

#POWERCON2023

Microsoft Intune: gestione completa del
modern workplace

Nicola Ferrini
Microsoft MVP



/NicolaFerrini.it



@nicolaFerrini



/nicolaFerrini

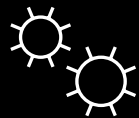
Agenda

- Microsoft Intune advantages
- New features

Microsoft Intune

A unified solution to manage endpoints anywhere

Simplify endpoint management



Protect a hybrid workforce



Power better user experiences



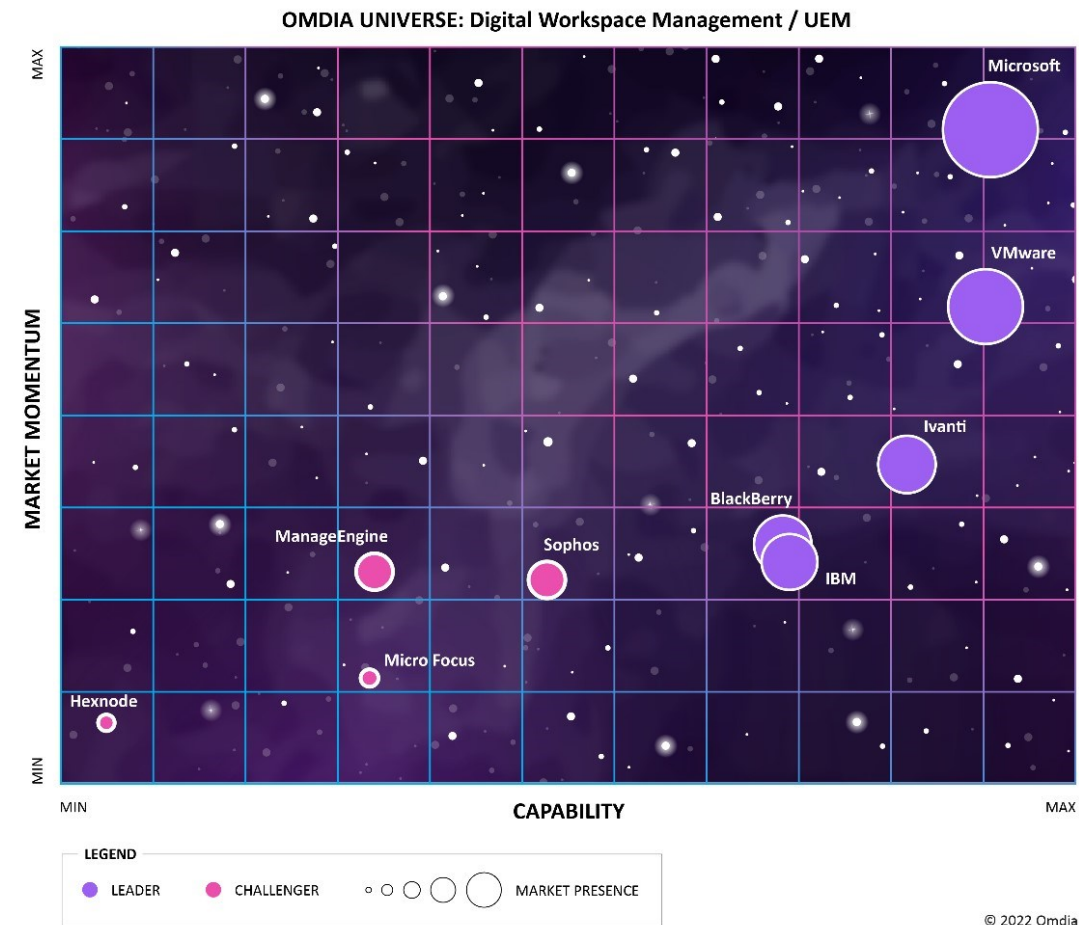
Microsoft is recognized as a leader for UEM tools

2022 Gartner® Magic Quadrant™ for Unified Endpoint Management Tools



Source: Gartner (August 2022)

2023 OMDIA UNIVERSE



Unified management saves time and resources

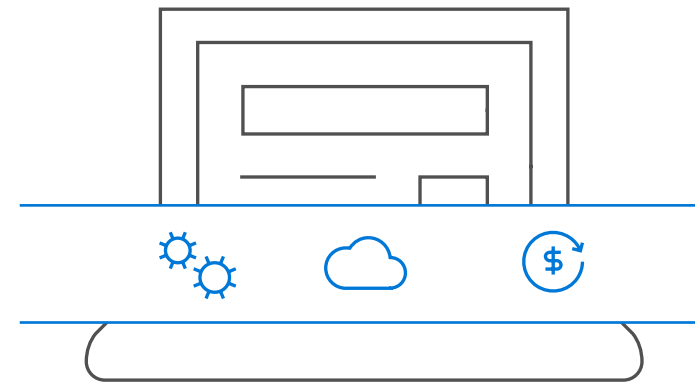
SIMPLIFY ENDPOINT MANAGEMENT 

Centrally manage on-premises and cloud-based endpoints.

Empower advanced endpoint management and security tools from a single, cloud-powered solution.

Reduce costs across hardware, licensing, maintenance.

Reduced IT time



Imagine if...

PROTECT A HYBRID WORKFORCE



...you could **protect hybrid workers** with integrated management and security

Today

- Growing attack surfaces
- Frequency of security breaches
- Complex corporate devices, BYOD, shared devices

The future powered by Microsoft Intune.

Data protection
regardless of
enrollment



Risk-based policies for
conditional access



Controls to enable
threat protection
across platforms



Integrated endpoint
security and compliance
for Zero Trust



Keep current, stay secure

PROTECT A HYBRID WORKFORCE



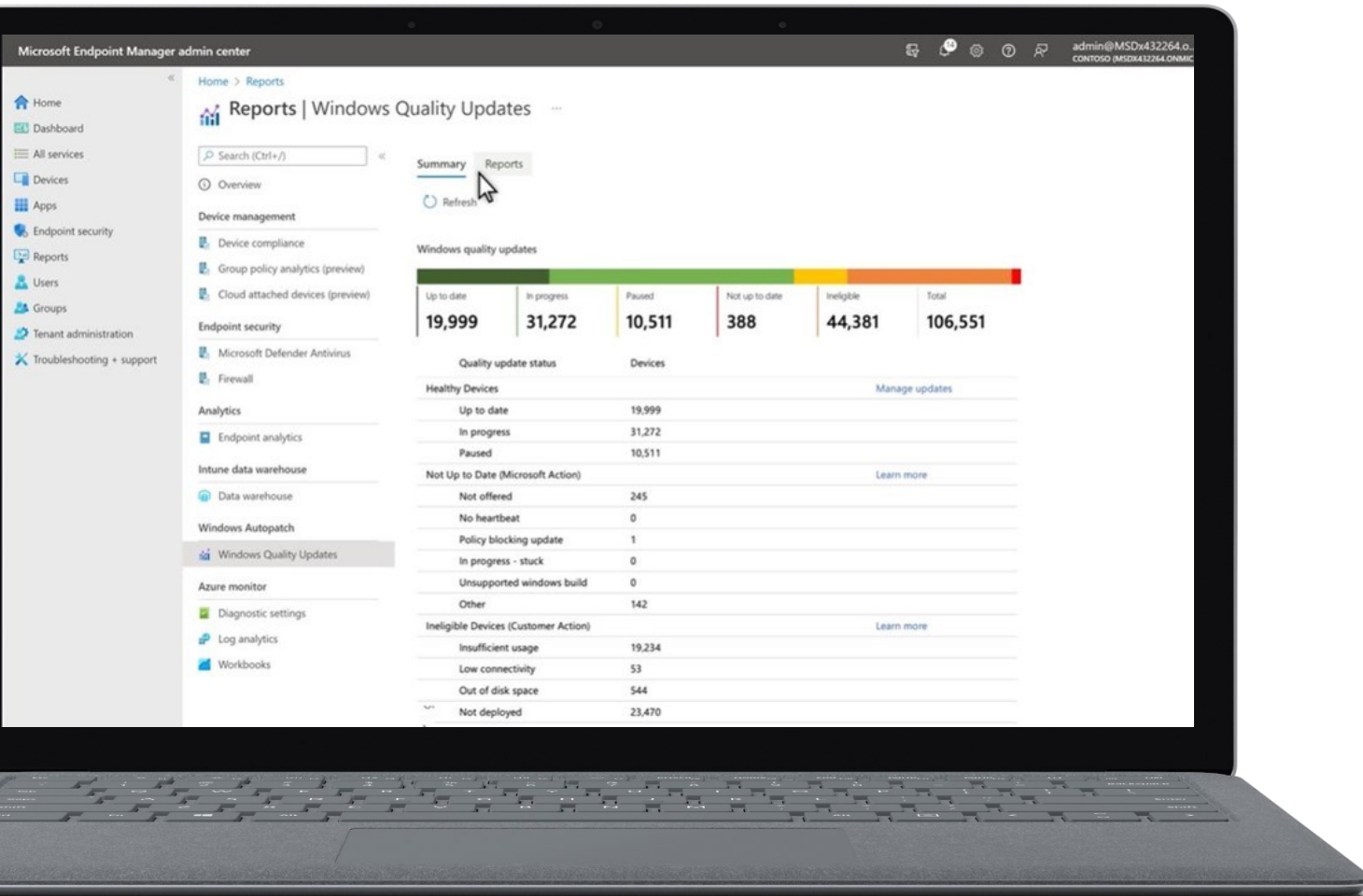
Automated updating gives time back to IT admins and peace of mind to security teams

Trust Microsoft to manage updates for Windows and Microsoft 365

Harden your posture against exploits and ransomware

Transparency and reporting keep you in control

Microsoft leverages insights to proactively address challenges and limit interruptions



Licensing

Intune Suite

Intune Plan 1

Included in EMS E3 or Microsoft 365 E3, ME5, F1, F3, and Business Premium plans



Intune Plan 2

Add to Plan 1 to utilize these features:

Included features

- Tunnel for Mobile App Management
- Specialty device management
- *Future advanced capabilities***

Prerequisite

- Intune Plan 1



Intune Suite

Add to Plan 1 to utilize these solutions

Included solutions*

- Remote help
- Endpoint Privilege Management
- Advanced Endpoint analytics
- Advanced app management
- Cloud certificate management
- *Future advanced solutions***
- All Intune Plan 2 features

Prerequisite

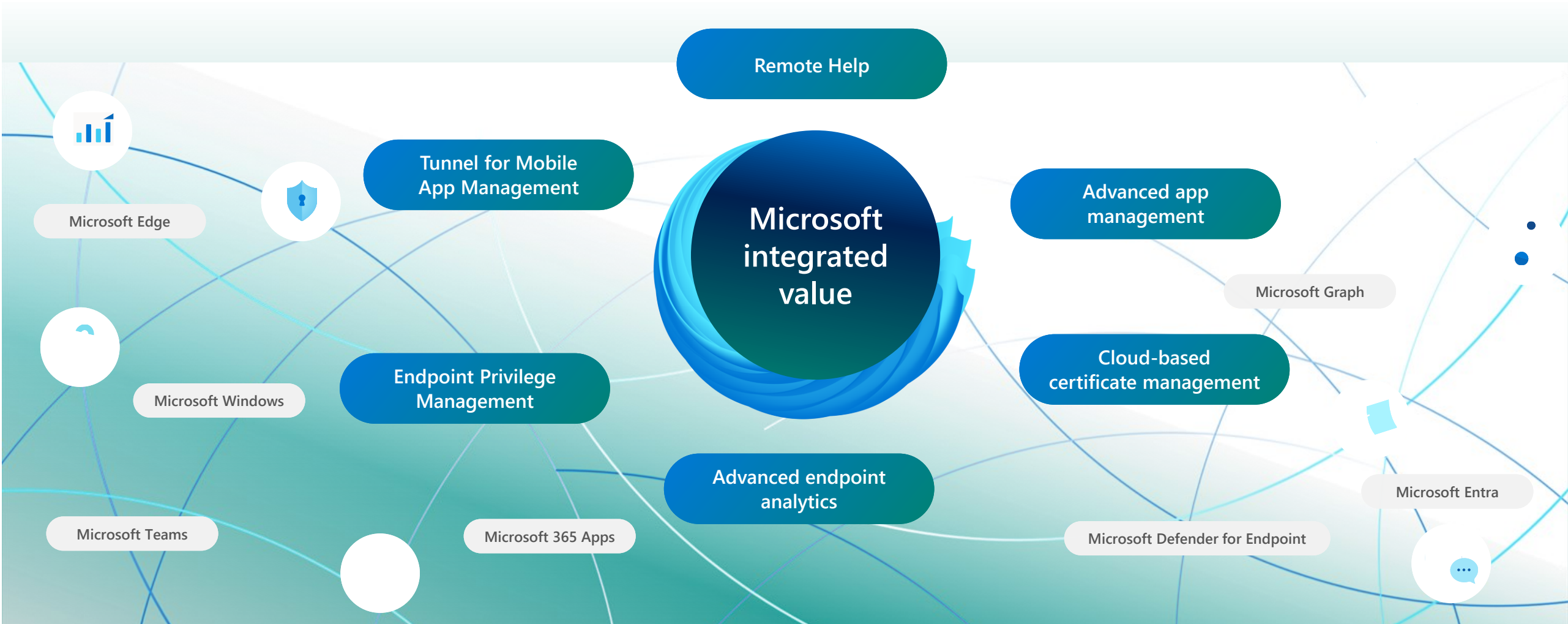
- Intune Plan 1

**Also available as individual add-ons*

***Additional advanced features to be added in future releases*

aka.ms/IntuneSuitePricing

Microsoft Intune Suite



Simplicity | Security | Savings

Microsoft 365 Business Premium

June 2023
m365maps.com

Microsoft 365 Business Premium

Office 365

Activity Reports

Adoption Score

Alert Policies

Audio Conferencing (free add-on)

Audit (standard)

Basic Mobility & Security

Bookings

Briefing Email

Compliance Manager

Content Search

Data Loss Prevention

Defender for Office 365 Plan 1

eDiscovery (standard)

Exchange Online Archiving

Exchange Online Plan 1

Information Protection for M365

Message Encryption (basic)

Microsoft 365 Apps for Business (with SCA)

Microsoft 365 Mobile App

Microsoft Dataverse for Teams

Microsoft Forms

Microsoft Lists

Microsoft Search

Microsoft Teams

Microsoft To Do

Microsoft Whiteboard

Office for the Web (incl Visio)

OneDrive for Business Plan 1

Planner

Power Apps for Office 365

Power Automate for Office 365

Power Virtual Agents for Teams

Project & Roadmap View Access

Secure Score

SharePoint Online Plan 1

Stream for Office 365

Sway

Viva Connections

Viva Engage

Viva Insights - Personal (basic)

Viva Learning (basic)

Webinars

Office 365

Enterprise Mobility + Security

Application Management

Device Management

Endpoint Analytics

Information Protection

Intune Plan 1 for Business

Administrative Units

Advanced Security Reports & Alerts

App Proxy, including PingAccess

Azure AD Connect Health

Cloud App Discovery

Conditional Access

Custom Security Attributes (preview)

Customized Sign-In Page

Dynamic Groups

Enterprise State Roaming

External Identities

Microsoft Identity Manager

Multi-Factor Auth (MFA)

Password Protection

Passwordless Authentication

Self-Service Group Management

Self-Service Password Reset in AD

Self-Service Activity Reports

Service Level Agreement

Shared Account Password Roll-Over

Single-Sign-On to other SaaS

SMS Sign-In

Temporary Access Pass

Terms of Use

Verified ID

Windows Autopilot

3rd Party MFA Integration

Azure AD Premium Plan 1

Enterprise Mobility + Security

Windows Pro

Application Control

Application Guard

AppLocker

Assigned Access

Azure AD Join

BitLocker

BitLocker to Go

Cortana

Defender Antivirus

Domain Join

Edge for Business

LAPS

Manage by MDM

Power Automate Attended Desktop Flows

Unbranded Boot

Universal Print

Windows Conditional Access

Windows Firewall

Windows Hello for Business

Windows Information Protection (retiring)

Windows Update for Business

24 months support for Windows 11

Microsoft 365 Business Premium includes Windows Pro upgrade from earlier Pro versions + Universal Print

Automated Investigations

Block at First Sight

Cross-Platform Support

Endpoint Detection & Response

Enhanced ASR

Mobile Threat Defence

Next Gen Protection

Tamper Protection

Threat Analytics

Vulnerability Management (core)

Web Content Filtering

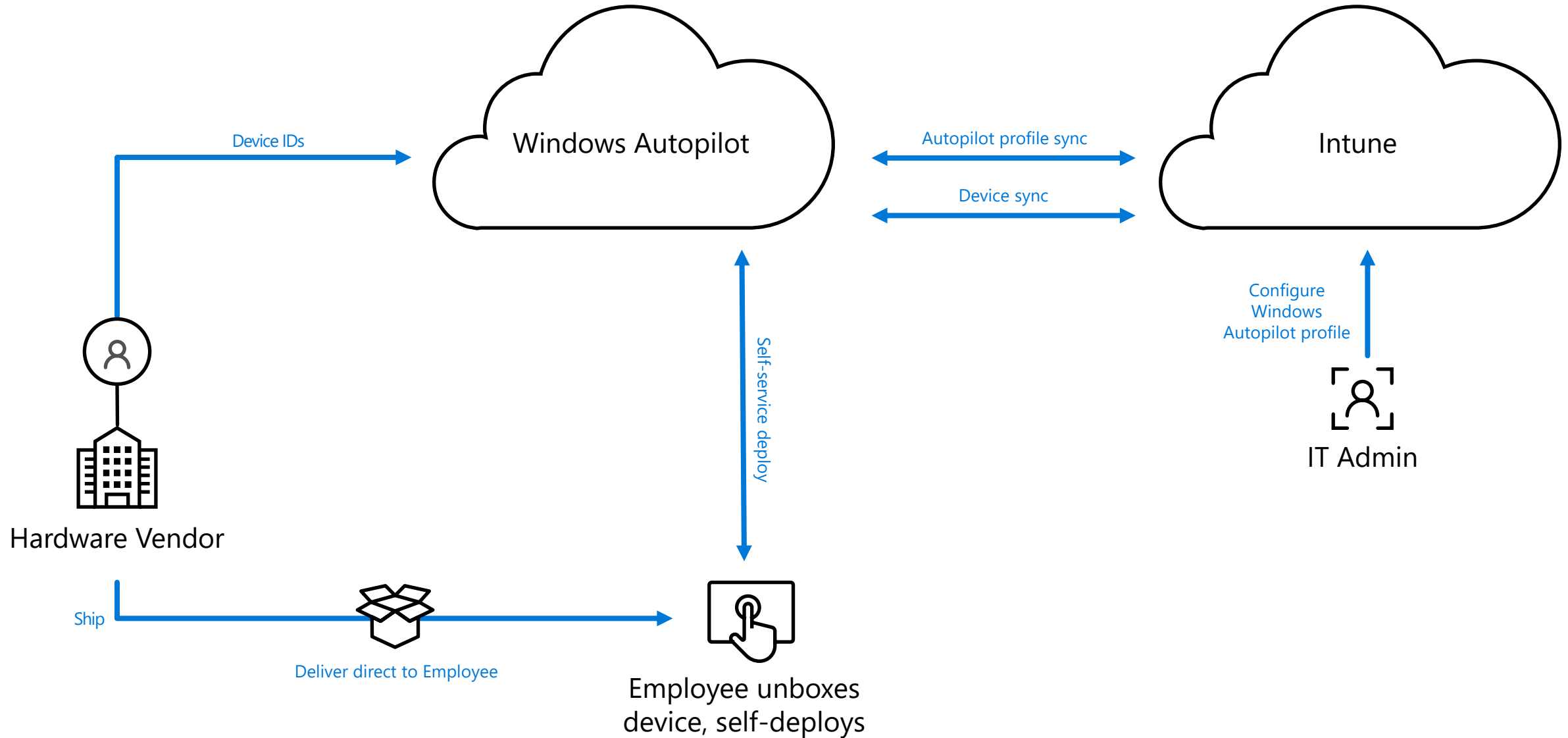
Defender for Business

Windows Pro

Microsoft 365 Business Premium | M365 Maps

Features

Windows Autopilot



More Platforms

- Linux is general available
- Support for
 - Ubuntu Desktop 22.04 or 20.04 LTS
 - A GNOME graphical desktop environment (automatically included with Ubuntu Desktop 22.04 and 20.04 LTS)
- Chrome OS preview
- Prerequisites
 - Chrome Enterprise Connector
 - Devices sync to Intune
 - Use Remote Actions
 - Compliance not supported



By platform

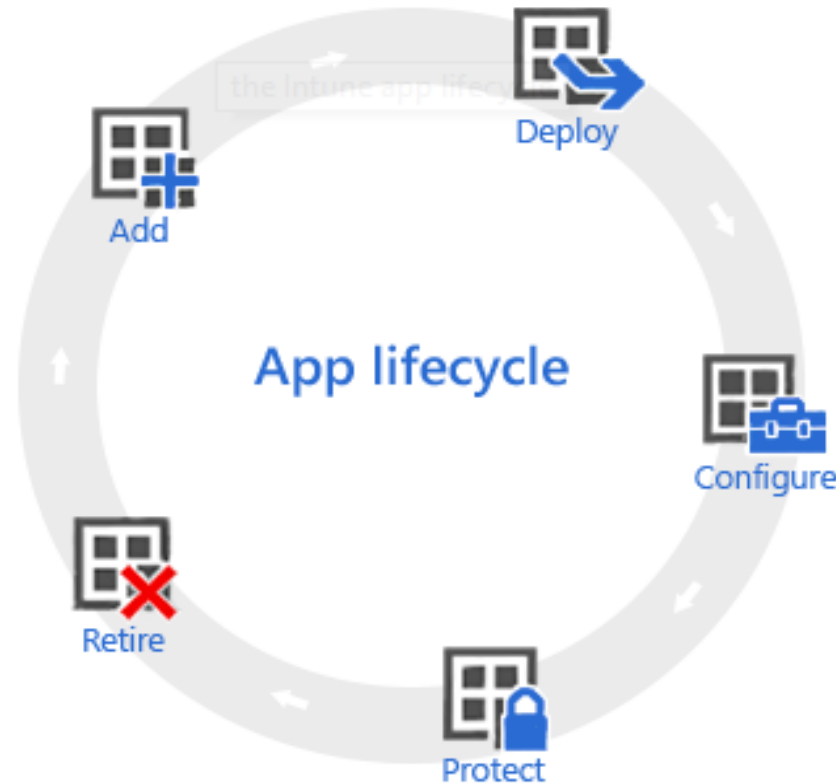
- Windows
- iOS/iPadOS
- macOS
- Android
- Chrome OS (preview)
- Linux



Application Management Lifecycle

Many application types are available including Store-, Web- or LOB (in-house) apps

Intune provides easy steps to remove assignments or retire devices and their apps


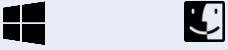










Easy deployment through groups having include/exclude options, Monitoring is available

Configuring application settings and updating new versions

Protection behavior, conditional access, compliance policies

App Types

	App type	Description
	Store app	Takes the user to the manufacturer store
	Microsoft 365 Apps	Configure and deploy Microsoft 365 apps (Office)
	Microsoft Edge	Configure and deploy Microsoft Edge browser
	Web link / application	Shortcut to a web app
	Defender for Endpoint	Defender for Endpoint agent deployment
	Built-in app	Curated managed apps (e.g. Office apps)
	Line-of-business app	Custom created apps, where you provide the source (apk, ipa, msi, appx, pkg)
	Win32 app	Lets you use own deployments and specify details like detection, requirements and dependencies
	macOS app (DMG)	Disk image file that contains one or more applications
	Android Enterprise system app	Enablement or removal of system apps (e.g. Contacts)

Cloud storage for Intune iOS and Android LOB apps is limited to 2 GB.
Total storage is unlimited (for trial subscriptions 2 GB).

Select app type

Create app

App type

Select app type

Store app

Android store app

iOS store app

Microsoft Store app (new)

Microsoft Store app (legacy)

Managed Google Play app

Microsoft 365 Apps

Windows 10 and later

macOS

Microsoft Edge, version 77 and later

Windows 10 and later

macOS

Microsoft Defender for Endpoint

macOS

Web Application

iOS/iPadOS web clip

Windows web link

Other

Web link

Built-In app

Line-of-business app

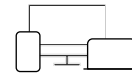
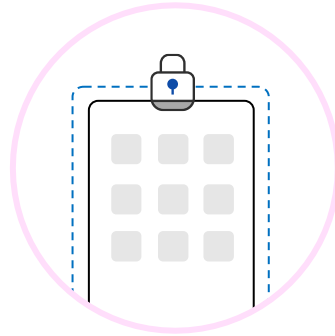
Windows app (Win32)

Protect your Data on Virtually any Device with Intune

Mobile **Device** Management (MDM)

Conditional Access:

Restrict access to managed and compliant devices.



Enroll devices for management.



Provision settings, certs, profiles.



Report & measure device compliance.

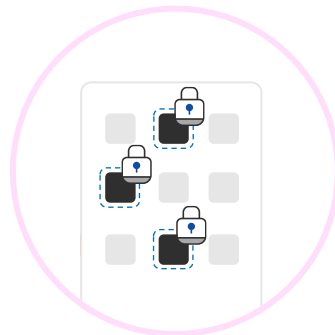


Remove corporate data from devices.

Mobile **Application** Management (MAM)

Conditional Access:

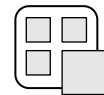
Restrict which apps can be used to access email or files.



Publish mobile apps to users.



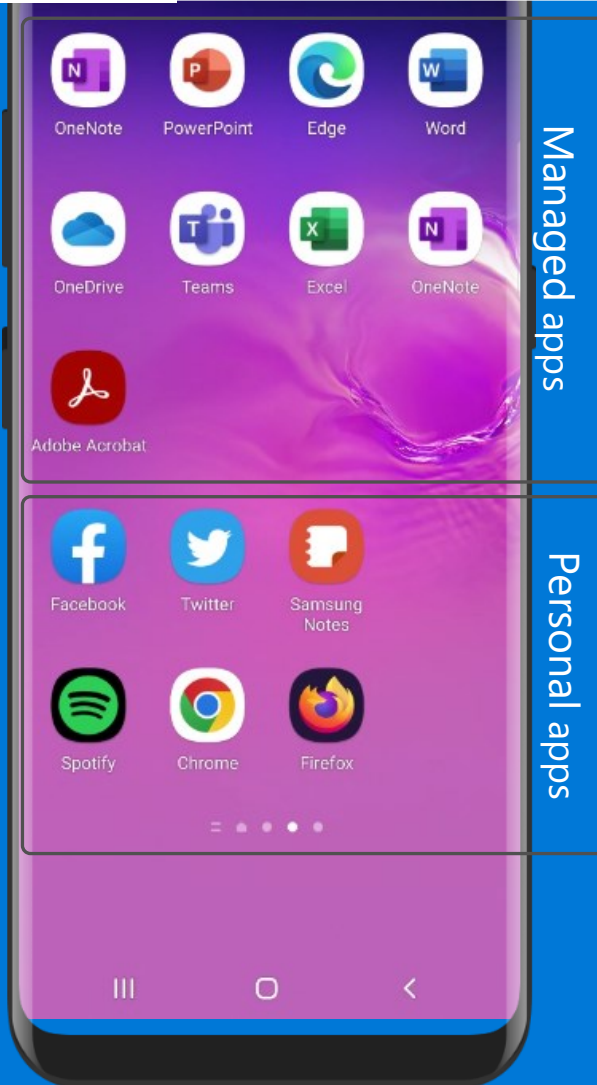
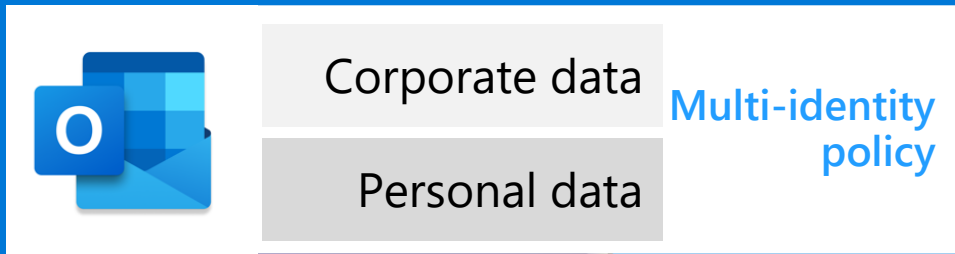
Configure and update apps.



Report app inventory & usage.



Secure & remove corporate data within mobile apps.



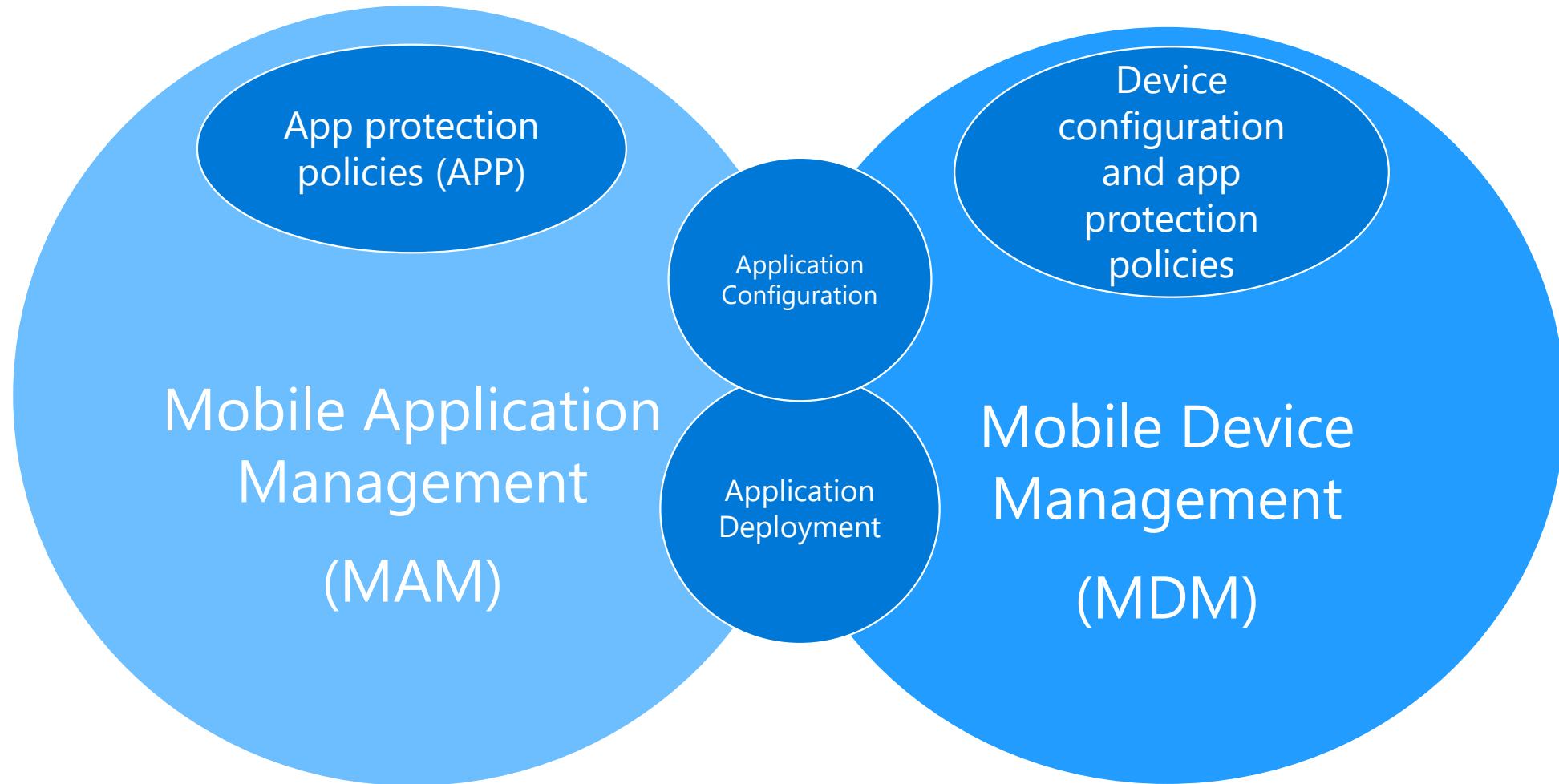
App Protection Policies for Personal Devices

Enables bring-your-own (BYO) and personal devices at work where users may be reluctant to “enroll” their device.

Ensures **corporate data cannot be copied** and pasted to personal apps within the device.

Intune App Protection policies are useful to protect Office 365 apps where devices are unmanaged or managed by 3rd party.

MAM vs. MDM



App Selective Wipe

Microsoft Intune admin center

Home > Apps

Apps | App selective wipe

Select user and device

Search

Create wipe request Export

Wipe requests User-Level Wipe

Search by user, app, or device name

User ↑↓	State ↑↓	App ↑↓	Device name ↑↓
IN-User1	<i>i</i> pending	Microsoft OneNote	Samsung SM-G97
IN-User1	<i>i</i> pending	Microsoft Edge	Motorola Moto g
IN-User1	<i>i</i> pending	Microsoft OneNote	Motorola Moto g
IN-User1	<i>i</i> pending	Microsoft Edge	iPhone

Org Data Removal

Your organization has removed its data associated with this app. (606)
To continue you must restart this app.
To reconnect to your organization, sign-in to your work or school account.

OK

IN-User1	<i>i</i> pending	Outlook	Samsung SM-G950F
IN-User1	<i>i</i> pending	Excel	Samsung SM-G950F
IN-User1	✓ completed	Word	iPad WS
IN-User1	<i>i</i> pending	PowerPoint	Samsung SM-G950F
IN-User1	✓ completed	Excel	Samsung SM-G950F

Multi Admin Approval - Creation

- Multi Admin Approval
 - Requires a second administrative account to approve a change
 - Access policies define what is protected and which groups are approvers
 - Supported access policies are for **Apps** and **Scripts**
 - The approver selects a business justification

Tenant admin | Multi Admin Approval

Search

- Azure AD Privileged Identity Management
- Diagnose settings
- Audit logs
- Device diagnostics
- Multi Admin Approval**
- Premium add-ons

End user experiences

- Customization

Received requests My requests **Access policies**

Access policies allow you to control which tasks and actions need approval along with the specific approval groups

+ Create Refresh

Search by name

Showing 1 to 1 of 1 records

< Previous

Page

1

of 1

Next >

Name ↑↓

Policy type ↑↓

Last modified date ↑↓

Approve creation of a ne...

apps

12/6/2022, 9:19:29 AM

...

Create an access policy

1 Basics

2 Approvers

3 Review + create

Name *

Approve creation of a new app ✓

Description

Profile type * ⓘ

Scripts

Apps

Scripts

ⓘ A script policy will limit any action on a

Configuration Profile Types

- Intune separates configuration policies for each device platform
 - Platform is selected prior creating profiles
- Templates
 - Wi-Fi profile, VPN profile, Certificate profile, ...
- Settings Catalog
 - Generated from the Windows 10/11 CSPs
 - Filter and search for settings

Create a profile

Platform
Windows 10 and later

Profile type
Templates
Settings catalog
Templates

Search

Template name ↑↓

Administrative templates

Custom ⓘ

Delivery optimization ⓘ

Device firmware configuration interface ⓘ

Device restrictions ⓘ

Device restrictions (Windows 10 Team) ⓘ

Domain join ⓘ

Edition upgrade and mode switch ⓘ

Email ⓘ

Endpoint protection ⓘ

Identity protection ⓘ

Imported Administrative templates (Preview)

Kiosk ⓘ

Microsoft Defender for Endpoint (Desktop devices running Windows 10 or later) ⓘ

Network boundary ⓘ

PKCS certificate ⓘ

PKCS imported certificate ⓘ

SCEP certificate ⓘ

Create

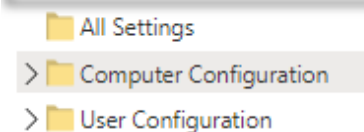
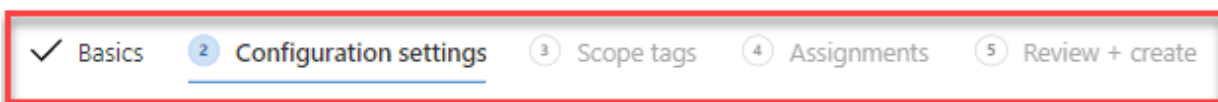
Administrative Templates

- Group Policy style configuration

[Home](#) > [Devices](#) > [Windows | Configuration profiles](#) >

Create profile

Administrative Templates



Computer Configuration

Computer Configuration

SmartScreen

Setting Name	State	Setting type	Path
SmartScreen settings			
SmartScreen settings			
Configure Microsoft Defender SmartScreen	Not configured	Device	\Microsoft Edge\SmartScreen settings
Configure Microsoft Defender SmartScreen	Not configured	Device	\Microsoft Edge - Default Settings (users can override)\SmartScreen settings
Configure Microsoft Defender SmartScreen to block potentially unwanted ...	Not configured	Device	\Microsoft Edge - Default Settings (users can override)\SmartScreen settings
Configure Microsoft Defender SmartScreen to block potentially unwanted ...	Not configured	Device	\Microsoft Edge\SmartScreen settings
Configure the list of domains for which Microsoft Defender SmartScreen w...	Not configured	Device	\Microsoft Edge\SmartScreen settings
Force Microsoft Defender SmartScreen checks on downloads from trusted ...	Not configured	Device	\Microsoft Edge\SmartScreen settings
Force Microsoft Defender SmartScreen checks on downloads from trusted ...	Not configured	Device	\Microsoft Edge - Default Settings (users can override)\SmartScreen settings

Settings Catalog

- Configurable settings all in one place
 - Generated from Windows 10/11 CSPs
 - Reduces the need for custom profile
 - Quickly add new Windows settings

Settings picker

Use commas "," among search terms to lookup settings by their keywords

+ Add filter

Browse by category

Authentication

Browser

Device Lock

Local Policies Security Options

results in the "Authentication" category

Setting name

☒ Allow Aad Password Reset

Select all these settings

✓ Basics

2 Configuration settings

3 Assignments

+ Add settings

Authentication

Remove category

Specifies whether password reset is enabled for AAD accounts.

[Learn more](#)

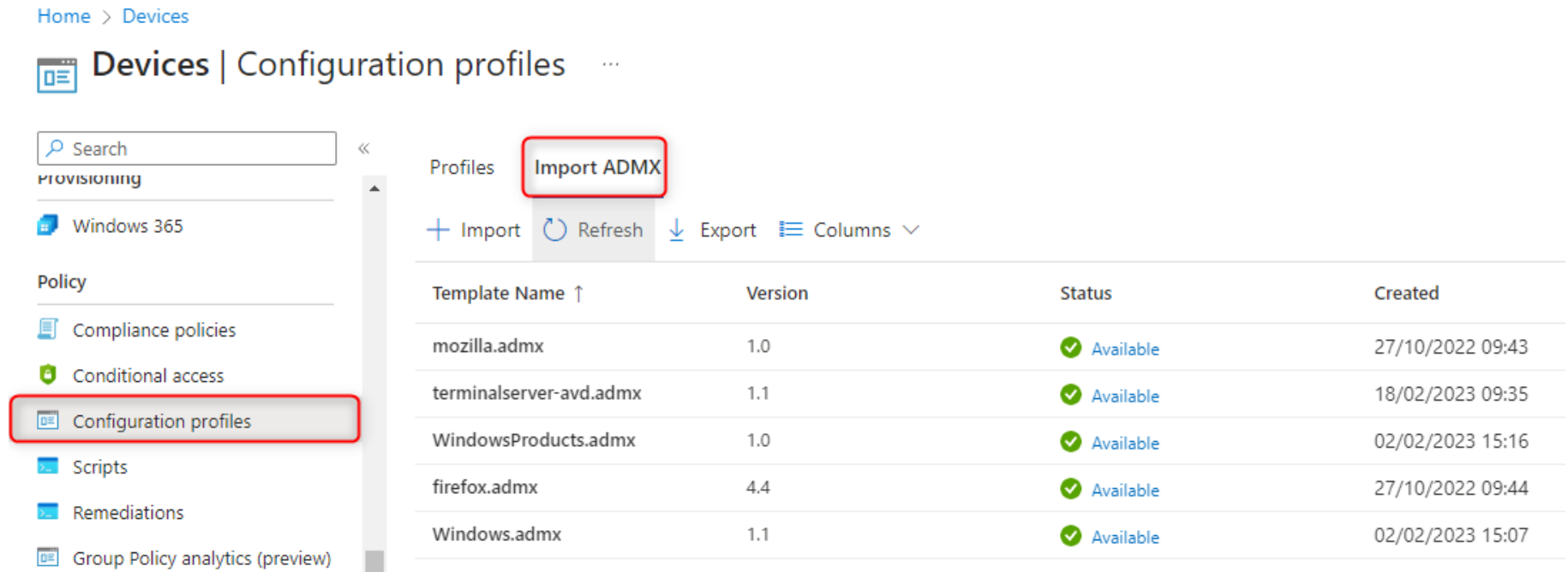
Allow Aad Password Reset ⓘ

☒ Allow

⊖

Import custom and 3rd party ADMX

- Natively integrate 3rd party ADMX
- admx **and** adml file are required
- After import, an **Imported Administrative Template** profile can be created and deployed



Home > Devices

Devices | Configuration profiles ...

Search

Provisioning

- Windows 365

Policy

- Compliance policies
- Conditional access
- Configuration profiles**
- Scripts
- Remediations
- Group Policy analytics (preview)

Profiles **Import ADMX**

+ Import Refresh Export Columns

Template Name ↑	Version	Status	Created
mozilla.admx	1.0	✓ Available	27/10/2022 09:43
terminalserver-avd.admx	1.1	✓ Available	18/02/2023 09:35
WindowsProducts.admx	1.0	✓ Available	02/02/2023 15:16
firefox.admx	4.4	✓ Available	27/10/2022 09:44
Windows.admx	1.1	✓ Available	02/02/2023 15:07

Upload and Deploy a Powershell Script

[Home](#) >

Devices | Overview ...

Overview

All devices

Device onboarding

Cloud PC creation

Enrollment

Manage devices

Configuration

Compliance

Conditional access

Scripts

Windows 10 and later updates

Apple updates

Group Policy analytics (preview)

eSIM cellular profiles (preview)

Policy sets

Android FOTA deployments
(preview)

Device clean-up rules

Add PowerShell script

✓ Basics

2 Script settings

3 Assignments

4 Review + add

Script location * ⓘ

Remove-Appx.ps1

Run this script using the logged on
credentials ⓘ

Yes

No

Enforce script signature check ⓘ

Yes

No

Run script in 64 bit PowerShell Host ⓘ

Yes

No

- Upload your Powershell script
- Configure settings
- Assign to group
- Can be managed by multi admin approval policies
- Depends on Management extension schedule (hourly)

Group Policy Analytics

- Tool to analyze on-premises GPOs
 - Helps translating to cloud settings
 - Import saved XML GPO report
 - Get a migration readiness report

Home > Devices

Devices | Group Policy analytics (preview)

Search

Conditional access

Configuration profiles

Scripts

Remediations

Group Policy analytics (preview)

Update rings for Windows 10 and later

Feature updates for Windows 10 and later

Use Group Policy analytics to analyze your on-prem Group Policy Objects (GPO) and determine your level of modern management support. Click "Import" to begin the process of migrating your settings to modern management. [Learn more](#)

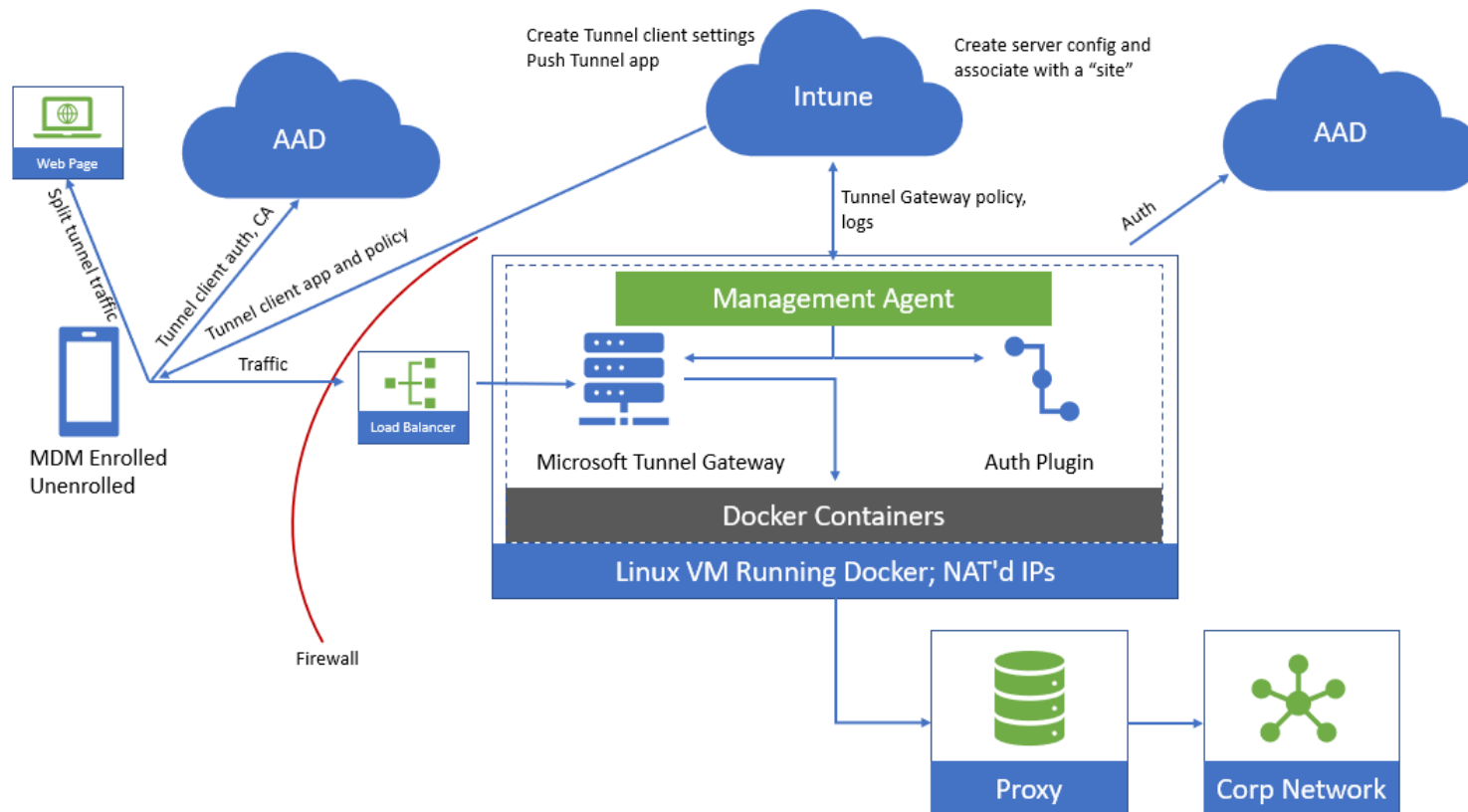
Search by Group Policy Name or Active Directory Target

Showing 1 to 1 of 1 records

Migrate ↑↓	Group policy name ↑↓	Active directory target ↑↓	MDM support ↑↓	Unknown settings ↑↓
<input checked="" type="checkbox"/>	gpmigrate	gpmigrate	85%	View

Microsoft Tunnel

- Intune VPN gateway solution
 - Access on-premises resources from iOS and Android Enterprise devices
 - Docker container running on Linux



Multiple Linux servers behind load balancer possible

Tunnel for MAM available with Intune Plan 2

Intune Device Compliance Policy

✓ Basics **2 Compliance settings** 3 Actions for noncompliance 4 Assignments 5 Review + create

✓ Device Health

^ Device Properties

Operating System Version ⓘ

Minimum OS version ⓘ ✓

Maximum OS version ⓘ

Minimum OS version for mobile devices ⓘ

Maximum OS version for mobile devices ⓘ

Valid operating system builds

✓ Configuration Manager Compliance

✓ System Security

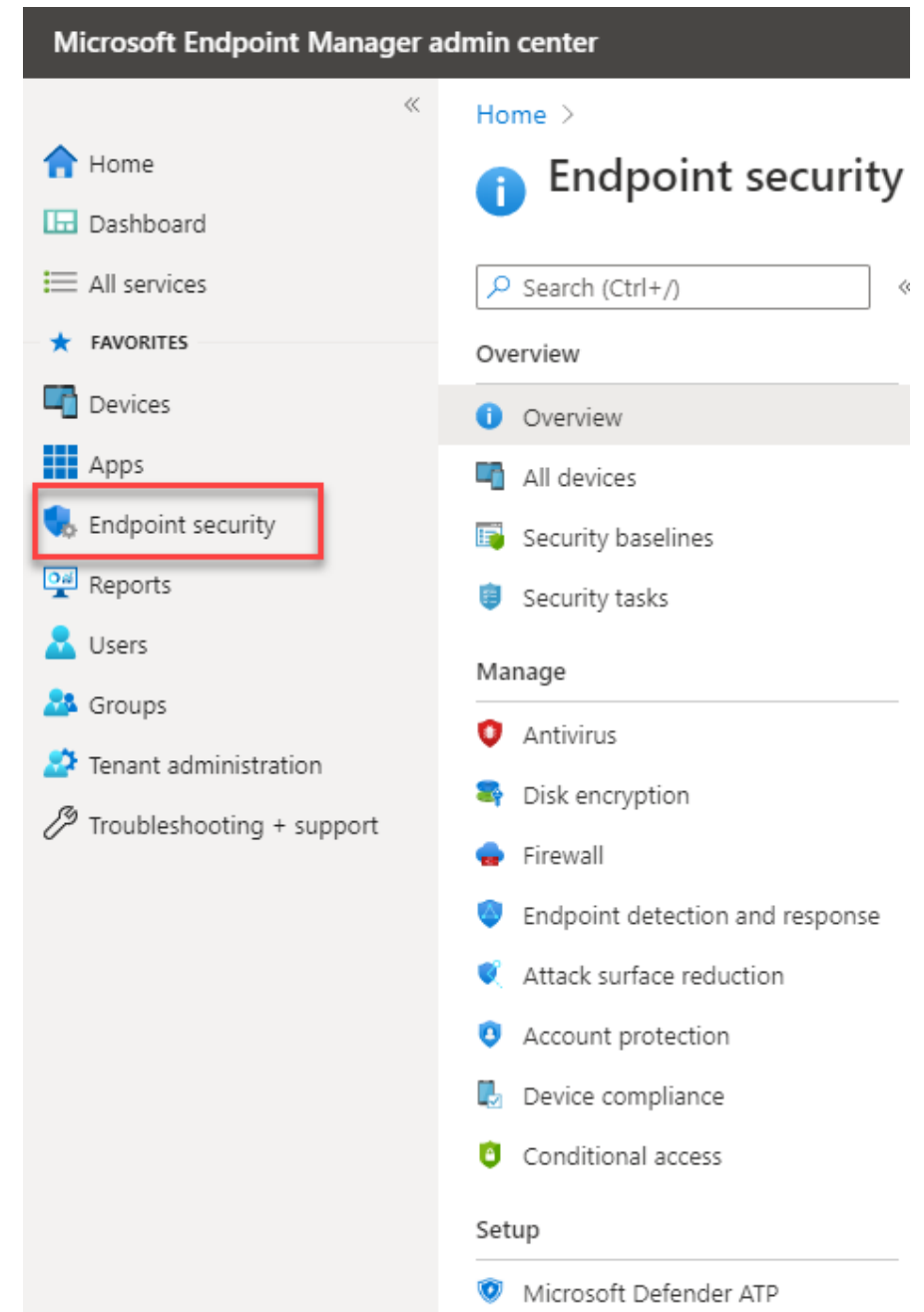
✓ Microsoft Defender for Endpoint

Check for:

- Secure Boot / Bitlocker
- Encryption
- Windows 10/11 versions
- Password
- Firewall / Defender
- Configuration Manager Compliance
- MDE risk score

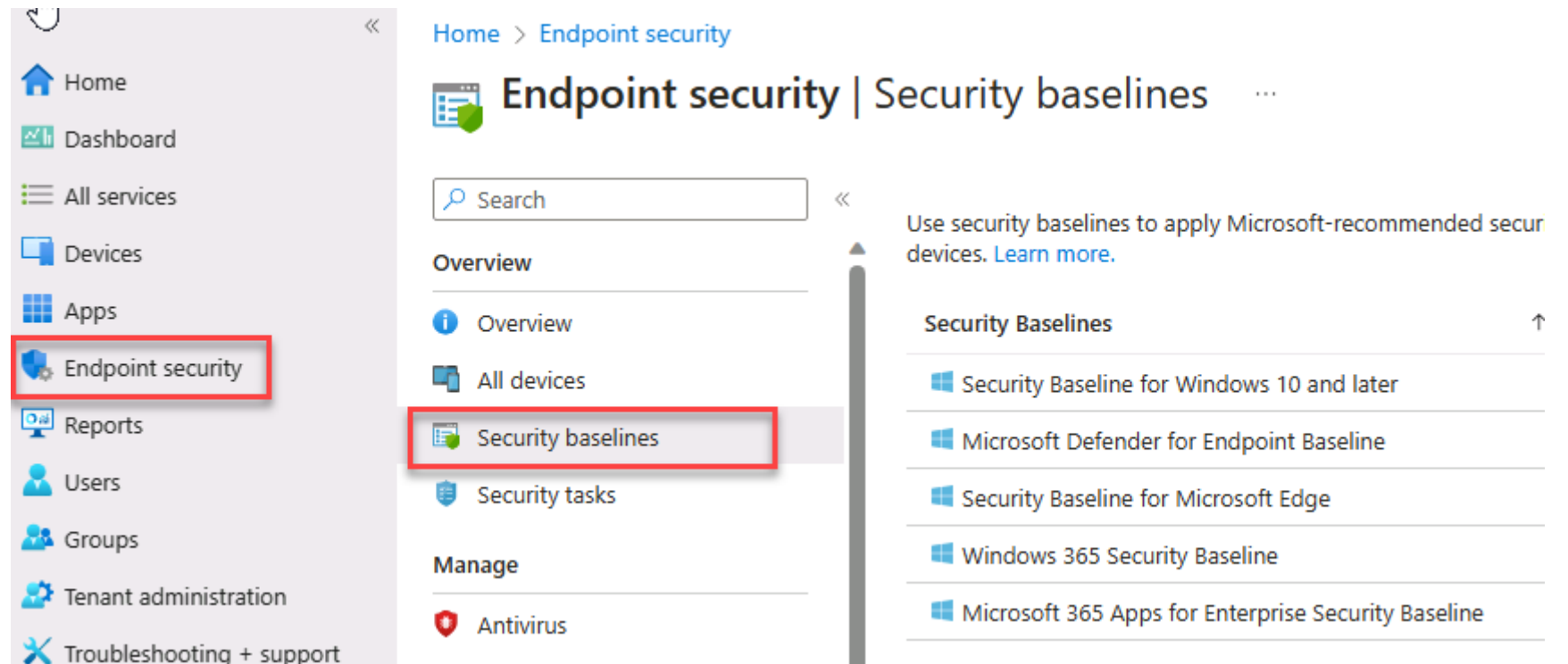
Endpoint security in Intune

- Endpoint security node
 - Groups all tools available through Intune to configure and manage security related tasks. These are the same policies as already configured with Device Configuration profiles.
 - > avoid conflicts
 - Baselines
 - Antivirus
 - Disk encryption
 - Endpoint Detection and response
 - Attack surface reduction
 - Account protection
 - Compliance and Conditional Access



Security Baseline

- Helps securing and protecting users and devices
- Automatically creates settings recommended by the security teams
 - Enables Bitlocker
 - Creates password settings
 - Disables basic authentication
 - ...



Endpoint detection and response

- Onboarding to Defender for Endpoint
 - For Intune managed devices
 - For Configuration Manager managed devices (Tenant attach required)

Create profile ...

Endpoint detection and response

✓ Basics 2 Configuration settings 3 Scope tags ...

Microsoft Defender for Endpoint

Microsoft Defender for Endpoint client configuration package type ⓘ

Not configured ▼

Sample Sharing ⓘ

Not configured ▼

Telemetry Reporting Frequency ⓘ

Not configured ▼

Option to use automatic (tenant connector) or specific onboarding package

Auto from connector ▼

Auto from connector

Onboard

Offboard

Not configured

Attack Surface Reduction

- Profiles for
 - Device control (Secures removable media access, USB)
 - Attack surface reduction rules (Behaviour monitoring)
 - App and browser isolation (Run app/browser in isolated VM)
 - Exploit protection (Applies process mitigations)
 - Web protection (Blocks access to malicious sites)
 - Application control (Restrict applications)

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

Web Protection

Enable network protection ⓘ

Enable



Require SmartScreen for Microsoft Edge ⓘ

Yes

Not configured

Block malicious site access ⓘ

Yes

Not configured

Block unverified file download ⓘ

Yes

Not configured

Account protection

- Profiles for
 - Windows Hello for Business
 - Credential Guard

Account Protection

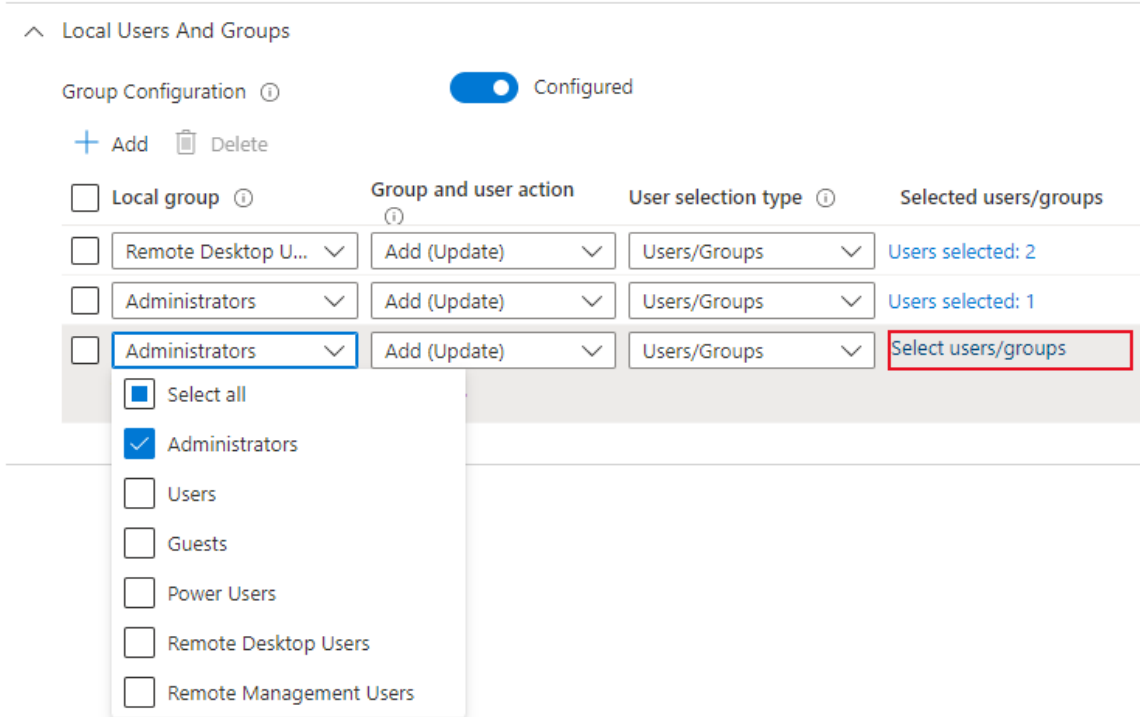
Block Windows Hello for Business ⓘ	Disabled ▼
Minimum PIN length: ⓘ	4 ✓
Maximum PIN length: ⓘ	4 ✓
Lowercase letters in PIN: ⓘ	Not allowed ▼
Uppercase letters in PIN: ⓘ	Not allowed
Special characters in PIN: ⓘ	Not allowed

Turn on Credential Guard ⓘ

Not configured
Disable
Enable with UEFI lock
Enable without UEFI lock
Not configured ▼

Account protection

- Local user group memberships
 - Windows 10 20H2 or newer required



Application Control (Preview)

- Defender Application Control
 - Windows Defender Application Control (WDAC) was introduced with Windows 10 and allows organizations to control which drivers and applications are allowed to run on Windows clients.
- Applocker (now available for all Windows 10/11 versions)

Home > Endpoint security | Application control (Preview) >

Create profile

Application control

✓ Basics 2 Configuration settings 3 Scope tags 4 Assignments 5 Review + create

Application Control

Configuration settings format ⓘ

Enter xml data

Application control policy ⓘ

"AllowMicrosoft2023-01-04.xml"

XML value *

```
<?xml version="1.0" encoding="utf-8"?>
<SiPolicy xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
PolicyType="Base Policy" xmlns="urn:schemas-microsoft-com:sipolicy">
  <VersionEx>10.0.0.0</VersionEx>
  <PlatformID>{2E07F7E4-194C-4D20-B7C9-6F44A6C5A234}
```

Application control (Preview)

Application control

Managed installer

To begin configuring the Intune Management Extension as a Managed installer, click the **Configure** button where the policy succeeded or resulted in an error. If necessary, you can also [set the Managed installer](#).



Refresh



Columns



Export



Configure

Policy name ↑↓

Author ↑↓

No data

Configure managed installer

Application control

ON will grant Microsoft permission to configure Intune Management Extension as a managed installer (an authorized source for application deployment) on applicable devices.

OFF will pause any scheduled policy to set the Intune Management Extension as a managed installer on applicable devices. Existing policies already deployed to devices will not be changed when configuring to OFF. If removal of existing policies is required, a cleanup script may be used. [Learn more about how Intune sets the managed installer.](#)

Set managed installer

Off

On

Next, you can create an Application control policy to specify the rules for which apps can run on your Windows devices. [Learn more about managed installers and Application control.](#)

Save

[Configurare Application Control in Microsoft Intune - ICT Power](#)

Windows LAPS

Edit profile - Windows LAPS

Settings catalog

1 Configuration settings 2 Review + save

^ LAPS

Backup Directory ⓘ

Backup the password to Azure AD only ▼

Password Age Days ⓘ

☒ Configured

14

Administrator Account Name ⓘ

☒ Configured

LAPSAdmin

Password Complexity ⓘ

Large letters + small letters + numbers ▼

Password Length ⓘ

☒ Configured

14

Post Authentication Actions ⓘ

Not configured ▼

Post Authentication Reset Delay ⓘ

☐ Not configured

**Built-in in Windows 10
and 11 since CU 2023-04**

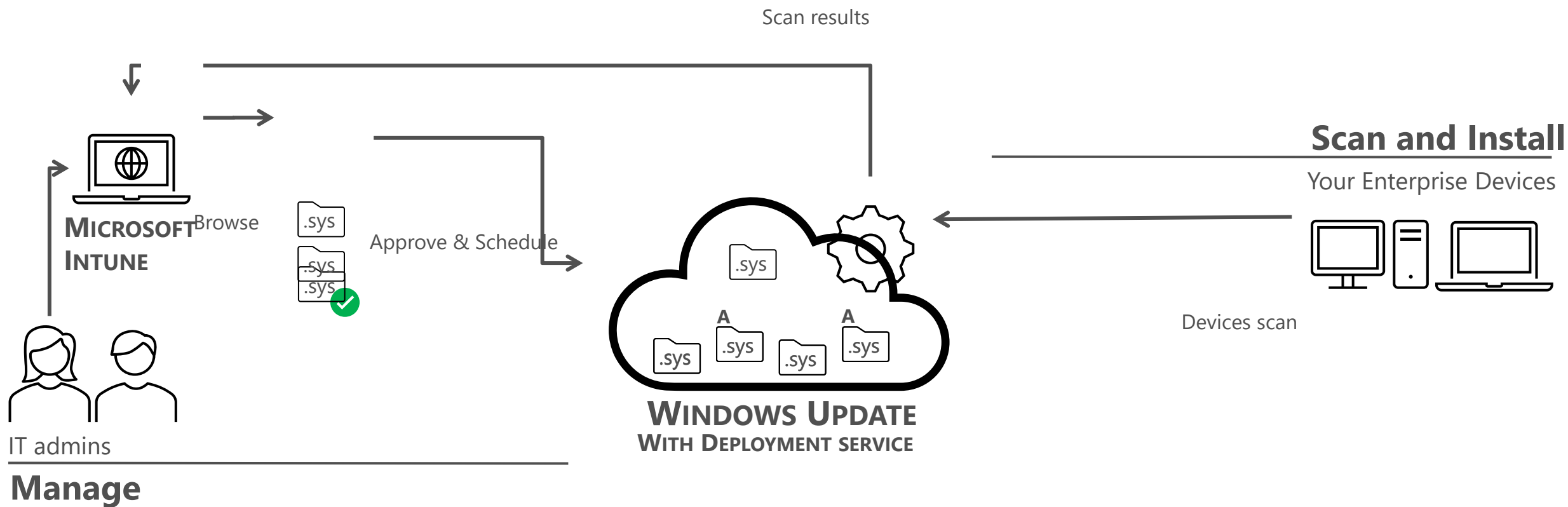
- Protection against pass-the-hash and lateral-traversal attacks
- Improved security for remote help desk scenarios
- Ability to sign in to and recover devices that are otherwise inaccessible
- Fine-grained security model
- Support for the Azure role-based access control model for securing passwords that are stored in Entra ID

Windows Update Types

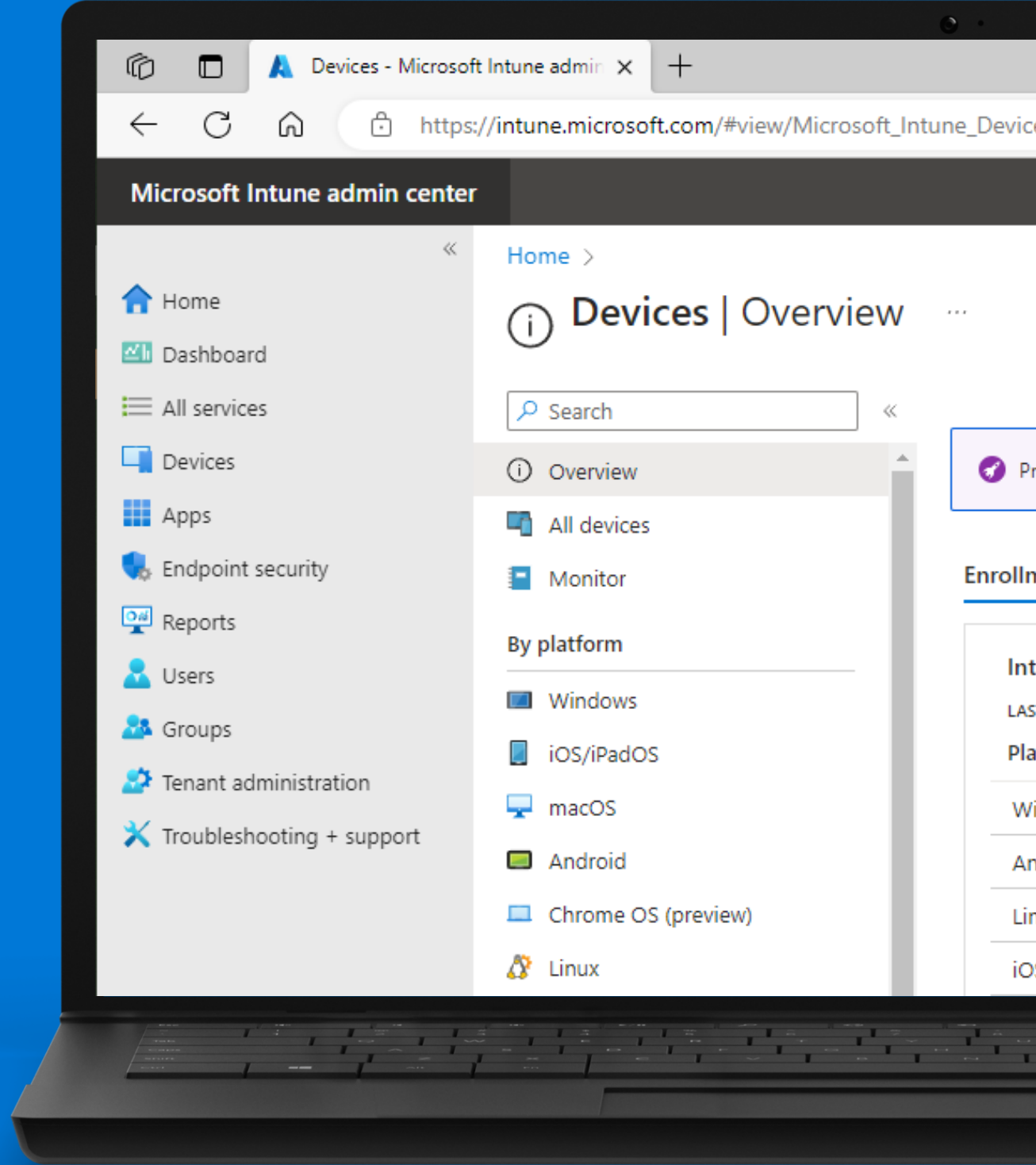
- **Feature Updates:** previously referred to as *upgrades*, Feature Updates contain significant feature additions and changes; they are released semi-annually.
- **Quality Updates:** traditional operating system updates, typically released the second Tuesday of each month. These include security, critical, and driver updates.
- **Non-deferrable updates:** Currently, antimalware and antispyware Definition Updates

Category	Maximum deferral	Deferral increments	Example
Feature Updates	365 days	Days	In Windows 10/11 maximum is 365 days
Quality Updates	30 days	Days	Security updates Drivers (optional) Non-security updates Microsoft updates (Office, Visual Studio, etc.)
Non-deferrable	No deferral	No deferral	Security Intelligence Updates (Definitions and engine)

Driver & Firmware Servicing



DEMO



Microsoft Intune Italian User Group

Grazie



Nicola Ferrini
Microsoft MVP



/NicolaFerrini.it



@nicolaFerrini



/nicolaFerrini