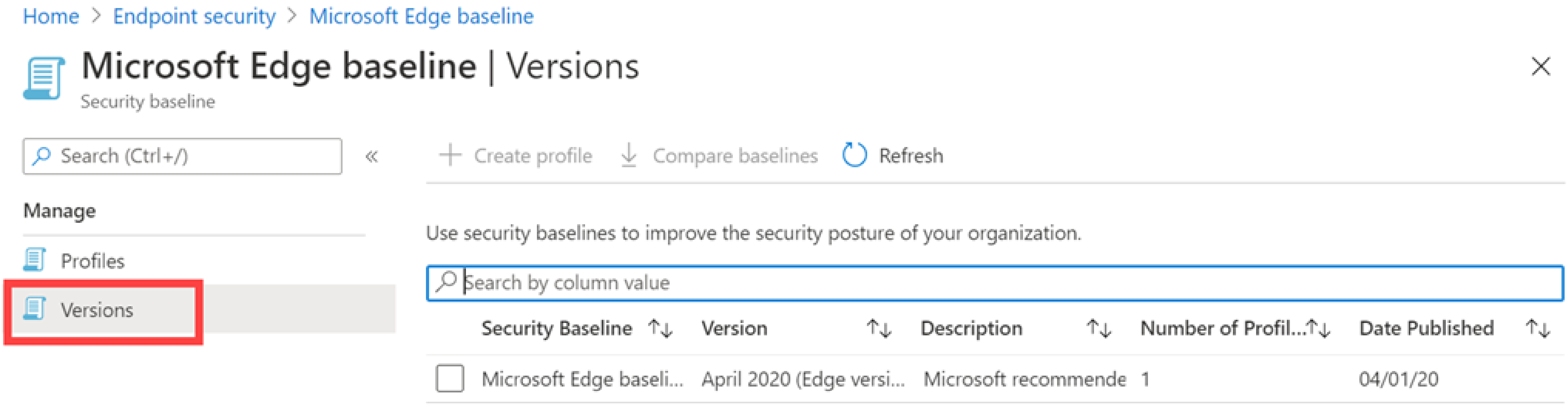
Block credential stealing from the Windows local security authority subsystem (lsass.exe)	Enable
Block Adobe Reader from creating child processes	Enable
Block Office applications from injecting code into other processes	Block
Block Office applications from creating executable content	Block
Block all Office applications from creating child processes	Block
Block Win32 API calls from Office macro	Block
Block Office communication apps from creating child processes	Enable
Block execution of potentially obfuscated scripts (js/vbs/ps)	Block
Block JavaScript or VBScript from launching downloaded executable content	Block
Block process creations originating from PSExec and WMI commands	Block
Block untrusted and unsigned processes that run from USB	Block
Block executable files from running unless they meet a prevalence, age, or trusted list criteria	Block
Block executable content download from email and webmail clients	Block
Use advanced protection against ransomware	Enable



Endpoint security | Security baselines

Manage and monitor the baseline security status of all your enrolled devices. For more information about the data reported here, see the Intune documentation.

Security Baselines	Associated Profiles	Versions	Last Published
Windows 10 Security Baseli	1	1	09/01/20, 12:00 AM
Microsoft Defender ATP Ba:	1	1	09/01/20, 12:00 AM
Microsoft Edge Baseline	1	1	04/01/20, 12:00 AM



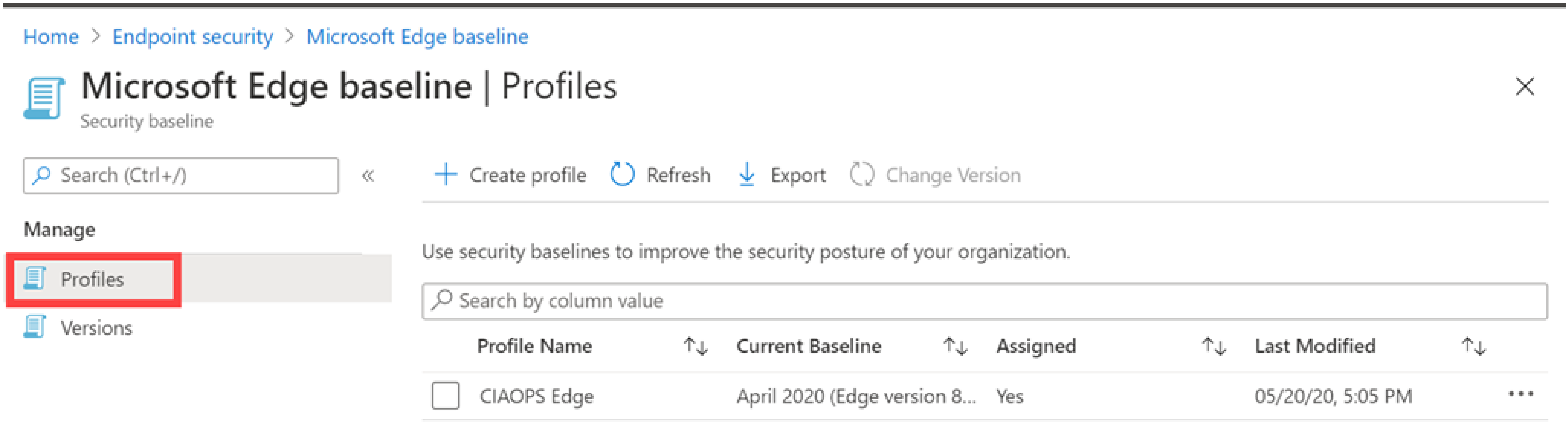
Microsoft Edge baseline | Versions

Security baseline

Use security baselines to improve the security posture of your organization.

Search by column value

	Security Baseline ↑↓	Version ↑↓	Description ↑↓	Number of Profil...↑↓	Date Published ↑↓
□	Microsoft Edge baseli...	April 2020 (Edge versi...	Microsoft recommende	1	04/01/20



Use security baselines to improve the security posture of your organization.

	Profile Name ↑↓	Current Baseline ↑↓	Assigned ↑↓	Last Modified ↑↓	
□	CIAOPS Edge	April 2020 (Edge version 8...	Yes	05/20/20, 5:05 PM	•••

Recommendations

- Maintain good documentation
- Define a naming convention up front and apply consistently
- Apply policies and updates in rings
- Ensure you have a ‘break glass’ account configured
- Grow into your settings

For resellers

- Have at least one physical device for each OS
- Use a demo tenant first time out
- Fully implement device management in your own production environment
- Configuration is never complete
- Leverage the power of automation

Resources

- Microsoft Endpoint Manager overview - https://docs.microsoft.com/en-us/mem/endpoint-manager-overview
- Windows 10 in cloud configuration - https://www.microsoft.com/en-au/microsoft-365/windows/cloud-configuration
- Unpacking endpoint management: the series – https://techcommunity.microsoft.com/t5/microsoft-endpoint-manager-blog/unpacking-endpoint-management-the-series/ba-p/2200356
- Microsoft Endpoint Manager documentation – https://docs.microsoft.com/en-us/mem/
- Device compliance docuemtation - https://docs.microsoft.com/en-us/mem/configmgr/compliance/

CIAOPS Resources

- Blog – http://blog.ciaops.com
- Github – http://github.com/directorcia
- Free Office 365, Azure Administration newsletter – http://bit.ly/cia-o365-tech
- Free Office 365, Azure video tutorials – http://www.youtube.com/directorciaops
- Free documents, presentations, eBooks – http://slideshare.net/directorcia
- Office 365, Azure, Cloud podcast – http://ciaops.podbean.com
- Office 365, Azure online training courses – http://www.ciaopsacademy.com
- Office 365 and Azure community – http://www.ciaopspatron.com

Twitter	Facebook	Email	Teams
@directorcia	https://www.facebook.com/ciaops	director@ciaops.com	admin@ciaops365.com