3.Intune

Cloud Advanced

Klaas Thys
klaas.thys@pxl.be

Microsoft Entra certification

Microsoft Learn

MD-102 Modern Desktop Administrator

3.Intune

1. **MDM introduction**
2. Enroll
3. Configure
4. Protect
5. Retire

Device Management

- **Mobile Device Management (MDM):** Configuring, managing, securiting and monitoring of an and device.

  Ex. Enforcing bitlocker encryption, automatic installation of company apps, settings for compliance

- **Mobile Application Management (MAM):** Implement security policies specifically for certain applications and their data without managing the entire device.

  Ex. Allow users to read emails using the Outlook client while restricting their ability to copy and paste data into other applications

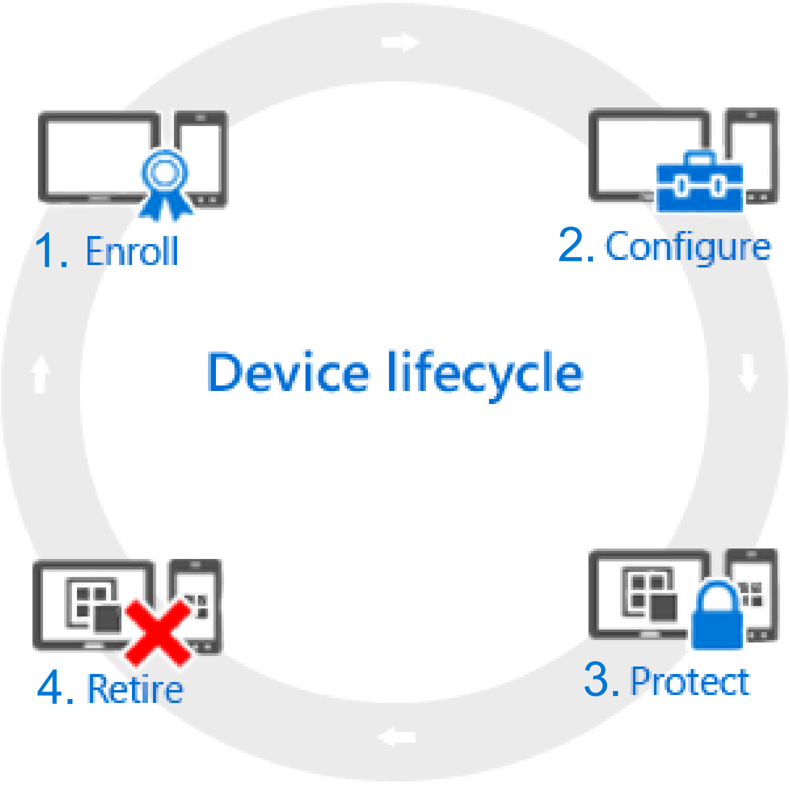
Mobile Device Management (MDM)

Configuring, managing, securiting and monitoring of an and device:

- **Configuration policies:** Configuring device settings
- **Deployment profiles:** automating OOBE (initial device setup process)
- Installing and updating **applications**
- Operating System **updates**
- **Endpoint Security**
- Remote **wipe** and **lock**

Device Lifecycle on prem environment

- Installing device with operating system.
- Enrolling device in management platform.



- Manage device settings
- Installing

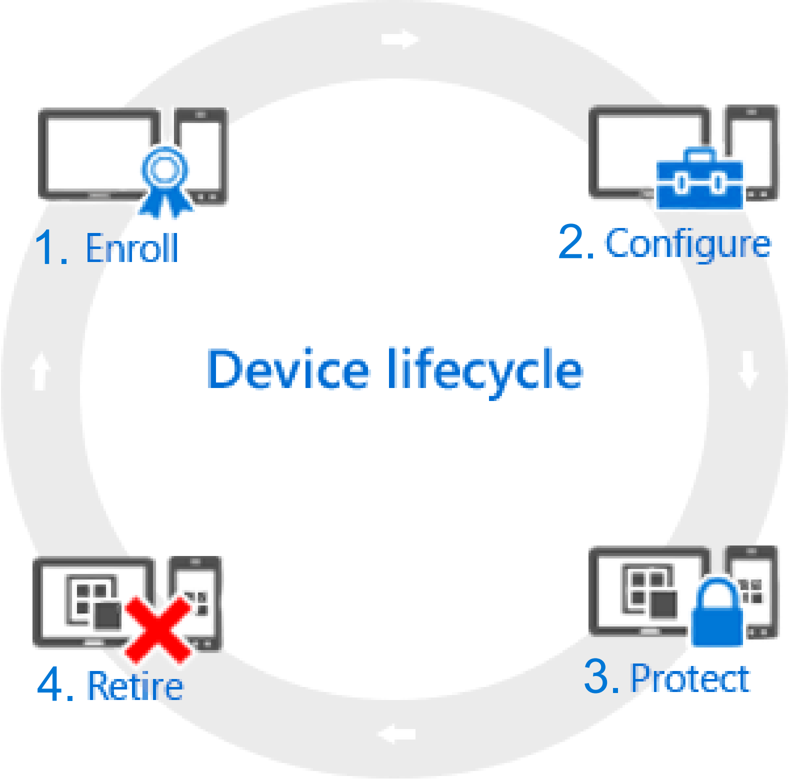
- Manage device settings: restrictions
- Endpoint security
- OS and software updates

- Wiping erasing a device for reuse, sale, or recycling.

Device Lifecycle on prem environment

- **SCCM:** Deploying the golden image onto the device
- The device is enrolled in **active directory**

- Manage device settings through **group policies**: network configurations, branding, OS settings,...
- **SCCM:** installing applications



- **SCCM:** reimage for reusage or wipe device for retirement.

- User and device restrictions through **group policies**(preventing removable media, blocking applications,…)
- Endpoint protection
- **SCCM:** deploying OS and software updates

1.Enroll: Imaging

Golden image: standardized, pre-configured operating system for deploying environments across multiple devices

- Base operating system
- Pre-installed applications
- Security settings and updates
- Custom configurations

1.Enroll: imaging

Benefits

- **Consistency:** All devices same configuration and software
- **Time-saving:** deployment eliminating manual setup
- **Ready-to-use:** When installed, device is immediately ready for end user.

Drawbacks

- **Maintenance:** Golden image quickly outdated
- **Flexibility:** multiple images for intended audience (HR, IT, technical staff,…)
- **Manual operation:** unpacking and connecting end device to network or USB device

2. Configure and protect

Limitations:

- **Limited platform support:** SCCM and Group Policies only support Windows operating systems, with no support for mobile devices or other operating systems.
- **Connectivity:** Require a connection to the on-premises environment to function properly.
- **Scalability:** adding a large number of devices or scaling to new geographical locations require investment in hardware, network and IT impact hardware, networking and IT staff.

3.Intune

1.MDM on prem environment

2.Enroll

3.Configure

4.Protect

5.Retire

Company - personal devices

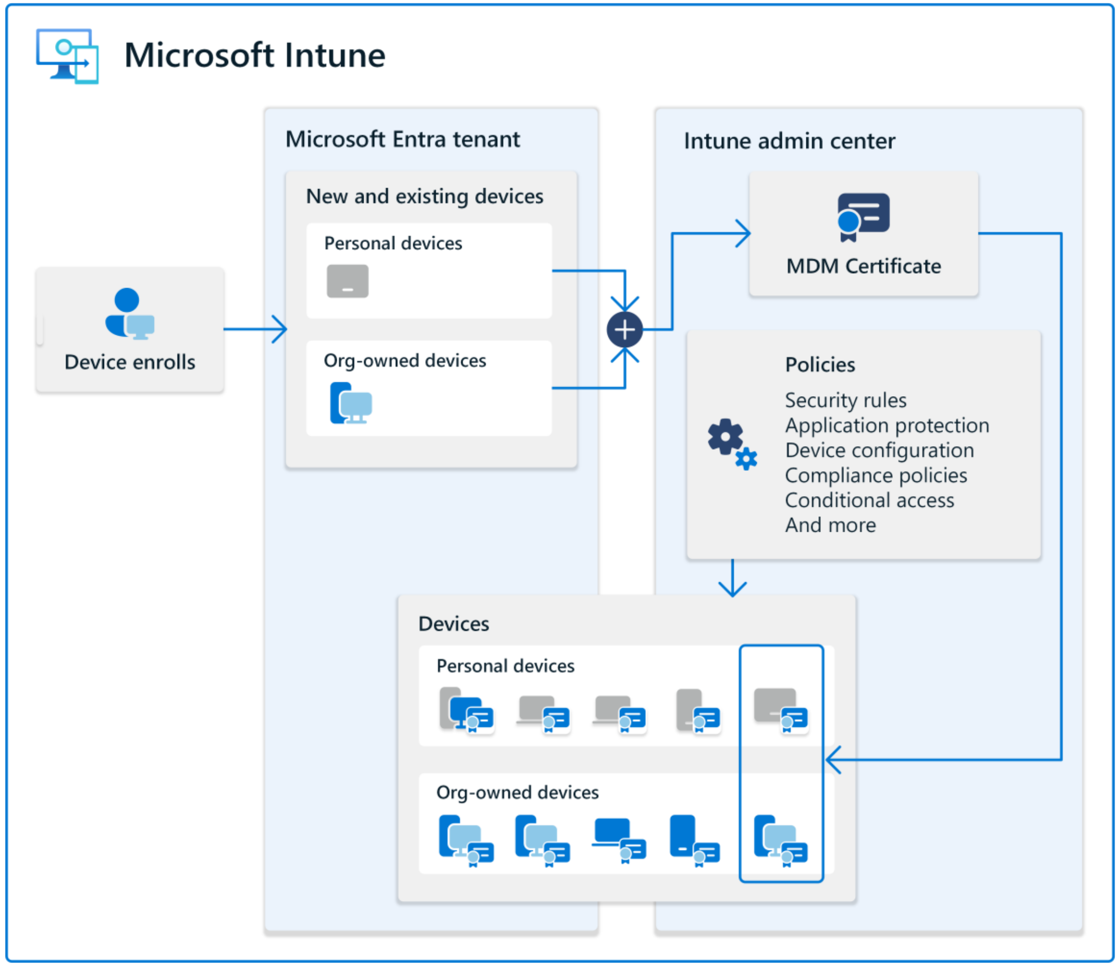
- **Company owned devices:** Devices that are purchased and managed by the company. ➔ Devices managed by MDM solution.
- **Personal devices:** Devices purchased by the staff member for personal use, but also used to access company resources (email, documents, applications, etc,…). ➔ not by managing the device itself by MDM, but by:
  - ***Compliance:*** *ensures that devices meet specific security and configuration requirements before granting access to company resources.*
    - *minimum OS requirements*
    - *device secured with password, pincode, lock pattern*
    - *Device storage is encrypted*
    - *…*
  - ***MAM (Mobile application management)***

Company-owned vs personal devices

The device is registered in the Microsoft Intune environment through Entra user authentication

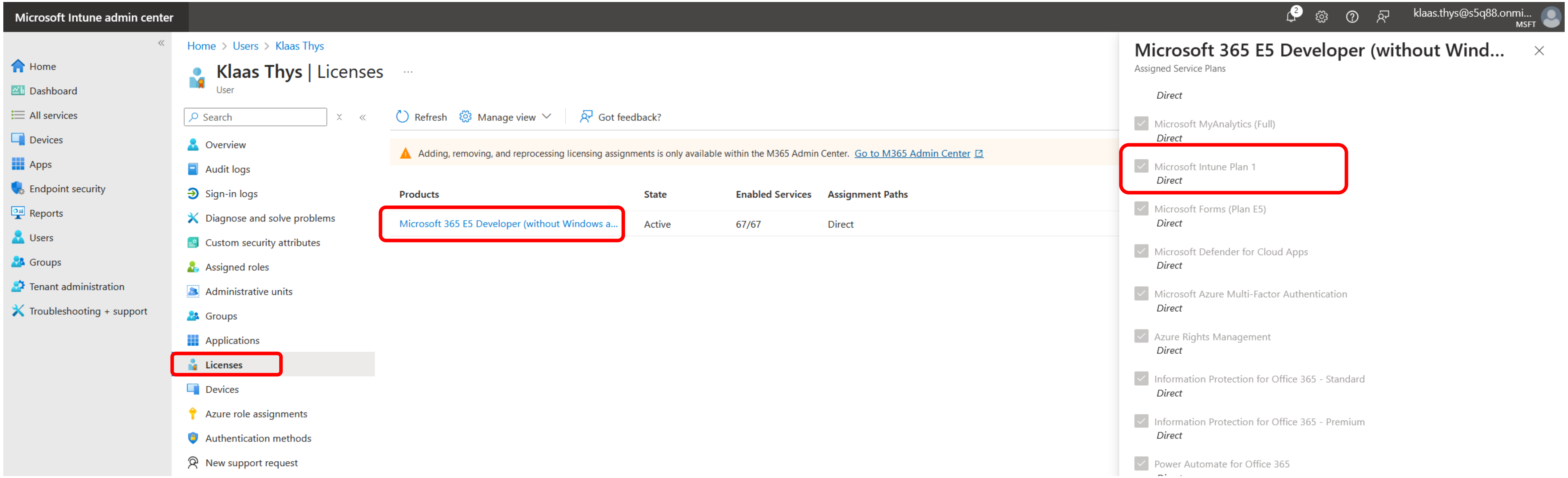
- **Org-owned devices:** devices purchased and owned by the organization
- **Personal devices:** devices purchased and owned by employee

Personally owned devices are blocked by default.



1.Enroll requirements

1. User License: Microsoft Intune Plan



Klaas Thys | Licenses

User

Adding, removing, and reprocessing licensing assignments is only available within the M365 Admin Center. Go to M365 Admin Center

Products	State	Enabled Services	Assignment Paths
Microsoft 365 E5 Developer (without Windows a...	Active	67/67	Direct

Microsoft 365 E5 Developer (without Wind...

Assigned Service Plans

Direct

☑ Microsoft MyAnalytics (Full)
Direct

☑ Microsoft Intune Plan 1
Direct

☑ Microsoft Forms (Plan E5)
Direct

☑ Microsoft Defender for Cloud Apps
Direct

☑ Microsoft Azure Multi-Factor Authentication
Direct

☑ Azure Rights Management
Direct

☑ Information Protection for Office 365 - Standard
Direct

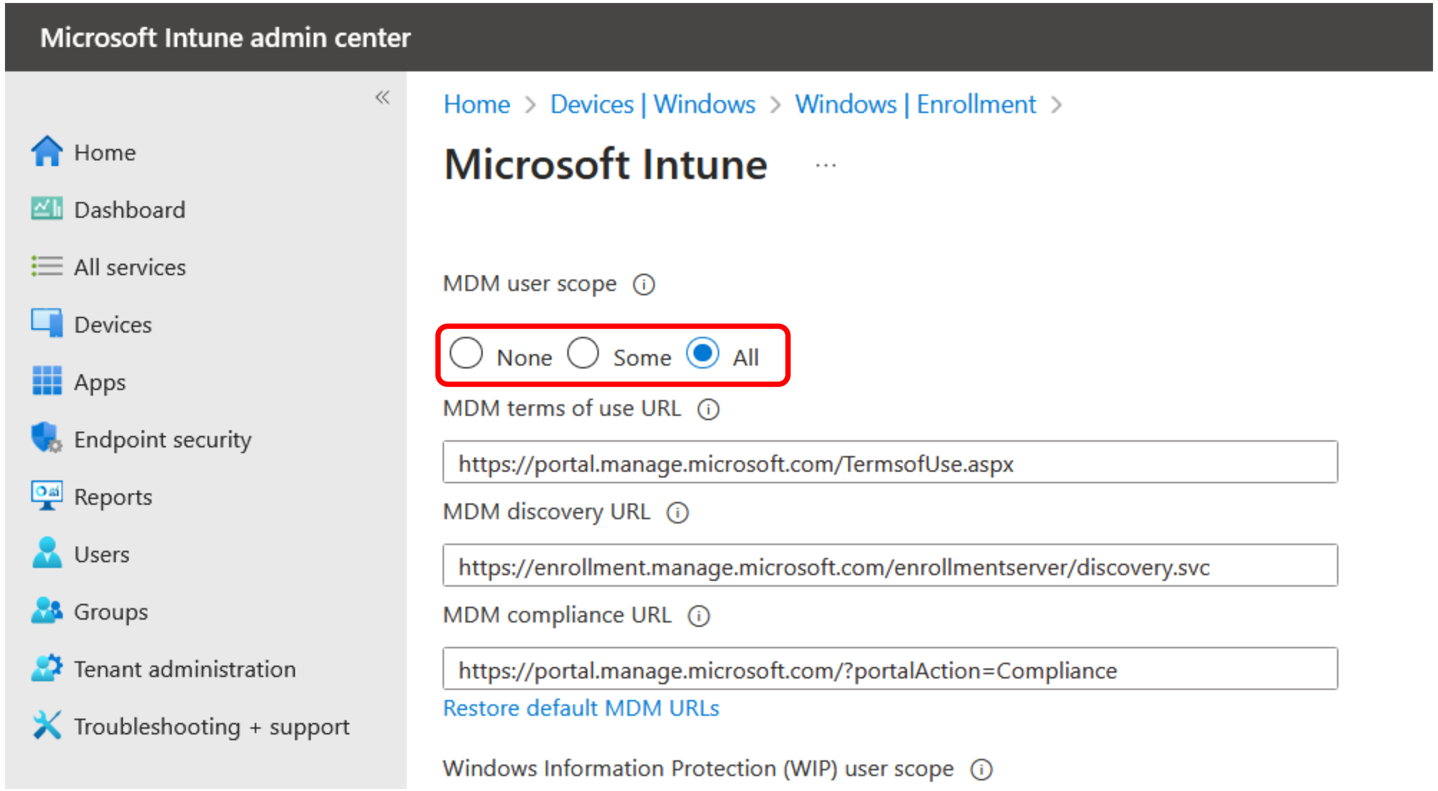
☑ Information Protection for Office 365 - Premium
Direct

☑ Power Automate for Office 365

1.Enroll requirements

2. Intune MDM settings:

- **None:** End devices cannot be registered.
- **All:** All users can register devices in Intune.
- **Some:** Members of certain groups can register devices in Intune



Microsoft Intune admin center

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

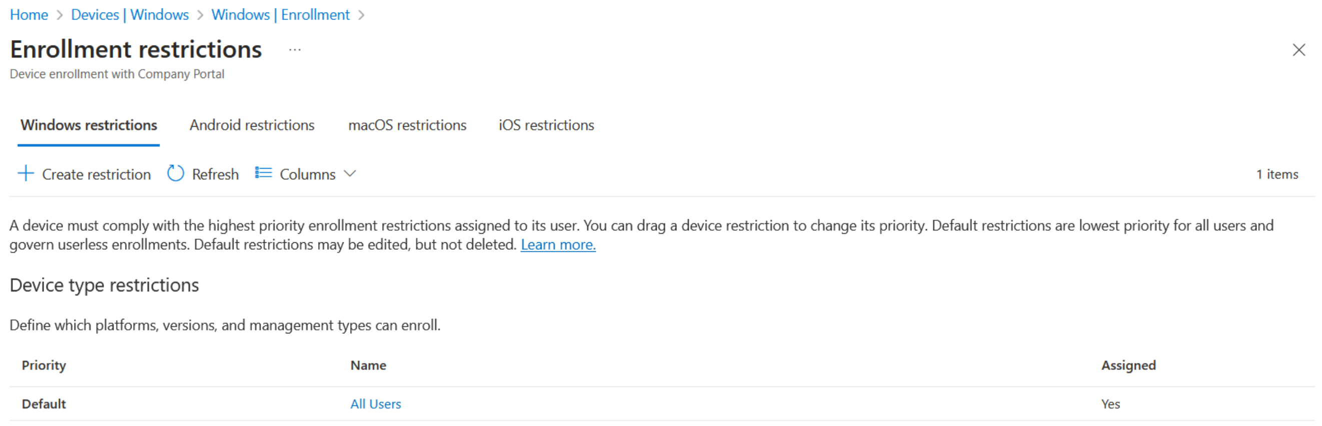
Restore default MDM URLs

Windows Information Protection (WIP) user scope ⓘ

1.Enroll requirements

3. Device restrictions:

- Allowing or blocking **operating systems** and or versions.
- **Limiting** number of devices per user.
- Allowing or blocking **personal devices**



Home > Devices | Windows > Windows | Enrollment >

Enrollment restrictions ···

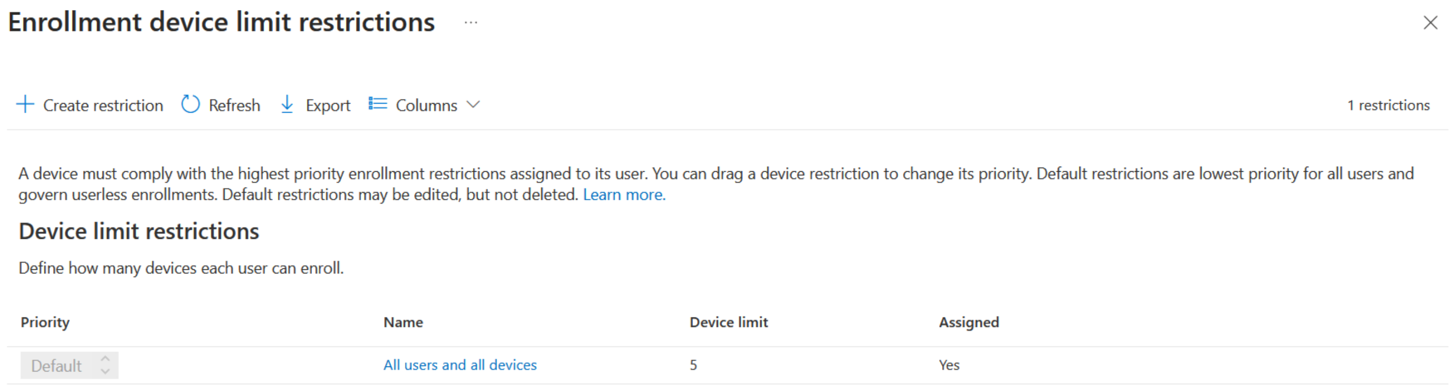
Device enrollment with Company Portal

A device must comply with the highest priority enrollment restrictions assigned to its user. You can drag a device restriction to change its priority. Default restrictions are lowest priority for all users and govern userless enrollments. Default restrictions may be edited, but not deleted. Learn more.

Device type restrictions

Define which platforms, versions, and management types can enroll.

Priority	Name	Assigned
Default	All Users	Yes



Enrollment device limit restrictions ···

A device must comply with the highest priority enrollment restrictions assigned to its user. You can drag a device restriction to change its priority. Default restrictions are lowest priority for all users and govern userless enrollments. Default restrictions may be edited, but not deleted. Learn more.

Device limit restrictions

Define how many devices each user can enroll.

Priority	Name	Device limit	Assigned
Default	All users and all devices	5	Yes

Intune: supported OS

- Android
- IOS/iPadOS
- macOS
- ChromeOS

Intune: Provisioning

Provisioning: Setting up the device during the users’ first login:

- Using the pre-installed operating system from factory
- Applying settings and policy configurations
- Deploying applications
- Enforcing security policies

Provisioning

Benefits

- **Consistency:** All devices same configuration and software
- **Flexibility:** Custumized configuration on users needs, rather than one-size fits-all (image). independent of the image.
- **No manual operation:** zero-touch deployment capabilities.
- **Scalability:** Deployment and configuration across multiple locations

Drawbacks

- **First use:** The device is not immediately ready for use; the time required depends on the configuration and applications.
- **Internet dependent:** Provisioning requires a stable network connection, any interruptions can delay or disrupt the process.

Intune Autopilot

- **Device enrollment:** It connects the end device tot the organization, even when the device is reinstalled, stolen or wiped.
- **Automates OOBE (Out of Box Experience):** Automates and simplifies the initial device setup process during first use.
- **Zero-Touch Deployment:** Devices can be deployed remotely, with no need for IT intervention or physical contact.
- **User-Driven:** Allows users to complete the setup process themselves, reducing the need for IT resources while maintaining security and compliance.

Intune Autopilot

Devices are added in Autopilot by:

1. Manual per device
   - Extract unique hardware hash out of device with powershell
   - Adding hardware hash to Intune Autopilot devices

2. Purchase
   - The hardware reseller provides the hardware hashes upon purchase.
   - Import all hardware hashes at once to Intune Autopilot devices

3.Intune

1. MDM on prem environment
2. Enroll
3. **Configure**
4. Protect
5. Retire

2.Configure: Configuration policies

Intune Configuration Policies apply OS settings to devices, similar to how Group Policies work in traditional on-prem environments.

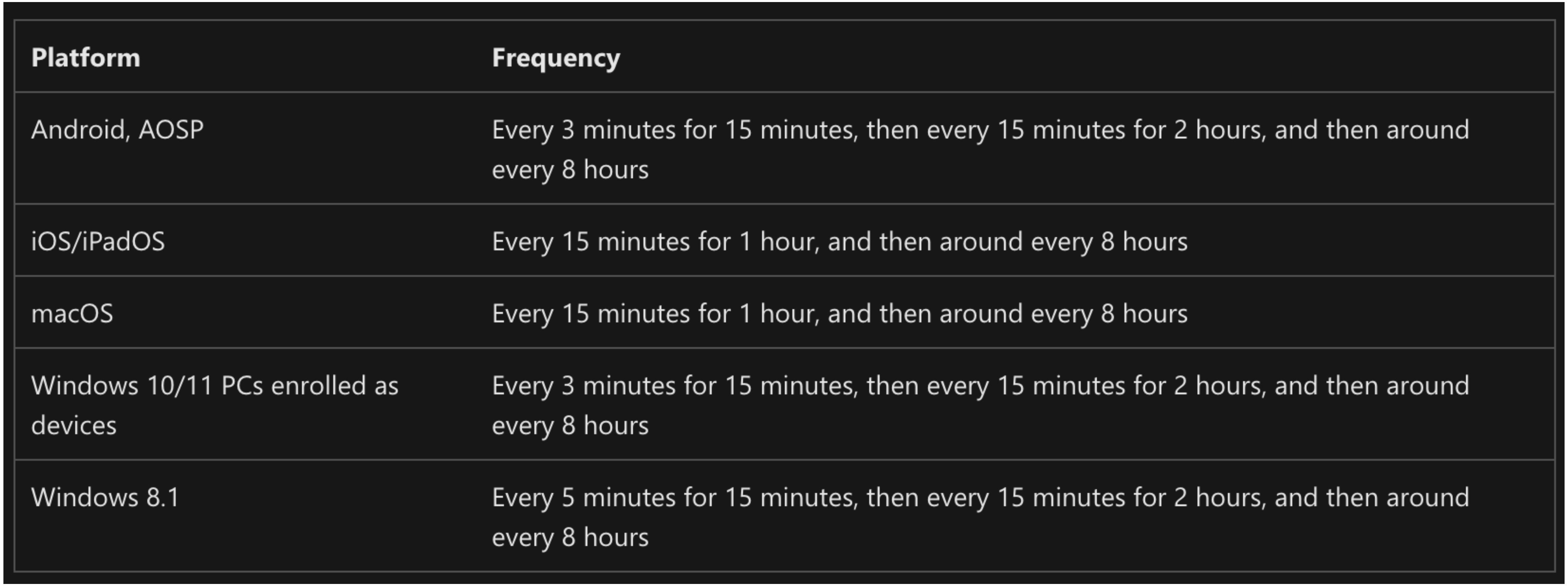
- Restricting removal media
- Restricting apps
- Restricting or configuring OS settings
- Redirecting storage folders (Documents, Pictures,…)
- …

2.Configure: Configuration policies

Configuration Profile Types:

1. **Settings catalog:** configure individual device settings, providing granular control over specific features and behaviors.
2. **Properties catalog**: This catalog allows you to gather and review detailed hardware information from the devices you manage.
3. **Templates:** pre-defined sets of configurations that group related settings together, simplifying the deployment of common policies or profiles for specific use cases.

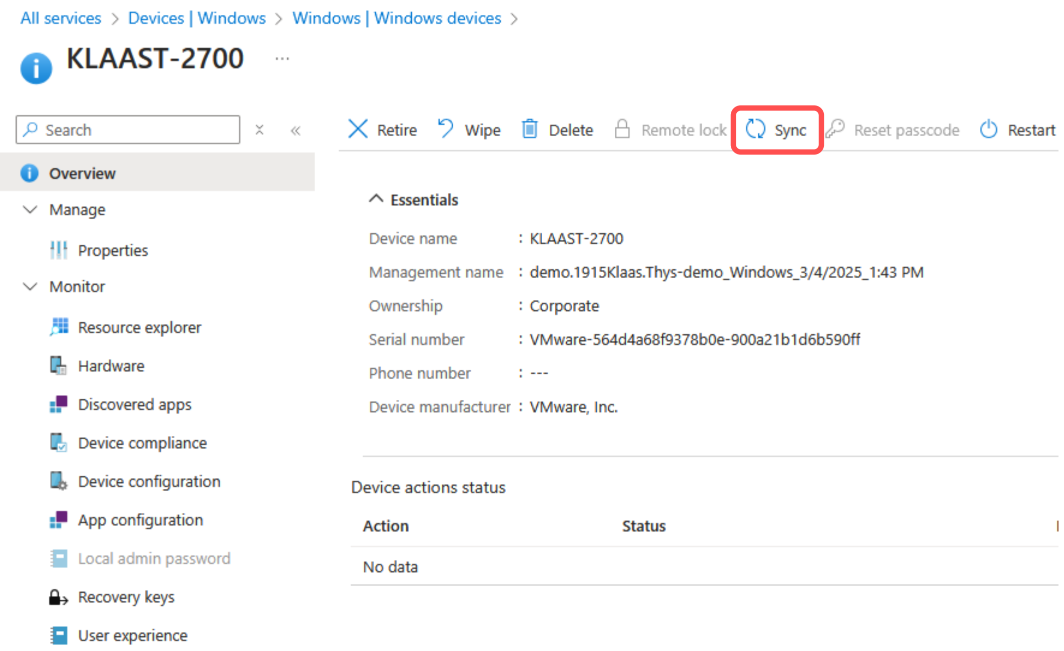
Client Sync intervals



Platform	Frequency
Android, AOSP	Every 3 minutes for 15 minutes, then every 15 minutes for 2 hours, and then around every 8 hours
iOS/iPadOS	Every 15 minutes for 1 hour, and then around every 8 hours
macOS	Every 15 minutes for 1 hour, and then around every 8 hours
Windows 10/11 PCs enrolled as devices	Every 3 minutes for 15 minutes, then every 15 minutes for 2 hours, and then around every 8 hours
Windows 8.1	Every 5 minutes for 15 minutes, then every 15 minutes for 2 hours, and then around every 8 hours

Manually sync

1.Sync - Intune



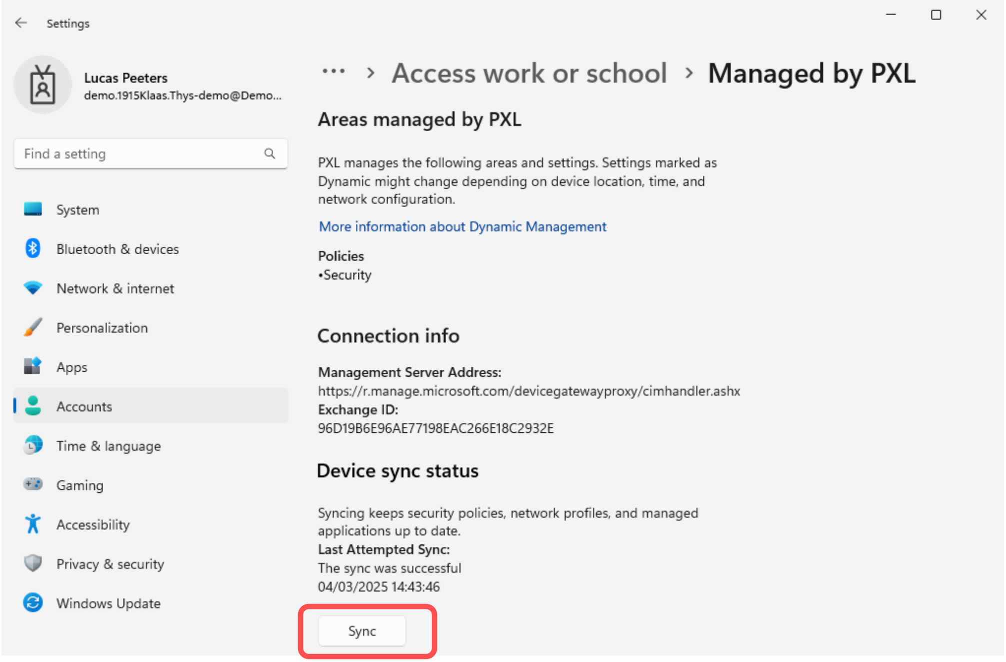
Essentials

Device name	: KLAAST-2700
Management name	: demo.1915Klaas.Thys-demo_Windows_3/4/2025_1:43 PM
Ownership	: Corporate
Serial number	: VMware-564d4a68f9378b0e-900a21b1d6b590ff
Phone number	: ---
Device manufacturer	: VMware, Inc.

Device actions status

Action	Status
No data	

2.Sync - Windows



Areas managed by PXL

PXL manages the following areas and settings. Settings marked as Dynamic might change depending on device location, time, and network configuration.

More information about Dynamic Management

Policies
•Security

Connection info

Management Server Address:
https://r.manage.microsoft.com/devicegatewayproxy/cimhandler.ashx
Exchange ID:
96D19B6E96AE77198EAC266E18C2932E

Device sync status

Syncing keeps security policies, network profiles, and managed applications up to date.
Last Attempted Sync:
The sync was successful
04/03/2025 14:43:46

3.Restarting Windows service “Microsoft Intune Management Extension”

When syncing through the Intune cloud portal or manually via Windows settings, the sync request is placed in a queue. Restarting the Intune Management Extension will trigger an immediate sync.

2.Configure: Applications

Centralized software installation on devices:

1.Required: The applications is automatically installed on the devices of the assigned groups.

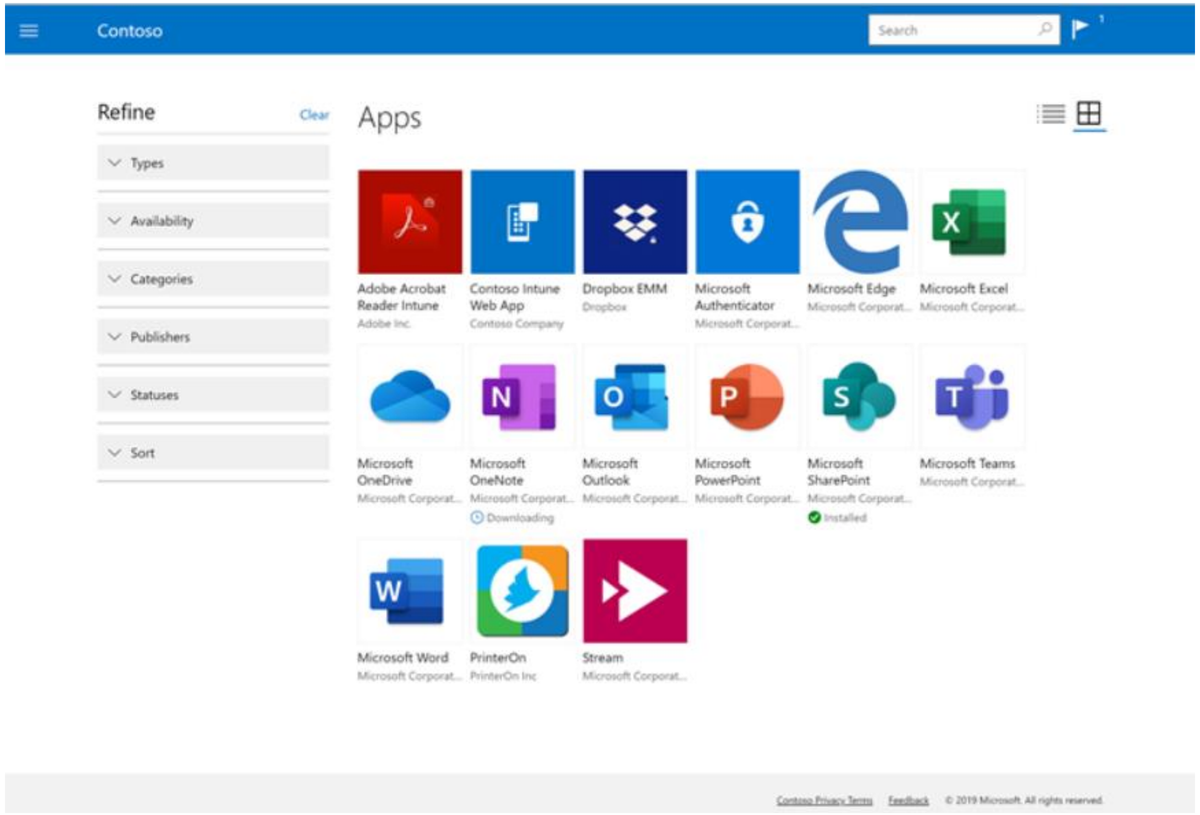
2.Available: The user can install the software themselves from the company portal.

2.Configure: Applications

Company portal

1. **Company portal app:** An application on the end device where available apps are listed, allowing employees to choose which ones they want to install.
2. **Company Portal Website:** remotely manage your work apps and enrolled personal devices.

https://portal.manage.microsoft.com



2.Configure: Applications updates

- Microsoft Store apps and Microsoft 365 apps are updated automatically.
- Line-of-business apps (MSI packages) and Windows Win32 apps are deployed through Intune but are not automatically updated.
    1. Maintaining versions of applications withing Intune ➔ time consuming
    2. managed through the **built-in updater** within the application.
    3. deploying through **package managers** like Winget or Chocolatey handles updates.

2.Configure: Applications

Supported application types:

1.Microsoft Store apps: Applications available in the Microsoft Store

2.Microsoft 365-apps: Office applications (Word, Excel, Powerpoint,…)

3.Line-Of-Business App: MSI packages

4.Web link: shortcuts to web applications

5. Windows app (Win32): Exe files.
EXE files cannot be uploaded directly, they must first be converted using IntuneWinAppUtil

2.Configure: Configuration policies

Applying configuration policies to user groups or device groups?

Rule of thumb: Policies should follow users, not devices.

User-Dependent settings:

Example: Access to terminal applications should depend on the user’s role, not the device. Assigning it to the device may restrict even local admins from accessing PowerShell.

Device Dependent Settings:

Settings which are applied directly to the device, Windows LAPS, Windows Hello, device encryption,…

3.Intune

1.MDM on prem environment

2.Enroll

3.Configure

4.Protect

5.Retire

3.Protect

Local Admin

- Is member of the local group **“Administrator”** on a Windows Device
- Full access to all system settings and configurations
- Can install, update or remove software
- Has elevated access in Command prompt and PowerShell
- Higher risk of malware due to extensive permissions

Standard user

- Limited access to system settings and configurations
- More secure against malware and unintended changes because of limited permissions
- Cannot install or remove software
- No elevated access in Command prompt or PowerShell.

3.Protect: Account protection

Local user group membership

- Select Entra users who are added as members of the local “Administrator” group.
- When one of these Entra users logs into an Intune-managed device, they will automatically be granted local administrator rights on that device.
- Less secure: Admin user will logon to these devices with his own Entra user credentials.

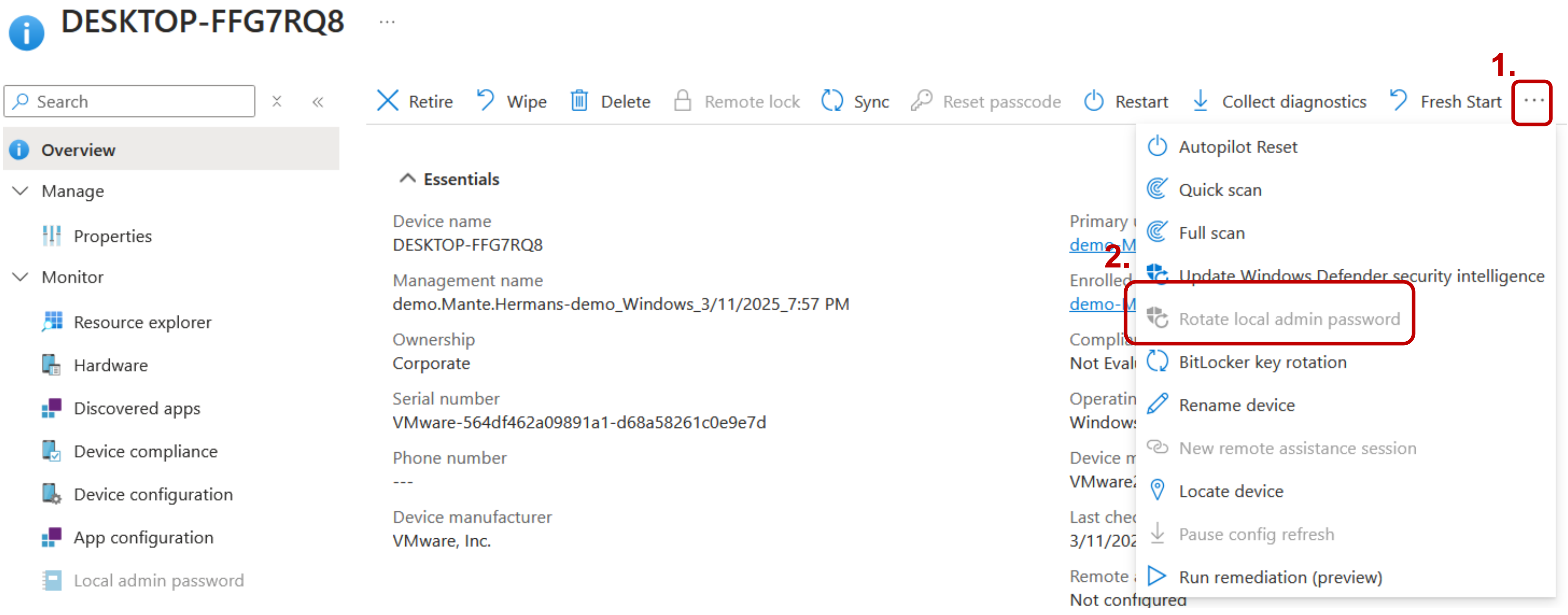
Windows LAPS

- Unique local admin account is created per device, separated from user accounts.
- Local Admin password is stored in Entra ID and automatically rotated.
- Follows the principles of Least Privilege access and Just-In-Time accces, retrieving the (rotated) password when needed.

3.Protect: Local Admin best practice

- Every user is a standard user on their own device. (Deployment profile settings).
- Users can install applications from the Company Portal without the need for admin privileges.
- If local admin rights are needed for IT support, an IT administrator can retrieve the temporary, automatically rotated LAPS password to gain local admin access and perform necessary tasks.

3.Protect: Local Admin best practice



DESKTOP-FFG7RQ8

Essentials

Device name
DESKTOP-FFG7RQ8

Management name
demo.Mante.Hermans-demo_Windows_3/11/2025_7:57 PM

Ownership
Corporate

Serial number
VMware-564df462a09891a1-d68a58261c0e9e7d

Phone number

Device manufacturer
VMware, Inc.

Primary u
demo-M

Enrolled
demo-M

Compli
Not Eval

Operatin
Window

Device m
VMware

Last chec
3/11/202

Remote a
Not configured

1.

2.

3.Protect: Windows Hello

Strong security: uses biometrics (face, fingerprint) or PIN, which are tied to the device and have no value outside the device.

Phishing protection: Users enters Windows Hello credentials instead of Entra credentials. Windows Hello credentials cannot be used to logon remotely by attackers.

Prevents password fatigue: Reduces the need for frequent password changes and complex password policies.

MFA by default: Windows Hello credentials (face, fingerprint, PIN,...) + device binding create a two-factor authentication scenario without extra steps.

Better compliance: Aligns with modern security frameworks like Zero Trust.

3.Protect: Encryption

1.Bitlocker

- **Protects Lost or Stolen Devices:** Prevents unauthorized access to data by blocking software attacks or hard drive transfers to another device.
- **Encrypts Entire Drives or Volumes:** Ensures comprehensive data encryption for full-disk security.
- On modern Windows devices, BitLocker stores the encryption key in the **TPM chip**, which releases it only if the system remains untampered.
- **Bitlocker recovery key** can be stored in Entra ID.

Microsoft Learn: Bitlocker

3.Protect: Encryption

2.Personal Data Encryption

- **User-Specific Encryption:** Encrypts files based on the user's identity, preventing unauthorized access.
- **Works Without BitLocker:** Functions independently but is recommended to be used alongside BitLocker for enhanced security.
- **Protects Personal Files:** Secures documents, pictures, and other user files without encrypting the entire drive.
- **Seamless Integration with Windows Hello for Business:** Uses authentication methods like PIN or biometrics to grant access.

Microsoft Learn: Personal Data Encryption

3.Protection: PED vs Bitlocker

Item	Personal Data Encryption	Bitlocker
Release of decryption key	At user sign-in via Windows Hello for Business	At boot
Decryption keys discarded	When user signs out of Windows or one minute after Windows lock screen is engaged	At shutdown
Protected content	All files in protected folders	Entire volume/drive
Authentication to access protected content	Windows Hello for Business	When Bitlocker with TPM + PIN is enabled, BitLocker PIN plus Windows sign-in

Microsoft recommends enabling BitLocker even though Personal Data Encryption (PDE) can function without it. PDE is designed to complement BitLocker for enhanced security, not to replace it.

3.Protect: Security Baseline

Security Baseline:

- is a group of preconfigured Windows settings that help you apply and enforce granular security settings that the relevant security teams recommend.
- Customize each baseline you deploy to enforce only those settings and values you require

Intune security baseline settings for Windows11

3.Protect: Updates

Type of Windows updates:

- **Feature updates:** Releases annually. Adding new features and functionality to Windows. Windows 11 23H2 > Windows 11 24H2.
- **Quality updates:** Quality updates deliver both security and nonsecurity fixes. Quality updates include security updates, critical updates, servicing stack updates, and driver updates. Released on second Tuesday of the month. (typically)
- **Driver updates**

Windows 11 release information

3.Protect: Updates

Update Rings are configuration profiles that allow you to manage and control Windows updates..

- **Update policy:** Define how quickly devices receive new updates.
- **Apply deferral periods:** Delay updates to allow time for testing.
- **Manage automatic restarts**
- **Set deadlines and postponement options**: Give users flexibility or enforce updates at a specific time.

Goal is to configure a gradual rollout:

1.Test Group: Receives updates first to check for compatibility issues.

2. Production Group: All devices receive the update once stability is confirmed.

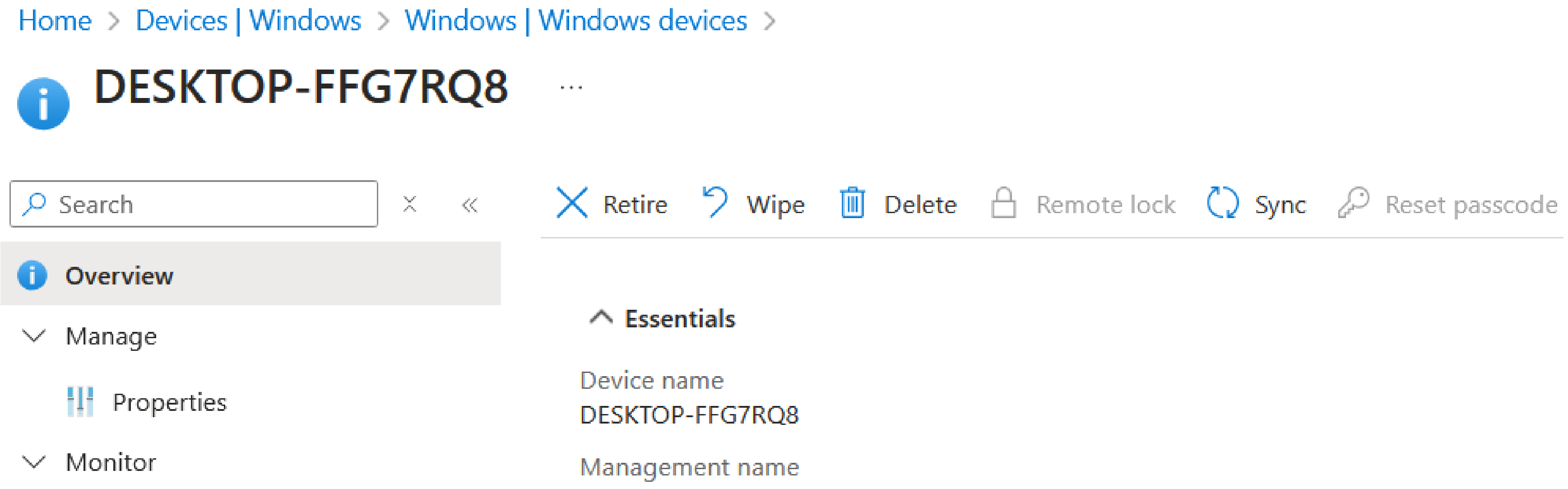
3.Intune

1. MDM on prem environment
2. Enroll
3. Configure
4. Protect
5. **Retire**

4.Retire:

There are three different device management actions used to control and secure corporate data on enrolled devices. Each serves a specific purpose in different scenarios:

1. **Wipe**
2. **Retire**
3. **Delete**



Device name
DESKTOP-FFG7RQ8

Management name

4.Retire: 1.Retire

Actions

- Device will be removed from Intune
- Removes company apps, data, settings, and email profiles.
- Keeps user data (such as photos, personal files, and installed apps) intact.

- **Scenarios**
- Employee leaves the company, but the device remains their personal property.
- When a device is no longer needed for work but is still in use by the employee.

4.Retire: 2.Wipe

Actions

- Completely resets the device to factory settings, erasing all data (personal and corporate data).
- Device will be removed from Intune.
- The device will be like new and require setup again.

Scenarios

- Device is lost or stolen.
- Before reissuing a device to another employee.
- Selling the device.

4.Retire: 3.Delete

Actions

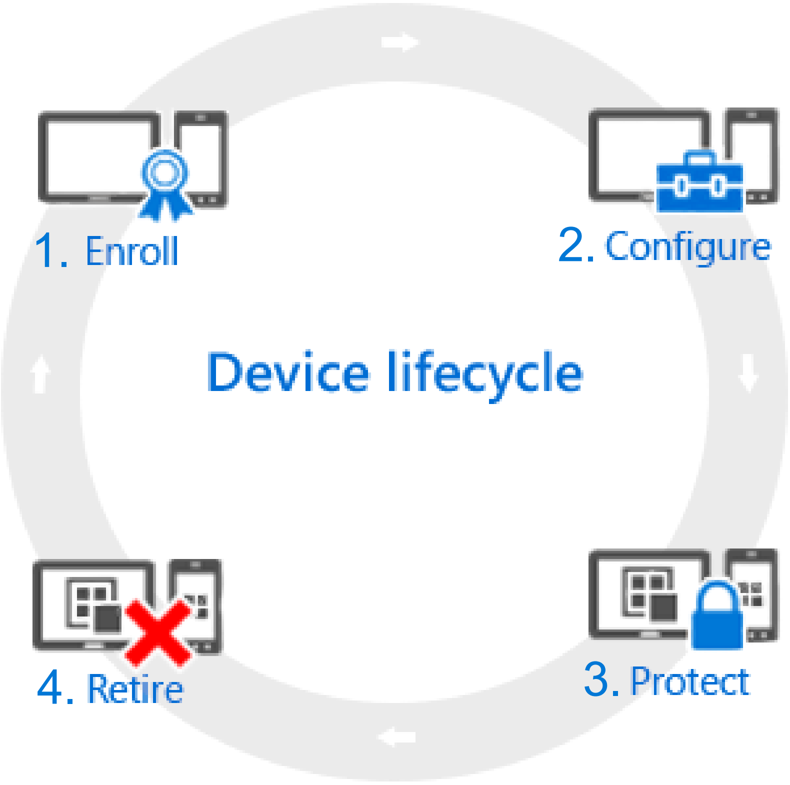
- Removes the device from the Intune.
- No action is performed on the device itself.
- The device still retain company apps, data and policies.

Scenarios

- Used when a device is incorrectly enrolled and needs to be removed from Intune.
- Cleaning up old, non-reporting devices from Intune inventory.

Device Lifecycle

- Add hardware hashes to **Autopilot**
- Configure Autopilot implementation profile
- Users register devices via Entra authentication



- Applying configuration profiles
- Installing required apps

- Applying configuration profiles
- Endpoint security settings: LAPS, device encryption, security baseline

- Wipe
- Retire
- Delete