NIC Cloud Connect

Oslo Spektrum
November 7 - 9

Cloud Connect

Simon Skotheimsvik

Unmasking 10 Frequent Intune Mistakes and How to Prevent Them

nic Cloud Connect

INTUNE

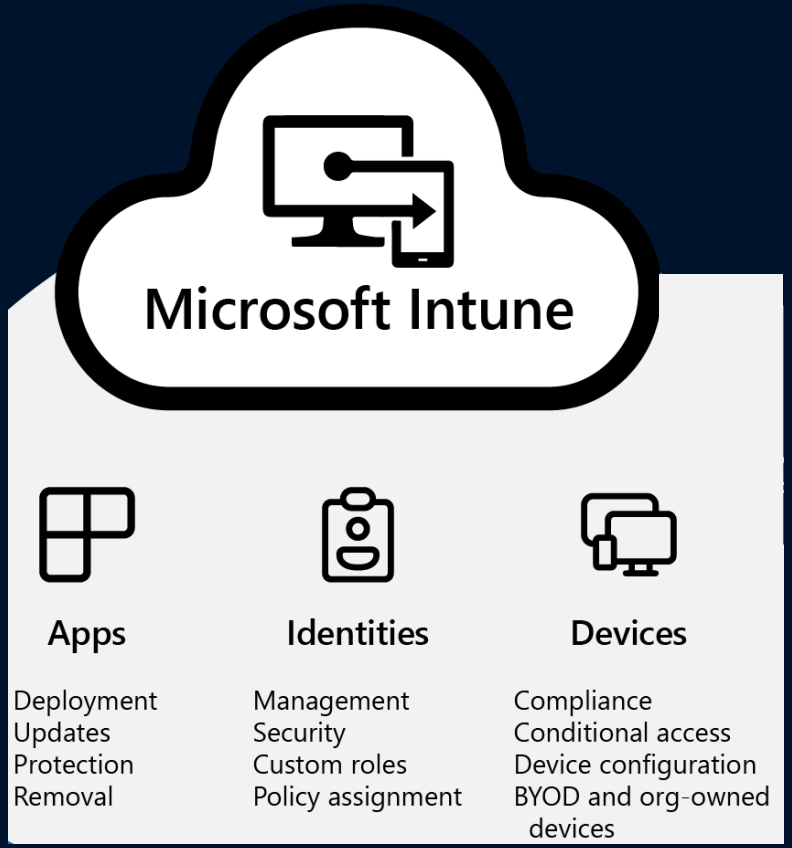
nic Cloud Connect

INTUNE

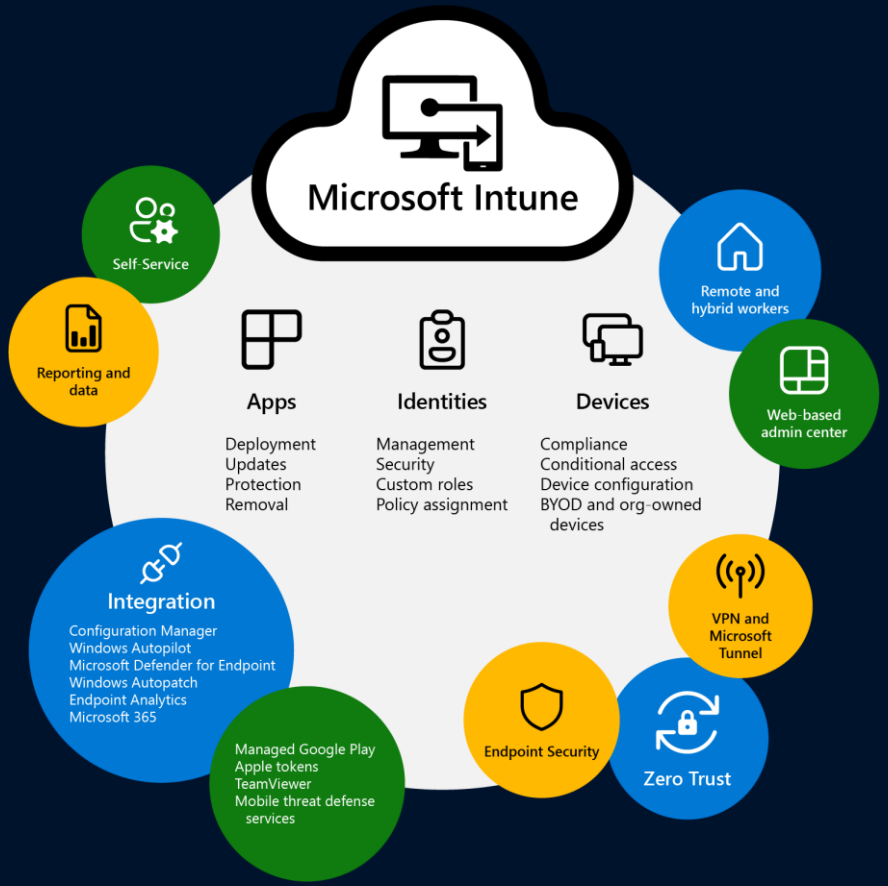
nic Cloud Connect

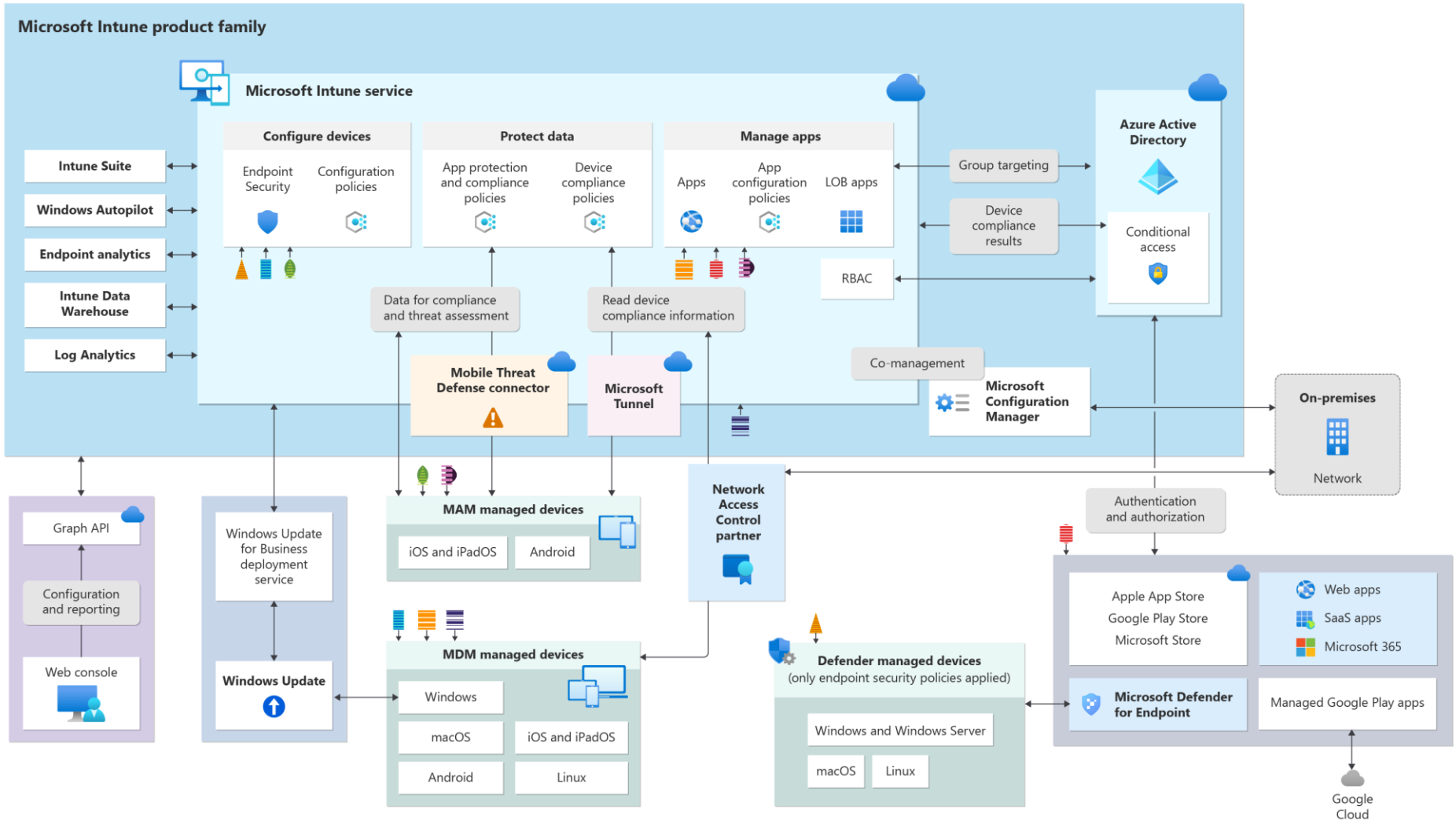
INTUNE

INTUNE

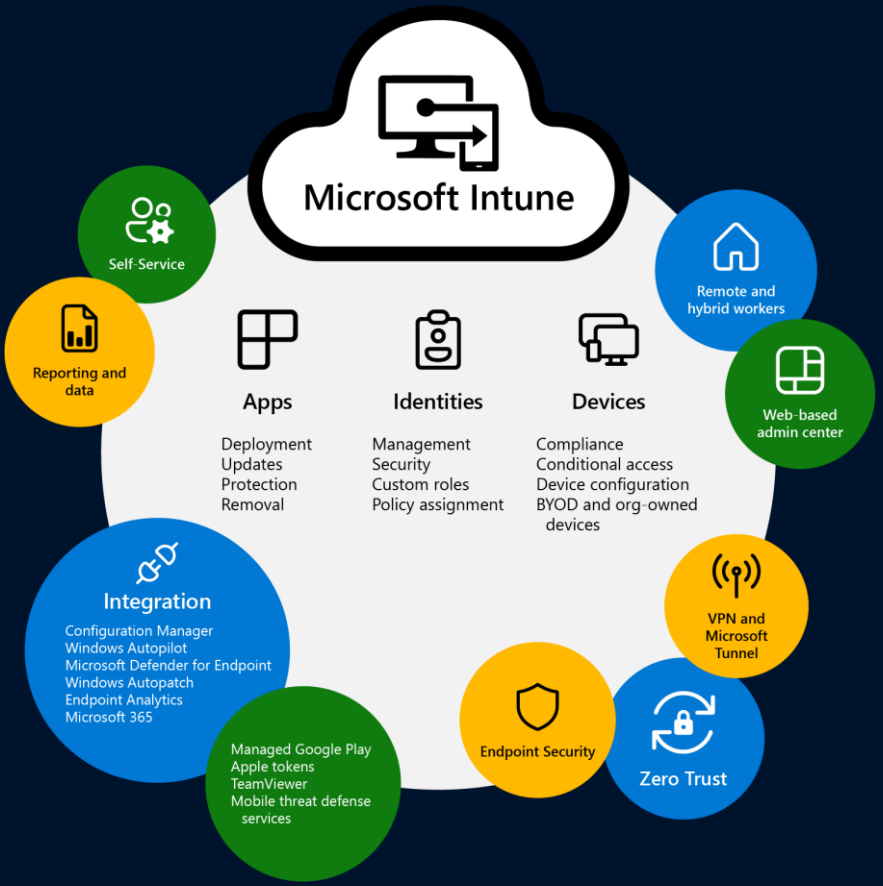

Microsoft Intune
Apps
Identities
Devices
Deployment
Updates
Protection
Removal
Management
Security
Custom roles
Policy assignment
Compliance
Conditional access
Device configuration
BYOD and org-owned devices

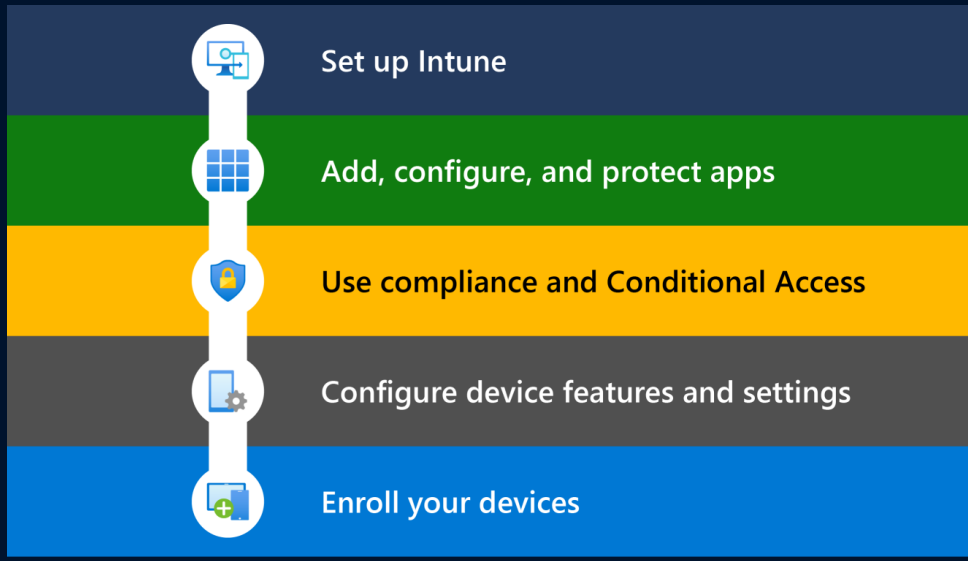
INTUNE


Microsoft Intune
Self-Service
Reporting and data
Remote and hybrid workers
Web-based admin center
Apps
Deployment
Updates
Protection
Removal
Identities
Management
Security
Custom roles
Policy assignment
Devices
Compliance
Conditional access
Device configuration
BYOD and org-owned devices
Integration
Configuration Manager
Windows Autopilot
Microsoft Defender for Endpoint
Windows Autopatch
Endpoint Analytics
Microsoft 365
Managed Google Play
Apple tokens
TeamViewer
Mobile threat defense services
Endpoint Security
VPN and Microsoft Tunnel
Zero Trust


Microsoft Intune product family
Microsoft Intune service
Configure devices
Endpoint Security
Configuration policies
Protect data
App protection and compliance policies
Device compliance policies
Manage apps
Apps
App configuration policies
LOB apps
Intune Suite
Windows Autopilot
Endpoint analytics
Intune Data Warehouse
Log Analytics
Group targeting
Device compliance results
RBAC
Azure Active Directory
Conditional access
Data for compliance and threat assessment
Read device compliance information
Co-management
Mobile Threat Defense connector
Microsoft Tunnel
Microsoft Configuration Manager
On-premises
Network
Graph API
Configuration and reporting
Web console
Windows Update for Business deployment service
Windows Update
MAM managed devices
iOS and iPadOS
Android
Network Access Control partner
Authentication and authorization
MDM managed devices
Windows
macOS
iOS and iPadOS
Android
Linux
Defender managed devices
(only endpoint security policies applied)
Windows and Windows Server
macOS
Linux
Apple App Store
Google Play Store
Microsoft Store
Web apps
SaaS apps
Microsoft 365
Microsoft Defender for Endpoint
Managed Google Play apps
Google Cloud

INTUNE


Microsoft Intune
Self-Service
Reporting and data
Remote and hybrid workers
Web-based admin center
Apps
Deployment
Updates
Protection
Removal
Identities
Management
Security
Custom roles
Policy assignment
Devices
Compliance
Conditional access
Device configuration
BYOD and org-owned devices
Integration
Configuration Manager
Windows Autopilot
Microsoft Defender for Endpoint
Windows Autopatch
Endpoint Analytics
Microsoft 365
VPN and Microsoft Tunnel
Managed Google Play
Apple tokens
TeamViewer
Mobile threat defense services
Endpoint Security
Zero Trust


Set up Intune
Add, configure, and protect apps
Use compliance and Conditional Access
Configure device features and settings
Enroll your devices

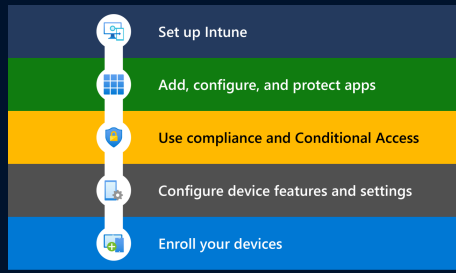
NIC Cloud Connect

SIMON SKOTHEIMSVIK

Senior Cloud Consultant

CloudWay

@SSkotheimsvik



Set up Intune

Configure

- Custom domain name
- Users and groups
- Licenses, roles, and admin permissions
- MDM authority
- Company portal

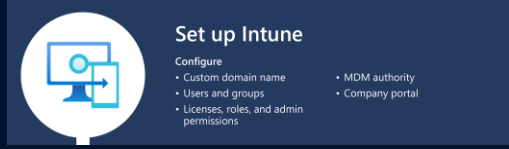
Add, configure, and protect apps

Use compliance and Conditional Access

Configure device features and settings

Enroll your devices

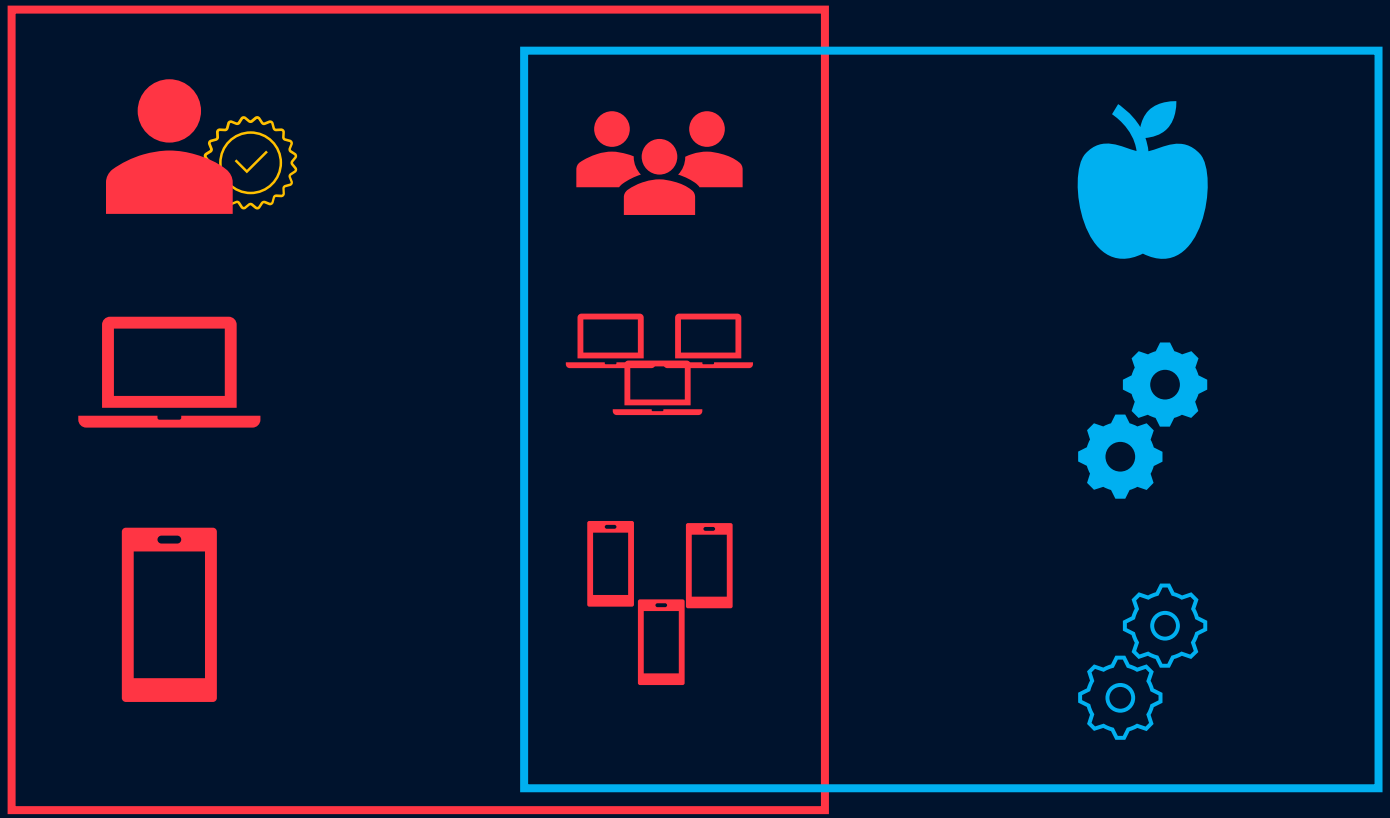
NIC Cloud Connect

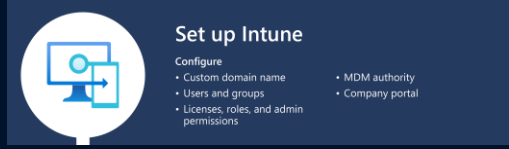


10 Users and Groups

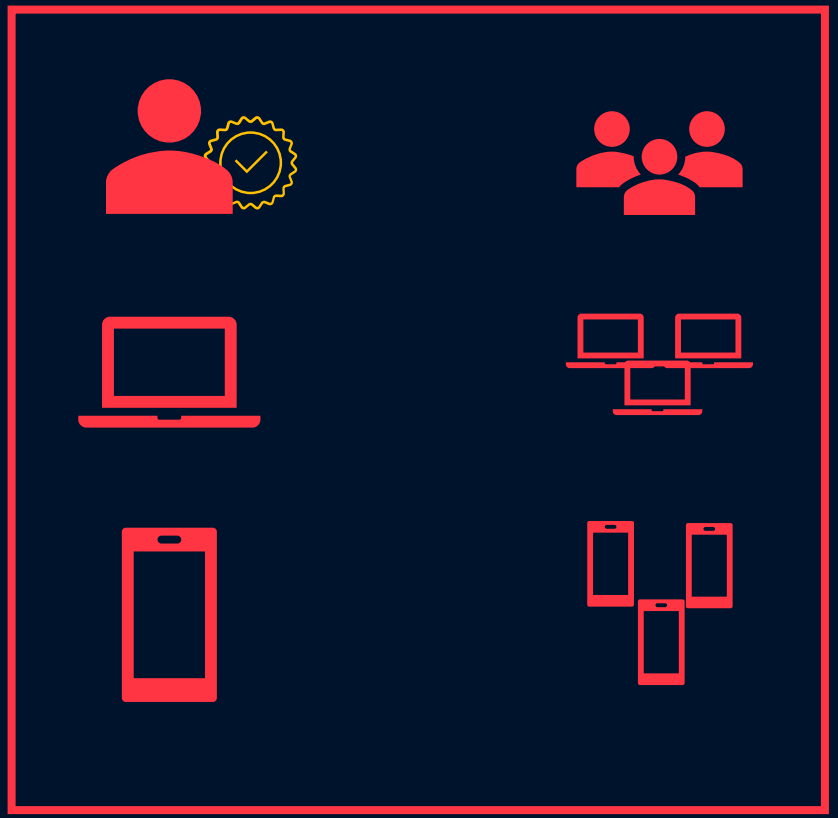
Unmasking 10 Frequent Intune Mistakes and How to Prevent Them

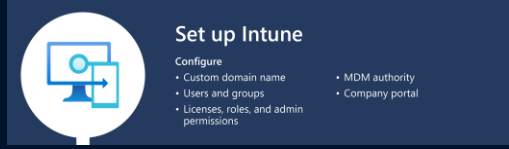
10. Users and Groups

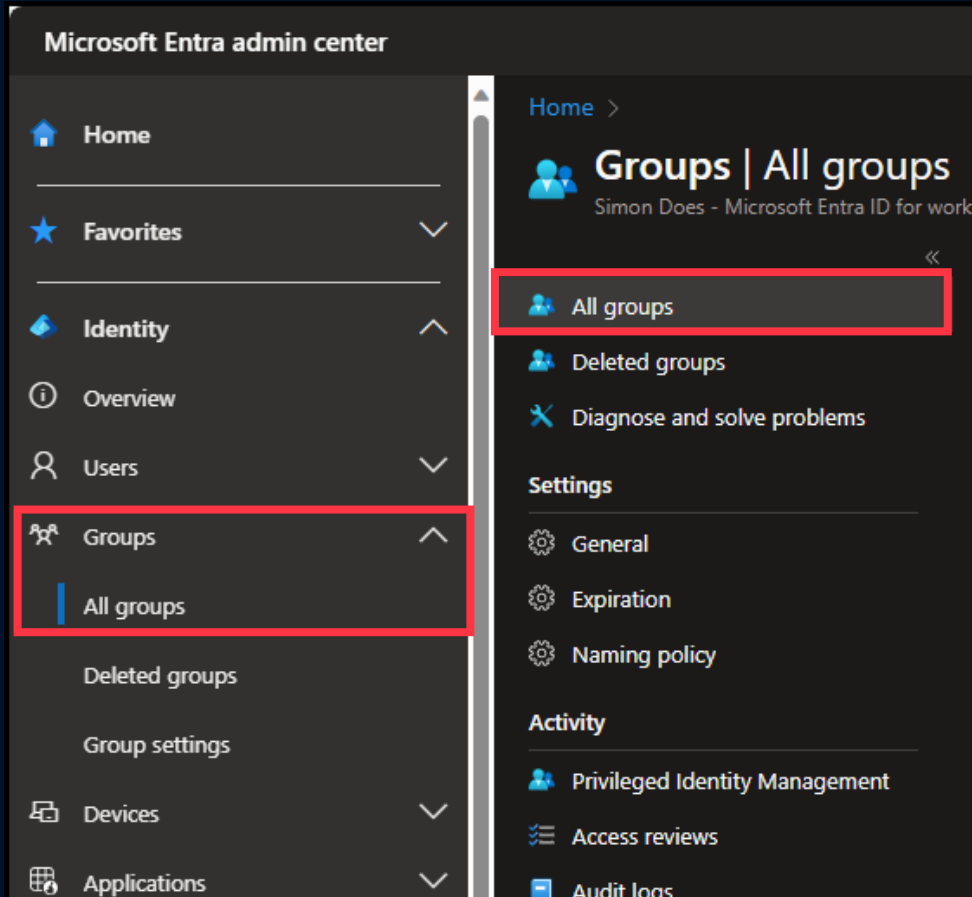


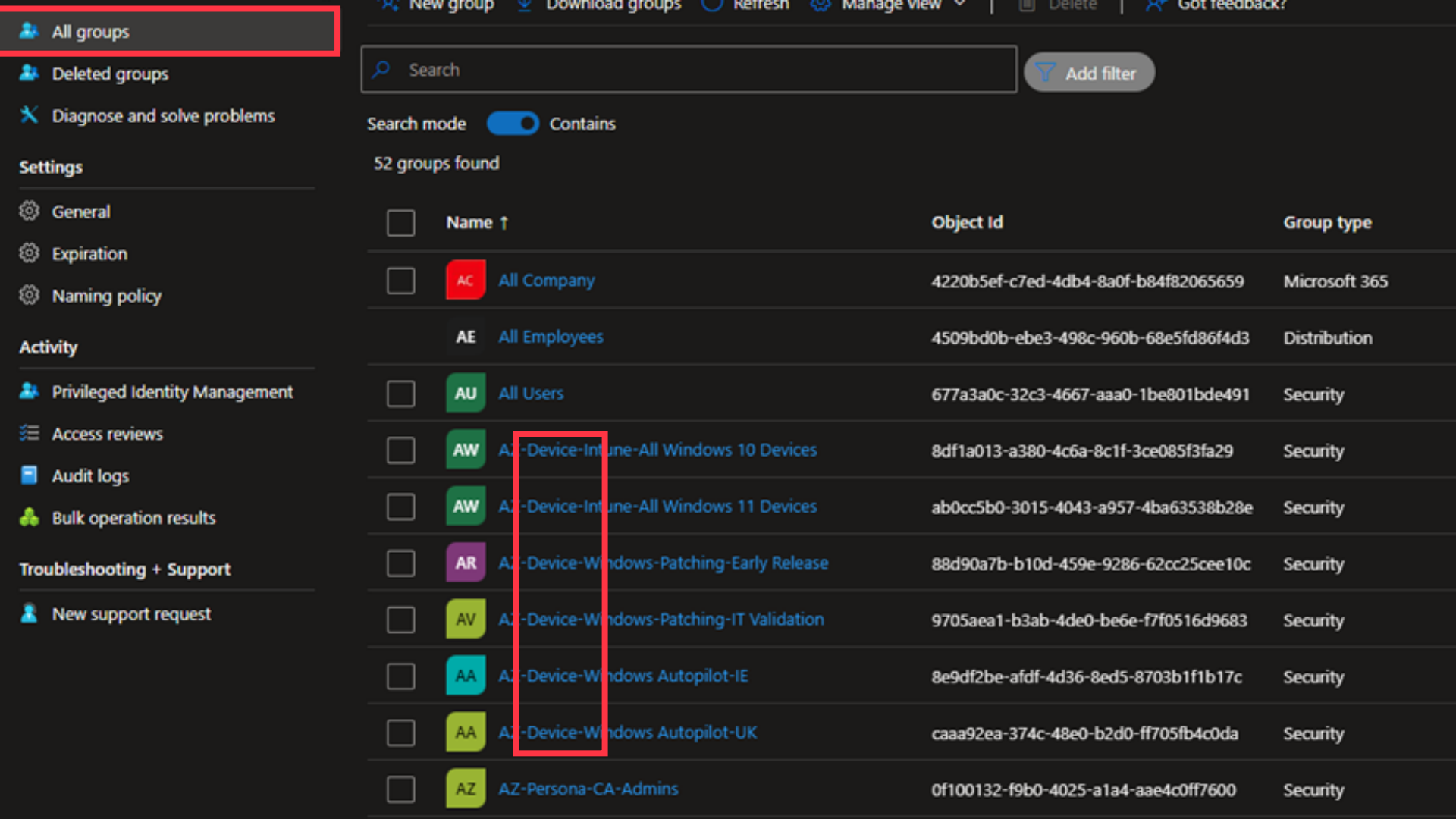


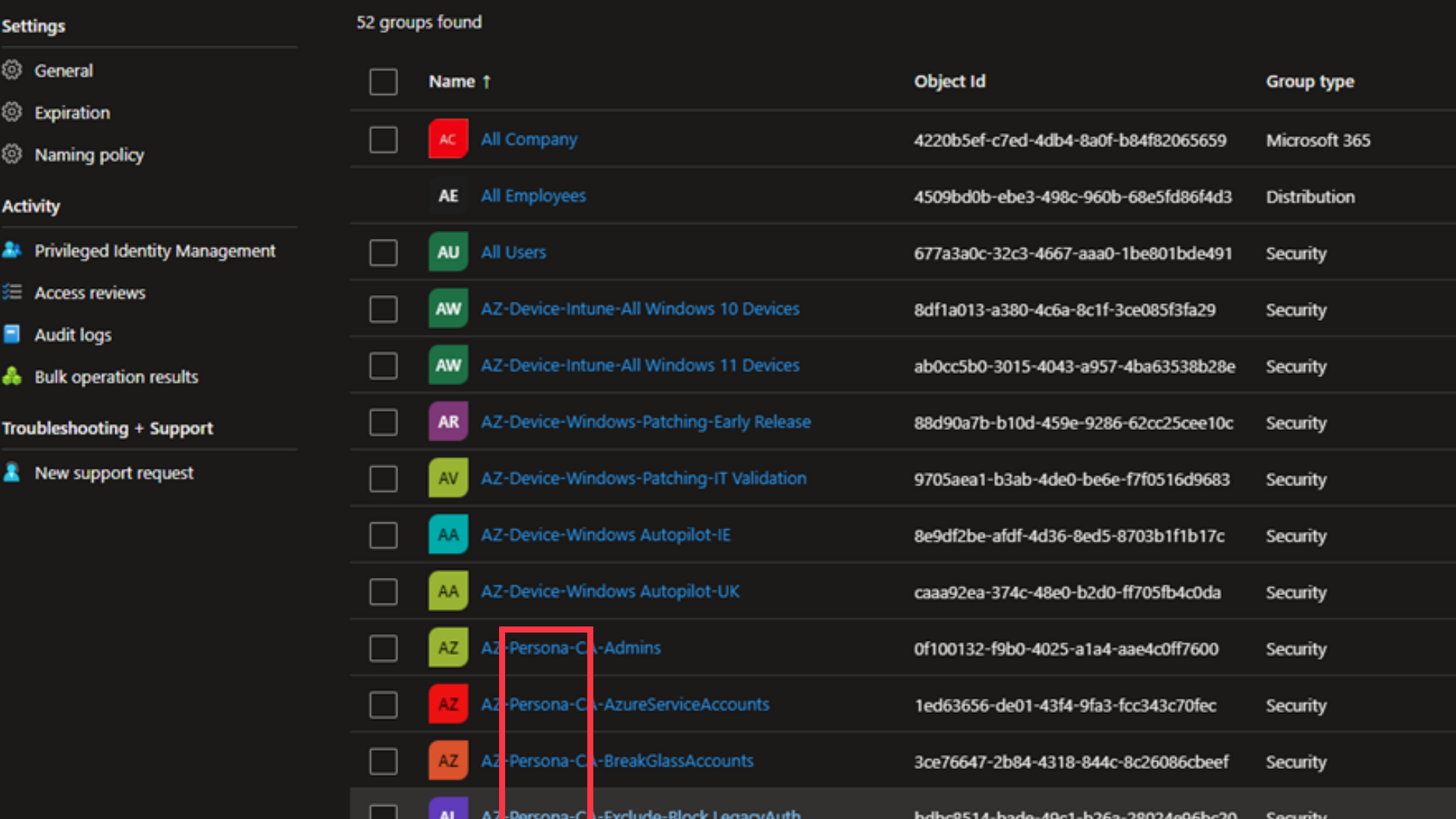
10. Users and Groups








All groups
Deleted groups
Diagnose and solve problems
Settings
General
Expiration
Naming policy
Activity
Privileged Identity Management
Access reviews
Audit logs
Bulk operation results
Troubleshooting + Support
New support request
New group
Download groups
Refresh
Manage view
Delete
Got feedback?
Search
Add filter
Search mode
Contains
52 groups found
Name ↑
Object Id
Group type
AC All Company 4220b5ef-c7ed-4db4-8a0f-b84f82065659 Microsoft 365
AE All Employees 4509bd0b-ebe3-498c-960b-68e5fd86f4d3 Distribution
AU All Users 677a3a0c-32c3-4667-aaa0-1be801bde491 Security
AW AZ-Device-Intune-All Windows 10 Devices 8df1a013-a380-4c6a-8c1f-3ce085f3fa29 Security
AW AZ-Device-Intune-All Windows 11 Devices ab0cc5b0-3015-4043-a957-4ba63538b28e Security
AR AZ-Device-Windows-Patching-Early Release 88d90a7b-b10d-459e-9286-62cc25cee10c Security
AV AZ-Device-Windows-Patching-IT Validation 9705aea1-b3ab-4de0-be6e-f7f0516d9683 Security
AA AZ-Device-Windows Autopilot-IE 8e9df2be-afdf-4d36-8ed5-8703b1f1b17c Security
AA AZ-Device-Windows Autopilot-UK caaa92ea-374c-48e0-b2d0-ff705fb4c0da Security
AZ AZ-Persona-CA-Admins 0f100132-f9b0-4025-a1a4-aae4c0ff7600 Security


Settings
General
Expiration
Naming policy
Activity
Privileged Identity Management
Access reviews
Audit logs
Bulk operation results
Troubleshooting + Support
New support request
52 groups found
Name ↑
Object Id
Group type
AC All Company 4220b5ef-c7ed-4db4-8a0f-b84f82065659 Microsoft 365
AE All Employees 4509bd0b-ebe3-498c-960b-68e5fd86f4d3 Distribution
AU All Users 677a3a0c-32c3-4667-aaa0-1be801bde491 Security
AW AZ-Device-Intune-All Windows 10 Devices 8df1a013-a380-4c6a-8c1f-3ce085f3fa29 Security
AW AZ-Device-Intune-All Windows 11 Devices ab0cc5b0-3015-4043-a957-4ba63538b28e Security
AR AZ-Device-Windows-Patching-Early Release 88d90a7b-b10d-459e-9286-62cc25cee10c Security
AV AZ-Device-Windows-Patching-IT Validation 9705aea1-b3ab-4de0-be6e-f7f0516d9683 Security
AA AZ-Device-Windows Autopilot-IE 8e9df2be-afdf-4d36-8ed5-8703b1f1b17c Security
AA AZ-Device-Windows Autopilot-UK caaa92ea-374c-48e0-b2d0-ff705fb4c0da Security
AZ AZ-Persona-CA-Admins 0f100132-f9b0-4025-a1a4-aae4c0ff7600 Security
AZ AZ-Persona-CA-AzureServiceAccounts 1ed63656-de01-43f4-9fa3-fcc343c70fec Security
AZ AZ-Persona-CA-BreakGlassAccounts 3ce76647-2b84-4318-844c-8c26086cbeef Security

Groups | All groups

Simon Does - Microsoft Entra ID for workforce

- All groups
- Deleted groups
- Diagnose and solve problems

Settings

- General
- Expiration
- Naming policy

Activity

- Privileged Identity Management
- Access reviews
- Audit logs
- Bulk operation results

Troubleshooting + Support

- New support request

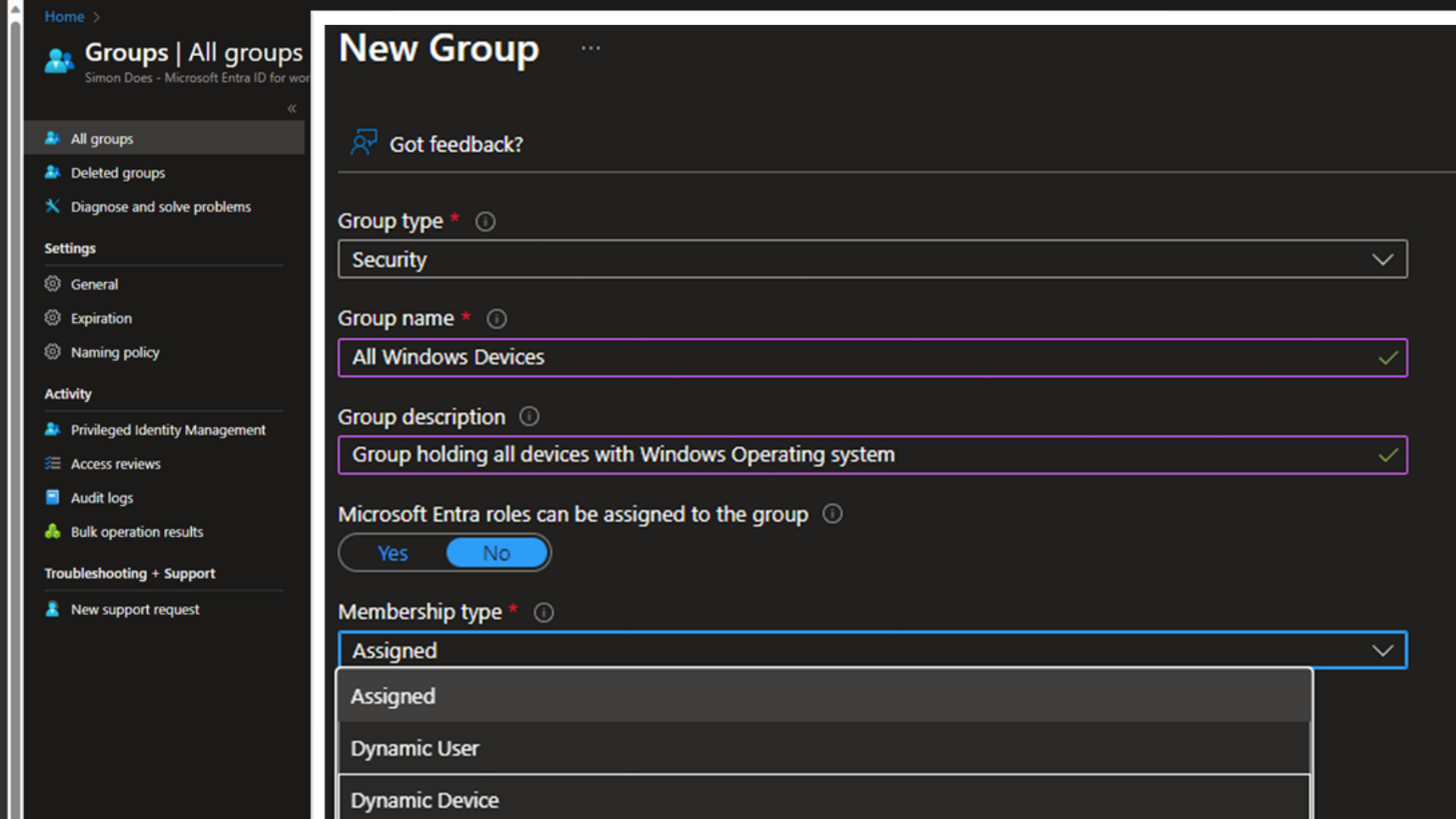
New group | Download groups | Refresh | Manage view | Delete | Got feedback?

Search | Add filter

Search mode: Contains

52 groups found

Name ↑	Object Id	Group type	Membership type
All Company	4220b5ef-c7ed-4db4-8a0f-b84f82065659	Microsoft 365	Assigned
All Employees	4509bd0b-ebe3-498c-960b-68e5fd86f4d3	Distribution	Assigned
All Users	677a3a0c-32c3-4667-aaa0-1be801bde491	Security	Dynamic
AZ-Device-Intune-All Windows 10 Devices	8df1a013-a380-4c6a-8c1f-3ce085f3fa29	Security	Dynamic
AZ-Device-Intune-All Windows 11 Devices	ab0cc5b0-3015-4043-a957-4ba63538b28e	Security	Dynamic
AZ-Device-Windows-Patching-Early Release	88d90a7b-b10d-459e-9286-62cc25cee10c	Security	Assigned
AZ-Device-Windows-Patching-IT Validation	9705aea1-b3ab-4de0-be6e-f7f0516d9683	Security	Assigned
AZ-Device-Windows Autopilot-IE	8e9df2be-afdf-4d36-8ed5-8703b1f1b17c	Security	Dynamic
AZ-Device-Windows Autopilot-UK	caaa92ea-374c-48e0-b2d0-ff705fb4c0da	Security	Dynamic
AZ-Persona-CA-Admins	0f100132-f9b0-4025-a1a4-aae4c0ff7600	Security	Assigned
AZ-Persona-CA-AzureServiceAccounts	1ed63656-de01-43f4-9fa3-fcc343c70fec	Security	Assigned


Home
Groups | All groups
Simon Does - Microsoft Entra ID for wor
All groups
Deleted groups
Diagnose and solve problems
Settings
General
Expiration
Naming policy
Activity
Privileged Identity Management
Access reviews
Audit logs
Bulk operation results
Troubleshooting + Support
New support request
New Group
Got feedback?
Group type *
Security
Group name *
All Windows Devices
Group description
Group holding all devices with Windows Operating system
Microsoft Entra roles can be assigned to the group
Yes
No
Membership type *
Assigned
Assigned
Dynamic User
Dynamic Device

Home >

Groups | All groups

Simon Does - Microsoft Entra ID for workforce

New group | Download groups | Refresh | Manage view | Delete | Got feedback?

All groups

Deleted g

Diagnose

Settings

General

Expiratio

Naming

Activity

Privilege

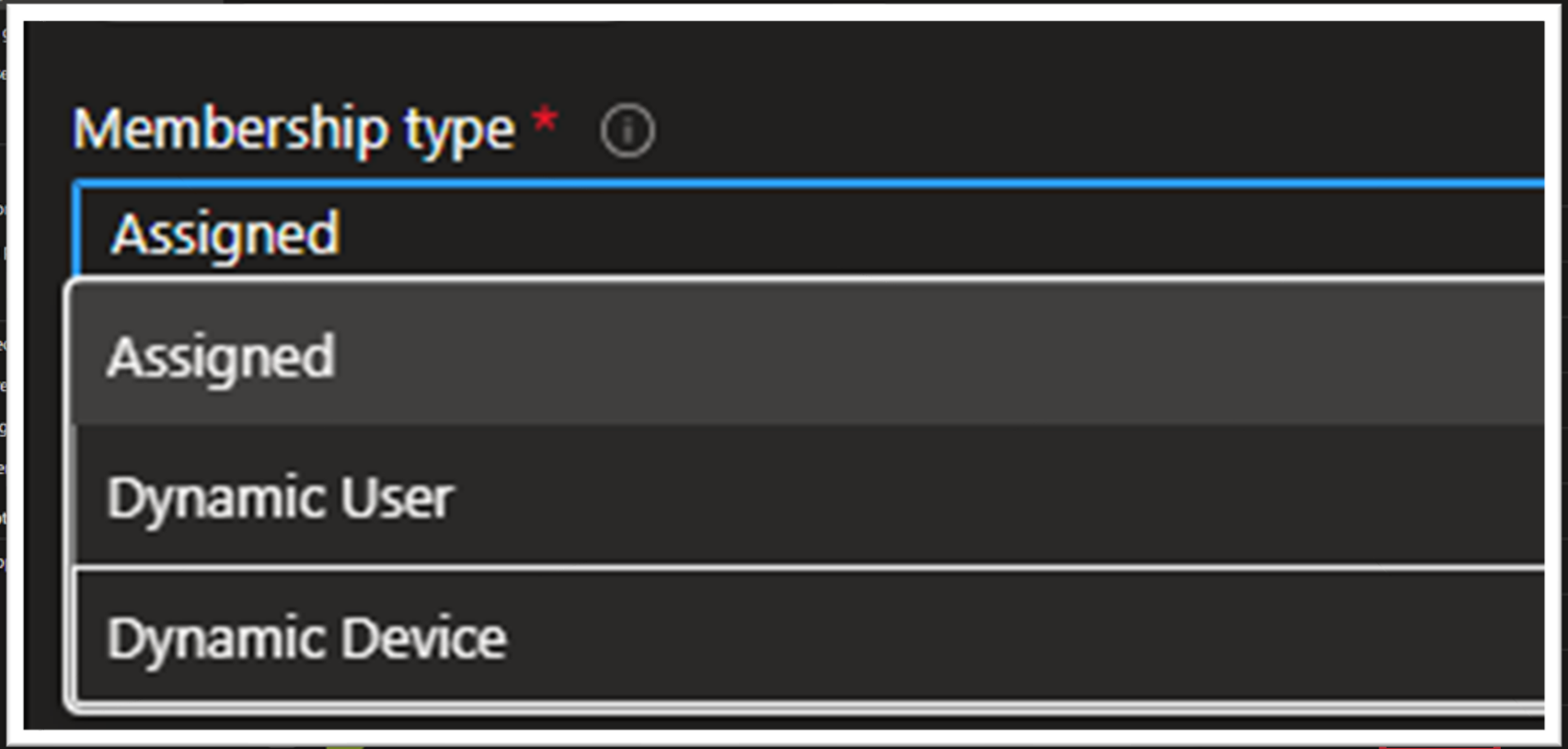
Access re

Audit log

Bulk ope

Troubleshoot

New sup



AZ AZ-Persona-CA-AzureServiceAccounts 1ed63656-de01-43f4-9fa3-fcc343c70fec Security Assigned

Home >

Groups | All groups

Simon Does - Microsoft Entra ID for workforce

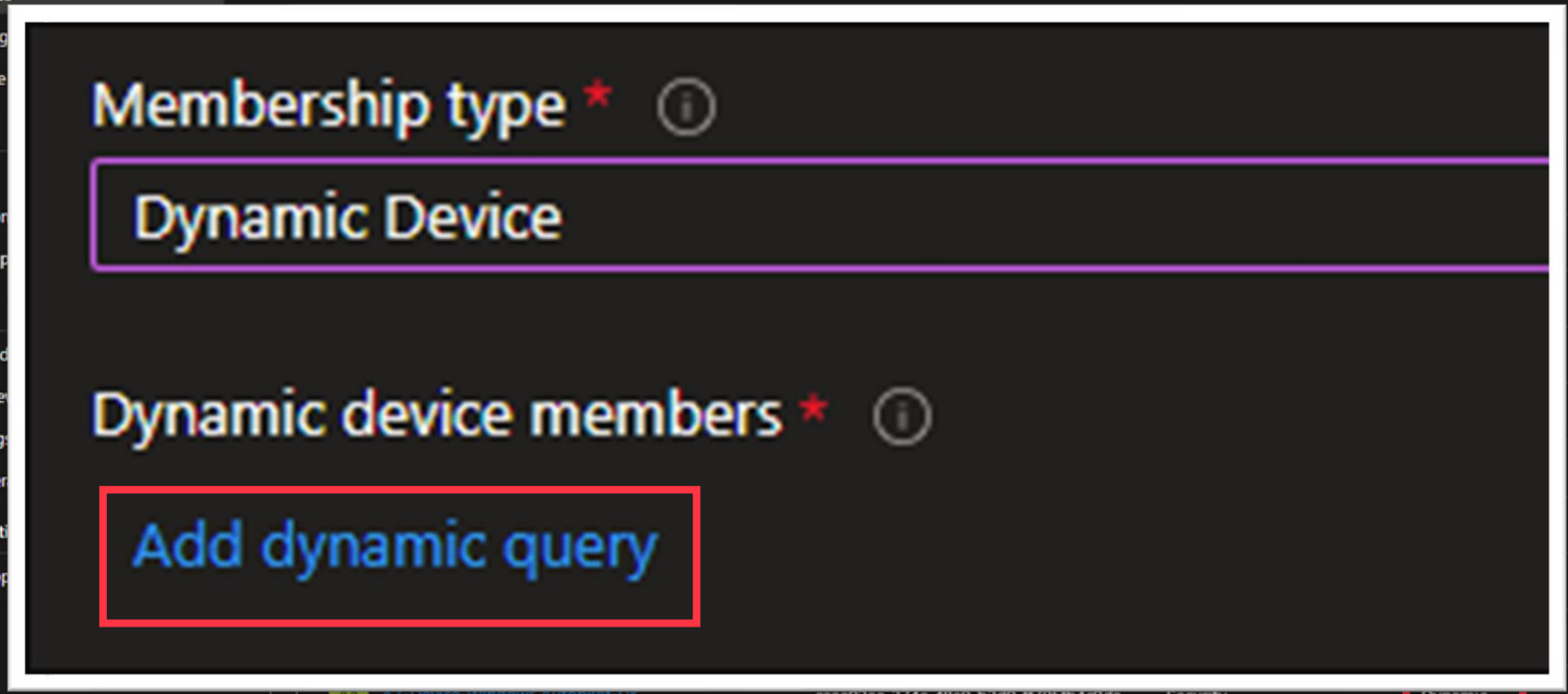
New group | Download groups | Refresh | Manage view | Delete | Got feedback?

All groups
Deleted g
Diagnose

Settings
General
Expiration
Naming p

Activity
Privileged
Access re
Audit log
Bulk oper

Troubleshooti
New supp



	AA	AZ-Device-Windows Autopilot-UK	caaa92ea-374c-48e0-b2d0-ff705fb4c0da	Security	Dynamic
	AZ	AZ-Persona-CA-Admins	0f100132-f9b0-4025-a1a4-aae4c0ff7600	Security	Assigned
	AZ	AZ-Persona-CA-AzureServiceAccounts	1ed63656-de01-43f4-9fa3-fcc343c70fec	Security	Assigned

Dynamic membership rules

Save | Discard | Got feedback?

Configure Rules | Validate Rules (Preview)

You can use the rule builder or rule syntax text box to create or edit a dynamic membership rule. Learn more

And/Or	Property	Operator	Value
	Choose a Property	Choose an Operator	Add a value

+ Add expression

Rule syntax

Edit

- accountEnabled
- objectId
- displayName
- isRooted
- deviceOSType
- deviceOSVersion
- deviceCategory
- deviceManufacturer
- deviceModel
- deviceOwnership

Dynamic membership rules

Save

Configure Rules | Validate Rules (Preview)

You can use the rule builder or rule syntax text box to create or edit a dynamic membership rule. Learn more

And/Or	Property	Operator	Value
	deviceOSType	Contains	Windows
And	deviceOSVersion	Starts With	10.0.22

Add expression

Rule syntax

```
(device.deviceOSType -contains "Windows") and (device.deviceOSVersion -startsWith "10.0.22")
```

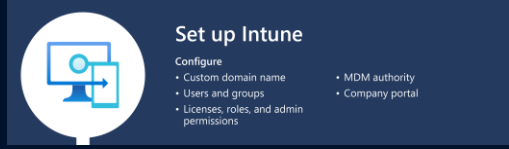
deviceCategory

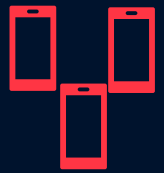
deviceManufacturer

deviceModel

deviceOwnership

10. Users and Groups





All Windows 10 devices
(device.deviceOSType -contains "Windows") and (device.deviceOSVersion -startsWith "10.0.19")

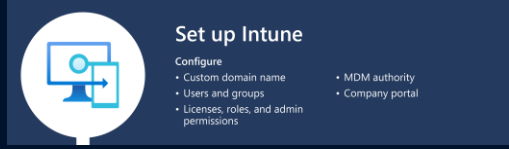
All Windows 11 devices
(device.deviceOSType -contains "Windows") and (device.deviceOSVersion -startsWith "10.0.22")

All Autopilot devices with Grouptag like IE
(device.devicePhysicalIds -any (_ -eq "[OrderID]:IE"))

All users on Sales Department
user.department -eq ”Sales“

https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-dynamic-membership

10. Users and Groups



All Windows 10 devices
(device.deviceOSType -contains "Windows") and (device.deviceOSVersion -startsWith "10.0.19")

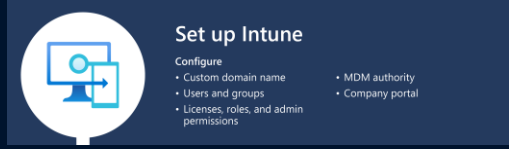
All Windows 11 devices
(device.deviceOSType -contains "Windows") and (device.deviceOSVersion -startsWith "10.0.22")

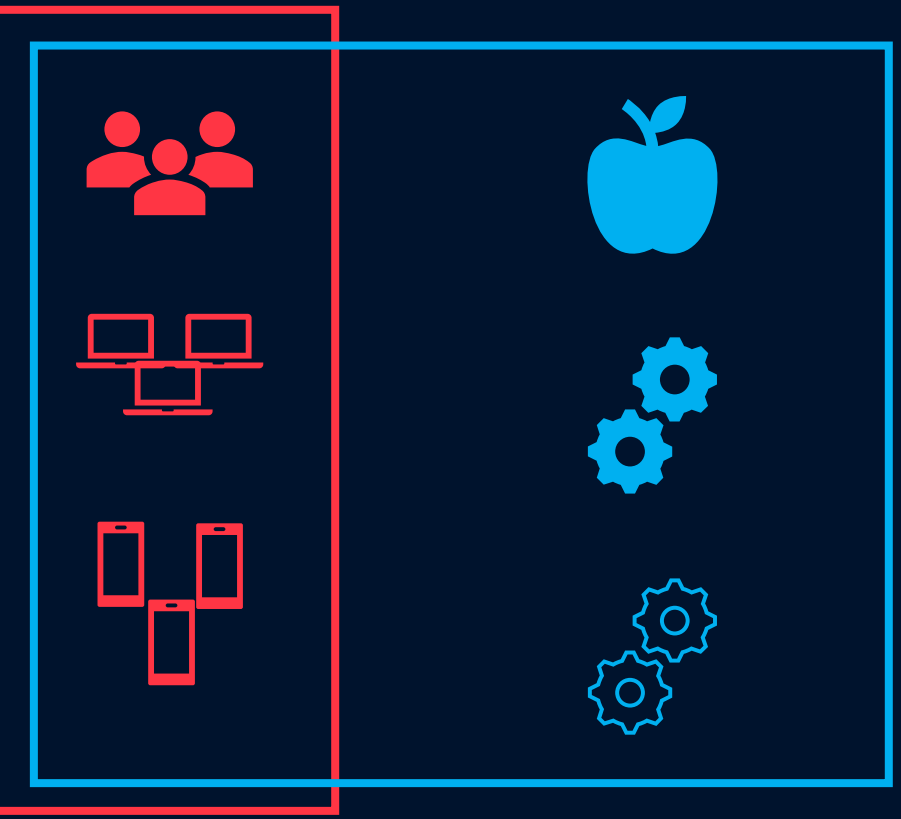
All Autopilot devices with Grouptag like
(device.devicePhysicalIds -any (_ -eq "[OrderID

All users on Sales Department
user.department -eq ”Sales“

https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-dynamic-membership

10. Users and Groups





User group vs Device group

https://learn.microsoft.com/en-us/mem/intune/configuration/device-profile-assign#user-groups-vs-device-groups

10. Users and Groups

User group vs Device group

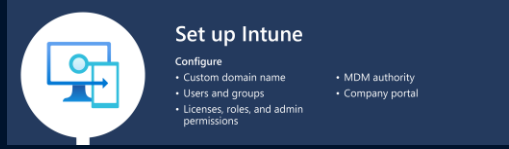
https://learn.microsoft.com/en-us/mem/intune/configuration/device-profile-assign#user-groups-vs-device-groups

10. Users and Groups

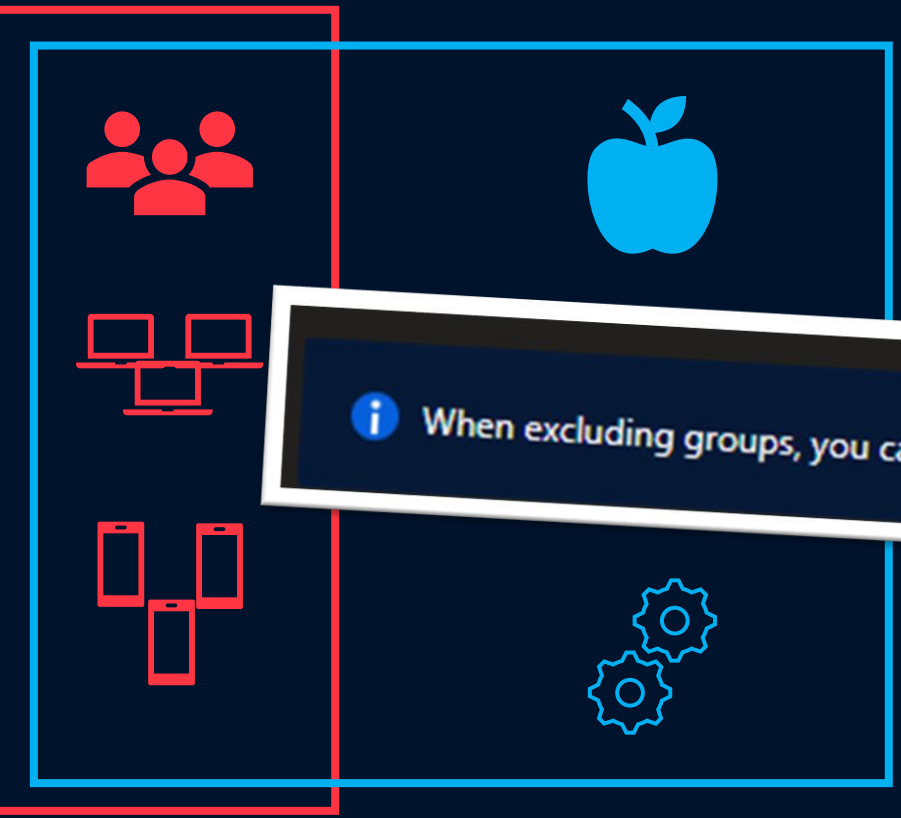
User group vs Device group

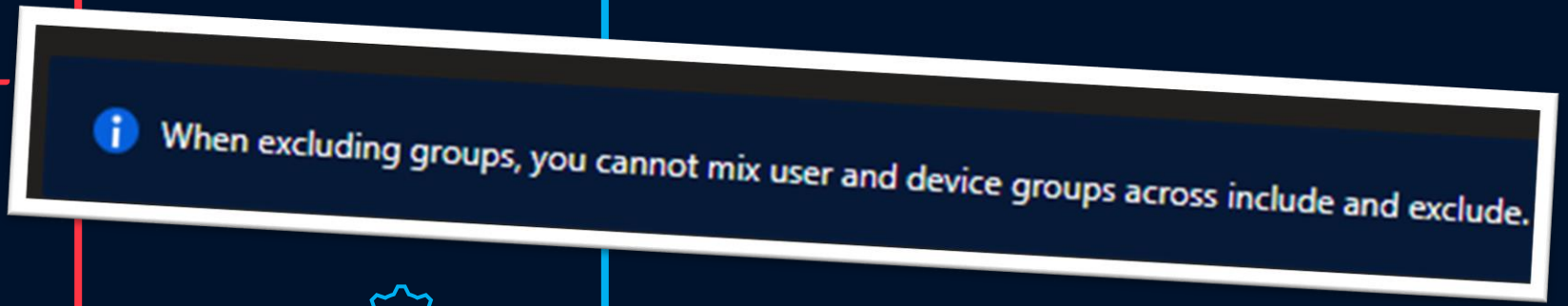
https://learn.microsoft.com/en-us/mem/intune/configuration/device-profile-assign#user-groups-vs-device-groups

10. Users and Groups



User group vs Device group





https://learn.microsoft.com/en-us/mem/intune/configuration/device-profile-assign#user-groups-vs-device-groups

10. Users and Groups

User group vs Device group

I don't see membership changes instantly when I add or change a rule, why not?

Dedicated … groups are slow

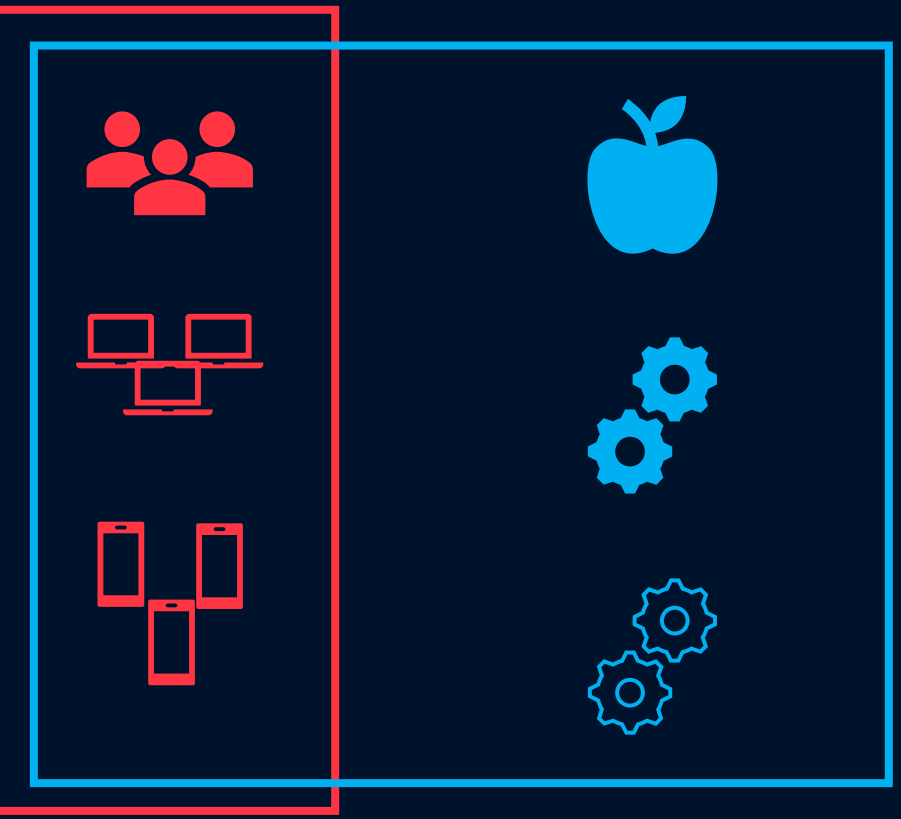
I configured a rule on a group but no memberships get updated in the group

Depending on the size of your Microsoft Entra organization, the group may take up to 24 hours for populating for the first time or after a rule change.

… asynchronous … ned by the number … as a result of the … see the group … a few minutes. Directories with a large … users can take 30 minutes or longer to populate.

https://learn.microsoft.com/en-gb/azure/active-directory/enterprise-users/groups-troubleshooting#troubleshooting-dynamic-memberships-for-groups

10. Users and Groups



User group vs Device group

Dynamic groups are slow

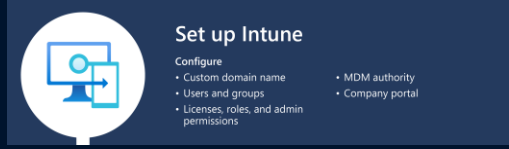
Use Intune Filters!

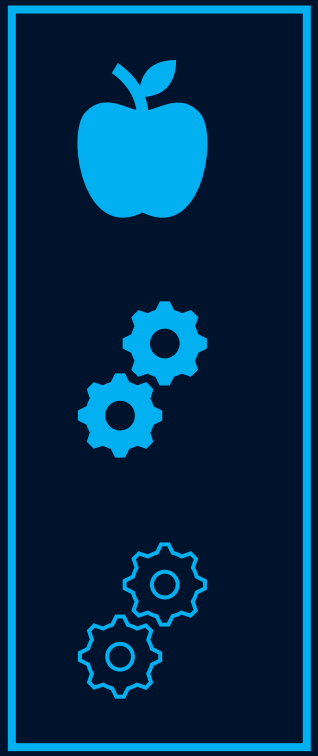
https://learn.microsoft.com/en-us/mem/intune/fundamentals/filters

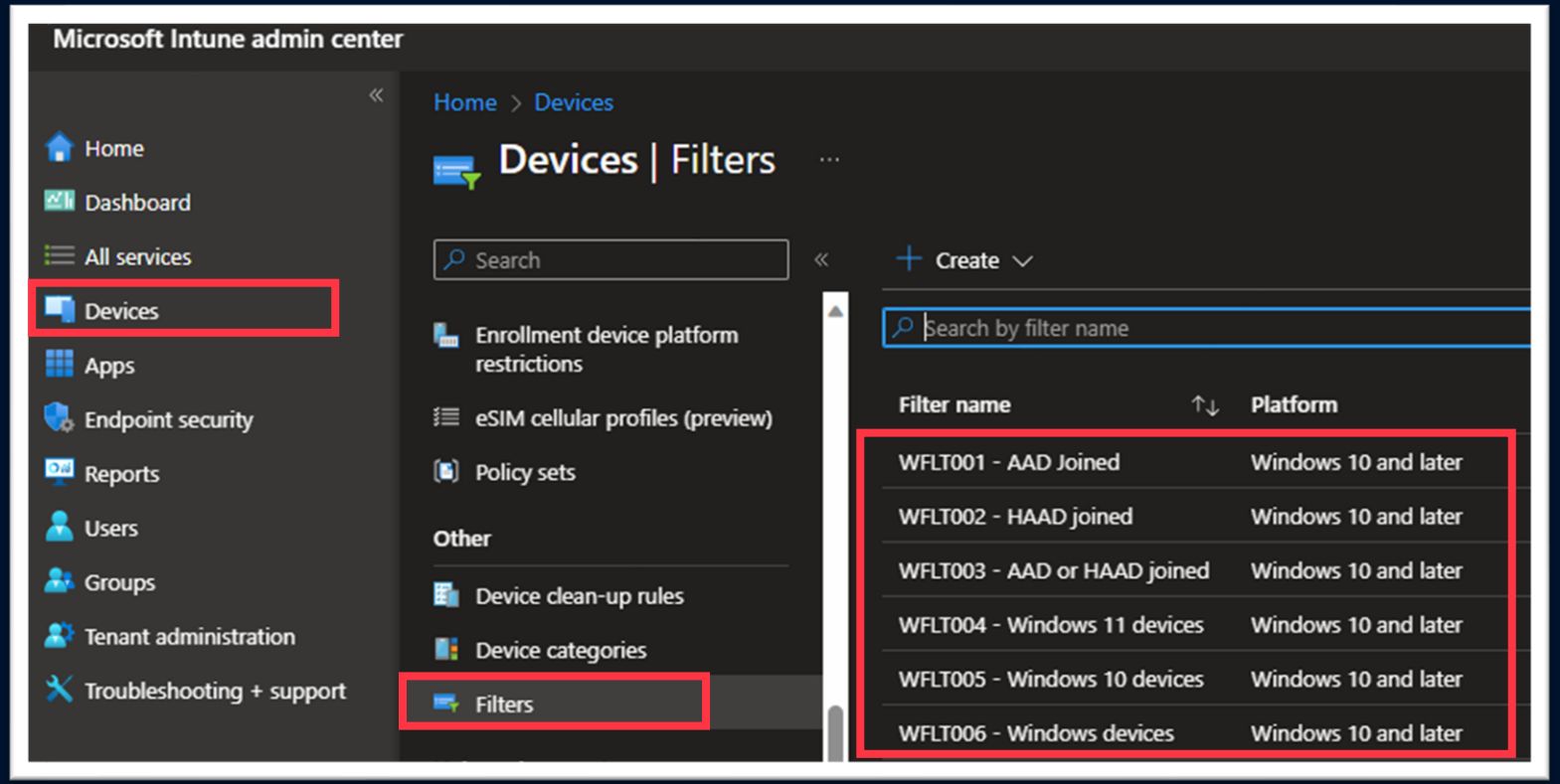
nic Cloud Connect

10. Users and Groups

Use Intune Filters!





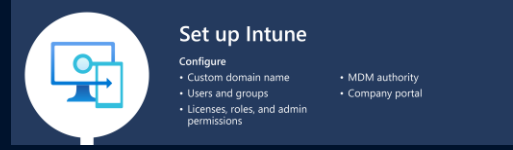


https://learn.microsoft.com/en-us/mem/intune/fundamentals/filters

Cloud Connect

10. Users and Groups

Use Intune Filters!



Microsoft Intune admin center

Home > Devices

Home

WFLT004 - Windows 11

Properties

Associated assignments

Filter name

Description

Platform

Rules Edit

(device.osVersion -startsWith "10.0.22")

WFLT001 - AAD Joined

Properties

Associated assignments

Filter name

WFLT001 - AAD Joined

Description

2023.09.26 - CloudWay template installed, Simon

Platform

Windows 10 and later

Rules Edit

(device.deviceTrustType -eq "Azure AD joined")

Windows 10 and later

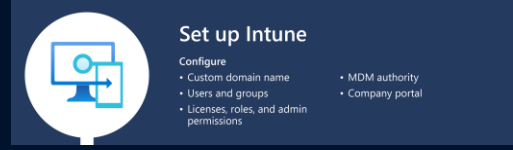
Windows 10 and later

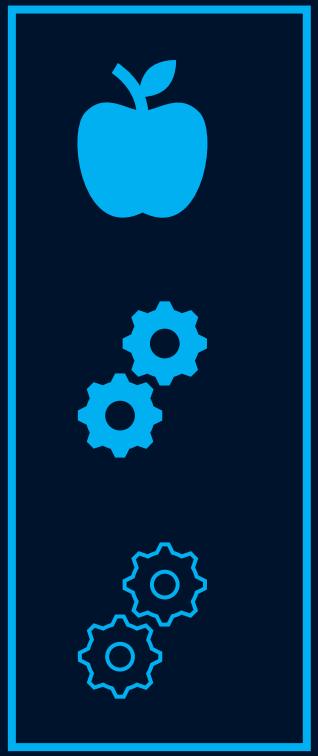
Windows 10 and later

https://learn.microsoft.com/en-us/mem/intune/fundamentals/filters

10. Users and Groups

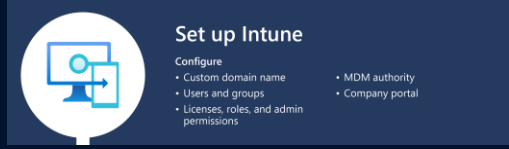
Use Intune Filters!





https://learn.microsoft.com/en-us/mem/intune/fundamentals/filters

NIC Cloud Connect

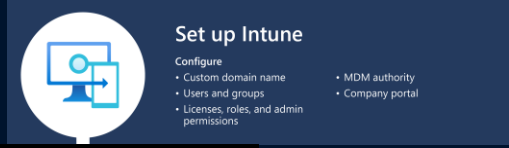


9

RBACs

Unmasking 10 Frequent Intune Mistakes and How to Prevent Them

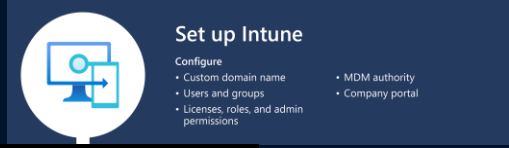
9. RBACs



Intune Administrator

https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#intune-administrator

9. RBACs



Intune Administrator

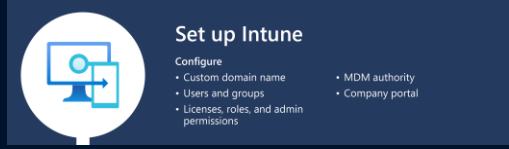
PRIVILEGED

This is a privileged role. Users with this role have global permissions within Microsoft Intune Online, when the service is present. Additionally, this role contains the ability to manage users and devices in order to associate policy, as well as create and manage groups. For more information, see Role-based administration control (RBAC) with Microsoft Intune.

This role can create and manage all security groups. However, Intune Administrator does not have admin rights over Office groups. That means the admin cannot update owners or memberships of all Office groups in the organization. However, he/she can manage the Office group that he creates which comes as a part of his/her end-user privileges. So, any Office group (not security group) that he/she creates should be counted against his/her quota of 250.

https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#intune-administrator

9. RBACs

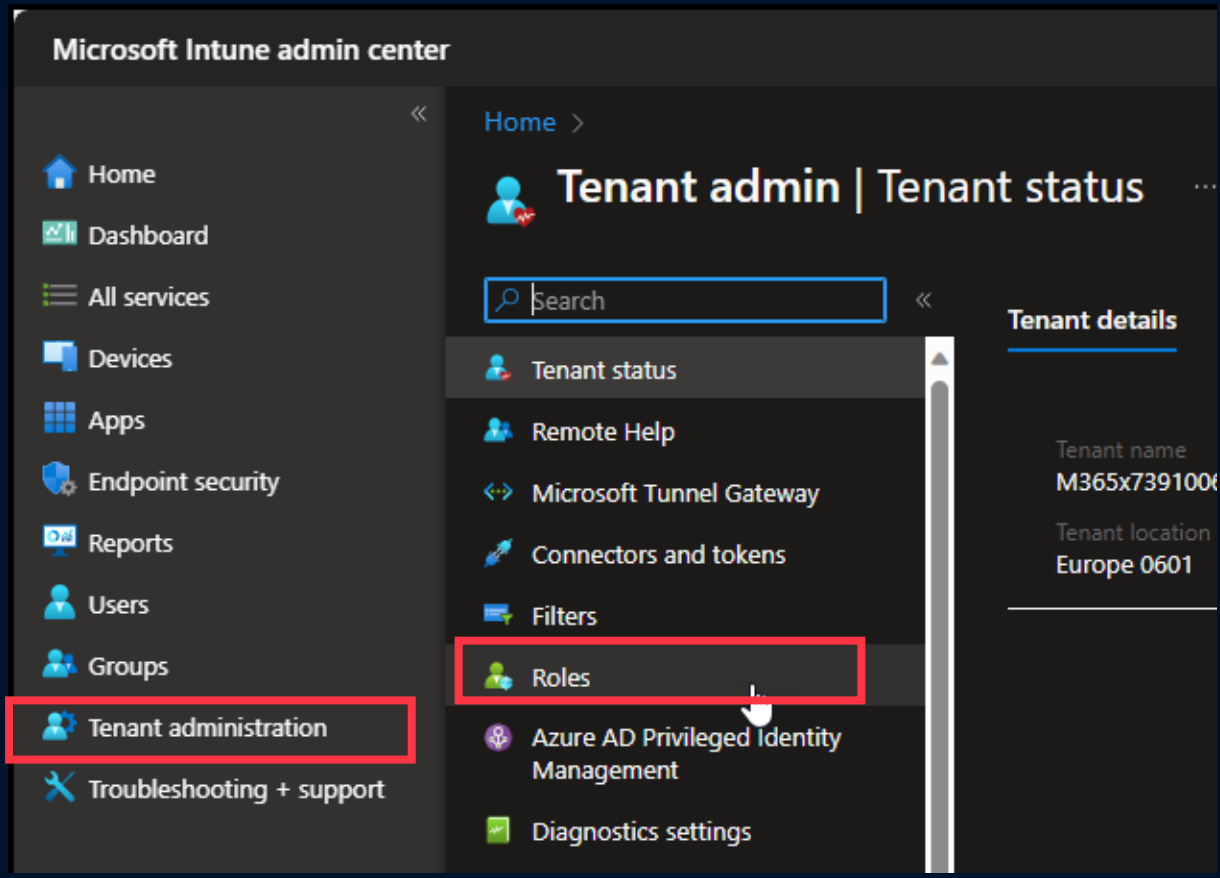


Intune Administrator

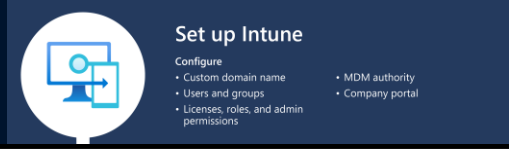
PRIVILEGED

This is a privileged role. Users with this role have global permissions within Microsoft Intune Online, when the service is present. Additionally, this role contains the ability to manage users and devices in order to associate policy, as well as create and manage groups. For more information, see Role-based administration control (RBAC) with Microsoft Intune.

This role can create and manage all security groups. However, Intune Administrator does not have admin rights over Office groups. That means the admin cannot update owners or memberships of all Office groups in the organization. However, he/she can manage the Office group that he creates which comes as a part of his/her end-user privileges. So, any Office group (not security group) that he/she creates should be counted against his/her quota of 250.



9. RBACs



Microsoft Intune admin center

Home > Tenant admin | Roles >

Endpoint Manager roles | All roles

Microsoft Intune

Search

Manage
- All roles
- Scope tags
- Administrator Licensing

Monitor
- My permissions

Help and support
- Help and support

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

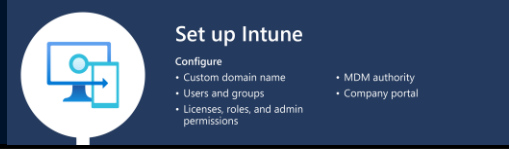
Create | Duplicate | Refresh

Endpoint Manager roles help you to assign permissions to administrators.

Search by name

Name	Type
Application Manager	Built-in Role
Endpoint Security Manager	Built-in Role
Organizational Messages Manager	Built-in Role
Endpoint Privilege Manager	Built-in Role
School Administrator	Built-in Role
Read Only Operator	Built-in Role
Endpoint Privilege Reader	Built-in Role
Intune Role Administrator	Built-in Role
Help Desk Operator	Built-in Role
Policy and Profile manager	Built-in Role

9. RBACs



Microsoft Intune admin center

Home > Tenant admin | Roles > Endpoint Manager roles

Endpoint Manager roles | Scope tags

Microsoft Intune

Search

Manage

All roles

Scope tags

Administrator Licensing

Monitor

My permissions

Help and support

Help and support

Home

Dashboard

All services

Devices

Apps

Endpoint security

Reports

Users

Groups

Tenant administration

Troubleshooting + support

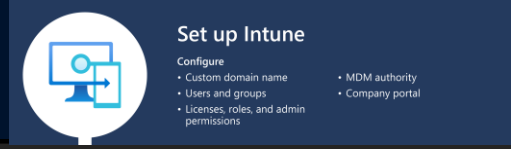
Scope tags define groups of Intune resources that align with specific Intune Role assignments. For example, a "Seattle Office" scope tag could be used to associate policies, profiles or applications with administrators that only apply to the Seattle office location.

Create Refresh Export Columns

Search

Name	Description
Default	By default, all Intune entities without scope tag are assigned to

9. RBACs



Microsoft Intune admin center

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

Home > Tenant admin | Roles > Endpoint Manager roles | Scope tags >

Create Scope Tag

Scope tag

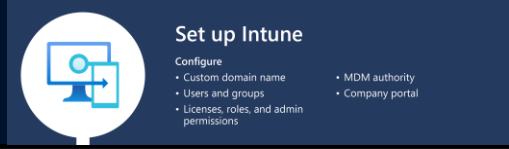
1 Basics 2 Assignments 3 Review + create

Scope tags define groups of Intune resources that align with specific Intune Role assignments. For example, a "Seattle Office" scope tag could be used to associate policies, profiles or applications with administrators that only apply to the Seattle office locations.

Name * iOS

Description All iOS devices.

9. RBACs



Microsoft Intune admin center

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

Home > Tenant admin | Roles > Endpoint Manager roles | Scope tags >

Create Scope Tag

Scope tag

Basics | 2 Assignments | 3 Review + create

Assign scope tags to all devices in select security groups

Included groups

Add groups

Groups	Remove
AZ-Device-iOS	Remove

nic Cloud Connect

9. RBACs

Set up Intune
Configure
• MDM authority
• Company portal

Microsoft Intune admin center

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

Home > Groups | All groups > AZ-Device-iOS

AZ-Device-iOS | Dynamic membership rules

Group

Save | Discard | Got feedback?

- Overview
- Diagnose and solve problems

Manage

- Properties
- Members
- Owners
- Roles and administrators
- Administrative units
- Group memberships
- Applications
- Licenses
- Azure role assignments
- Dynamic membership rules

Configure Rules | Validate Rules (Preview)

You can use the rule builder or rule syntax text box to create or edit a dynamic membership rule. Learn more

And/Or	Property	Operator	Value
	deviceOSType	Equals	iOS
Or	deviceOSType	Equals	IPhone
Or	deviceOSType	Equals	Ipad

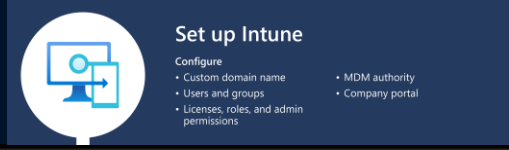
+ Add expression

Rule syntax

```
(device.deviceOSType -eq "iOS") or (device.deviceOSType -eq "IPhone") or (device.deviceOSType -eq "Ipad")
```

nic Cloud Connect

9. RBACs



Microsoft Intune admin center

Home > Devices | iOS/iPadOS > iOS/iPadOS

iOS/iPadOS | Configuration profiles

Search

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

Search

- iOS/iPadOS devices
- iOS/iPadOS enrollment

iOS/iPadOS policies

- Compliance policies
- Configuration profiles
- Update policies for iOS/iPadOS

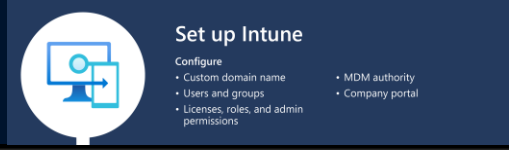
Profiles

Create profile | Refresh | Export | Columns

Search | Platform: iOS/iPadOS | Add filters

Profile name	Platform	Profile type
IDCP001 - OS - Device Restrictions	iOS/iPadOS	Device restrictions
IDCP002 - OS - Device Features	iOS/iPadOS	Device features
IDCP201 - APP - Microsoft Defender AutoVPN	iOS/iPadOS	VPN
IDCP202 - APP - Allow Sync Calendar and Contact	iOS/iPadOS	Email
iOS device restriction to block Game Center	iOS/iPadOS	Device restrictions

9. RBACs



Microsoft Intune admin center

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

Home > Devices | iOS/iPadOS > iOS/iPadOS | Configuration profiles >

IDCP001 - OS - Device Restrictions

Device Configuration Profiles

Delete

Included groups

Group	Filter	Filter mode
All Devices	None	None

Excluded groups

Group
No results.

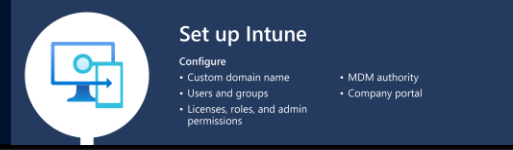
Scope tags Edit

Default
iOS

Configuration settings Edit

Built-in apps

9. RBACs



Microsoft Intune admin center

Home > Tenant admin | Roles >

Endpoint Manager roles | All roles

Microsoft Intune

Search

Manage
- All roles
- Scope tags
- Administrator Licensing

Monitor
- My permissions

Help and support
- Help and support

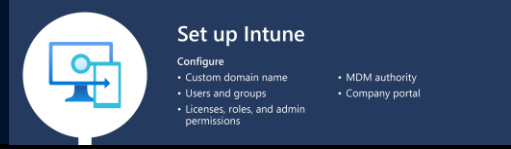
+ Create | Duplicate | Refresh

Endpoint Manager roles help you to assign permissions to administrators.

Search by name

Name	Type
Application Manager	Built-in Role
Endpoint Security Manager	Built-in Role
Organizational Messages Manager	Built-in Role
Endpoint Privilege Manager	Built-in Role
School Administrator	Built-in Role
Read Only Operator	Built-in Role
Endpoint Privilege Reader	Built-in Role
Intune Role Administrator	Built-in Role
Help Desk Operator	Built-in Role

9. RBACs



Microsoft Intune admin center

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

Home > Tenant admin | Roles > Endpoint Manager roles | All roles >

Duplicate role

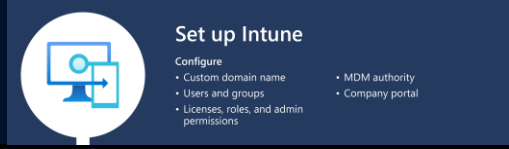
Copy role's existing description and permissions

1 Basics | 2 Permissions | 3 Scope tags | 4 Review + create

Name *: iOS Operator

Description: Custom role based on Help Desk Operators perform remote tasks on applications or policies related to iOS.

9. RBACs



Microsoft Intune admin center

Home > Tenant admin | Roles > Endpoint Manager roles | All roles >

Duplicate role

Copy role's existing description and permissions

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

Basics | 2 Permissions | 3 Scope tags | 4 Review + create

Select a category below to configure settings.

Android Enterprise

Android FOTA

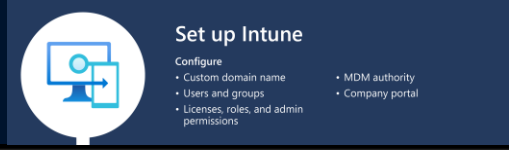
Read	No	Yes
Create	No	Yes
Delete	No	Yes
Assign	No	Yes
Update	No	Yes

Audit data

Certificate Connector

nic Cloud Connect

9. RBACs



Microsoft Intune admin center

iOS Operator | Properties

Microsoft Intune

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

Search

Overview

Manage

Properties
Assignments

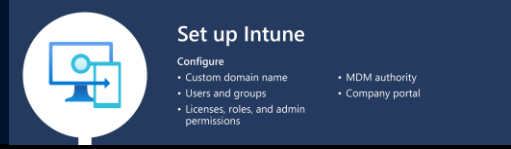
Basics Edit

Name	iOS Operator
Description	Custom role based on Help Desk Operators perform remote tasks on applications or policies related to iOS.

Permissions Edit

Certificate Connector	Read
Cloud attached devices	Take application actions Enroll Now
Customization	Read
Derived Credentials	Read
Device compliance policies	Read View reports
Device configurations	Read View Reports
Device enrollment managers	Read

9. RBACs



Microsoft Intune admin center

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

Home > iOS Operator

iOS Operator | Assignments

Microsoft Intune

Search

Overview

Manage

Properties

Assignments

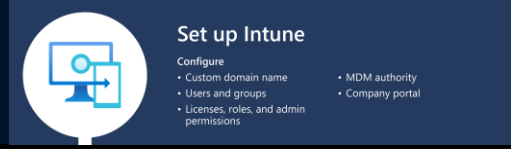
Role assignments tie together a role definition with members and scopes. There can be one or more role assignments per role. This applies to custom and built-in roles.

+ Assign | Refresh | Export | Columns

Search

Name	Description

9. RBACs



Microsoft Intune admin center

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

Home > iOS Operator | Assignments >

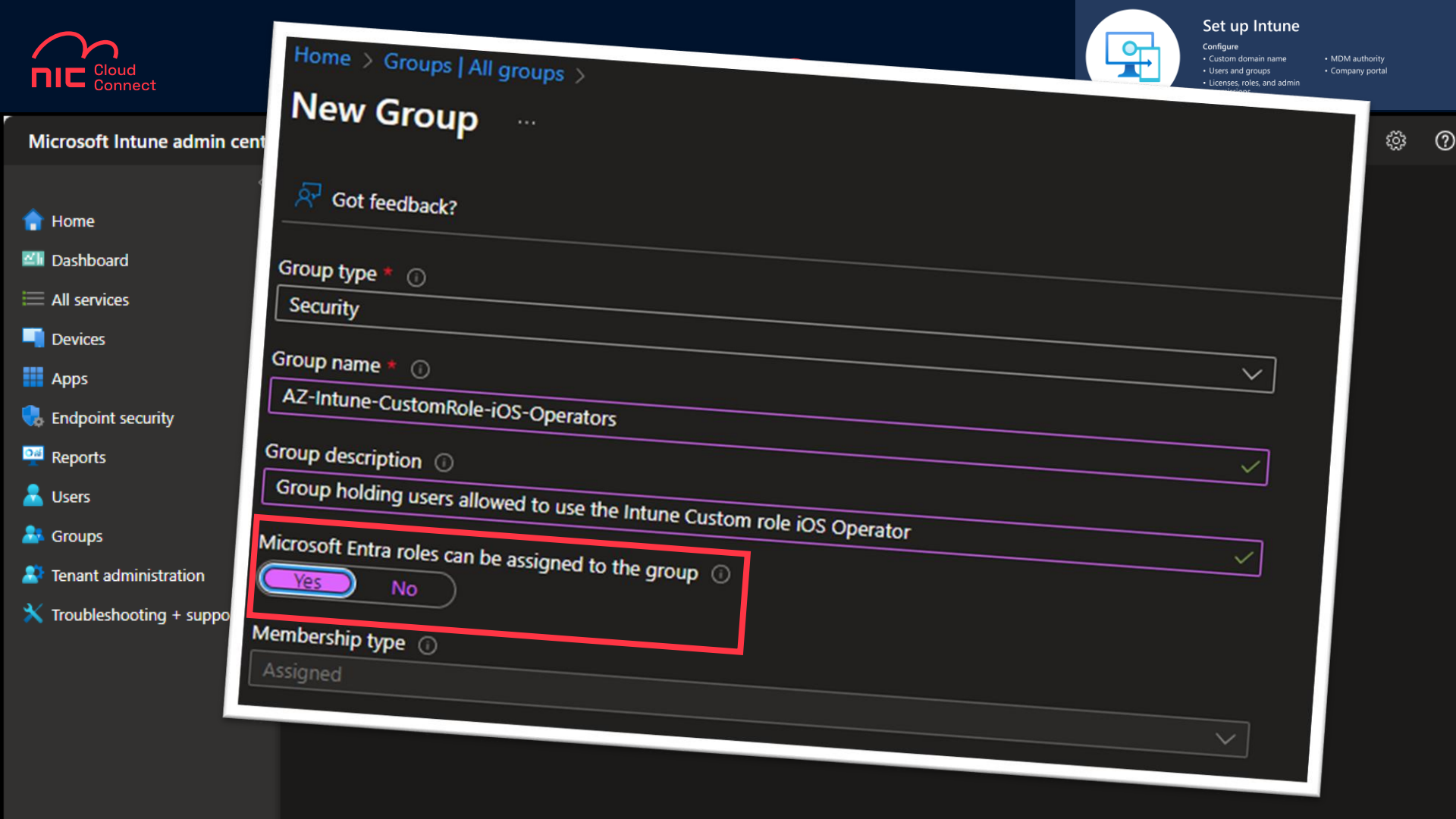
Add Role Assignment

iOS Operator

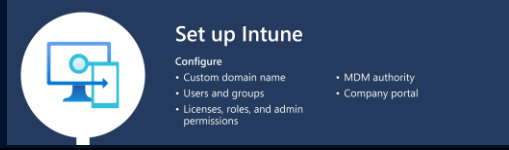
1 Basics | 2 Admin Groups | 3 Scope Groups | 4 Scope tags | 5 Review + create

Name *: iOS Operator Assignment

Description: Assigning users, scope groups and scope tags to custom role.


Cloud Connect
Microsoft Intune admin cent
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + suppo
Set up Intune
Configure
• Custom domain name
• Users and groups
• Licenses, roles, and admin
• MDM authority
• Company portal
Home > Groups | All groups >
New Group
...
Got feedback?
Group type *
Security
Group name *
AZ-Intune-CustomRole-iOS-Operators
Group description
Group holding users allowed to use the Intune Custom role iOS Operator
Microsoft Entra roles can be assigned to the group
Yes
No
Membership type
Assigned

9. RBACs



Microsoft Intune admin center

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

Home > iOS Operator | Assignments >

Add Role Assignment

iOS Operator

Basics | Admin Groups | 3 Scope Groups | 4 Scope tags | 5 Review + create

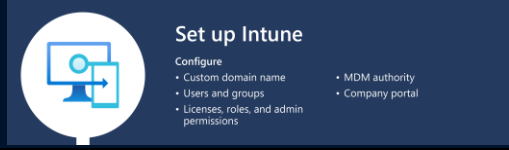
Administrators in this role assignment can target policies, applications and remote tasks

Included groups

Add groups | Add all users | Add all devices

Groups	Remove
AZ-Device-iOS	Remove

9. RBACs



Microsoft Intune admin center

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

Home > iOS Operator | Assignments >

Add Role Assignment

iOS Operator

Basics | Admin Groups | Scope Groups | 4 Scope tags | 5 Review + create

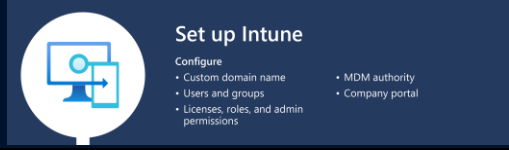
Configure scope tags for this role

Scope tags

iOS

+ Select scope tags

9. RBACs



Microsoft Intune admin center

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

Home > iOS Operator | Assignments >

Add Role Assignment

iOS Operator

Basics ✓ | Admin Groups ✓ | Scope Groups ✓ | Scope tags ✓ | 5 Review + create

Summary

Basics

Name	iOS Operator Assignment
Description	Assigning users, scope groups and scope tags to custom role.

Admin Groups

Included groups	AZ-Intune-CustomRole-iOS-Operators

Scope Groups

Included groups	AZ-Device-iOS

Scope tags

iOS

9. RBACs

Microsoft Intune admin center

admin@M365x
SIMON DOES (M365

Home > Tenant admin | Roles >

Endpoint Manager roles | All roles

Microsoft Intune

Search

Manage
- All roles
- Scope tags
- Administrator Licensing

Monitor
- My permissions

Help and support
- Help and support

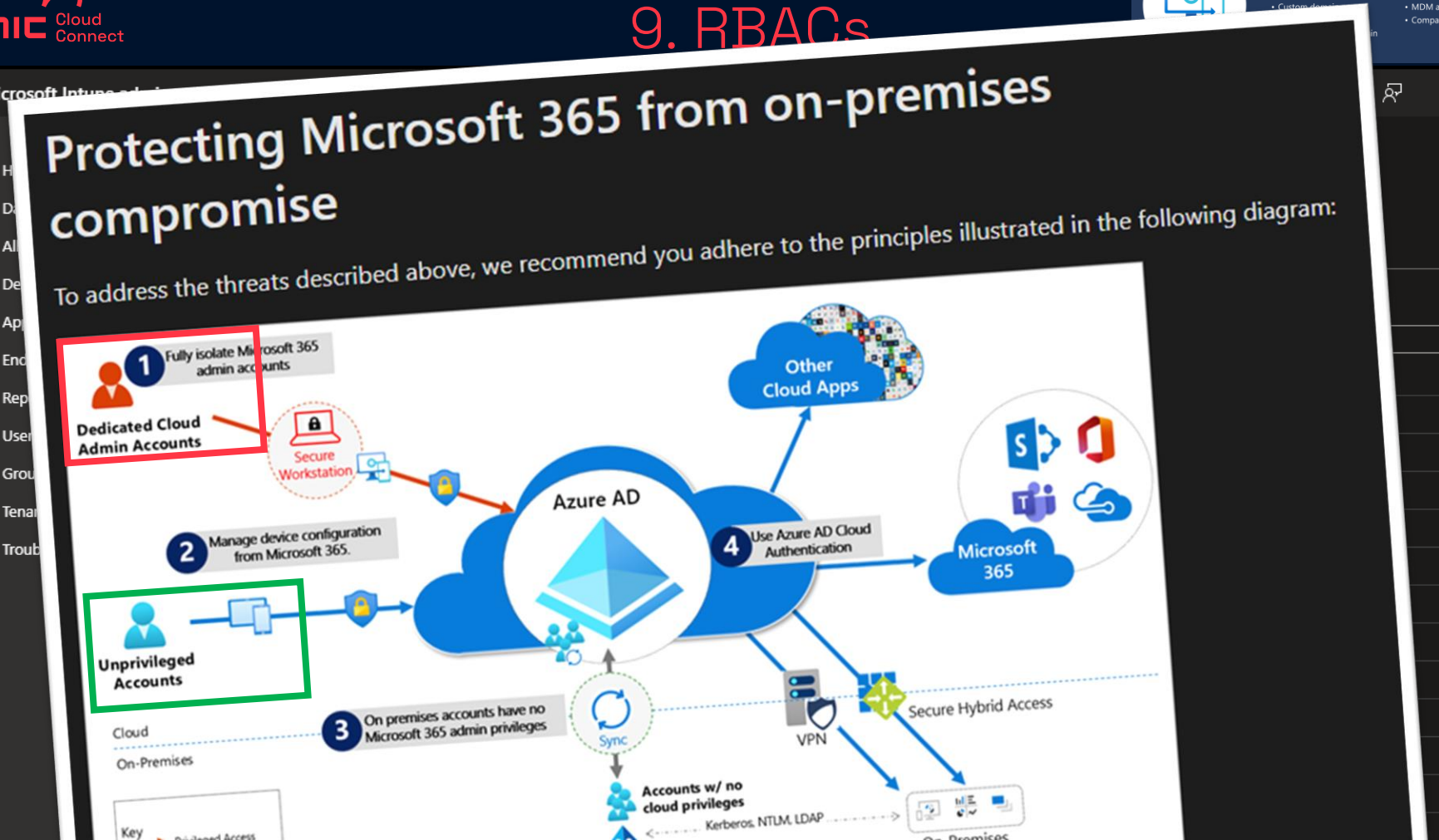
+ Create | Duplicate | Refresh

Endpoint Manager roles help you to assign permissions to administrators.

Search by name

Name	Type
Application Manager	Built-in Role
Endpoint Security Manager	Built-in Role
Organizational Messages Manager	Built-in Role
Endpoint Privilege Manager	Built-in Role
School Administrator	Built-in Role
Read Only Operator	Built-in Role
Endpoint Privilege Reader	Built-in Role
Intune Role Administrator	Built-in Role
Help Desk Operator	Built-in Role
Policy and Profile manager	Built-in Role
iOS Operator	Custom Intune role

9. RBACs


Protecting Microsoft 365 from on-premises compromise
To address the threats described above, we recommend you adhere to the principles illustrated in the following diagram:
1 Fully isolate Microsoft 365 admin accounts
Dedicated Cloud Admin Accounts
Secure Workstation
Other Cloud Apps
Azure AD
2 Manage device configuration from Microsoft 365.
4 Use Azure AD Cloud Authentication
Microsoft 365
Unprivileged Accounts
3 On premises accounts have no Microsoft 365 admin privileges
Sync
VPN
Secure Hybrid Access
Cloud
On-Premises
Accounts w/ no cloud privileges
Kerberos, NTLM, LDAP
Key

9. RBACs

Set up Intune

Configure

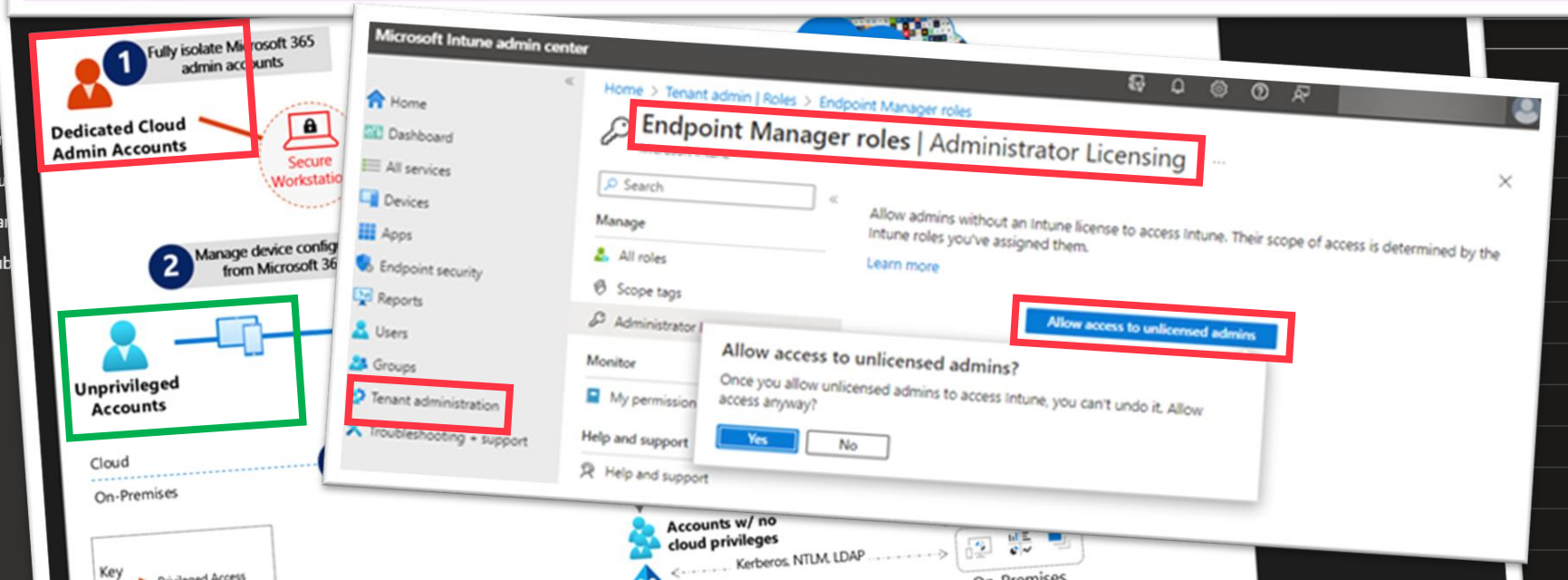
• MDM authority
• Company portal

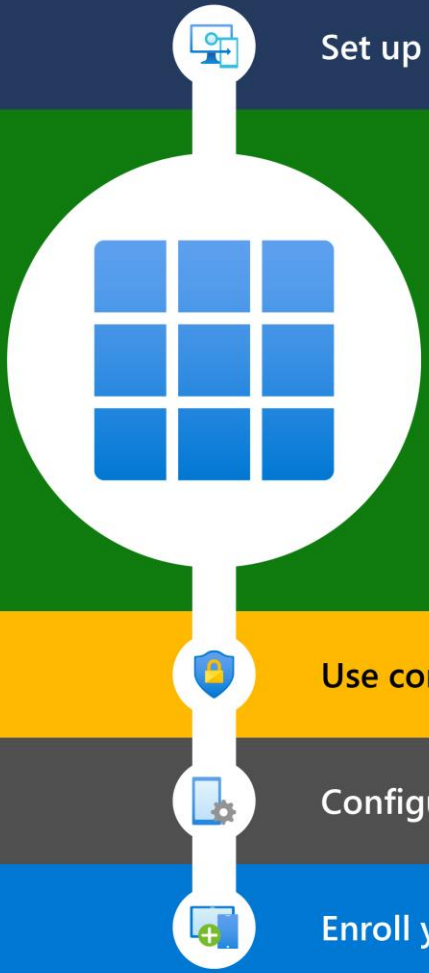
admin@M365x
SIMON DOES (M365

from on-premises

Note

To be able to administer Intune you must have an Intune license assigned. Alternatively, you can allow non-licensed users to administer Intune by setting **Allow access to unlicensed admins** to Yes.





Set up Intune

Add, configure, and protect apps

Configure

- Baseline apps list
- Microsoft Outlook and Edge
- VPN

Use

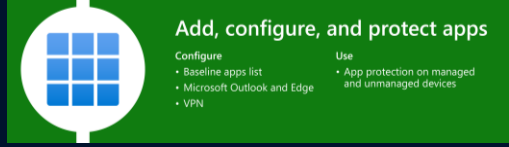
- App protection on managed and unmanaged devices

Use compliance and Conditional Access

Configure device features and settings

Enroll your devices

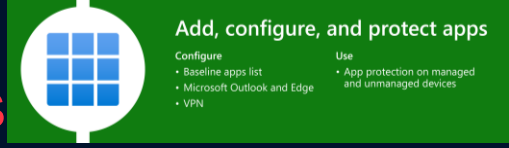
nic Cloud Connect



8 Application Distributions

Unmasking 10 Frequent Intune Mistakes and How to Prevent Them

8. Application Distributions



Microsoft Intune admin center

Home > Apps

Apps | All apps

Search

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
Quiet time

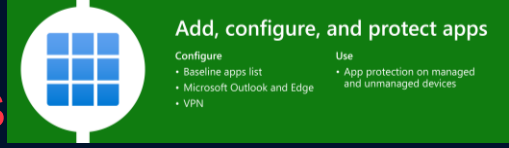
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support

Add | Refresh | Filter | Export | Columns

Search by name or publisher

Name	Type	Status	Version
Adobe Acrobat Reader DC	Microsoft Store app (new)		
Adobe Acrobat Reader for Intune Android (De...	Android store app		
Adobe Acrobat Reader for Microsoft Intune (D...	iOS store app		
Company Portal	Microsoft Store app (new)		
Excel	Android store app		
Excel	iOS store app		
M365 Apps for Enterprise	Windows app (Win32)		1.1
Managed Browser	Android store app		
Managed Browser	iOS store app		
Microsoft 365 (Office)	iOS store app		
Microsoft Defender	iOS store app		
Microsoft OneDrive	iOS store app		
Microsoft Outlook	iOS store app		
Microsoft Remote Desktop	Microsoft Store app (new)		

8. Application Distributions



Microsoft Intune admin center

Home > Apps | Windows >

Windows | Windows apps

Search

Add | Refresh | Filter | Export | Columns

Windows apps

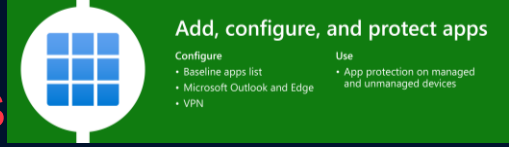
Filters applied: Platform, App type

Search by name or publisher

Name	Type	Status	Version	Assigned
Adobe Acrobat Reader DC	Microsoft Store app (new)			Yes
Company Portal	Microsoft Store app (new)			Yes
M365 Apps for Enterprise	Windows app (Win32)		1.1	No
Microsoft Remote Desktop	Microsoft Store app (new)			Yes
Microsoft To Do: Lists, Tasks & Remin...	Microsoft Store app (new)			Yes
Microsoft Whiteboard	Microsoft Store app (new)			Yes
TeamViewer: Remote Control	Microsoft Store app (new)			Yes
Zip Unzip - rar, 7zip compression	Microsoft Store app (new)			Yes

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

8. Application Distributions



Microsoft Intune admin center

Home > Apps | Windows

Select app type

Create app

App type

Select app type

Store app

Microsoft Store app (new)

Microsoft Store app (legacy)

Microsoft 365 Apps

Windows 10 and later

Microsoft Edge, version 77 and later

Windows 10 and later

Web Application

Windows web link

Other

Web link

Line-of-business app

Windows app (Win32)

MSEndpointMgr

Home Intune Identity Windows ConfigMgr Media

```
<Property Name="SharedComputerLicensing" Value="0" />
<Property Name="FORCEAPPSHUTDOWN" Value="TRUE" />
<Property Name="DeviceBasedLicensing" Value="0" />
<Property Name="SCLCacheOverride" Value="0" />
<Updates Enabled="TRUE" />
<AppSettings>
  <Setup Nam
```

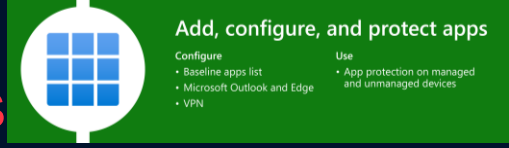
Installing M365 Apps as Win32 App in Intune

Jan Ketil Skanke 2022-10-23 4 comments 4 min read

If you have ever having issues with Autopilot or Enrollment Status page failing or timing out due to issues with Office installation, this blog post is for you. Over the years working in this area, the Office CSP has caused countless issues and deployments to fail. The Office CSP, commonly knows as the built-in **"Microsoft 365 Apps for Windows 10 and later"** is actually not an app distribution in

https://msendpointmgr.com/2022/10/23/installing-m365-apps-as-win32-app-in-intune/

8. Application Distributions



Microsoft Intune admin center

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

Home > Apps | Windows >

Windows | Windows apps

Search

Windows apps

Add | Refresh | Filter | Export | Columns

Filters applied: Platform, App type

Search by name or publisher

Name	Type
Adobe Acrobat Reader DC	Microsoft Store app (new)
Company Portal	Microsoft Store app (new)
M365 Apps for Enterprise	Windows app (Win32)
Microsoft Remote Desktop	Microsoft Store app (new)
Microsoft To Do: Lists, Tasks & ...	Microsoft Store app (new)
Microsoft Whiteboard	Microsoft Store app (new)
TeamViewer: Remote Control	Microsoft Store app (new)
Zip Unzip - rar, 7zip compressi...	Microsoft Store app (new)

Select app type

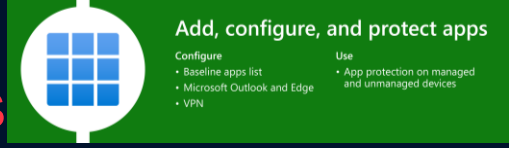
Create app

App type

Select app type

- **Store app**
- Microsoft Store app (new)
- Microsoft Store app (legacy)
- **Microsoft 365 Apps**
- Windows 10 and later
- **Microsoft Edge, version 77 and later**
- Windows 10 and later
- **Web Application**
- Windows web link
- **Other**
- Web link
- Line-of-business app
- Windows app (Win32)

8. Application Distributions



Microsoft Intune admin center

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

Home > Apps | Windows >

Windows | Windows apps

Search

Windows apps

Add | Refresh | Filter | Export | Columns

Filters applied: Platform, App type

Search by name or publisher

Name	Type
Adobe Acrobat Reader DC	Microsoft Store app (new)
Company Portal	Microsoft Store app (new)
M365 Apps for Enterprise	Windows app (Win32)
Microsoft Remote Desktop	Microsoft Store app (new)
Microsoft To Do: Lists, Tasks & ...	Microsoft Store app (new)
Microsoft Whiteboard	Microsoft Store app (new)
TeamViewer: Remote Control	Microsoft Store app (new)
Zip Unzip - rar, 7zip compressi...	Microsoft Store app (new)

Select app type

Create app

App type

Select app type

Store app

Microsoft Store app (new)

Microsoft Store app (legacy)

Microsoft 365 Apps

Windows 10 and later

Microsoft Edge, version 77 and later

Windows 10 and later

Web Application

Windows web link

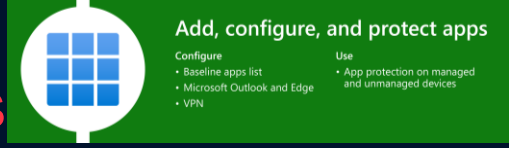
Other

Web link

Line-of-business app

Windows app (Win32)

8. Application Distributions



Microsoft Intune admin center

admin@M365x7391006...
SIMON DOES (M365X73910067.O...

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

Home > Apps | Windows >

Windows | Windows apps

Search

Windows apps

Add | Refresh | Filter | Export | Columns

Filters applied: Platform, App type

Search by name or publisher

Name	Type
Adobe Acrobat Reader DC	Microsoft Store app (new)
Company Portal	Microsoft Store app (new)
M365 Apps for Enterprise	Windows app (Win32)
Microsoft Remote Desktop	Microsoft Store app (new)
Microsoft To Do: Lists, Tasks & ...	Microsoft Store app (new)
Microsoft Whiteboard	Microsoft Store app (new)
TeamViewer: Remote Control	Microsoft Store app (new)
Zip Unzip - rar, 7zip compressi...	Microsoft Store app (new)

Select app type

Create app

App type: Line-of-business app

Line-of-business app

To add a custom or in-house app, upload the app's installation file. Make sure the file extension matches the app's intended platform. Intune supports the following line-of-business app platforms and extensions:

- Android (APK)
- iOS (IPA)
- macOS (.pkg)
- Windows (.msi, appx, .appxbundle, .msix, and .msixbundle)

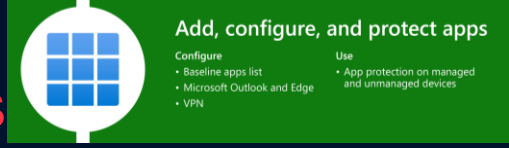
Learn more about Line-of-business apps

Validate your applications using Test Base for Microsoft 365

Test Base is a cloud validation service that allows you to easily onboard your applications through the Azure portal. You can quickly view deep insights including test results, performance metrics, and crash/hang signals. Through a Microsoft managed environment, you can gain access to world-class intelligence about the performance and reliability of your applications.

Get started on Test Base

8. Application Distributions



Microsoft Intune admin center

admin@M365x7391006...
SIMON DOES (M365X73910067.O...

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

Home > Apps | Windows >

Windows | Windows apps

Search

Windows apps

+ Add | Refresh | Filter | Export | Columns

Filters applied: Platform, App type

Search by name or publisher

Name	Type
Adobe Acrobat Reader DC	Microsoft Store app (new)
Company Portal	Microsoft Store app (new)
M365 Apps for Enterprise	Windows app (Win32)
Microsoft Remote Desktop	Microsoft Store app (new)
Microsoft To Do: Lists, Tasks & ...	Microsoft Store app (new)
Microsoft Whiteboard	Microsoft Store app (new)
TeamViewer: Remote Control	Microsoft Store app (new)
Zip Unzip - rar, 7zip compressi...	Microsoft Store app (new)

Select app type

Create app

App type: Windows app (Win32)

Windows app (Win32)

Add a custom or in-house Win32-based app. Upload the app's installation file in .intunewin format.

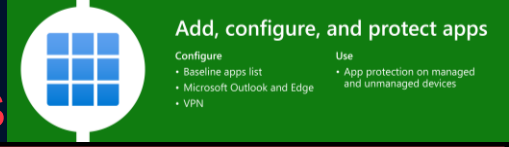
Learn more about Win32-based apps

Validate your applications using Test Base for Microsoft 365

Test Base is a cloud validation service that allows you to easily onboard your applications through the Azure portal. You can quickly view deep insights including test results, performance metrics, and crash/hang signals. Through a Microsoft managed environment, you can gain access to world-class intelligence about the performance and reliability of your applications.

Get started on Test Base

8. Application Distributions



Thursday, 09 November 2023

	1 Security	2 Architecture	4 Operations and Automation	5 Cloud	6 Data & AI	7 Server & Client
08:30	Crouching Tiger, Hidden Data: What's New & Cool in Microsoft 365 Security & Compliance Andy Malone	Tales from Incident Response Mikael Nystrom Viktor Hedberg	Dive Headfirst into	Hybrid cloud with	Getting started with the Windows 11 CoPilot Jannik Reinhard	Microsoft Intune - One service to manage them all - utopia or reality? Simon Binder
09:50	So, you thought it was always about you! John Craddock	Hybrid- and Mul Cloud Server Management wi Azure Arc Gregor Reiming				Fully automated Win32 application packaging in Intune Nickolaj Andersen
11:10	The Clash of the Defenders: how to handle more Microsoft Defenders you could ever imagine. Alex de Jong	Using the power OpenAI with you data: what's pos and how to start Maxim Salnikov Jon			Unlock the potential of the Enterprise data universe with Microsoft Purview Mohit Sharma	Stay Ahead of the Game: What's new with Microsoft Enterprise Client Management Ronni Pedersen

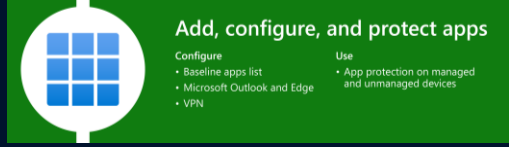
Nickolaj Andersen

Fully automated Win32 application packaging in Intune

Imagine a world where Win32 apps in Intune would just download, package and publish themselves, all made ready for your end users to consume the apps they want. Does that pique your interest? Join this session to get a deep technical understanding of tools and community solutions available today that can ease your daily administrative tasks associated with application packaging and take them to the next level, more or less fully automated. This will be a session where there's more PowerShell code shown than PowerPoint slides! We will go through the IntuneWin32App module, IntuneWin32AppFramework and finally touch point on how these tools can be combined into a fully automated Azure DevOps Pipeline powered solution, the Intune App Factory.

7 SERVER & CLIENT | Thu 09:50 - 10:50

NIC Cloud Connect

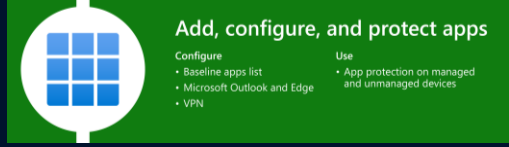


7

Applications in Autopilot ESP

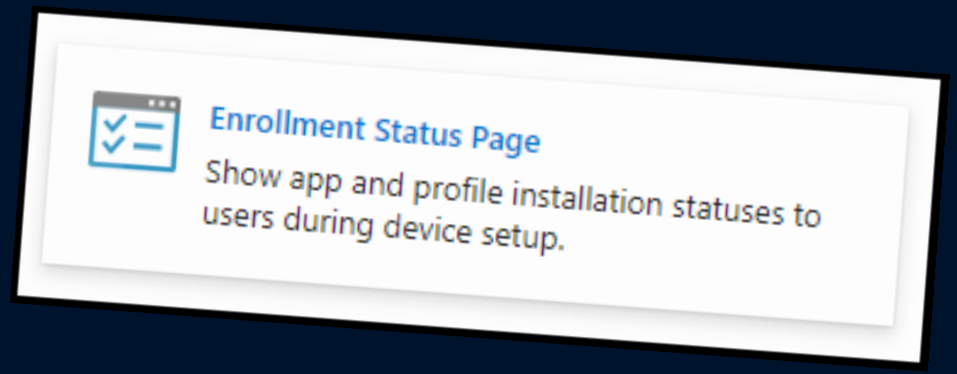
Unmasking 10 Frequent Intune Mistakes and How to Prevent Them

nic Cloud Connect

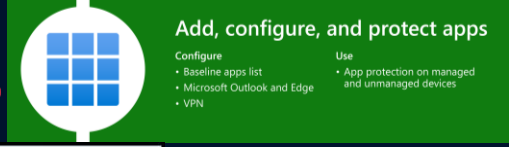


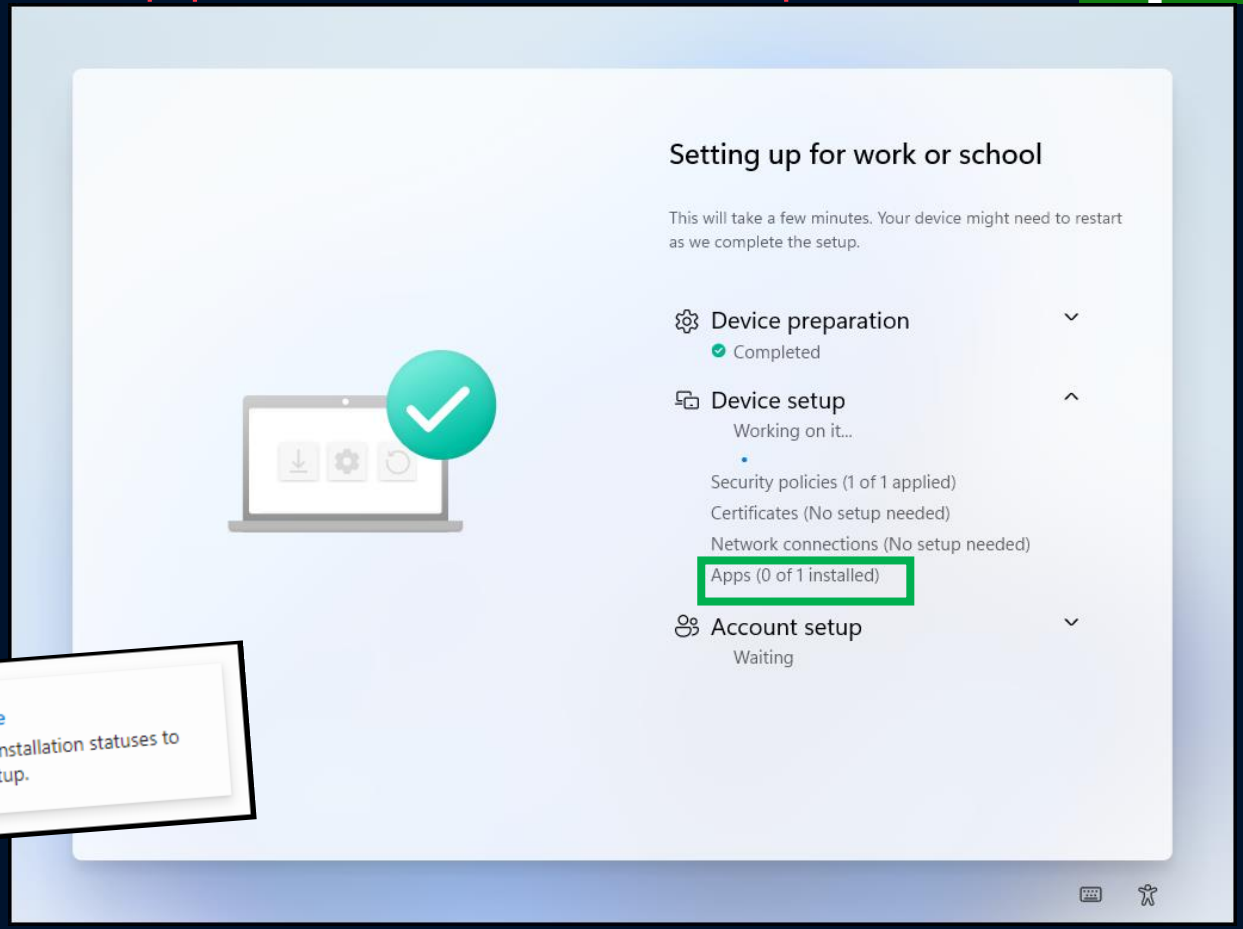
7

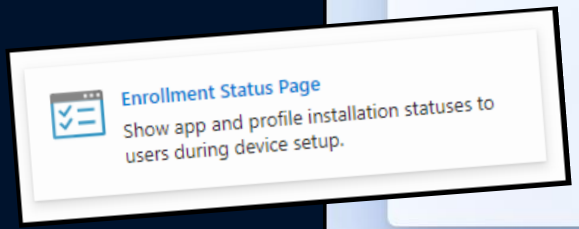
Applications in Autopilot ESP



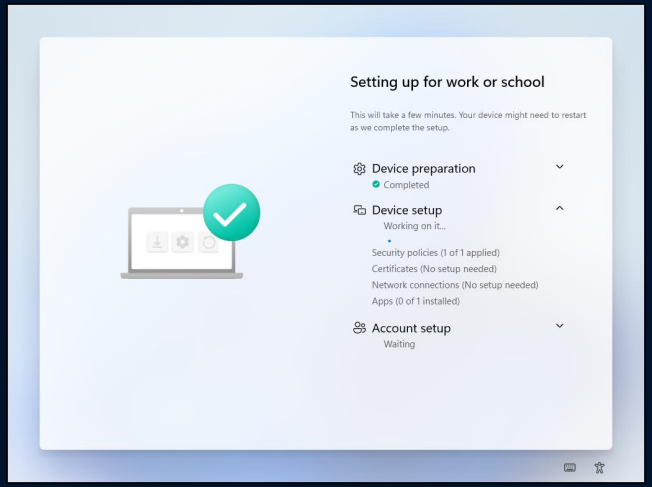
7. Applications in Autopilot ESP

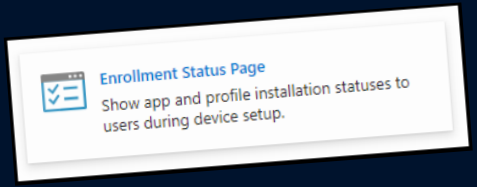


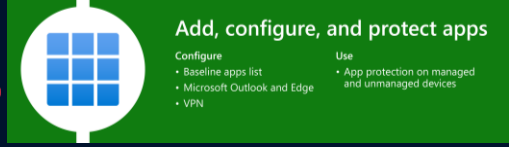


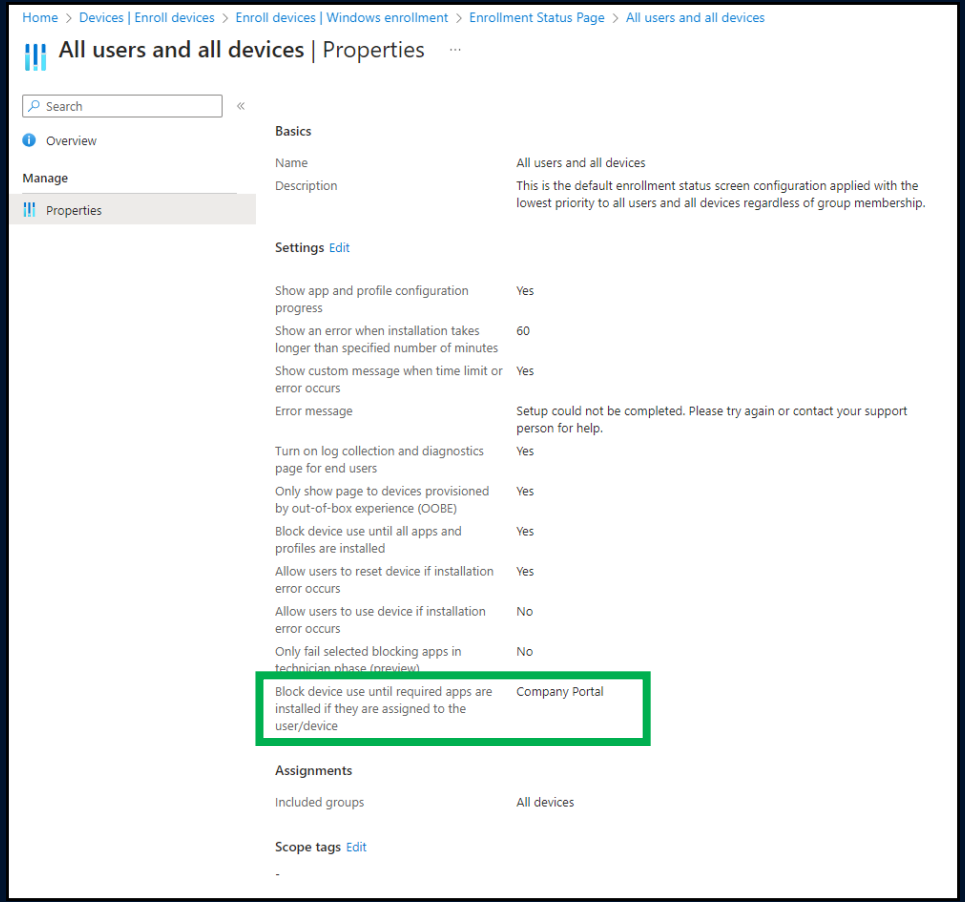


7. Applications in Autopilot ESP

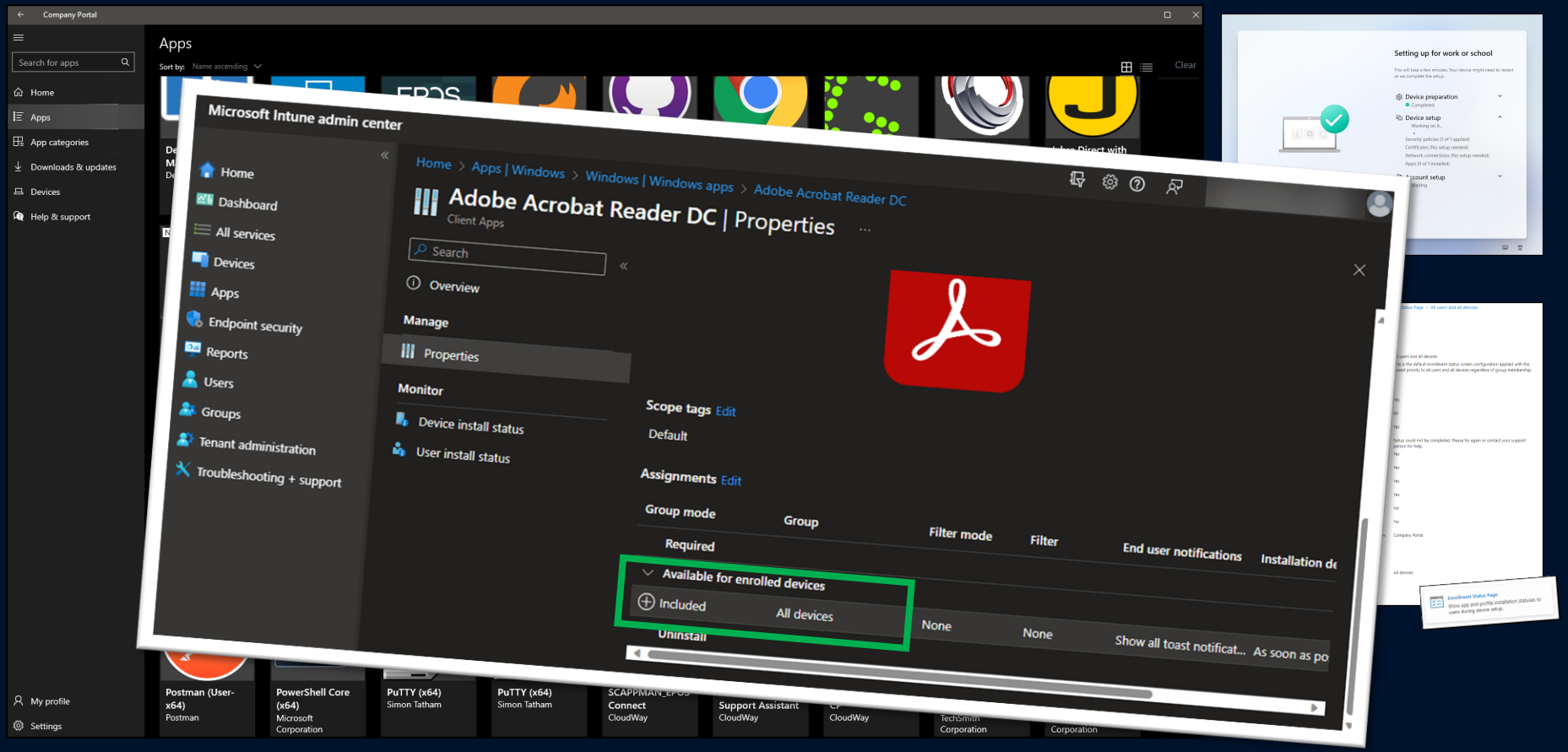








7. Applications in Autopilot ESP



Set up Intune

Add, configure, and protect apps

Use compliance and Conditional Access

Configure

- Compliance policies for users and devices
- Response for noncompliance

Enforce

- Compliance with Conditional Access

Configure device features and settings

Enroll your devices

NIC Cloud Connect

6 Compliance Policies

Unmasking 10 Frequent Intune Mistakes and How to Prevent Them

6. Compliance Policies

Microsoft Intune admin center

Home > Devices | Compliance policies > Compliance policies

Compliance policies | Compliance policy settings

Search

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

- Policies
- Notifications
- Retire noncompliant devices
- Compliance policy settings
- Scripts

Save Discard

These settings configure the way the compliance service treats devices. Each device evaluates these as a "Built-in Device Compliance Policy", which is reflected in

Mark devices with no compliance policy assigned as ⓘ — Compliant

Compliance status validity period (days) ⓘ — 30 *

6. Compliance Policies

Microsoft Intune admin center

Home > Devices | Compliance policies > Compliance policies

Compliance policies | Compliance policy settings

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

Search

- Policies
- Notifications
- Retire noncompliant devices
- Compliance policy settings
- Scripts

Save | Discard

These settings configure the way the compliance service treats devices. Each device evaluates these as a "Built-in Device Compliance Policy", which is reflected in

Mark devices with no compliance policy assigned as ⓘ — Not compliant

Compliance status validity period (days) ⓘ — 30 *

6. Compliance Policies

Microsoft Intune admin center

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

Home > Devices | Windows > Windows

Windows | Compliance policies

Search

- Windows devices
- Windows enrollment

Windows policies

- Compliance policies
- Configuration profiles
- Scripts
- Update rings for Windows 10 and later
- Feature updates for Windows 10 and later
- Quality updates for Windows 10 and later
- Driver updates for Windows 10 and later

Configured Windows compliance policies use the Machine Risk Score setting but do not have an active Microsoft Defender

Create policy | Refresh | Export | Columns

Search

Platform or OS: **Windows 10 and later, Windows 8.1 and la**

Policy name	Platform or OS	Policy type
WCOP001 - Device Health - BitLocker and Secure boot	Windows 10 and later	Windows 10/11
WCOP002 - Device Properties - Minimum OS version	Windows 10 and later	Windows 10/11
WCOP003 - System Security - Microsoft Defender	Windows 10 and later	Windows 10/11
WCOP004 - System Security - Device Security	Windows 10 and later	Windows 10/11
WCOP005 - System Security - Require Encryption	Windows 10 and later	Windows 10/11
WCOP006 - Microsoft Defender for Enpoint Risk Score	Windows 10 and later	Windows 10/11

6. Compliance Policies

Microsoft Intune admin center

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

Home > Devices | Windows > Windows | Compliance policies >

WCOP001 - Device Health - BitLocker and Secure boot

Compliance policy - Windows 10 and later

Monitor | **Properties**

Basics Edit

Name	WCOP001 - Device Health - BitLocker and Secure boot
Description	2023.09.26 - CloudWay template installed, Simon
Platform	Windows 10 and later
Profile type	Windows 10/11 compliance policy

Compliance settings Edit

Device Health

Bitlocker	Required
Secure Boot	Required
Code Integrity	Required

Actions for noncompliance Edit

Action	Schedule	Message template	Additional recipients (via email)
Mark device noncompliant	2 Days		None selected

6. Compliance Policies

Microsoft Intune admin center

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

Home > Devices | Windows > Windows | Compliance policies >

WCOP002 - Device Properties - Minimum OS version

Compliance policy - Windows 10 and later

Monitor | **Properties**

Basics Edit

Name	WCOP002 - Device Properties - Minimum OS version
Description	2023.09.26 - CloudWay template installed, Simon
Platform	Windows 10 and later
Profile type	Windows 10/11 compliance policy

Compliance settings Edit

Device Properties

Minimum OS version	10.0.19044

Actions for noncompliance Edit

Action	Schedule	Message template	Additional recipients (via email)
Mark device noncompliant	Immediately		None selected

Required password type	Device default

6. Compliance Policies

Microsoft Intune admin center

Home > Devices | iOS/iPadOS > iOS/iPadOS | Compliance policies >

ICOP003 - System Security - App Blacklist

Compliance policy - iOS/iPadOS

Delete

Monitor | Properties

Basics Edit

Name	ICOP003 - System Security - App Blacklist
Description	2023.09.26 - CloudWay template installed, Simon
Platform	iOS/iPadOS
Profile type	iOS compliance policy

Compliance settings Edit

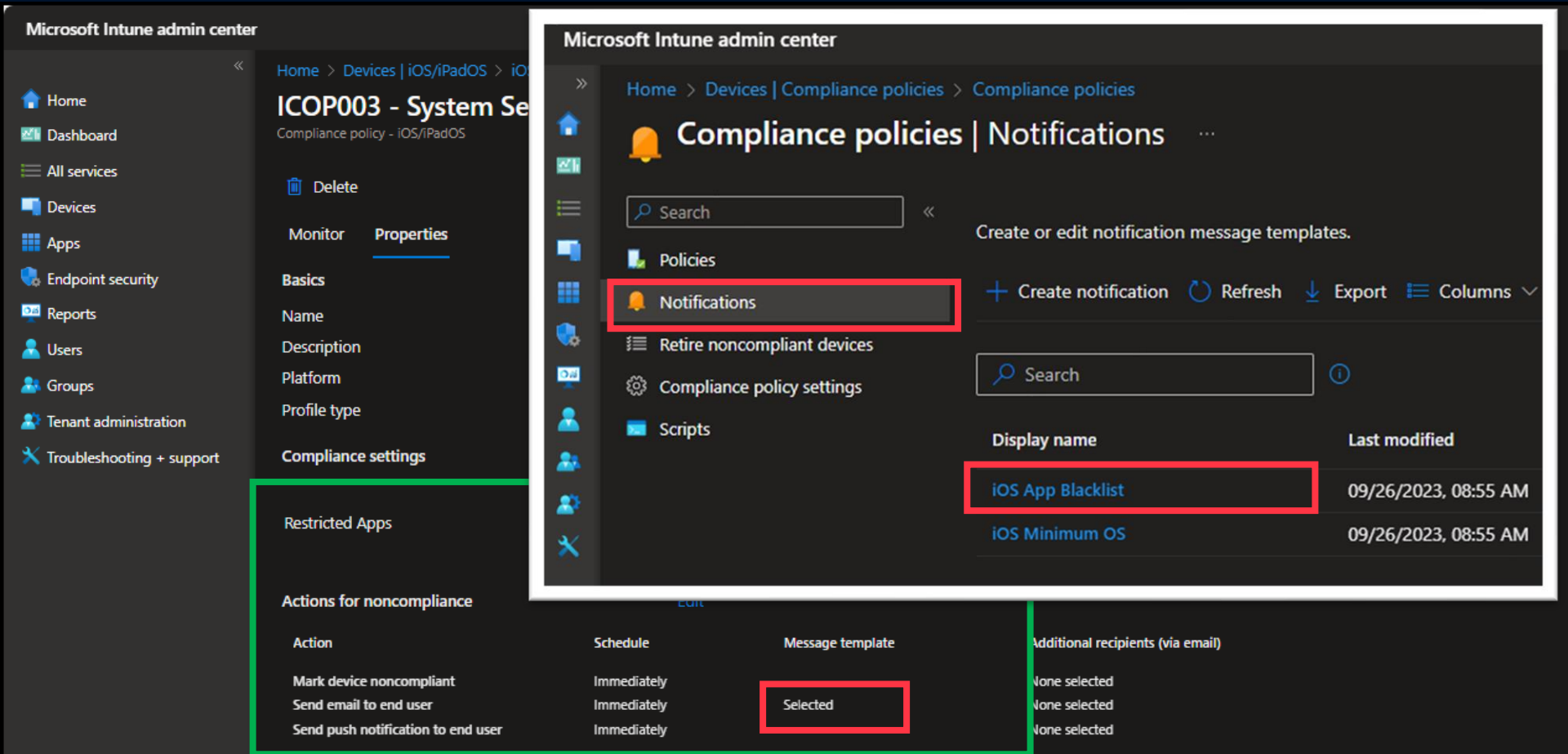
Restricted Apps

Name	App Id
TikTok	com.zhiliaoapp.musically
Telegram Messenger	ph.telegra.Telegraph

Actions for noncompliance Edit

Action	Schedule	Message template	Additional recipients (via email)
Mark device noncompliant	Immediately		None selected
Send email to end user	Immediately	Selected	None selected
Send push notification to end user	Immediately		None selected

6. Compliance Policies



6. Compliance Policies

Microsoft Intune admin center

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

Home > Devices | iOS/iPadOS > iO

ICOP003 - System Se

Compliance policy - iOS/iPadOS

Delete

Monitor | Properties

Basics

Name
Description
Platform
Profile type

Compliance settings

Restricted Apps

Actions for noncompliance

Action	Schedule
Mark device noncompliant	Immediately
Send email to end user	Immediately
Send push notification to end user	Immediately

Selected

None selected
None selected
None selected

Microsoft Intune admin center

Home

Edit notification iOS App Blacklist

Notification message templates | Review + save

Locale	Subject	Message	Is Default
Norwegian, Bokmål	Oppdaget illegal ap...	Vi har oppdaget en illegal app på din ...	
English (United Kingdom)	Uncovered an Una...	We have identified an unauthorized app on your mobile phone. Please check the information in the Company Portal app on your device to determine which app is in question.	

6. Compliance Policies

Microsoft Intune admin center

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

Home > Endpoint security | Conditional access > Conditional Access | Policies >

CA200-Internals-AllApps-AnyPlatform-CompliantorMFA-Grant

Conditional Access policy

Delete | View policy information

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *
CA200-Internals-AllApps-AnyPlatform-Com...

Assignments

Users
Specific users included and specific users excluded

Target resources
All cloud apps included and 3 apps excluded

Conditions
1 condition selected

Access controls

Grant
2 controls selected

Session

Grant

Control access enforcement to block or grant access. Learn more

- Block access
- Grant access
  - [x] Require multifactor authentication
  - [ ] Require authentication strength
  - [x] Require device to be marked as compliant
  - [ ] Require Microsoft Entra hybrid joined device
  - [ ] Require approved client app
    See list of approved client apps
  - [ ] Require app protection policy
    See list of policy protected client apps
  - [ ] Require password change

For multiple controls
- Require all the selected controls
- Require one of the selected controls

6. Compliance Policies

Microsoft Intune admin center

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

Home > Endpoint security | Conditional access > Conditional Access | Policies >

CA200-Internals-AllApps-AnyPlatform-CompliantorMFA-Grant

Conditional Access policy

Delete | View policy information

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *
CA200-Internals-AllApps-AnyPlatform-Com...

Assignments

Users
Specific users included and specific users excluded

Target resources
All cloud apps included and 3 apps excluded

Conditions
1 condition selected

Access controls

Grant
2 controls selected

Session

Grant

Control access enforcement to block or grant access. Learn more

- (○) Block access
- (●) Grant access
- [x] Require multifactor authentication
- [ ] Require authentication strength
- [x] Require device to be marked as compliant
- [ ] Require Microsoft Entra hybrid joined device
- [ ] Require approved client app
  See list of approved client apps
- [ ] Require app protection policy
  See list of policy protected client apps
- [ ] Require password change

For multiple controls
- (○) Require all the selected controls
- (●) Require one of the selected controls

6. Compliance Policies

Microsoft Intune admin center

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

Home > Endpoint security | Conditional access > Conditional Access | Policies >

CA200-Internals-AllApps-AnyPlatform-CompliantorMFA-Grant

Conditional Access policy

Delete | View policy information

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *
CA200-Internals-AllApps-AnyPlatform-Com...

Assignments

Users
Specific users included and specific users excluded

Target resources
All cloud apps included and 3 apps excluded

Conditions
1 condition selected

Access controls

Grant
2 controls selected

Session

Control access based on all or specific network access traffic, cloud apps or actions. Learn more

Select what this policy applies to
Cloud apps

Include | Exclude

Select the cloud apps to exempt from the policy

Edit filter (Preview)
None

Select excluded cloud apps
Universal Store Service APIs and Web Application and 2 more

- Microsoft Intune
  0000000a-0000-0000-c000-000000000000
- MI Microsoft Intune Enrollment
  d4ebce55-015a-49b5-a083-c84d1797ae8c
- US Universal Store Service APIs an...
  45a330b1-b1ec-4cc1-9161-9f03992aa49f

Grant

Control access enforcement to block or grant access. Learn more

- Block access
- Grant access
  - [x] Require multifactor authentication
  - [ ] Require authentication strength
  - [x] Require device to be marked as compliant
  - [ ] Require Microsoft Entra hybrid joined device
  - [ ] Require approved client app
    See list of approved client apps
  - [ ] Require app protection policy
    See list of policy protected client apps
  - [ ] Require password change

For multiple controls
- Require all the selected controls
- Require one of the selected controls

Set up Intune

Add, configure, and protect apps

Use compliance and Conditional Access

Configure device features and settings

Configure

- Security baseline
- Access to organization resources

Enhance

- Protections and configurations

Enroll your devices

nic Cloud Connect

5 Configurations

Unmasking 10 Frequent Intune Mistakes and How to Prevent Them

5. Configurations

Microsoft Intune admin center

Home > Endpoint security

Endpoint security | Security baselines

Search

Use security baselines to apply Microsoft-recommended security configuration settings to your enrolled devices. Learn more.

Security Baselines	Last Published
Security Baseline for Windows 10 and later	10/22/21, 12:00 AM
Microsoft Defender for Endpoint Baseline	12/09/20, 12:00 AM
Security Baseline for Microsoft Edge	05/25/23, 2:00 AM
Windows 365 Security Baseline	10/21/21, 12:00 AM
Microsoft 365 Apps for Enterprise Security Baseline	05/25/23, 2:00 AM

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

Overview

- Overview
- All devices
- Security baselines
- Security tasks

Manage

- Antivirus

5. Configurations

Available security baselines

The following security baseline instances are available for use with Intune. Use the links to view the settings for recent instances of each baseline.

- **Security Baseline for Windows 10 and later**
  - November 2021
  - December 2020
  - August 2020
- **Microsoft Defender for Endpoint baseline**
  (To use this baseline your environment must meet the prerequisites for using Microsoft Defender for Endpoint).
  - Version 6
  - Version 5
  - Version 4
  - Version 3

> **Note**
> The Microsoft Defender for Endpoint security baseline has been optimized for physical devices and is currently not recommended for use on virtual machines (VMs) or VDI endpoints. Certain baseline settings can impact remote interactive sessions on virtualized environments. For more information, see **Increase compliance to the Microsoft Defender for Endpoint security baseline** in the Windows documentation.

- **Microsoft 365 Apps for Enterprise**
  - May 2023 (Office baseline)
- **Microsoft Edge Baseline**
  - May 2023 (Edge Version 112 and later)
  - September 2020 (Edge version 85 and later)
  - April 2020 (Edge version 80 and later)
  - Preview: October 2019 (Edge version 77 and later)
- **Windows 365 Security Baseline**
  - October 2021

Microsoft In

Home
Dashboard
All services
Devices
Apps
Endpoint sec
Reports
Users
Groups
Tenant admini
Troubleshootin

aselines ...

lines to apply Microsoft-recommended security configuration settings to your enrolled devices. Learn more.

es	Last Published
eline for Windows 10 and later	10/22/21, 12:00 AM
fender for Endpoint Baseline	12/09/20, 12:00 AM
line for Microsoft Edge	05/25/23, 2:00 AM
Security Baseline	10/21/21, 12:00 AM
Apps for Enterprise Security Baseline	05/25/23, 2:00 AM

https://learn.microsoft.com/en-us/mem/intune/protect/security-baselines#available-security-baselines

5. Configurations

Available security baselines

The following security baseline instances are available for use with Intune. Use the links to view the settings for recent instances of each baseline.

- Security Baseline for Windows 10 and later
  - November 2021
  - December 2020
  - August 2020
- Microsoft Defender for Endpoint baseline
  (To use this baseline your environment must meet the prerequisites for using Microsoft Defender for Endpoint).
  - Version 6
  - Version 5
  - Version 4
  - Version 3

> **Note**
> The Microsoft Defender for Endpoint security baseline has been optimized for physical devices and is currently not recommended for use on virtual machines (VMs) or VDI endpoints. Certain baseline settings can impact remote interactive sessions on virtualized environments. For more information, see **Increase compliance to the Microsoft Defender for Endpoint security baseline** in the Windows documentation.

- Microsoft 365 Apps for Enterprise
  - May 2023 (Office baseline)
- Microsoft Edge Baseline
  - May 2023 (Edge Version 112 and later)
  - September 2020 (Edge version 85 and later)
  - April 2020 (Edge version 80 and later)
  - Preview: October 2019 (Edge version 77 and later)
- Windows 365 Security Baseline
  - October 2021

Microsoft

Learn / Microsoft Intune / Intune service /

Documentation

List of the settings in the Windows 10/11 MDM security baseline in Intune

Article • 02/23/2023 • 11 contributors

Feedback

Choose a version

November 2021 | December 2020 | August 2020

In this article

Security Baseline for Windows 10/11 for November 2021

Above Lock

- Voice activate apps from locked screen:
  Baseline default: *Disabled*
  Learn More
- Block display of toast notifications:
  Baseline default: *Yes*
  Learn More

App Runtime

- Microsoft accounts optional for Microsoft store apps:
  Baseline default: *Enabled*
  Learn more

Microsoft Intune

Home
Dashboard
All services
Devices
Apps
Endpoint sec
Reports
Users
Groups
Tenant admini
Troubleshootin

evices. Learn more.

Last Published
10/22/21, 12:00 AM
12/09/20, 12:00 AM
05/25/23, 2:00 AM
10/21/21, 12:00 AM
05/25/23, 2:00 AM

https://learn.microsoft.com/en-us/mem/intune/protect/se

5. Config

Available security baselines

The following security baseline instances are available for use with Intune. Use the links to view the settings for recent instances of each baseline.

- Security Baseline for Windows 10 and later
  - November 2021
  - December 2020
  - August 2020
- Microsoft Defender for Endpoint baseline
  (To use this baseline your environment must meet the prerequisites for using Microsoft Defender for Endpoint).
  - Version 6
  - Version 5
  - Version 4
  - Version 3

> **Note**
>
> The Microsoft Defender for Endpoint security baseline has been optimized for physical devices and is currently not recommended for use on virtual machines (VMs) or VDI endpoints. Certain baseline settings can impact remote interactive sessions on virtualized environments. For more information, see **Increase compliance to the Microsoft Defender for Endpoint security baseline** in the Windows documentation.

- Microsoft 365 Apps for Enterprise
  - May 2023 (Office baseline)
- Microsoft Edge Baseline
  - May 2023 (Edge Version 112 and later)
  - September 2020 (Edge version 85 and later)
  - April 2020 (Edge version 80 and later)
  - Preview: October 2019 (Edge version 77 and later)
- Windows 365 Security Baseline
  - October 2021

- Block display of toast notifications:
  Baseline default: *Yes*
  Learn More

App Runtime

- Microsoft accounts optional for Microsoft store apps:
  Baseline default: *Enabled*
  Learn more

BitLocker

- BitLocker removable drive policy:
  Baseline default: *Configure*
  Learn more
  - Block write access to removable data-drives not protected by BitLocker:
    Baseline default: *Yes*
    Learn more

Browser

- Block Password Manager:
  Baseline default: *Yes*
  Learn more
- Require SmartScreen for Microsoft Edge Legacy:
  Baseline default: *Yes*
  Learn more
- Block malicious site access:
  Baseline default: *Yes*
  Learn more
- Block unverified file download:
  Baseline default: *Yes*
  Learn more
- Prevent user from overriding certific

Microsoft In

Home
Dashboard
All services
Devices
Apps
Endpoint sec
Reports
Users
Groups
Tenant admini
Troubleshootin

ce features

Enhance
• Protections and configurations

es. Learn more.

Last Published
10/22/21, 12:00 AM
12/09/20, 12:00 AM
05/25/23, 2:00 AM
10/21/21, 12:00 AM
05/25/23, 2:00 AM

https://learn.microsoft.com/en-us/mem/intune/protect/secu

5. Config

Available security baselines

The following security baseline instances are available for use with Intune. Use the links to view the settings for recent instances of each baseline.

- Security Baseline for Windows 10 and later
  - November 2021
  - December 2020
  - August 2020
- Microsoft Defender for Endpoint baseline
  (To use this baseline your environment must meet the prerequisites for using Microsoft Defender for Endpoint).
  - Version 6
  - Version 5
  - Version 4
  - Version 3

> **Note**
> The Microsoft Defender for Endpoint security baseline has been optimized for physical devices and is currently not recommended for use on virtual machines (VMs) or VDI endpoints. Certain baseline settings can impact remote interactive sessions on virtualized environments. For more information, see **Increase compliance to the Microsoft Defender for Endpoint security baseline** in the Windows documentation.

- Microsoft 365 Apps for Enterprise
  - May 2023 (Office baseline)
- Microsoft Edge Baseline
  - May 2023 (Edge Version 112 and later)
  - September 2020 (Edge version 85 and later)
  - April 2020 (Edge version 80 and later)
  - Preview: October 2019 (Edge version 77 and later)
- Windows 365 Security Baseline
  - October 2021

Connectivity

- **Configure secure access to UNC paths:**
  Baseline default: *Configure Windows to only allow access to the specified UNC paths after fulfilling additional security requirements*
  Learn more
  - **Hardened UNC path list:**
    Baseline default: *Not configured by default. Manually add one or more hardened UNC paths.*
- **Block downloading of print drivers over HTTP:**
  Baseline default: *Enabled*
  Learn more
- **Block Internet download for web publishing and online ordering wizards:**

Device Installation

- **Block hardware device installation by setup classes:**
  Baseline default: *Yes*
  Learn more
  - **Remove matching hardware devices:**
    Baseline default: *Yes*
  - **Block list:**
    Baseline default: *Not configured by default. Manually add one or more Identifiers.*

Device Lock

- **Require password:**
  Baseline default: *Yes*
  Learn more
  - **Required password:**
    Baseline default: *Alphanumeric*
    Learn more
  - **Password expiration (days):**
    Baseline default: *60*
    Learn more

Microsoft In
Home
Dashboard
All services
Devices
Apps
Endpoint sec
Reports
Users
Groups
Tenant admini
Troubleshootin

ces. Learn more.

Last Published
10/22/21, 12:00 AM
12/09/20, 12:00 AM
05/25/23, 2:00 AM
10/21/21, 12:00 AM
05/25/23, 2:00 AM

ice features
Enhance
• Protections and configurations

https://learn.microsoft.com/en-us/mem/intune/protect/secu

5. Config

Available security baselines

The following security baseline instances are available for use with Intune. Use the links to view the settings for recent instances of each baseline.

- Security Baseline for Windows 10 and later
  - November 2021
  - December 2020
  - August 2020
- Microsoft Defender for Endpoint baseline
  (To use this baseline your environment must meet the prerequisites for using Microsoft Defender for Endpoint).
  - Version 6
  - Version 5
  - Version 4
  - Version 3

> **Note**
> The Microsoft Defender for Endpoint security baseline has been optimized for physical devices and is currently not recommended for use on virtual machines (VMs) or VDI endpoints. Certain baseline settings can impact remote interactive sessions on virtualized environments. For more information, see **Increase compliance to the Microsoft Defender for Endpoint security baseline** in the Windows documentation.

- Microsoft 365 Apps for Enterprise
  - May 2023 (Office baseline)
- Microsoft Edge Baseline
  - May 2023 (Edge Version 112 and later)
  - September 2020 (Edge version 85 and later)
  - April 2020 (Edge version 80 and later)
  - Preview: October 2019 (Edge version 77 and later)
- Windows 365 Security Baseline
  - October 2021

- Prevent reuse of previous passwords:
  Baseline default: *24*
  Learn more
- Minimum password length:
  Baseline default: *8*
  Learn more
- Number of sign-in failures before wiping device:
  Baseline default: *10*
  Learn more
- Block simple passwords:
  Baseline default: *Yes*
  Learn more

- Password minimum age in days:
  Baseline default: *1*
  Learn more
- Prevent use of camera:
  Baseline default: *Enabled*
  Learn more
- Prevent slide show:
  Baseline default: *Enabled*
  Learn more

DMA Guard

- Enumeration of external devices incompatible with Kernel DMA Protection:
  Baseline default: *Block all*

Event Log Service

- Application log maximum file size in KB:
  Baseline default: *32768*
  Learn more
- System log maximum file size in KB:
  Baseline default: *32768*

ice features

Enhance
• Protections and configurations

Microsoft In

Home
Dashboard
All services
Devices
Apps
Endpoint sec
Reports
Users
Groups
Tenant admini
Troubleshootin

ces. Learn more.

Last Published
10/22/21, 12:00 AM
12/09/20, 12:00 AM
05/25/23, 2:00 AM
10/21/21, 12:00 AM
05/25/23, 2:00 AM

https://learn.microsoft.com/en-us/mem/intune/protect/secu

5. Configu

Available security baselines

The following security baseline instances are available for use with Intune. Use the links to view the settings for recent instances of each baseline.

- **Security Baseline for Windows 10 and later**
  - November 2021
  - December 2020
  - August 2020
- **Microsoft Defender for Endpoint baseline**
  (To use this baseline your environment must meet the prerequisites for using Microsoft Defender for Endpoint).
  - Version 6
  - Version 5
  - Version 4
  - Version 3

> **Note**
> The Microsoft Defender for Endpoint security baseline has been optimized for physical devices and is currently not recommended for use on virtual machines (VMs) or VDI endpoints. Certain baseline settings can impact remote interactive sessions on virtualized environments. For more information, see **Increase compliance to the Microsoft Defender for Endpoint security baseline** in the Windows documentation.

- **Microsoft 365 Apps for Enterprise**
  - May 2023 (Office baseline)
- **Microsoft Edge Baseline**
  - May 2023 (Edge Version 112 and later)
  - September 2020 (Edge version 85 and later)
  - April 2020 (Edge version 80 and later)
  - Preview: October 2019 (Edge version 77 and later)
- **Windows 365 Security Baseline**
  - October 2021

Experience

- **Block Windows Spotlight:**
  Baseline default: *Yes*
  Learn more
  - **Block third-party suggestions in Windows Spotlight:**
    Baseline default: *Not configured*
    Learn more
  - **Block consumer specific features:**
    Baseline default: *Not configured*
    Learn more

File Explorer

- **Block data execution prevention:**
  Baseline default: *Disabled*
  Learn more
- **Block heap termination on corruption:**
  Baseline default: *Disabled*
  Learn more

Firewall

For more information, see 2.2.2 FW_PROFILE_TYPE in the Windows Protocols documentation.

- **Firewall profile domain:**
  Baseline default: *Configure*
  Learn more
  - **Inbound connections blocked:**
    Baseline default: *Yes*
    Learn more
  - **Outbound connections required:**
    Baseline default: *Yes*
    Learn more
  - **Inbound notifications blocked:**

Microsoft In
Home
Dashboard
All services
Devices
Apps
Endpoint sec
Reports
Users
Groups
Tenant admini
Troubleshootin

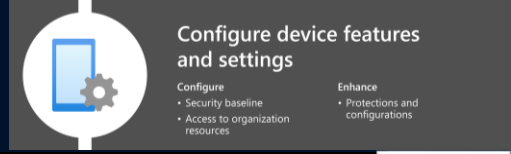
features
Enhance
• Protections and configurations

. Learn more.
Last Published
10/22/21, 12:00 AM
12/09/20, 12:00 AM
05/25/23, 2:00 AM
10/21/21, 12:00 AM
05/25/23, 2:00 AM

https://learn.microsoft.com/en-us/mem/intune/protect/securi

NIC Cloud Connect

5. Configurations



Microsoft Intune admin center

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

Home > Devices | Windows > Windows

Windows | Configuration profiles

Search

- Windows devices
- Windows enrollment

Windows policies

- Compliance policies
- Configuration profiles
- Scripts
- Update rings for Windows 10 and later
- Feature updates for Windows 10 and later
- Quality updates for Windows 10 and later
- Driver updates for Windows 10 and later

+ Create profile | Refresh | Export | Columns

Search | Platform: Windows Phone 8.1, Windows 8.1 and later, Windo... +1 | Add filters

Profile name	Platform	Profile type
WDCP000 - OS - Device Guard and Virtualization Based Technology and DMA guard	Windows 10 and later	Settings catalog
WDCP001 - OS - Security Baseline	Windows 10 and later	Settings catalog
WDCP002 - OS - Security Baseline - Internet Options	Windows 10 and later	Settings catalog
WDCP003 - OS - Windows Health Monitoring	Windows 10 and later	Windows health
WDCP004 - OS - Device Restrictions	Windows 10 and later	Settings catalog
WDCP005 - OS - Microsoft Defender Smartscreen	Windows 10 and later	Settings catalog
WDCP006 - OS - Windows Update For Business	Windows 10 and later	
WDCP007 - OS - Windows Update For Business reports	Windows 10 and later	Settings catalog
WDCP008 - OS - Delivery Optimization	Windows 10 and later	Settings catalog
WDCP009 - OS - Device Lock - Password Policy for local accounts	Windows 10 and later	Settings catalog
WDCP010 - OS - Device Lock - Screen lock out 5 mintues	Windows 10 and later	Settings catalog
WDCP011 - OS - Lock Screen Image	Windows 10 and later	Settings catalog
WDCP012 - OS - Password reset on lock screen	Windows 10 and later	Settings catalog

5. Configurations

Home > Devices | Windows > Windows | Configuration profiles >

Endpoint protection ...

Windows 10 and later

Basics | 2 Configuration settings | 3 Scope tags | 4 Assignments | 5 Applicability Rules | 6 Review + create

- Microsoft Defender Application Guard
- Microsoft Defender Firewall
- Microsoft Defender SmartScreen
- Windows Encryption

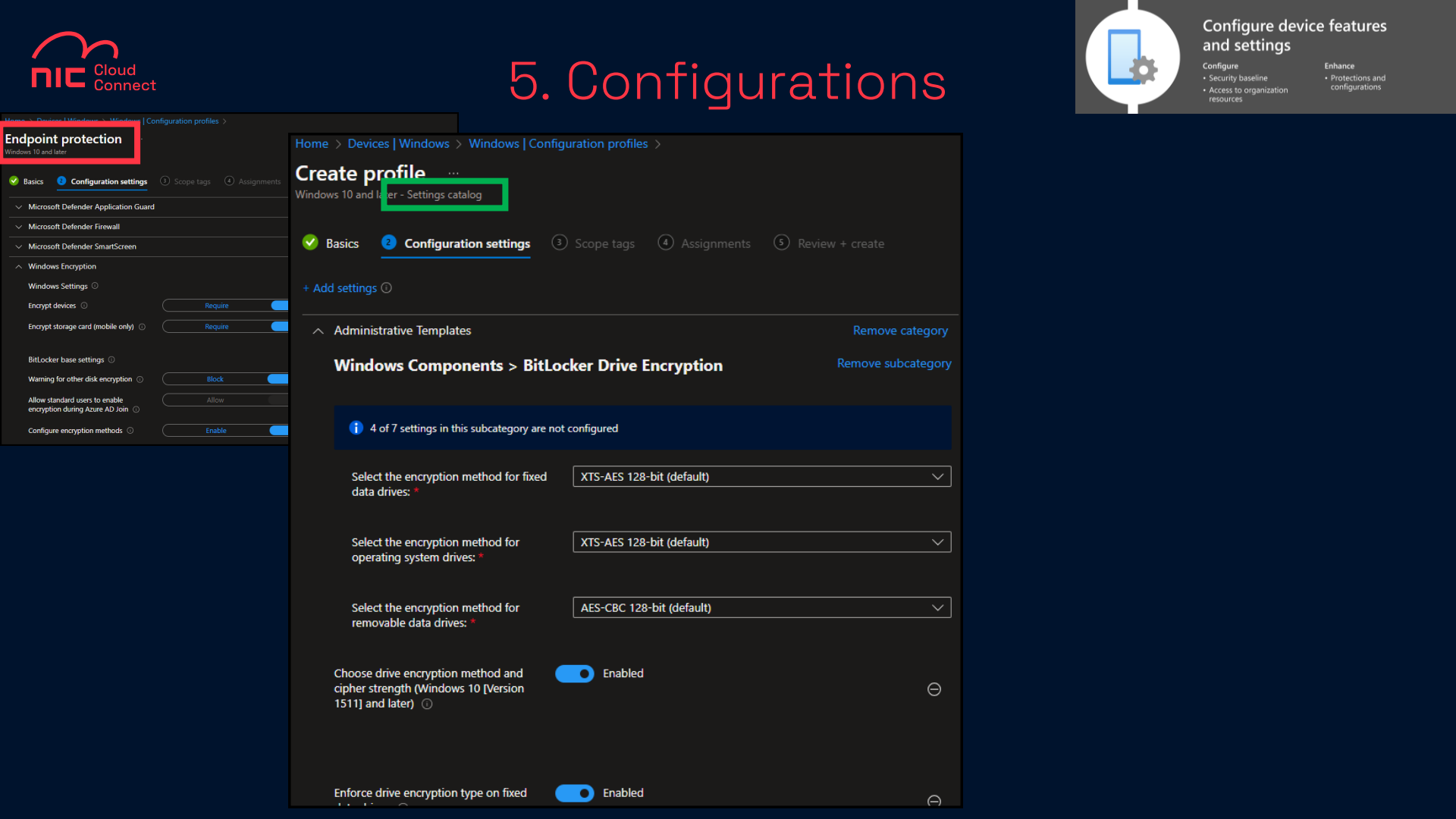
Windows Settings

Encrypt devices	Require	Not configured
Encrypt storage card (mobile only)	Require	Not configured

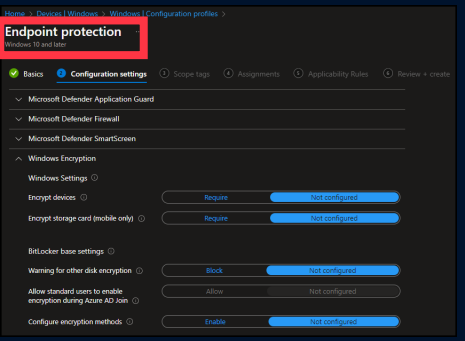
BitLocker base settings

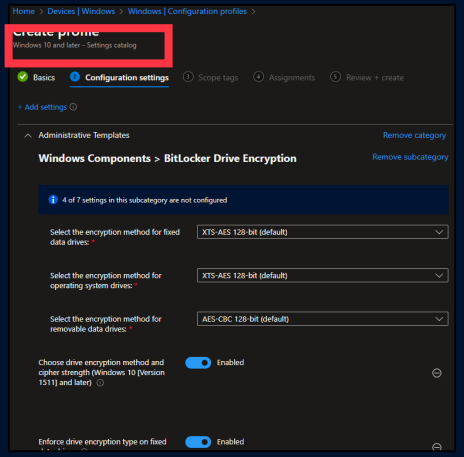
Warning for other disk encryption	Block	Not configured
Allow standard users to enable encryption during Azure AD Join	Allow	Not configured
Configure encryption methods	Enable	Not configured

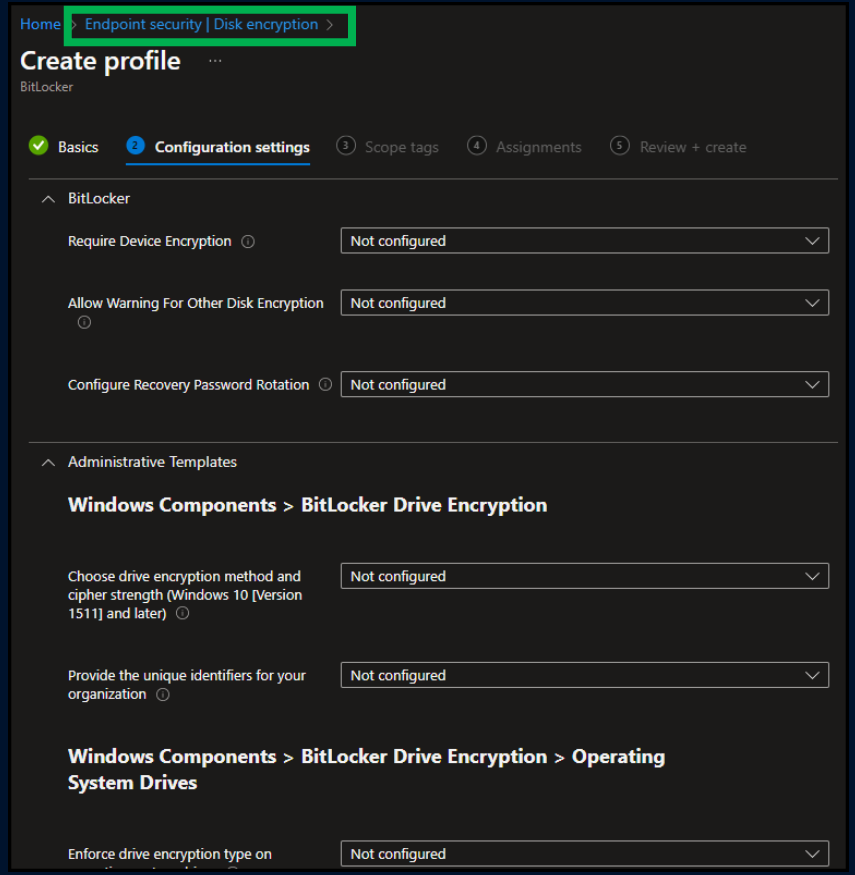
5. Configurations



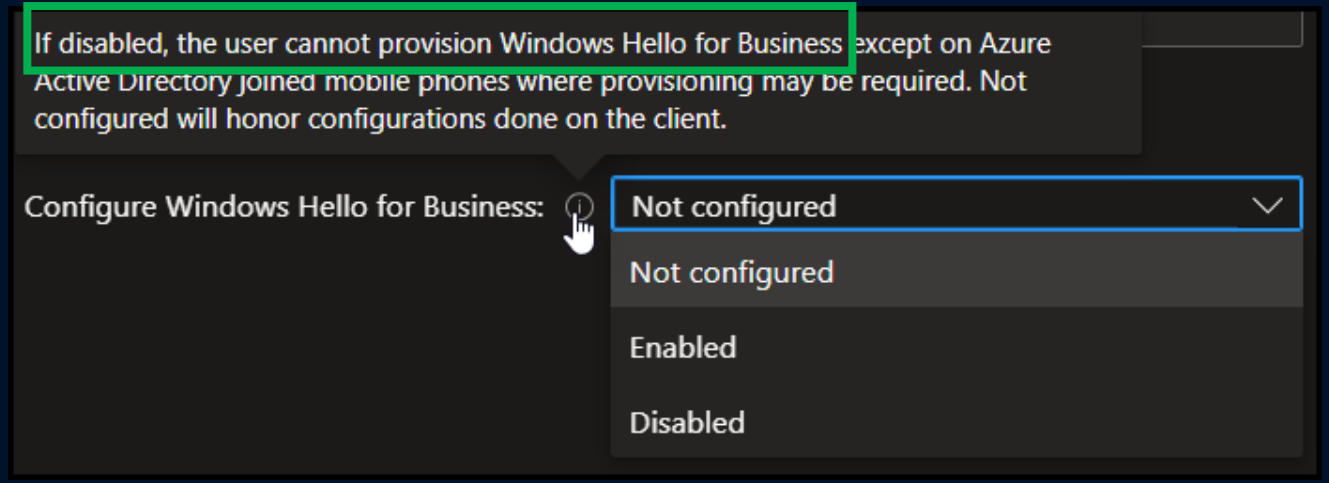
5. Configurations







5. Configurations



5. Configurations

If disabled, the user cannot provision Windows Hello for Business except on Azure Active Directory joined mobile phones where provisioning may be required. Not configured will honor configurations done on the client.

Configure Windows Hello for Business: Not configured

- Not configured
- Enabled
- Disabled

Configuration settings Edit

Block Windows Hello for Business
Windows Hello for Business is an alternative method for signing into Windows by replacing passwords, Smart Cards, and Virtual Smart Cards. If you disable or do not configure this policy setting, the device provisions Windows Hello for Business. If you enable this policy setting, the device does not provision Windows Hello for Business for any user.

Block Windows Hello for Business: Disabled

5. Configurations

Home > Devices | Windows > Windows | Configuration profiles >

Create profile ...

Windows 10 and later - Settings catalog

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

This policy setting lets you prevent apps and features from working with files on OneDrive. If you enable this policy setting: users can't access OneDrive from the OneDrive app and file picker; Microsoft Store apps can't access OneDrive using the WinRT API; OneDrive doesn't appear in the navigation pane in File Explorer; OneDrive files aren't kept in sync with the cloud; Users can't automatically upload photos and videos from the camera roll folder. If you disable or do not configure this policy setting, apps and features can work with OneDrive file storage.

Learn more

Remove category

Disable One Drive File Sync

Sync enabled.

Sync enabled.

Sync disabled.

5. Configurations

Home > Devices | Windows > Windows | Configuration profiles >

Create profile

Windows 10 and later - Setting...

Registry Editor

File Edit View Favorites Help

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PolicyManager\providers\5613E3DF-193F-4DDE-BCF5-DDCE07CD62FC\default\Device\System

- RemoteDesktopServices
- RemoteManagement
- RemoteProcedureCall
- Search
- Security
- Settings
- SmartScreen
- System
- SystemServices
- Update
- updatev95~Policy~Cat_EdgeUpdate~Cat_Applications~Cat_Micro
- WebThreatDefense
- WindowsConnectionManager
- WindowsDefenderSecurityCenter
- WindowsInkWorkspace
- WindowsPowerShell

Name	Type	Data
(Default)	REG_SZ	(value not set)
AllowBuildPreview	REG_DWORD	0x00000002 (2)
AllowMicrosoftManagedDesktopProcessing	REG_DWORD	0x00000020 (32)
AllowMicrosoftManagedDesktopProcessing_...	REG_DWORD	0x00000001 (1)
AllowTelemetry	REG_SZ	0x00000003 (3)
BootStartDriverInitialization	REG_DWORD	<enabled /><d
BootStartDriverInitialization_LastWrite	REG_DWORD	0x00000001 (1)
DisableOneDriveFileSync	REG_DWORD	0x00000001 (1)
LimitDiagnosticLogCollection	REG_DWORD	0x00000001 (1)
LimitDumpCollection	REG_DWORD	0x00000001 (1)
LimitEnhancedDiagnosticDataWindowsAnal...	REG_DWORD	0x00000001 (1)

Sync enabled.

Sync disabled.

1 Security | 2 Architecture | 3 Partner | Automation | 5 Cloud | 6 Data & AI | 7 Server & Client

08:00
EXPO 8:00 — 30 min
Doors open
NIC Cloud Connect

08:30
1 SECURITY

10:00
10:00 — 60 min
Forward to the Past and Back to the Future - Cybercrime in 2022/2023
Sami Laiho

10:00 — 60 min
Azure Hybrid with Azure Stack HCI
Jan-Tore Pedersen

10:00 — 60 min
Part… AVD… Solu… 2023
Neil M… Vegas…

10:00 — 60 min
…ted with …r DevOps

10:00 — 60 min
CoPilot for Data Protection and classification of data
Roy Apalnes

10:00 — 60 min
Beyond the Thunderdome: Microsoft 365 Guest & External Access Inside & Out!
Andy Malone

11:20
11:20 — 60 min
Hacker's Perspective on New Risks: Revising the Cybersecurity Priorities for 2023
Paula Januszkiewicz

11:20
Unde… Shari… to Ba… Colla… Secu…
Ståle H… Simon…

…ganization …pilot Ready?
…sen

11:20 — 60 min
Deep dive into Graph API and Intune
Nickolaj Andersen

12:20
EXPO 12:20 — 60 min
Lunch break

13:20
13:20 — 60 min
The Best Teacher is the Last Mistake: Top Things You Can Do to Improve your Incident Response Plan
Paula Januszkiewicz

13:20 — 60 min
Microsoft Teams 2.0: A deep dive into the new client and architecture
Peter Schmidt

13:20 — 60 min
Backing up Cloud Native workloads with Kasten K10 by Veeam
Timothy Dewin

13:20 — 30 min
Automating the Transition to Log Ingestion API & Data Collection Rules for your Logs in LogAnalytics

13:20 — 60 min
Cybersecurity Top Gun! Bullet proof your Hybrid Cloud.
Andy Malone

13:20 — 60 min
Why There's Never Been a Better Time to Dive into Data with Microsoft Fabric
Puneet Vijwani
Thomas Bjarvåg

13:20 — 60 min
Unlocking the Secrets of Intune Troubleshooting: A Deep Dive into Mastery
Ronni Pedersen
Jörgen Nilsson

Ronni Pedersen Jörgen Nilsson

Unlocking the Secrets of Intune Troubleshooting: A Deep Dive into Mastery

Get to the root of you moden managed Windows client issues with Microsoft Intune. In this session, we'll cover everything you need to know about troubleshooting Configuration Profiles, Enrollment, Settings, App deployment and more.
We'll take a deep dive into real-world examples and share field-tested tips and tricks for identifying and resolving common problems. Whether you're new to Microsoft Intune or a seasoned pro, this session will give you the tools you need to troubleshoot effectively.

7 SERVER & CLIENT | Wed 13:20 - 14:20

4

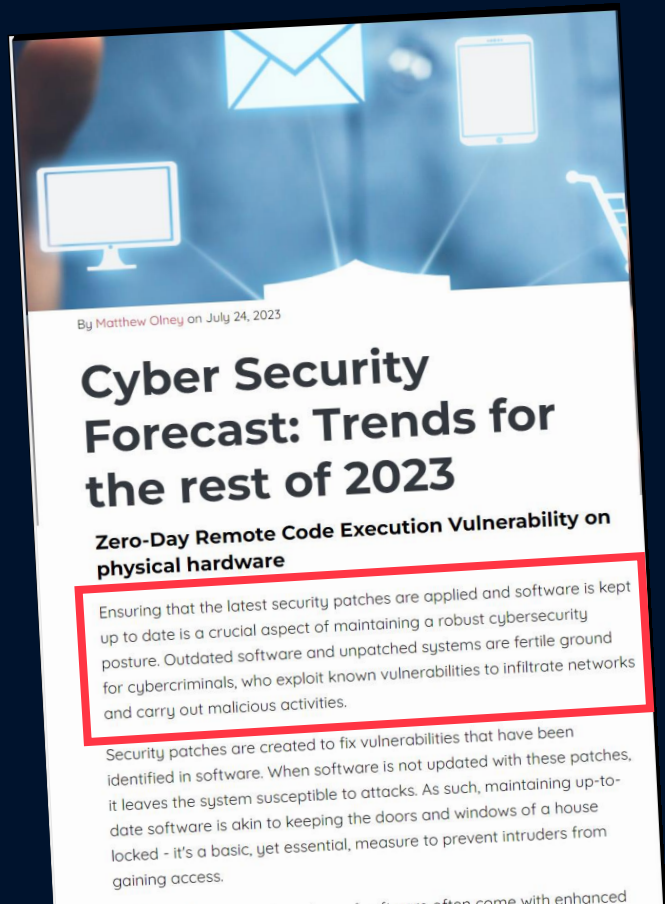
Updates and Patches

Unmasking 10 Frequent Intune Mistakes and How to Prevent Them

Cloud Connect

4

Updates and Patches



By Matthew Olney on July 24, 2023

Cyber Security Forecast: Trends for the rest of 2023

Zero-Day Remote Code Execution Vulnerability on physical hardware

Ensuring that the latest security patches are applied and software is kept up to date is a crucial aspect of maintaining a robust cybersecurity posture. Outdated software and unpatched systems are fertile ground for cybercriminals, who exploit known vulnerabilities to infiltrate networks and carry out malicious activities.

Security patches are created to fix vulnerabilities that have been identified in software. When software is not updated with these patches, it leaves the system susceptible to attacks. As such, maintaining up-to-date software is akin to keeping the doors and windows of a house locked - it's a basic, yet essential, measure to prevent intruders from gaining access.

4. Updates and Patches

Microsoft Intune admin center

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

All services > Devices

Devices | Update rings for Windows 10 and later

Search

Policy

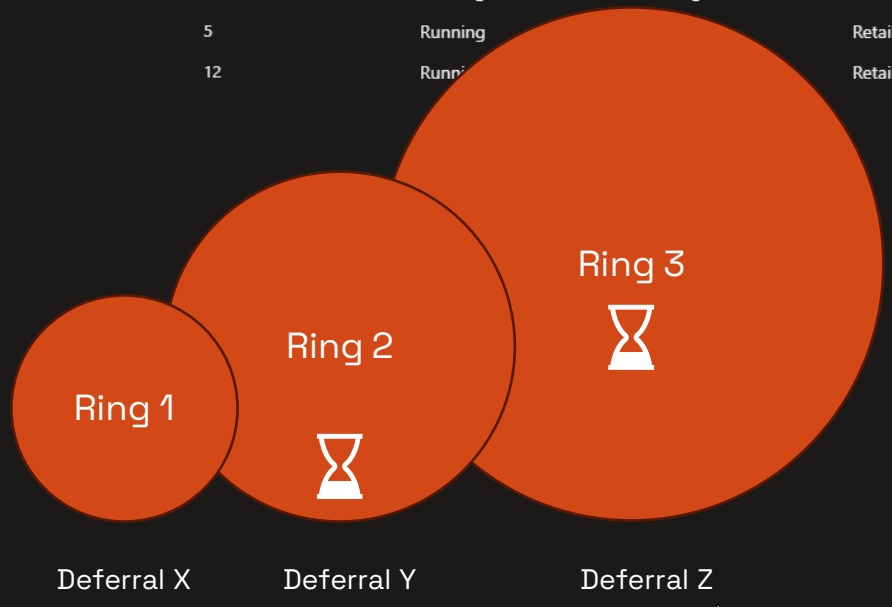
- Compliance policies
- Conditional access
- Configuration profiles
- Scripts
- Remediations
- Group Policy analytics
- Update rings for Windows 10 and later
- Feature updates for Windows 10 and later

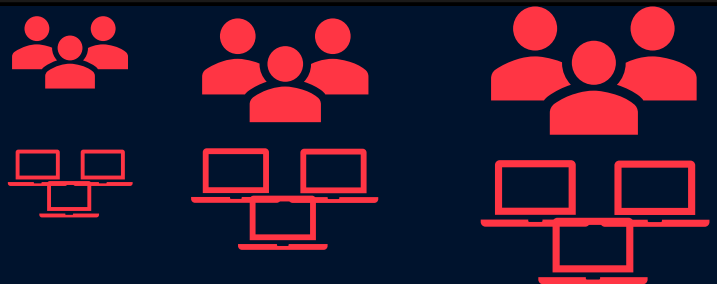
+ Create profile | Refresh | Export | Columns

Search | Add filter

Name	Feature deferral
WUP001 - Windows - Patching - Ring 1	0
WUP002 - Windows - Patching - Ring 2	0
WUP003 - Windows - Patching - Production	0

Name	Feature deferral	Quality deferral	Feature	Quality	Servicing channel	Scope tags
WUP001 - Windows - Patching - Ring 1	0	1	Running	Running	Retail channel	Yes
WUP002 - Windows - Patching - Ring 2	0	5	Running		Retail channel	Yes
WUP003 - Windows - Patching - Production	0	12	Runni		Retail channel	Yes





4. Updates and Patches

Microsoft Intune admin center

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

All services > Devices

Devices | Update rings for Windows 10 and later

Search

Policy

- Compliance policies
- Conditional access
- Configuration profiles
- Scripts
- Remediations
- Group Policy analytics
- Update rings for Windows 10 and later
- Feature updates for Windows 10 and later

+ Create profile | Refresh | Export | Columns

Search | Add filter

Name	Feature deferral
WUP001 - Windows - Patching - Ring 1	0
WUP002 - Windows - Patching - Ring 2	0
WUP003 - Windows - Patching - Production	0

4. Updates and Patches

Microsoft Intune admin center

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

All services > Devices

Devices | Feature updates for Windows 10 and later

Search

Policy

- Compliance policies
- Conditional access
- Configuration profiles
- Scripts
- Remediations
- Group Policy analytics
- Update rings for Windows 10 and later
- Feature updates for Windows 10 and later

Create profile | Refresh | Export | Columns

Name	Feature update version
WFU001 - Windows10 - Ring 1	Windows 10, version 22H2
WFU002 - Windows10 - Ring 2	Windows 10, version 21H2
WFU003 - Windows10 - Production	Windows 10, version 22H2
WFU004 - Windows11 - Ring 1	Windows 11, version 22H2
WFU005 - Windows11 - Ring 2	Windows 11, version 22H2
WFU006 - Windows11 - Production	Windows 11, version 22H2

4. Updates and Patches

Microsoft Intune admin center

All services > Devices

Devices | Feature updates for Windows 10 and later

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

Search

Policy

- Compliance policies
- Conditional access
- Configuration profiles
- Scripts
- Remediations
- Group Policy analytics
- Update rings for Windows 10 and later
- Feature updates for Windows 10 and later

Create profile | Refresh | Export | Columns

Name	Feature update version
WFU001 - Windows10 - Ring 1	Windows 10, version 22H2
WFU002 - Windows10 - Ring 2	Windows 10, version 21H2
WFU003 - Windows10 - Production	Windows 10, version 22H2
WFU004 - Windows11 - Ring 1	Windows 11, version 22H2
WFU005 - Windows11 - Ring 2	Windows 11, version 22H2
WFU006 - Windows11 - Production	Windows 11, version 22H2

4. Updates and Patches

Microsoft Intune admin center

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

All services > Devices

Devices | Feature updates for Windows 10 and later

Search

Policy

- Compliance policies
- Conditional access
- Configuration profiles
- Scripts
- Remediations
- Group Policy analytics
- Update rings for Windows 10 and later
- Feature updates for Windows 10 and later

Create profile | Refresh | Export | Columns

Name	Feature update version
WFU001 - Windows10 - Ring 1	Windows 10, version 22H2
WFU002 - Windows10 - Ring 2	Windows 10, version 21H2
WFU003 - Windows10 - Production	Windows 10, version 22H2
WFU004 - Windows11 - Ring 1	Windows 11, version 22H2
WFU005 - Windows11 - Ring 2	Windows 11, version 22H2
WFU006 - Windows11 - Production	Windows 11, version 22H2

4. Updates and Patches

Microsoft Intune admin center

Home > Devices | Feature updates for Windows 10 and later > WFU004 - Windows11 - Ring 1 | Properties >

Edit feature update deployment

Feature update deployments

1 Deployment settings 2 Review + save

Enable Windows health monitoring and select Windows Update scope to get detailed device states and errors. Learn more

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

Name * WFU004 - Windows11 - Ring 1

Description 2023.09.26 - CloudWay template installed, Simon

Feature deployment settings

Feature update to deploy: Windows 11, version 23H2

When a device isn't capable of running Windows 11, install the latest Windows 10 feature update

4. Updates and Patches

Microsoft Intune admin center

Home > Devices | Feature updates for Windows 10 and later > WFU004 - Windows11 - Ring 1 | Properties >

Edit feature update deployment

Feature update deployments

1 Deployment settings 2 Review + save

Enable Windows health monitoring and select Windows Update scope to get detailed device states and errors. Learn more

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

Name * WFU004 - Windows11 - Ring 1

Description 2023.09.26 - CloudWay template installed, Simon

Feature deployment settings

Feature update to deploy: Windows 11, version 23H2

When a device isn't capable of running Windows 11, install the latest Windows 10 feature update

4. Updates and Patches

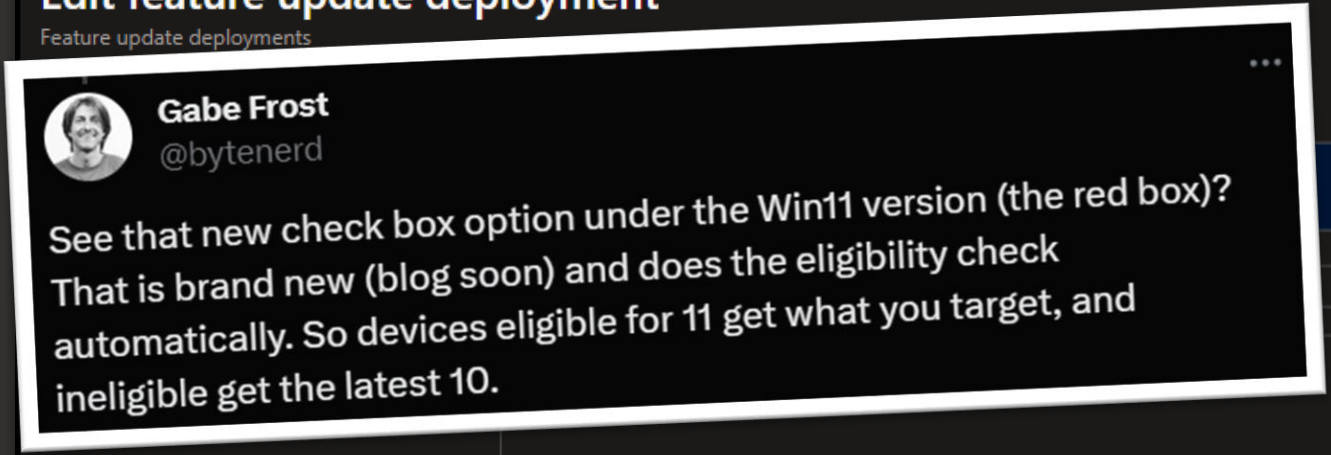
Microsoft Intune admin center

Home > Devices | Feature updates for Windows 10 and later > WFU004 - Windows11 - Ring 1 | Properties >

Edit feature update deployment

Feature update deployments

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



Feature deployment settings

Feature update to deploy: Windows 11, version 23H2

When a device isn't capable of running Windows 11, install the latest Windows 10 feature update

4. Updates and Patches

Microsoft Intune admin center

Home > Devices | Feature updates for Windows 10 and later > WFU004 - Windows11 - Ring 1 | Properties >

Edit feature update deployment

Feature update deployments

- Home
- Dashboard
- All services
- Devices
- Apps
- Endpoint security
- Reports
- Users
- Groups
- Tenant a
- Troublesh

Gabe Frost
@bytenerd

See that new check box option under the Win11 version (the red box)? That is brand new (blog soon) and does the eligibility check automatically. So devices eligible for 11 get what you target, and ineligible get the latest 10.

Gabe Frost @bytenerd · Oct 31

...so when you're ready for Win11 (and you should be by now) you can just use one Win11 feature update deployment policy to get ALL your Win10 & Win11 devices on the latest version.

Feature update to deploy ⓘ — Windows 11, version 23H2

☐ When a device isn't capable of running Windows 11, install the latest Windows 10 feature update

4. Updates and Patches

Microsoft Intune admin center

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

All services > Devices

Devices | Driver updates for Windows 10 and later

Search

Policy

- Compliance policies
- Conditional access
- Configuration profiles
- Scripts
- Remediations
- Group Policy analytics
- Update rings for Windows 10 and later
- Feature updates for Windows 10 and later
- Quality updates for Windows 10 and later
- Driver updates for Windows 10 and later

Create profile | Refresh | Export | Columns

Name	Assigned	Approval method
WDU001 - Driver Update - Ring 1	Yes	Automatic
WDU002 - Driver Update - Ring 2	Yes	Automatic
WDU003 - Driver Update - Production	Yes	Automatic
WDU004 - Driver Update - Manual Update	Yes	Manual

4. Updates and Patches

Microsoft Intune admin center

SIMON DOES (M365X73910067.O...

Home > Tenant admin

Tenant admin | Tenant enrollment

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

Search

- Intune add-ons

End user experiences

- Customization
- Organizational messages
- Custom notifications
- Terms and conditions

Windows Autopatch

- Tenant enrollment

Microsoft Managed Desktop

- Tenant enrollment

Help and support

- Help and support

Windows Autopatch

Windows Autopatch is an automated patch management service for Windows 10/11 Pro & Enterprise, Windows 365 clients, Microsoft 365 apps, Microsoft Teams, Azure Virtual Desktop, and Microsoft Edge. Windows 10/11 Enterprise E3 (or higher) customers can enroll into this service after meeting the required prerequisites. Learn more about our prerequisites. Windows Autopatch demos are available for all users regardless of prerequisites here.

For technical information, learn more about Microsoft Autopatch. If you're unfamiliar with Windows Autopatch, learn more about the service generally.

To check eligibility, start with the readiness assessment tool

The readiness assessment tool checks certain details of your Intune and Microsoft Entra settings to ensure they're ready for the best experience when you enroll in Windows Autopatch. Run this tool whenever you want to confirm you've taken care of any reported issues.

We'll give you a list of things you need to do before enrolling in the tool. You must be signed in as at least Intune admin to run this tool. Some checks require additional permissions. Learn more about these checks. permissions, and data

4. Updates and Patches

Microsoft Intune admin center

SIMON DOES (M365X73910067.O...

Home > Tenant admin

Tenant admin | Tenant enrollment

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

Search

- Intune add-ons

End user experiences

- Customization
- Organizational messages
- Custom notifications
- Terms and conditions

Windows Autopatch

- Tenant enrollment

Microsoft Managed Desktop

- Tenant enrollment

Help and support

- Help and support

you've taken care of any reported issues.

We'll give you a list of things you need to do before enrolling in the tool. You must be signed in as at least Intune admin to run this tool. Some checks require additional permissions. Learn more about these checks, permissions, and data storage. Once the tool shows you're ready, you can enroll your tenant into the service. You will not need to run the tool again. You must be a Global Administrator to enroll into the service.

This tool collects, assesses, and stores data in the service to perform the assessment. We do not collect or store personal data, nor share your data with other services. However, we do collect system metadata and organizational information to complete this assessment. We retain data for 12 months after you last use this tool to provide and improve the service. After 12 months, we retain it in de-identified form without company name. You can choose to delete the data we collect. Learn more about the checks and review the privacy statement.

Select check box to allow Microsoft to assess and store results for the readiness assessment, and then select **Agree**.

Agree

4. Updates and Patches

Microsoft Intune admin center

SIMON DOES (M365X73910067.O...

Home > Tenant admin

Tenant admin | Tenant enrollment

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

Search

- Intune add-ons

End user experiences

- Customization
- Organizational messages
- Custom notifications
- Terms and conditions

Windows Autopatch

- Tenant enrollment

Microsoft Managed Desktop

- Tenant enrollment

Help and support

- Help and support

Results

Run checks | Export all | Delete all data | About this tool

This tool confirms that various Intune and Microsoft Entra settings are appropriate and meet prerequisites for Windows Autopatch. Learn more about Windows Autopatch

Readiness status

LAST REFRESHED 10/27/2023, 2:28:49 PM

Ready

You are ready to enroll in Windows Autopatch, but you still have Advisory tasks. Review these before you set up your first device.

Select **Enroll** to start your enrollment process.

Enroll

Management settings

Ready	Not ready	Advisory
1	0	2

View details

4. Updates and Patches

Microsoft Intune admin center

SIMON DOES (M365X73910067.O...

Home

Dashboard

All services

Devices

Apps

Endpoint security

Reports

Users

Groups

Tenant administration

Troubleshooting + support

Home >

Windows Autopatch

- Create a Microsoft application that we use to run the Windows Autopatch service. Learn more about Windows Autopatch enterprise applications
- Create the policies, groups and scripts necessary to run the service. This involves excluding Windows Autopatch device groups, where applicable, for any of your existing policies that may cause conflicts. Windows Autopatch update policies must take precedence to avoid any conflicts. Learn more about Changes made at tenant enrollment
- Manage devices using Intune.
- Collect and share info on usage, status, and compliance for devices and apps.
- Collect and share Windows Diagnostic data on usage, status, and compliance for devices and apps. Learn more about the data we collect
- Store Windows Autopatch data securely in Azure data centers based on your data residency. Learn more about Windows Autopatch data storage

I give Microsoft permission to manage my Microsoft Entra organization on my behalf.

Revoking this access at any point terminates the servic

Agree

4. Updates and Patches

Microsoft Intune admin center

SIMON DOES (M365X73910067.O...

Home

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

Home >

Windows Autopatch

Autopatch Operations can work with to help you with issues that are outside the scope of your own IT operations.

We might have to contact this contact at any time, so choose contacts you're sure will be available. Microsoft Privacy statement

Primary Admin | Secondary Admin

Provide contact info for your organization's Windows Autopatch admin.

Phone number *	+47 91123260
Email *	simon@skotheimsvik.no
First Name *	Simon
Last Name *	Skotheimsvik
Preferred Language *	English

Previous | Next

4. Updates and Patches

Microsoft Intune admin center

SIMON DOES (M365X73910067.O...

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

Home >

Windows Autopatch

Setting up Windows Autopatch

We're setting up policies and configuration for your tenant. This will take a few minutes.

4. Updates and Patches

Microsoft Intune admin center

SIMON DOES (M365X73910067.O...

Home

Windows Autopatch

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

Windows Autopatch setup is complete

Select **Continue** to start registering devices.

Continue

4. Updates and Patches

Microsoft Intune admin center

SIMON DOES (M365X73910067.O...

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

Home > Windows Autopatch >

Devices

Autopatch groups set up is in progress

We're enabling Autopatch groups to manage in more detail how Windows Autopatch deploys updates. Learn more about Autopatch groups.

This could take up to 30 minutes. If you run into any issues, submit a support request ticket.

4. Updates and Patches

Microsoft Intune admin center

Home

Devices | Overview

Search

Overview
All devices
Monitor

Windows Autopatch
Devices
Release management

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

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

Preview upcoming changes to Devices and provide feedback. →

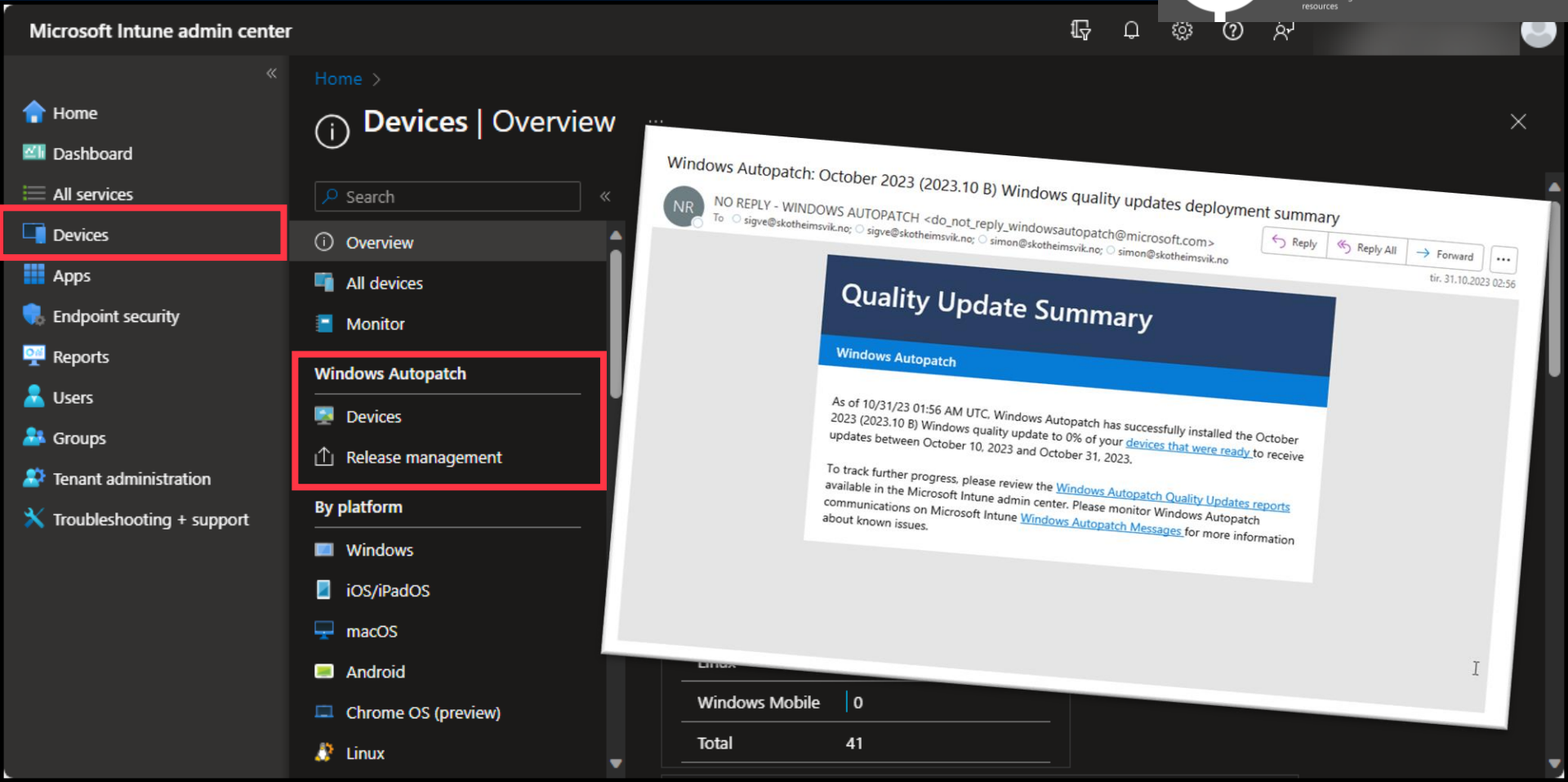
Enrollment status | Enrollment alerts | Cloud PC performance (preview)

Intune enrolled devices

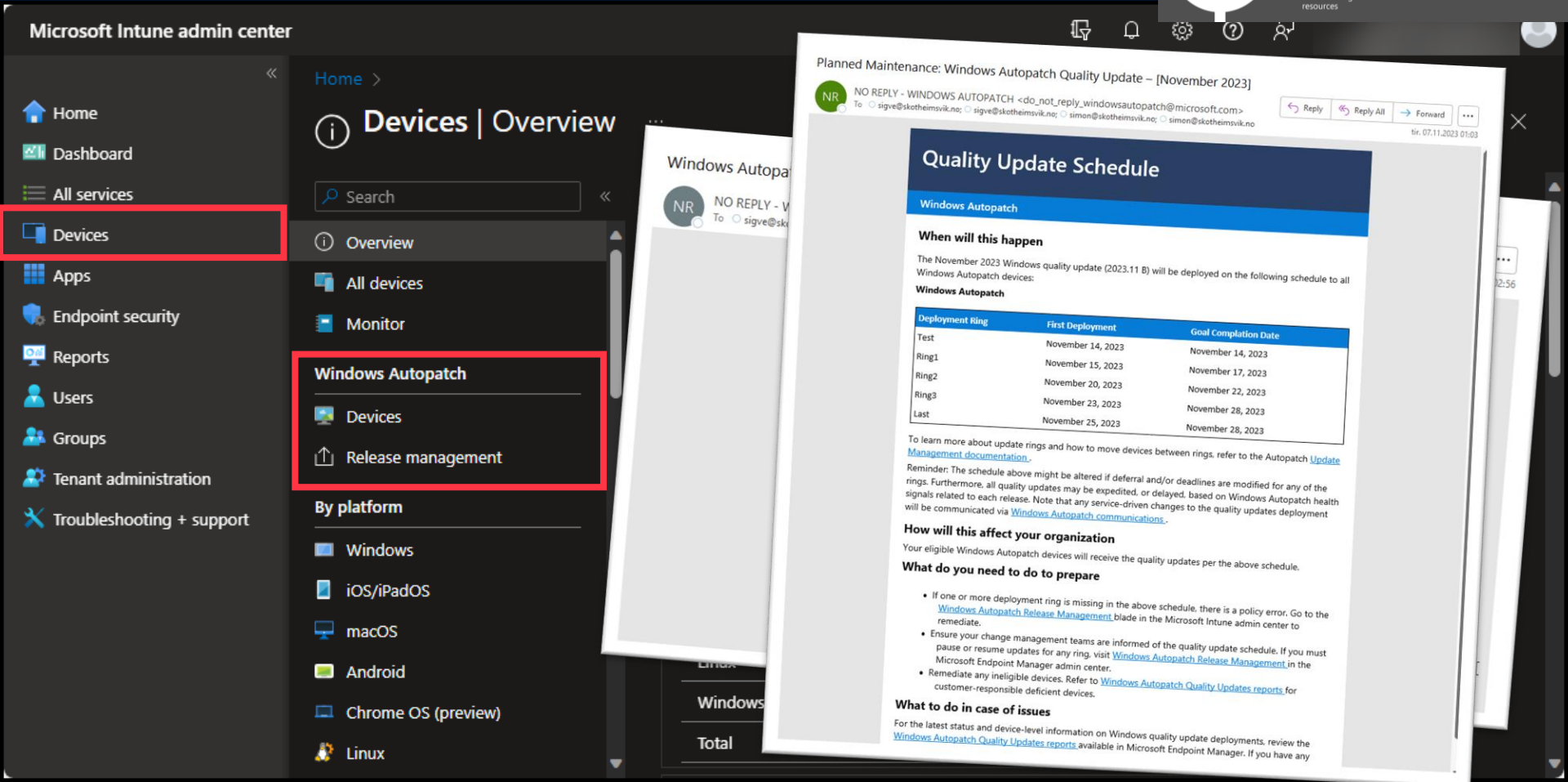
LAST UPDATED 10/27/23, 3:56 PM

Platform	Devices
Windows	23
iOS/iPadOS	8
Android	5
macOS	5
Linux	0
Windows Mobile	0
Total	41

4. Updates and Patches



4. Updates and Patches



4. Updates and Patches

Microsoft Intune admin center

admin@M365x7391006...
SIMON DOES (M365X73910067.O...

Home > Devices

Devices | Update policies for macOS

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

Search

- Update rings for Windows 10 and later
- Feature updates for Windows 10 and later
- Quality updates for Windows 10 and later
- Driver updates for Windows 10 and later
- Update policies for iOS/iPadOS
- Update policies for macOS
- Android FOTA deployments
- Enrollment device limit restrictions
- Enrollment device platform restrictions
- eSIM cellular profiles (preview)

Create profile | Refresh | Export | Columns

2 items

Search | Add filter

Name	Schedule type	Time zone	Time windows
MUP001 - macOS - Ring1	Update at next check-in	N/A	N/A
MUP002 - macOS - Ring2	Update during scheduled time	UTC+2	1

4. Updates and Patches

Microsoft Intune admin center

admin@M365x7391006...
SIMON DOES (M365X73910067.O...

Home > Devices

Devices | Update policies for macOS

Search

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

- Update rings for Windows 10 and later
- Feature updates for Windows 10 and later
- Quality updates for Windows 10 and later
- Driver updates for Windows 10 and later
- Update policies for iOS/iPadOS
- Update policies for macOS
- Android FOTA deployments
- Enrollment device limit restrictions
- Enrollment device platform restrictions
- eSIM cellular profiles (preview)

MUP001 - macOS - Ring1 | Properties

MacOS software update

Search

Overview

Manage

Properties

Basics Edit

Name	MUP001 - macOS - Ring1
Description	No Description

Update policy settings Edit

Critical updates	Install immediately
Firmware updates	Install immediately
Configuration file updates	Install immediately
All other updates (OS, built-in apps)	Install immediately
Schedule type	Update at next check-in

Assignments Edit

4. Updates and Patches

Microsoft Intune admin center

admin@M365x7391006...
SIMON DOES (M365X73910067.O...

Home > Devices

Devices | Update policies for macOS

Search

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

- Update rings for Windows 10 and later
- Feature updates for Windows 10 and later
- Quality updates for Windows 10 and later
- Driver updates for Windows 10 and later
- Update policies for iOS/iPadOS
- Update policies for macOS
- Android FOTA deployments
- Enrollment device limit restrictions
- Enrollment device platform restrictions
- eSIM cellular profiles (preview)

MUP001 - macOS - Ring1 | Properties

MacOS software update

Search

Overview

Manage

Properties

Basics Edit

Name MUP001 - macOS - Ring1

CloudWay

EPOS Connect requires an update. Please close **EPOS Connect**, or click Postpone. You have 2 postponements remaining.

The app(s) will be closed in:
1:29:44

Close Programs | Postpone

4. Updates and Patches

Microsoft Intune admin center

Home > Apps | Monitor > Monitor

Monitor | Discovered apps

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

Search

- App licenses
- Discovered apps
- App install status
- App Protection status
- App Configuration Status

Refresh | Export

Search by application name

Showing 1 to 20 of 4,958 records | < Previous | Page 1 of 248 | Next >

Application name	Application version	Device count
22094SynapticsIncorporate.SmartAudio3		
25724LightIT.84085B5755BB		
3 Button Navigation Bar		
34791E63.CanonInkjetPrintUtility		
360 Reality Audio Settings		
360 Reality Audio System		
360° Bilderedigering		
4505Fortemedia.FMAPOControl		
4DF9E0F8.Netflix		

CloudWay

EPOS Connect requires an update. Please close **EPOS Connect**, or click Postpone. You have 2 postponements remaining.

The app(s) will be closed in:
1:29:44

Close Programs | Postpone

4. Updates and Patches

Home > Apps | Monitor > Monitor

Monitor | Discovered apps

Search

- App licenses
- Discovered apps
- App install status
- App Protection status
- App Configuration Status

Refresh Export

adobe acrobat

Showing 1 to 18 of 18 records

< Previous Page 1 of 1 Next >

Application name	Application version	Device count
Adobe Acrobat	23.006.20320	2
Adobe Acrobat	23.006.20360	14
Adobe Acrobat	23.003.20284	1
Adobe Acrobat	23.003.20269	1
Adobe Acrobat (64-bit)	23.006.20360	59
Adobe Acrobat (64-bit)	23.003.20284	29
Adobe Acrobat (64-bit)	23.003.20215	1
Adobe Acrobat (64-bit)	22.003.20282	1
Adobe Acrobat (64-bit)	23.006.20320	1
Adobe Acrobat (64-bit)	23.001.20174	1
Adobe Acrobat (64-bit)	23.001.20093	1

CloudWay

EPOS Connect requires an update. Please close **EPOS Connect**, or click Postpone. You have 2 postponements remaining.

The app(s) will be closed in:
1:29:44

Close Programs | Postpone

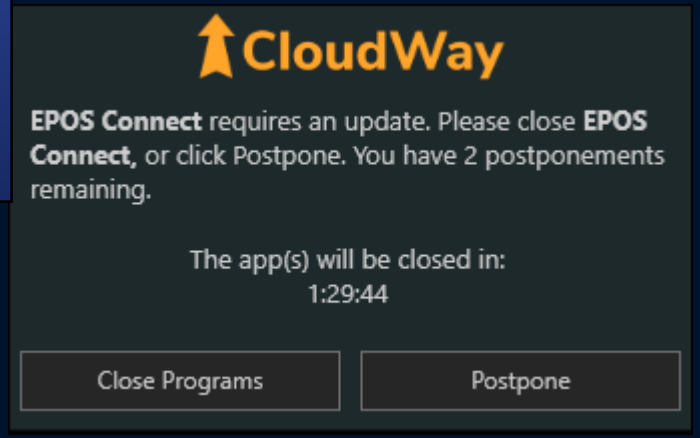
4. Updates and Patches

4. Updates and Patches

SCAPPMAN part of PATCH MY PC

Automate your application installations and updates in Microsoft Intune

A 100%-cloud solution that automatically installs all the necessary updates for your applications



Set up Intune

Add, configure, and protect apps

Use compliance and Conditional Access

Configure device features and settings

Enroll your devices

Configure

- Devices for enrollment
- Enrollment policies and restrictions

Use

- Enrollment profiles
- Windows Autopilot

3

Know your devices

Unmasking 10 Frequent Intune Mistakes and How to Prevent Them

3. Know your devices

Microsoft Intune admin center

admin@M365x7391006...
SIMON DOES (M365X73910067.O...

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

Simon Does

Welcome to the fresh look for Intune

Explore the updated homepage. Inside is still the familiar unified management solution for all your endpoints.

Give us your feedback

Status

Devices not in compliance **0**	Connector errors **0**
Configuration policies with error or conflict **0**	Service health **Healthy**
Client app install failure **0**	Account status **Active**

3. Know your devices

Microsoft Intune admin center

admin@M365x7391006...
SIMON DOES (M365X73910067.O...

Home > Devices

Devices | Enrollment device platform restrictions

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

Search

- Update policies for macOS
- Android FOTA deployments
- Enrollment device limit restrictions
- Enrollment device platform restrictions
- eSIM cellular profiles (preview)
- Policy sets

Other

- Device clean-up rules
- Device categories
- Filters

Help and support

- Help and support

Windows restrictions | Android restrictions | macOS restrictions | iOS restrictions

+ Create restriction

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

3. Know your devices

Microsoft Intune admin center

admin@M365X7391006...
SIMON DOES (M365X73910067.O...

Home > Devices | Enrollment device platform restrictions > All Users | Properties >

Edit restriction

Device type restriction

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

Specify the platform configuration restrictions that must be met for a device to enroll. Use compliance policies to restrict devices after enrollment. Define versions as major.minor.build. Version restrictions only apply to devices enrolled with the Company Portal. Intune classifies devices as personally-owned by default. Additional action is required to classify devices as corporate-owned. Learn more.

Type	Platform	versions	Personally owned	Device manufacturer
Android Enterprise (work profile)	Allow / Block	Allow min/max range: Min / Max	Allow / Block	Manufacturer name
Android device administrator	Allow / Block	Allow min/max range: Min / Max	Allow / Block	Manufacturer name
iOS/iPadOS	Allow / Block	Allow min/max range: Min / Max	Allow / Block	Restriction not supported
macOS	Allow / Block	Restriction not supported	Allow / Block	Restriction not supported
Windows (MDM)	Allow / Block	Allow min/max range: Min / Max	Allow / Block	Restriction not supported

Review + save | Cancel

3. Know your devices

Microsoft Intune admin center

admin@M365x7391006...
SIMON DOES (M365X73910067.O...

Home > Devices | Enrollment device platform restrictions > All Users | Properties >

Edit restriction

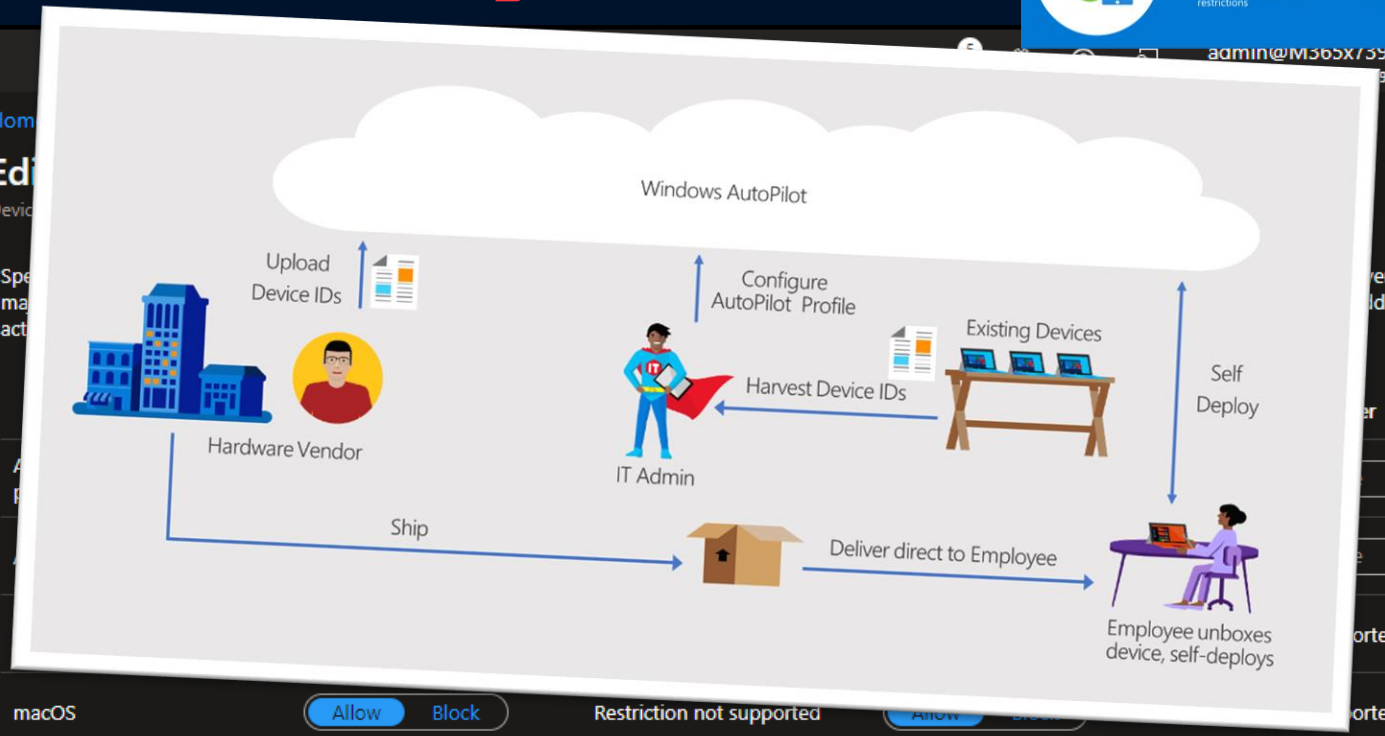
Device type restriction

Specify the platform configuration restrictions that must be met for a device to enroll. Use compliance policies to restrict devices after enrollment. Define versions as major.minor.build. Version restrictions only apply to devices enrolled with the Company Portal. Intune classifies devices as personally-owned by default. Additional action is required to classify devices as corporate-owned. Learn more.

Type	Platform	versions	Personally owned	Device manufacturer
Android Enterprise (work profile)	Allow / Block	Allow min/max range: Min / Max	Allow / Block	Manufacturer name
Android device administrator	Allow / Block	Allow min/max range: Min / Max	Allow / Block	Manufacturer name
iOS/iPadOS	Allow / Block	Allow min/max range: Min / Max	Allow / Block	Restriction not supported
macOS	Allow / Block	Restriction not supported	Allow / Block	Restriction not supported
Windows (MDM)	Allow / Block	Allow min/max range: Min / Max	Allow / Block	Restriction not supported

Review + save | Cancel

3. Know your devices



Microsoft Intune admin center

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

macOS | Allow | Block | Restriction not supported

Windows (MDM) | Allow | Block | Allow min/max range: Min Max | Allow | Block | Restriction not supported

Review + save | Cancel

3. Know your devices

Microsoft Intune admin center

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

Home >

Devices | Overview

Search

Overview
All devices
Monitor

Windows Autopatch

Devices
Release management

By platform

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

Preview upcoming changes to Devices and provide feedback. →

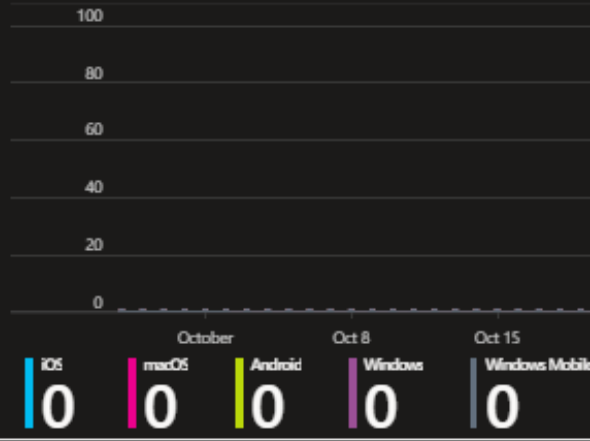
Enrollment status | Enrollment alerts | Cloud PC performance (preview) | Compliance status | Configuration

Intune enrolled devices

LAST UPDATED 10/27/23, 11:28 AM

Platform	Devices
Windows	23
iOS/iPadOS	8
Android	5
macOS	5
Linux	0
Windows Mobile	0
Total	41

Enrollment failures by OS



2

No Local Admin Rights

Unmasking 10 Frequent Intune Mistakes and How to Prevent Them

2. No Local Admin Rights

“If I don’t have admin rights, I can’t fix my computer”

2. No Local Admin Rights

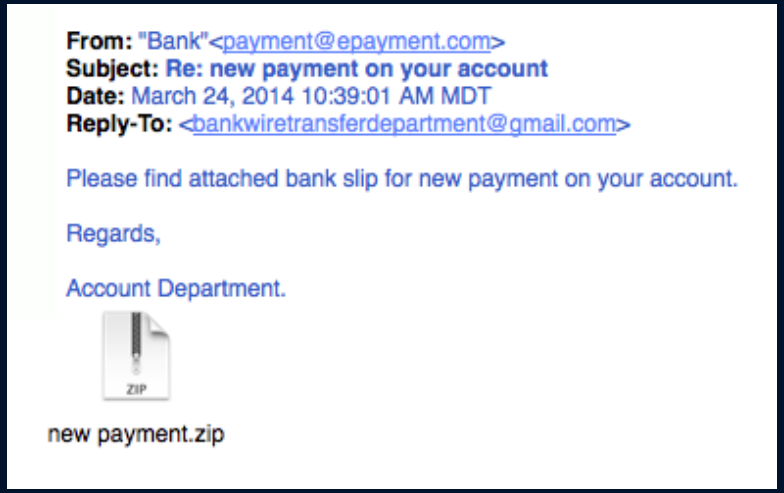
"If I don't have admin rights, I can't fix my computer"

If you don't have admin rights, you can't break your computer!

2. No Local Admin Rights

"If I don't have admin rights, I can't fix my computer"

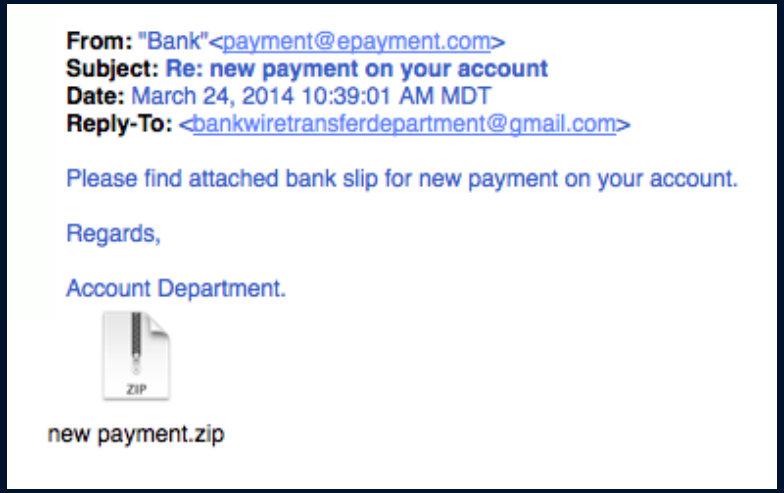
If you don't have admin rights, you can't break your computer!

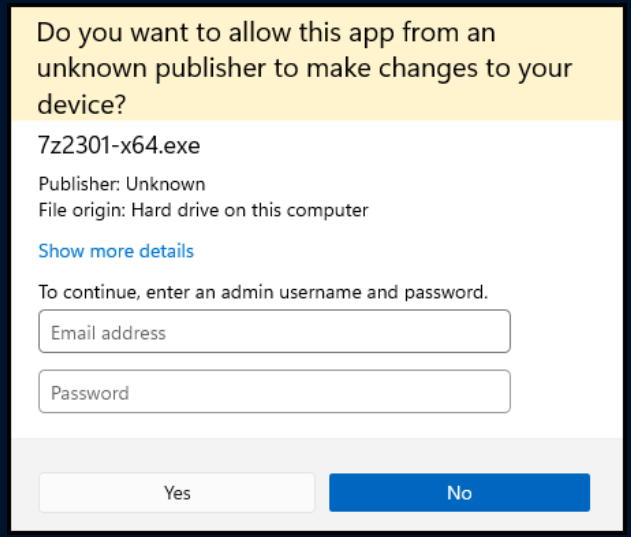


2. No Local Admin Rights

"If I don't have admin rights, I can't fix my computer"

If you don't have admin rights, you can't break your computer!





2. No Local Admin Rights

If you don’t have admin rights,
you can’t break your computer!

75% less Helpdesk tickets

60% less reinstallations

2. No Local Admin Rights

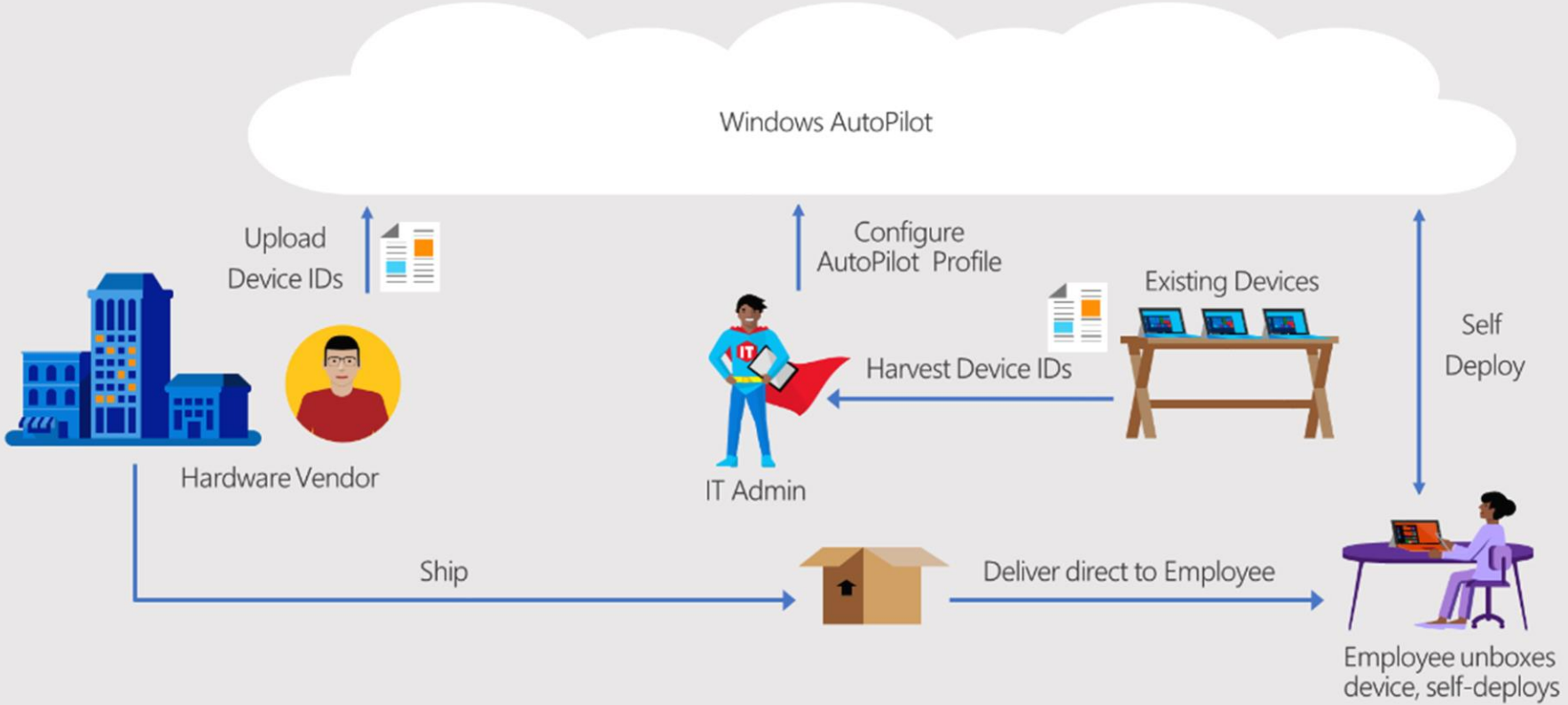
Principle of Least Privilege

- In Windows there is no Security if you logon as an admin
- The security subsystem was not built to withstand the use of admin rights
- With "No-Admin" approach
  - We get better performance
  - We get less tickets
  - We get less reinstallation
  - We get more productive users!
  - We get less malware
  - We get to be lazier as admins!

7 %

less H tallations

2. No Local Admin Rights



2. No Local Admin Rights

Deliver direct to Employee

Employee unboxes device, self-deploys

2. No Local Admin Rights

Configure AutoPilot Profile

Harvest Device IDs

IT Admin

2. No Local Admin Rights

Microsoft Intune admin center

admin@M365x7391006...
SIMON DOES (M365X73910067.O...

Home > Devices | Enroll devices >

Enroll devices | Windows enrollment

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

Search

- Windows enrollment
- Apple enrollment
- Android enrollment
- Enrollment device limit restrictions
- Enrollment device platform restrictions
- Corporate device identifiers
- Device enrollment managers

Co-management Settings
Configure co-management settings for Configuration Manager integration

Windows Autopilot Deployment Program

Deployment Profiles
Customize the Windows Autopilot provisioning experience.

Devices
Manage Windows Autopilot devices.

Intune Connector for Active Directory
Configure Microsoft Entra hybrid joined devices

2. No Local Admin Rights

Microsoft Intune admin center

admin@M365x7391006...
SIMON DOES (M365X73910067.O...

Home > Devices | Enroll devices > Enroll devices | Windows enrollment > Windows Autopilot deployment profiles > Autopilot Profile

Autopilot Profile | Properties

Windows PC

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

Search

- Overview

Manage

- Properties
- Assigned devices

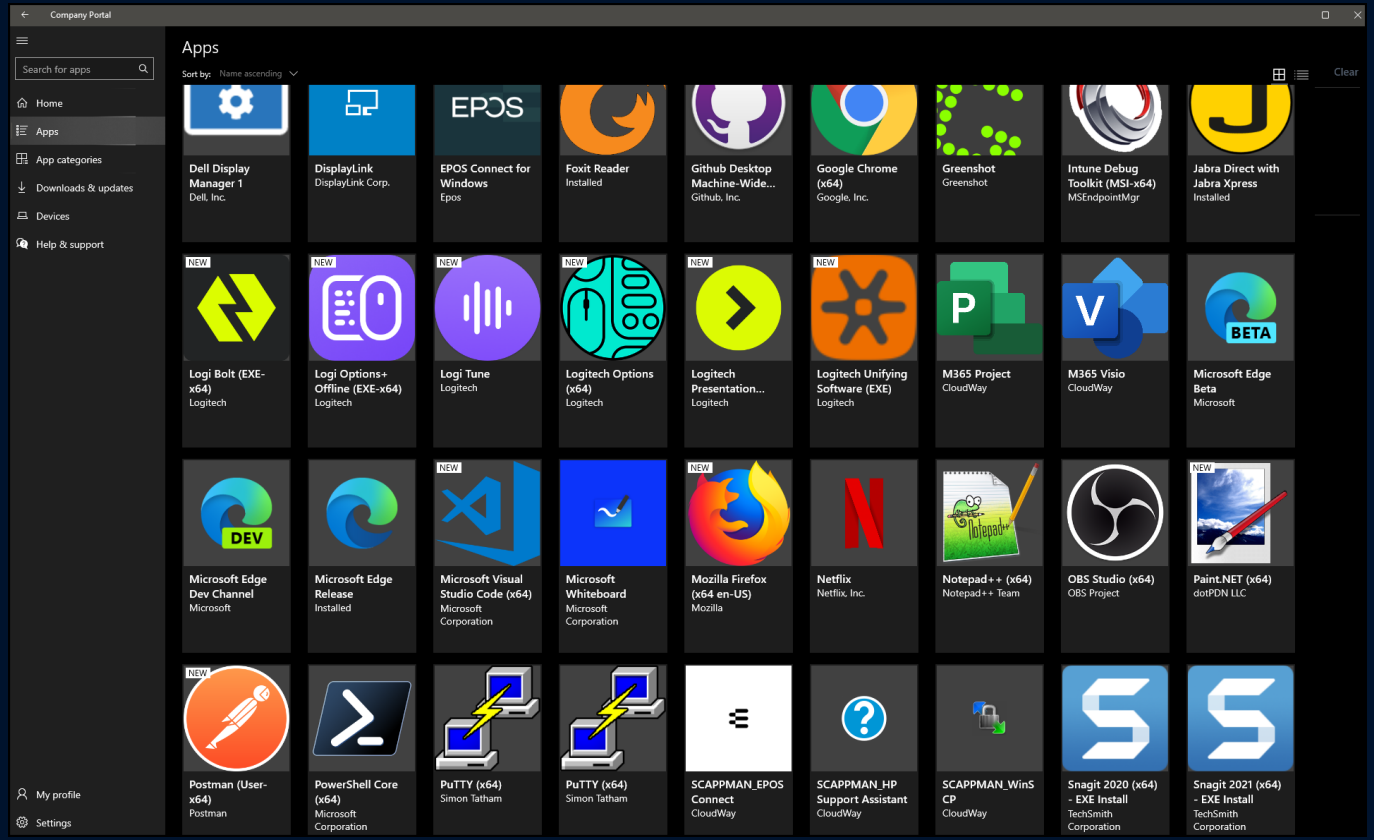
Basics Edit

Name	Autopilot Profile
Description	No Description
Convert all targeted devices to Autopilot	No
Device type	Windows PC

Out-of-box experience (OOBE) Edit

Deployment mode	User-Driven
Join to Microsoft Entra ID as	Microsoft Entra joined
Language (Region)	Operating system default
Automatically configure keyboard	No
Microsoft Software License Terms	Hide
Privacy settings	Hide
Hide change account options	Show
User account type	Standard
Allow pre-provisioned deployment	No
Apply device name template	No

2. No Local Admin Rights



2. No Local Admin Rights

Microsoft Entra admin center

Search resources, services, and docs (G+/)

admin@M365x7391006...
SIMON DOES (M365X73910067.O...

Home

Favorites

Identity

Overview

Users

Groups

Devices

Overview

All devices

BitLocker keys

Applications

Learn & support

Home > Devices

Devices | Device settings

Simon Does - Microsoft Entra ID

Overview

All devices

Manage

Device settings

Enterprise State Roaming

BitLocker keys (Preview)

Local administrator password recovery

Activity

Audit logs

Bulk operation results (Preview)

Troubleshooting + Support

New support request

Diagnose and solve problems

Save | Discard | Got feedback?

50

Local administrator settings

Manage Additional local administrators on all Microsoft Entra joined devices

Enable Microsoft Entra Local Administrator Password Solution (LAPS)

Yes | No

Other settings

Restrict users from recovering the BitLocker key(s) for their owned devices

Yes | No

2. No Local Admin Rights

Microsoft Intune admin center

admin@M365X7391006...
SIMON DOES (M365X73910067.O...

Home > Devices | Windows > Windows | Scripts > WPS001 - Windows LAPS Account

WPS001 - Windows LAPS Account | Properties

Windows 10 and later

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

Search

- Overview

Manage

- Properties

Monitor

- Device status
- User status

Name	WPS001 - Windows LAPS Account
Description	2023.09.26 - CloudWay template installed, Simon

Script settings Edit

PowerShell script	Create-LocalAdminLAPS.ps1
Run this script using the logged on credentials	No
Enforce script signature check	No
Run script in 64 bit PowerShell Host	Yes

Scope tags Edit

Default

Assignments Edit

Included groups	AZ-Device-Intune-All Windows 10 Devices AZ-Device-Intune-All Windows 11 Devices
Excluded groups	No Excluded groups

2. No Local Admin Rights

Microsoft Intune admin center

admin@M365x7391006...
SIMON DOES (M365X73910067.O...

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

Home > Endpoint security

Endpoint security | Account protection

Search

- Firewall
- Endpoint Privilege Management
- Endpoint detection and response
- App Control for Business (Preview)
- Attack surface reduction
- Account protection
- Device compliance
- Conditional access

Monitor

- Assignment failures

Setup

- Microsoft Defender for Endpoint

Create Policy | Refresh | Export

Search by profile name

Policy name	Policy type	Assigned
WESP501 - ACP - Windows Hello for Business	Account protection (Preview)	Yes
WESP502 - ACP - Windows LAPS	Local admin password solution (Windows LAPS)	Yes
WESP503 - ACP - Local Administrators	Local user group membership	Yes

2. No Local Admin Rights

Microsoft Intune admin center

admin@M365x7391006...
SIMON DOES (M365X73910067.O...

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

Home > Endpoint security | Account protection > WESP502 - ACP - Windows LAPS >

Edit profile - WESP502 - ACP - Windows LAPS

Settings catalog

LAPS

Backup Directory	Backup the password to Azure AD only
Password Age Days	Configured
*	7
Administrator Account Name	Configured
	SSLocalAdmin
Password Complexity	Large letters + small letters + numbers + special characters
Password Length	Configured
*	21
Post Authentication Actions	Reset the password and logoff the managed account: upon expiry of ...
Post Authentication Reset Delay	Configured
*	2

Review + save | Cancel

2. No Local Admin Rights

Microsoft Intune admin center

admin@M365x7391006...
SIMON DOES (M365X73910067.O...

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

Home > Endpoint security | Account protection > WESP502 - ACP - Windows LAPS >

Edit profile - WESP502 - ACP - Windows LAPS

Settings catalog

LAPS

Backup Directory	Backup the password to Azure AD only
Password Age Days	Configured
*	7
Administrator Account Name	Configured
	SSLocalAdmin
Password Complexity	Large letters + small letters + numbers + special characters
Password Length	Configured
*	21
Post Authentication Actions	Reset the password and logoff the managed account: upon expiry of ...
Post Authentication Reset Delay	Configured
*	2

Review + save | Cancel

2. No Local Admin Rights

Microsoft Intune admin center

admin@M365x7391006...
SIMON DOES (M365X73910067.O...

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

Home > Endpoint security | Account protection > WESP502 - ACP - Windows LAPS >

Edit profile - WESP502 - ACP - Windows LAPS

Settings catalog

LAPS

Backup Directory	Backup the password to Azure AD only
Password Age Days	Configured
*	7
Administrator Account Name	Configured
	SSLocalAdmin
Password Complexity	Large letters + small letters + numbers + special characters
Password Length	Configured
*	21
Post Authentication Actions	Reset the password and logoff the managed account: upon expiry of ...
Post Authentication Reset Delay	Configured
*	2

Review + save | Cancel

2. No Local Admin Rights

Microsoft Intune admin center

admin@M365x7391006...
SIMON DOES (M365X73910067.O...

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

Home > Endpoint security | Account protection > WESP502 - ACP - Windows LAPS >

Edit profile - WESP502 - ACP - Windows LAPS

Settings catalog

LAPS

Backup Directory	Backup the password to Azure AD only
Password Age Days	Configured: 7
Administrator Account Name	Configured: SSLocalAdmin
Password Complexity	Large letters + small letters + numbers + special characters
Password Length	Configured: 21
Post Authentication Actions	Reset the password and logoff the managed account: upon expiry of ...
Post Authentication Reset Delay	Configured: 2

Review + save | Cancel

2. No Local Admin Rights

Microsoft Intune admin center

admin@M365x7391006...
SIMON DOES (M365X73910067.O...

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

Home > Endpoint security

Endpoint security | Account protection

Search

- Firewall
- Endpoint Privilege Management
- Endpoint detection and response
- App Control for Business (Preview)
- Attack surface reduction
- Account protection
- Device compliance
- Conditional access

Monitor

- Assignment failures

Setup

- Microsoft Defender for Endpoint

Create Policy | Refresh | Export

Search by profile name

Policy name	Policy type	Assigned
WESP501 - ACP - Windows Hello for Business	Account protection (Preview)	Yes
WESP502 - ACP - Windows LAPS	Local admin password solution (Windows LAPS)	Yes
WESP503 - ACP - Local Administrators	Local user group membership	Yes

2. No Local Admin Rights

Microsoft Intune admin center

admin@M365x7391006...
SIMON DOES (M365X73910067.O...

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

Home > Endpoint security | Account protection > WESP503 - A

Edit profile - WESP503 - ACP - Local

Settings catalog

1 Configuration settings 2 Review + save

Local Users And Groups

+ Add Delete

Local group	Group and user action
Administrators	Add (Replace)

Review + save Cancel

Add users

Add users to be managed as part of select local groups. Enter one or more user identifiers as they appear on the device. You can use the following formats:

- Username
- Domain\username
- SID (security identifier)

Invalid identifiers will not be applied to policy. Click to learn more about troubleshooting invalid entries.

Delete Sort Export

- SSLocalAdmin
- S-1-12-1-158575896-1174998709-2722327981-3318271026
- S-1-12-1-424057452-1234611653-408369830-3020408508
- Administrator

OK

2. No Local Admin Rights

Microsoft Intune admin center

admin@M365x7391006...
SIMON DOES (M365X73910067.O...

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

... > Windows | Configuration profiles > WDCP019 - OS - Disable Local Administrator >

Edit profile - WDCP019 - OS - Disable Local Administrator

Settings catalog

1 Configuration settings 2 Review + save

+ Add settings

Local Policies Security Options Remove category

48 of 50 settings in this category are not configured

Accounts Enable Administrator Account Status: Disable

Accounts Rename Administrator Account: BuiltInAdmin

Review + save Cancel

2. No Local Admin Rights

Microsoft Intune admin center

Home > Devices | Windows > Windows | Windows devices > CLOUDWAY-875

CLOUDWAY-875 | Local admin password

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

Search

- Overview

Manage

- Properties

Monitor

- Hardware
- Discovered apps
- Device compliance
- Device configuration
- App configuration
- Local admin password
- Recovery keys
- User experience
- Device diagnostics

Refresh | Got feedback?

Learn more about Local Administrator Password Sol

Local administrator password	Last passwo
Show local administrator password	10/23/2023,

Local administrator password

Account name

Security ID

S-1-5-21-2995564115-2958326359-3012837770-500

Local administrator password

******** Show

Last password rotation

10/23/2023, 12:09:13 PM

Next password rotation

10/30/2023, 11:09:13 AM

2. No Local Admin Rights

Microsoft Intune admin center

admin@M365x7391006...
SIMON DOES (M365X73910067.O...

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

Home > Endpoint security

Endpoint security | Endpoint Privilege Management

Search

Overview

- Overview
- All devices
- Security baselines
- Security tasks

Manage

- Antivirus
- Disk encryption
- Firewall
- Endpoint Privilege Management
- Endpoint detection and response
- App Control for Business (Preview)

Reports | Policies

Endpoint Privilege Management is now generally available. To use this add-on, your Global or Billing Administrator can start a trial or buy licenses.

Create Policy | Refresh | Export

Search by profile name

Policy name	Policy type	Assigned	Platform	Target
No results				

2. No Local Admin Rights

Microsoft Intune admin center

admin@M365x7391006...
SIMON DOES (M365X73910067.O...

Home > Endpoint security

Endpoint security | Endpoint Privilege Management

Capability	Standalone add-on	Intune Plan 2	Intune Suite
Advanced endpoint analytics			✓
Endpoint Privilege Management	✓		✓
Firmware-over-the-air update		✓	✓
Microsoft Tunnel for Mobile Application Management		✓	✓
Remote help	✓		✓
Specialized devices management		✓	✓

Endpoint detection and response

App Control for Business (Preview)

NIC Cloud Connect

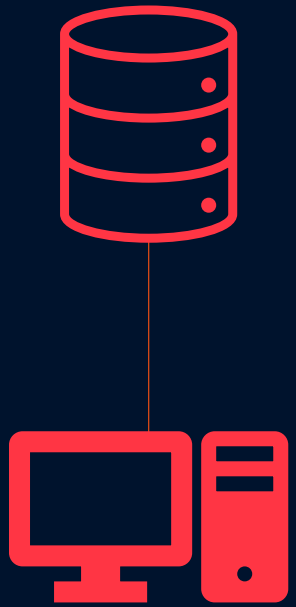
1

Hybrid

Unmasking 10 Frequent Intune Mistakes and How to Prevent Them

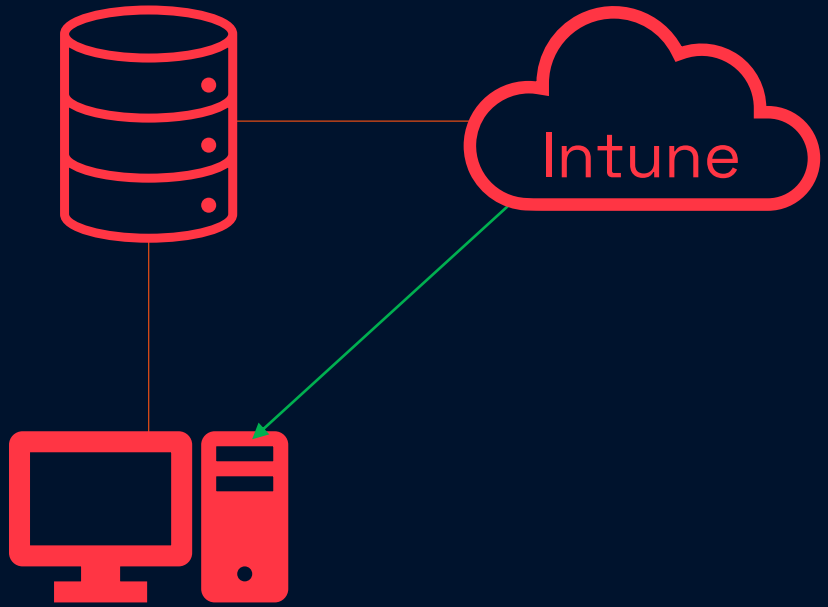
1. Hybrid


Enroll your devices
Configure
• Devices for enrollment
• Enrollment policies and restrictions
Use
• Enrollment profiles
• Windows Autopilot



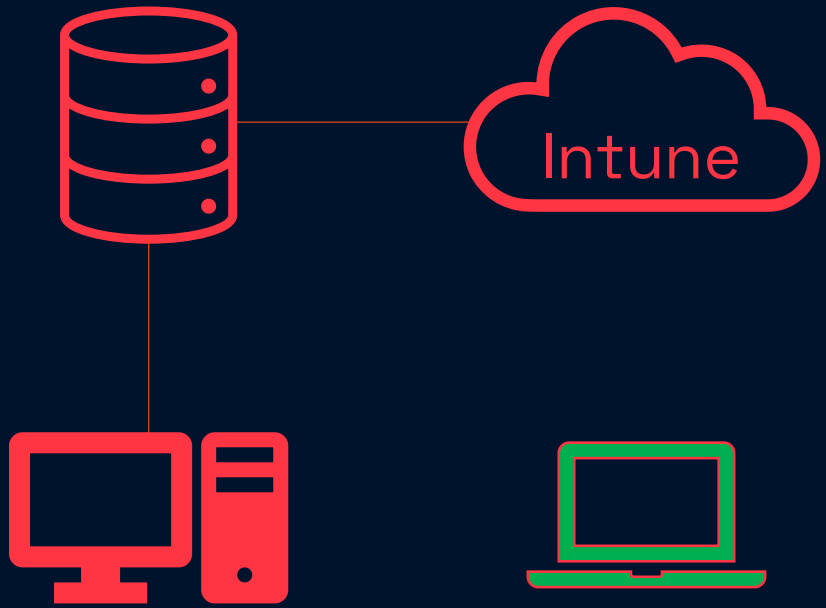
1. Hybrid


Enroll your devices
Configure
• Devices for enrollment
• Enrollment policies and restrictions
Use
• Enrollment profiles
• Windows Autopilot


Intune

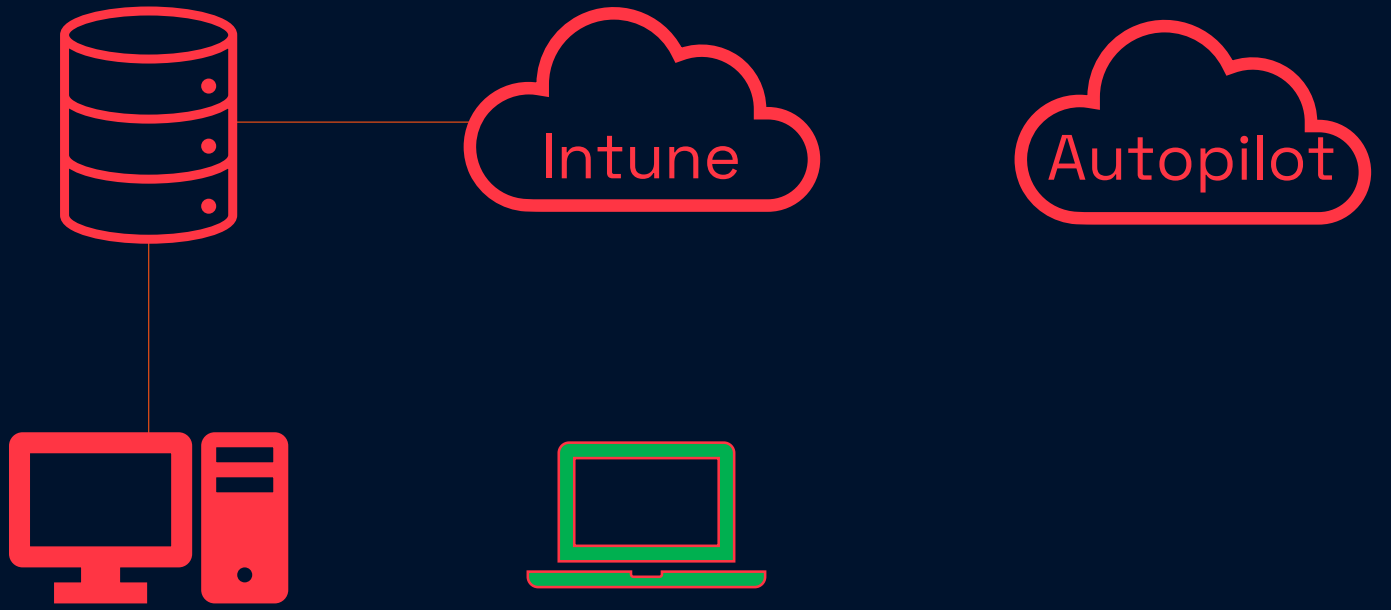
1. Hybrid


Enroll your devices
Configure
• Devices for enrollment
• Enrollment policies and restrictions
Use
• Enrollment profiles
• Windows Autopilot


Intune

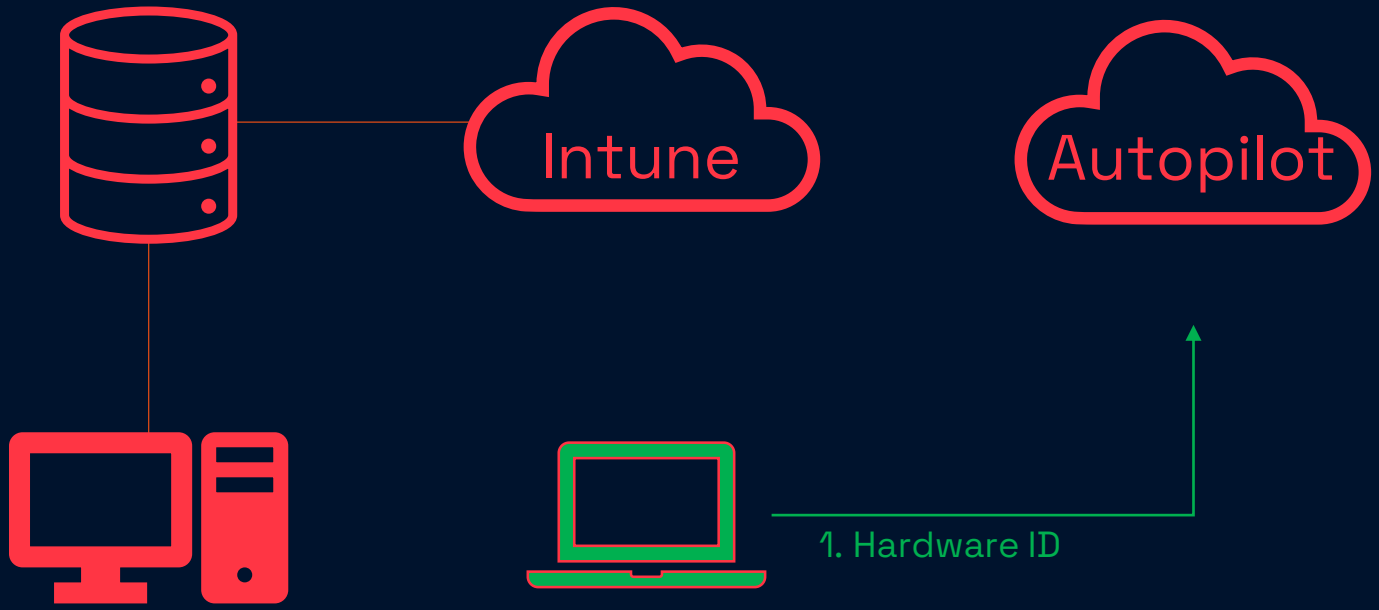
1. Hybrid


Enroll your devices
Configure
• Devices for enrollment
• Enrollment policies and restrictions
Use
• Enrollment profiles
• Windows Autopilot


Intune
Autopilot

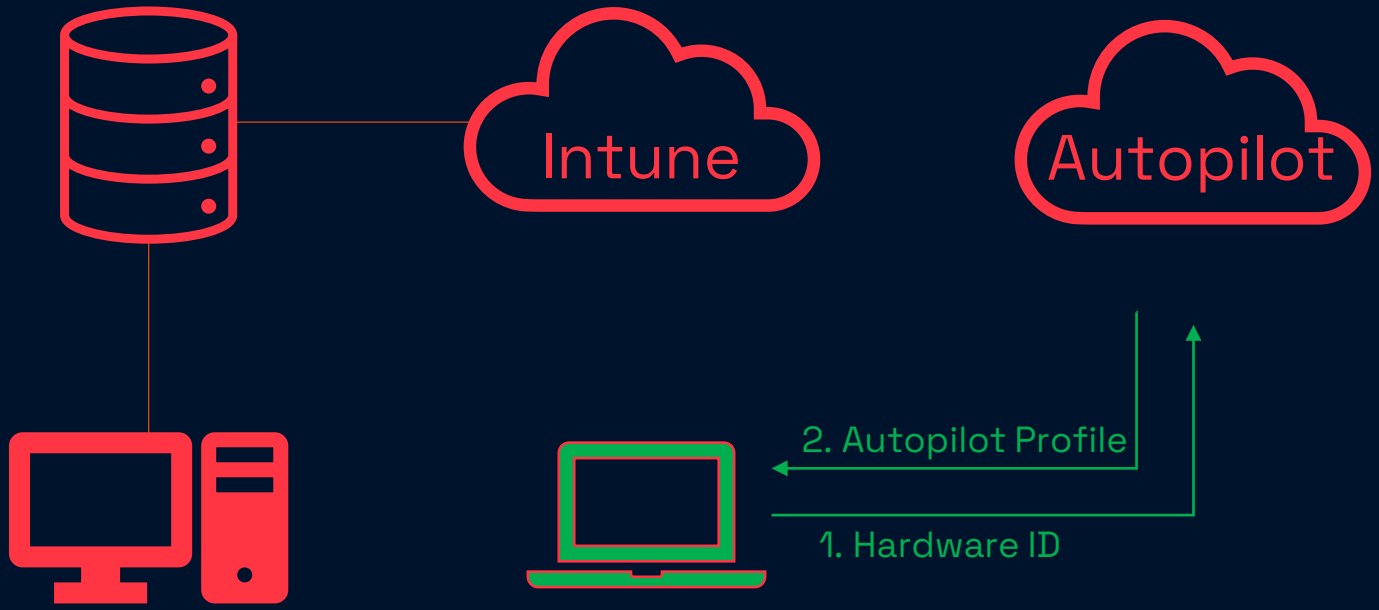
1. Hybrid


Enroll your devices
Configure
• Devices for enrollment
• Enrollment policies and restrictions
Use
• Enrollment profiles
• Windows Autopilot


Intune
Autopilot
1. Hardware ID

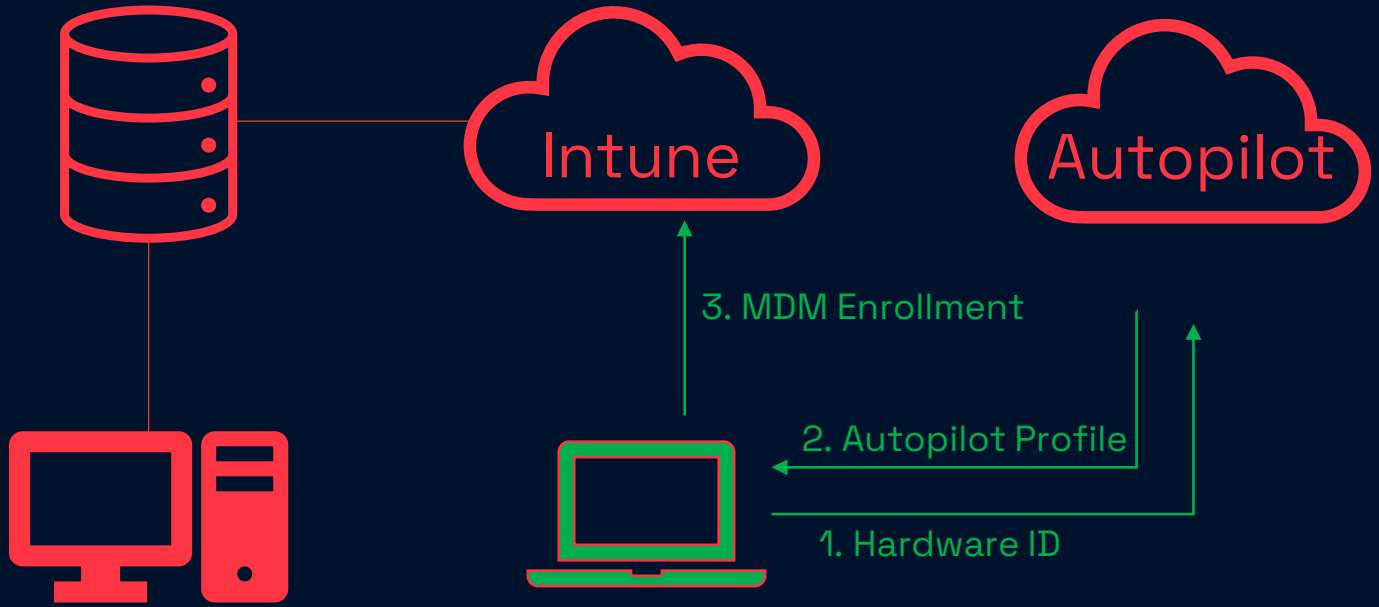
1. Hybrid


Enroll your devices
Configure
• Devices for enrollment
• Enrollment policies and restrictions
Use
• Enrollment profiles
• Windows Autopilot


Intune
Autopilot
2. Autopilot Profile
1. Hardware ID

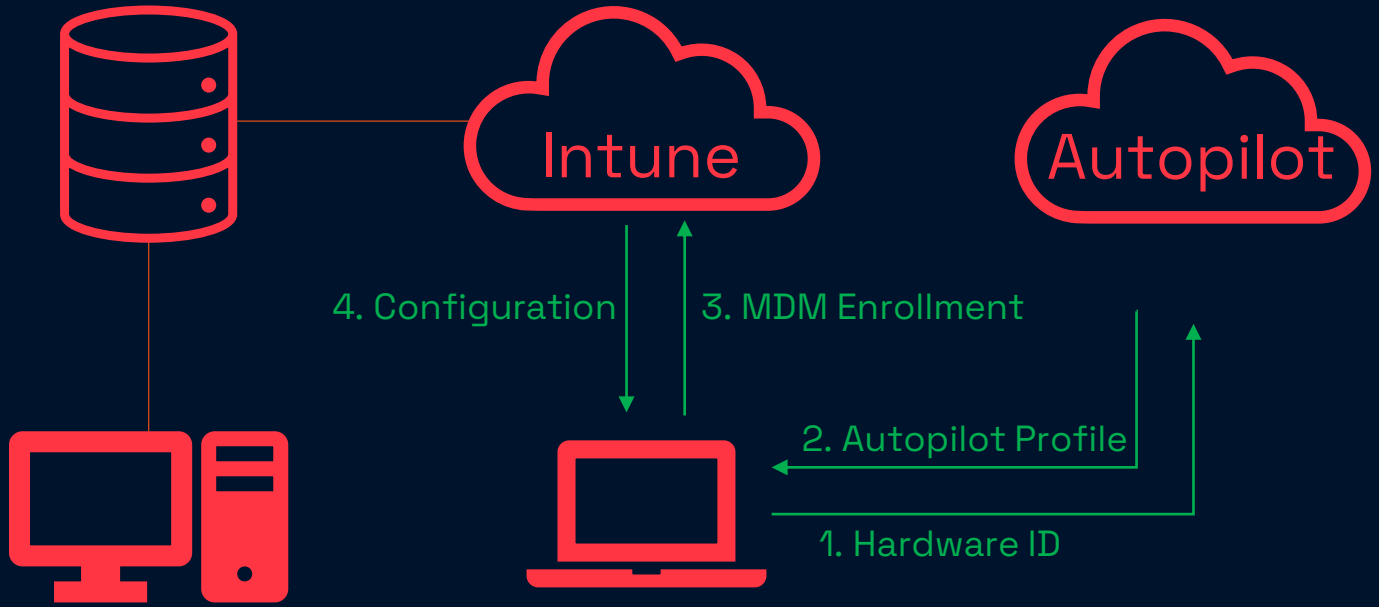
1. Hybrid


Enroll your devices
Configure
• Devices for enrollment
• Enrollment policies and restrictions
Use
• Enrollment profiles
• Windows Autopilot


Intune
Autopilot
3. MDM Enrollment
2. Autopilot Profile
1. Hardware ID

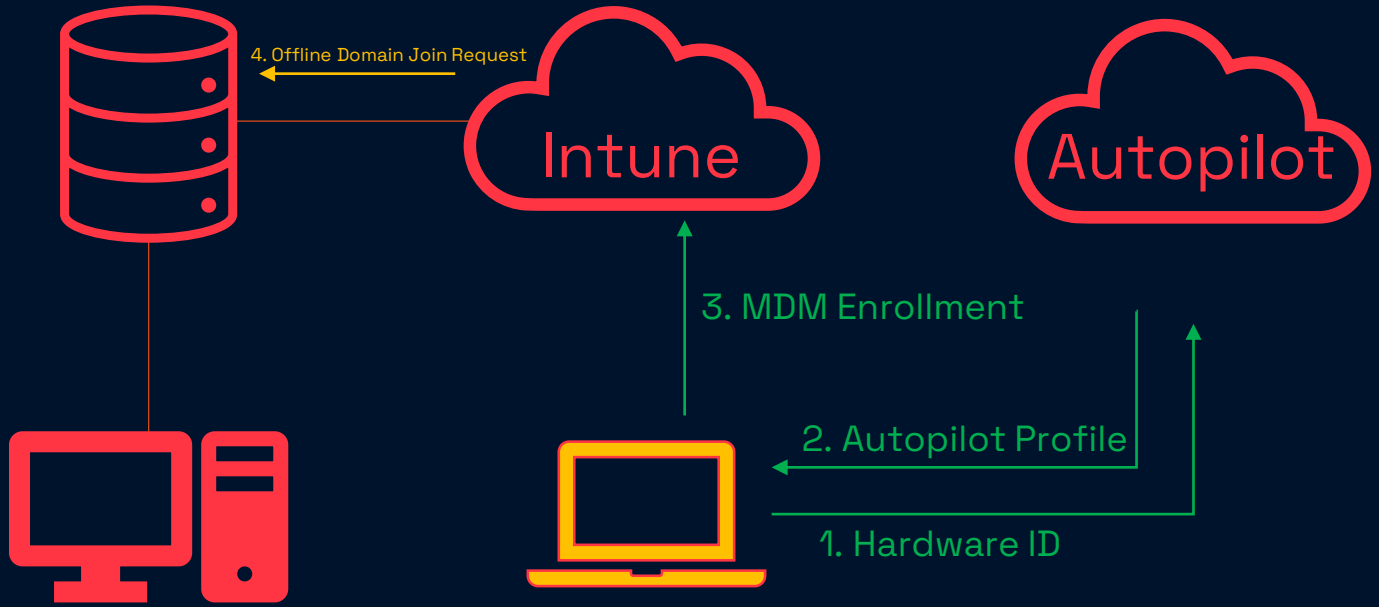
1. Hybrid


Enroll your devices
Configure
• Devices for enrollment
• Enrollment policies and restrictions
Use
• Enrollment profiles
• Windows Autopilot


Intune
Autopilot
4. Configuration
3. MDM Enrollment
2. Autopilot Profile
1. Hardware ID

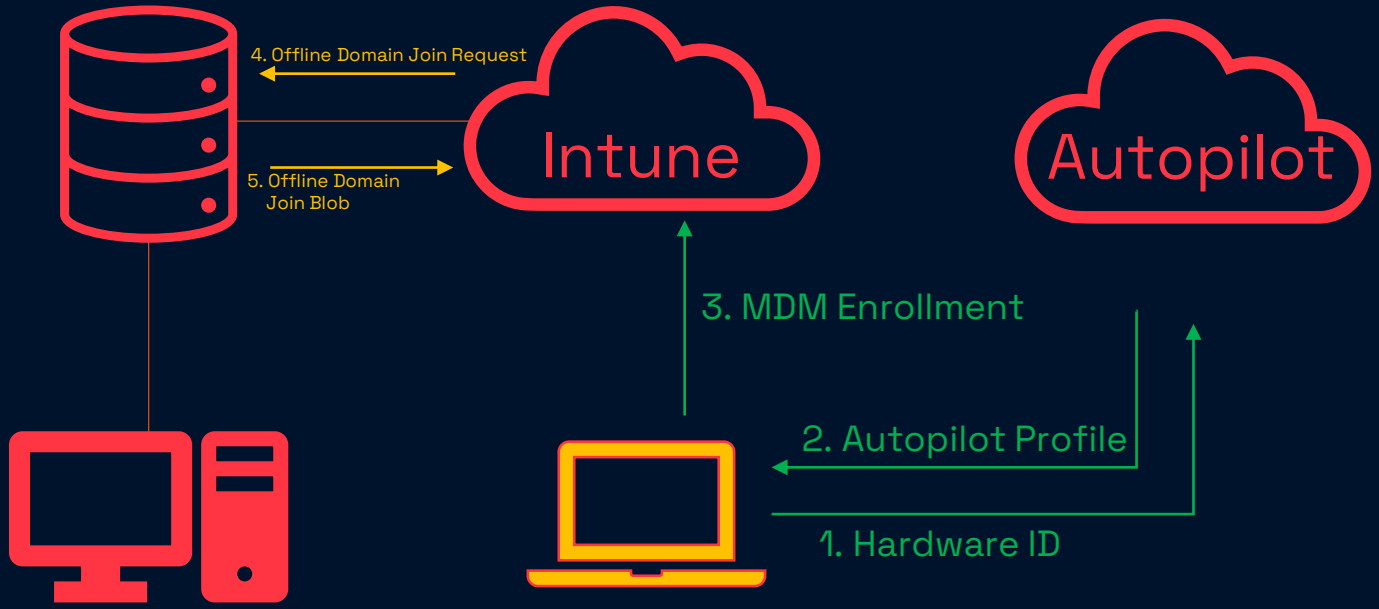
1. Hybrid


Enroll your devices
Configure
• Devices for enrollment
• Enrollment policies and restrictions
Use
• Enrollment profiles
• Windows Autopilot


4. Offline Domain Join Request
Intune
Autopilot
3. MDM Enrollment
2. Autopilot Profile
1. Hardware ID

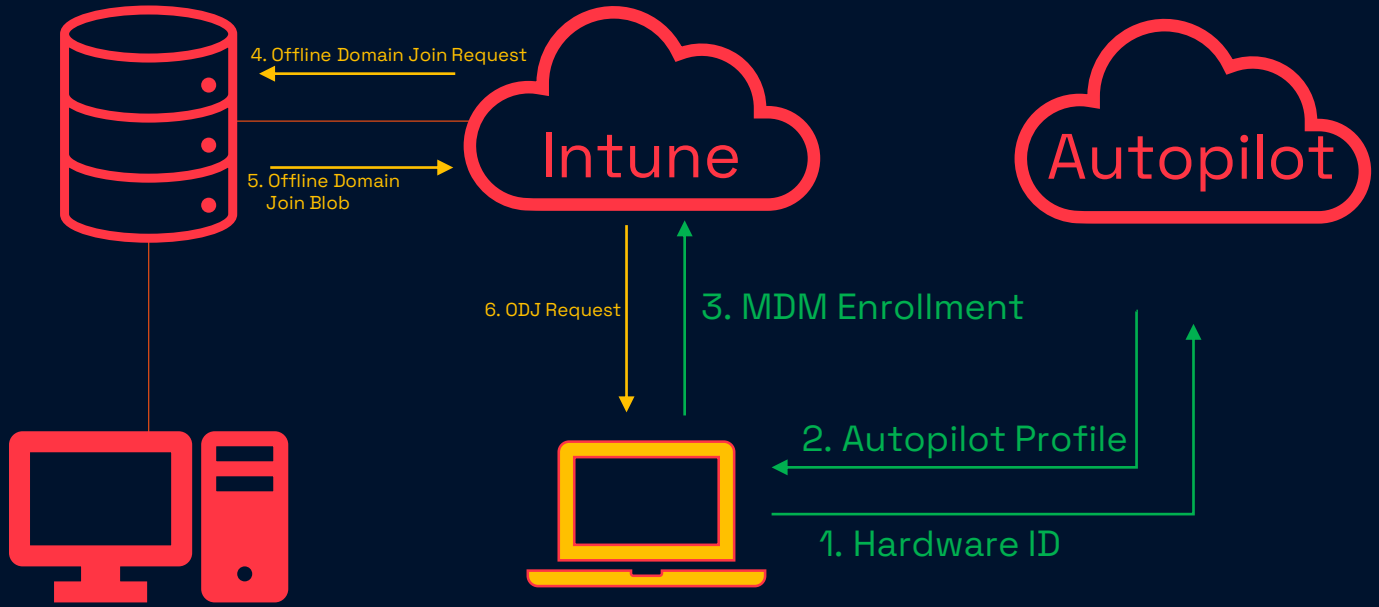
1. Hybrid


Enroll your devices
Configure
• Devices for enrollment
• Enrollment policies and restrictions
Use
• Enrollment profiles
• Windows Autopilot


4. Offline Domain Join Request
5. Offline Domain Join Blob
Intune
Autopilot
3. MDM Enrollment
2. Autopilot Profile
1. Hardware ID

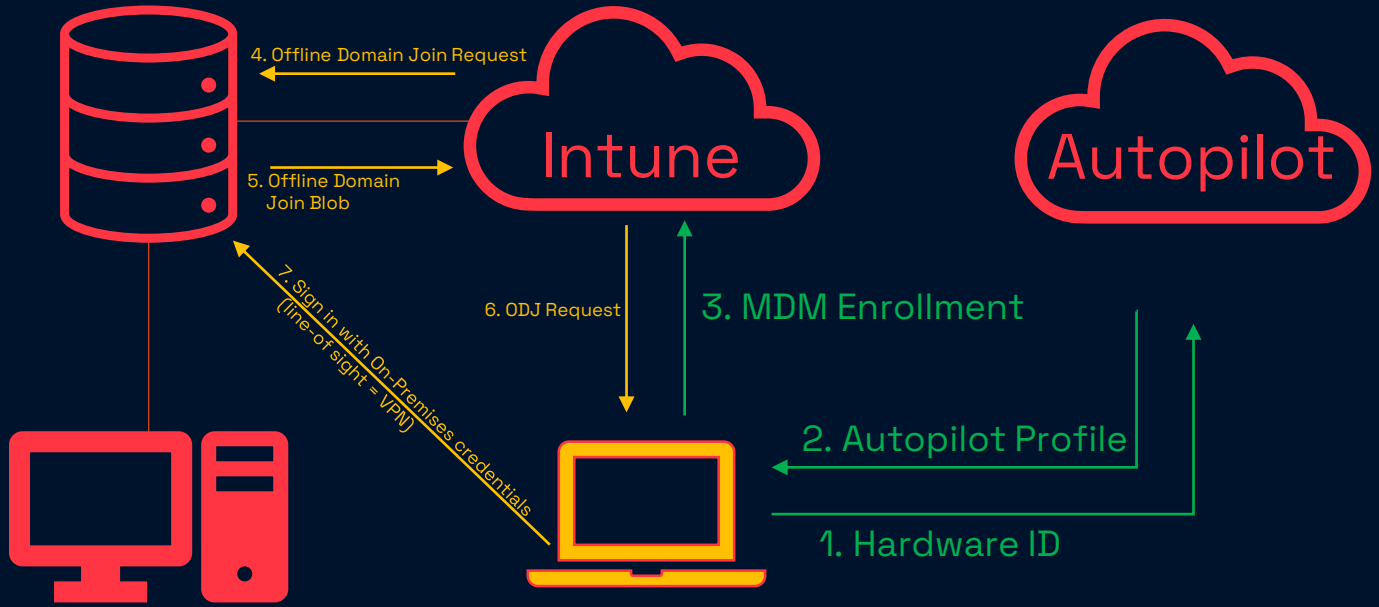
1. Hybrid


Enroll your devices
Configure
• Devices for enrollment
• Enrollment policies and restrictions
Use
• Enrollment profiles
• Windows Autopilot


4. Offline Domain Join Request
5. Offline Domain Join Blob
Intune
Autopilot
6. ODJ Request
3. MDM Enrollment
2. Autopilot Profile
1. Hardware ID

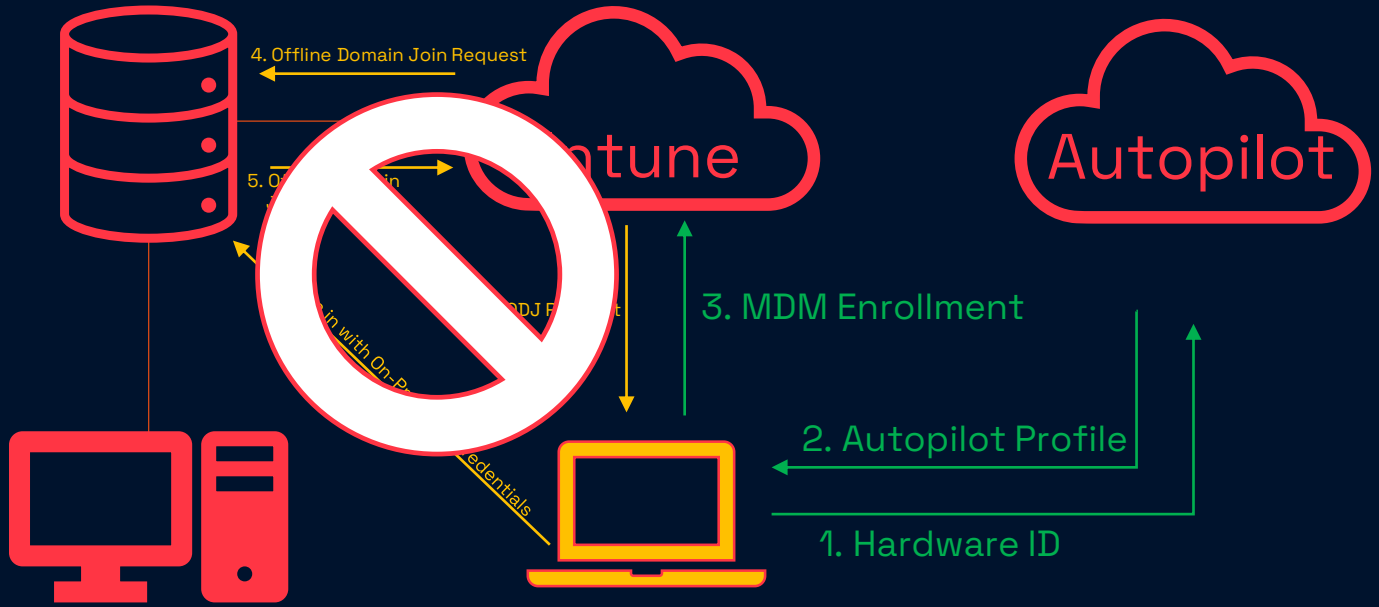
1. Hybrid


Enroll your devices
Configure
• Devices for enrollment
• Enrollment policies and restrictions
Use
• Enrollment profiles
• Windows Autopilot


4. Offline Domain Join Request
5. Offline Domain Join Blob
Intune
Autopilot
7. Sign in with On-Premises credentials (line-of sight = VPN)
6. ODJ Request
3. MDM Enrollment
2. Autopilot Profile
1. Hardware ID

1. Hybrid


Enroll your devices
Configure
• Devices for enrollment
• Enrollment policies and restrictions
Use
• Enrollment profiles
• Windows Autopilot


4. Offline Domain Join Request
ntune
Autopilot
3. MDM Enrollment
2. Autopilot Profile
1. Hardware ID

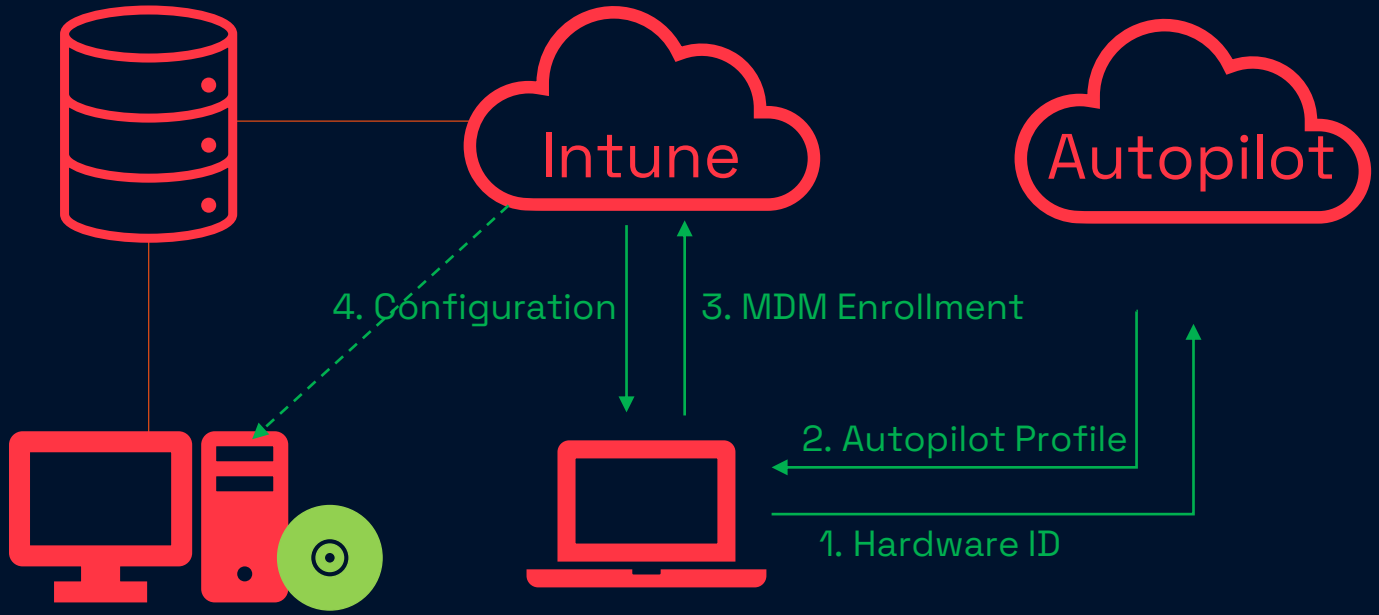
1. Hybrid

“Hybrid Autopilot was worth the effort”

- Nobody

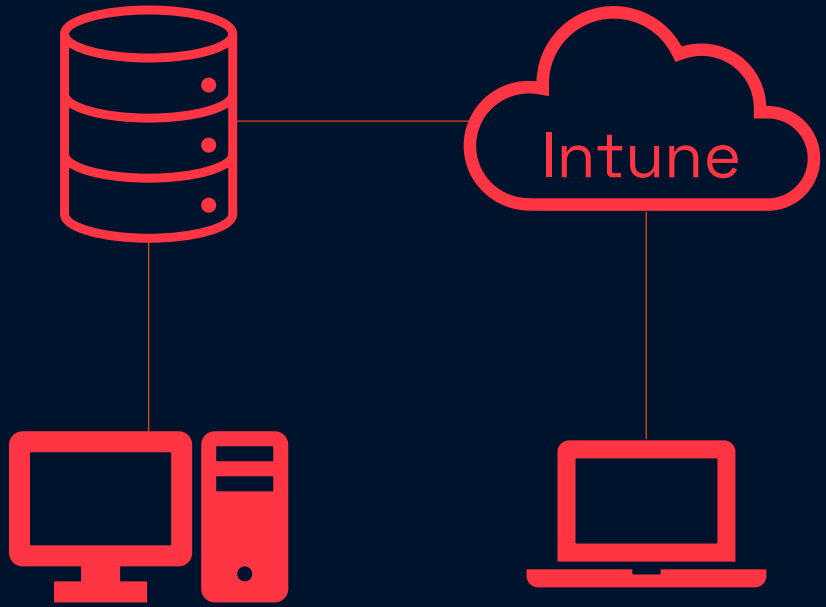
1. Hybrid


Enroll your devices
Configure
• Devices for enrollment
• Enrollment policies and restrictions
Use
• Enrollment profiles
• Windows Autopilot


Intune
Autopilot
4. Configuration
3. MDM Enrollment
2. Autopilot Profile
1. Hardware ID

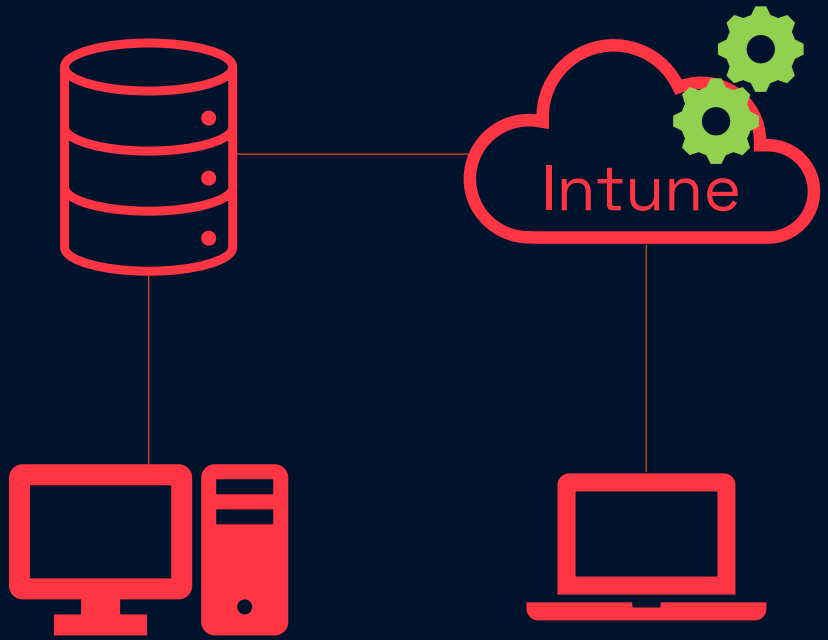
1. Hybrid


Enroll your devices
Configure
• Devices for enrollment
• Enrollment policies and restrictions
Use
• Enrollment profiles
• Windows Autopilot

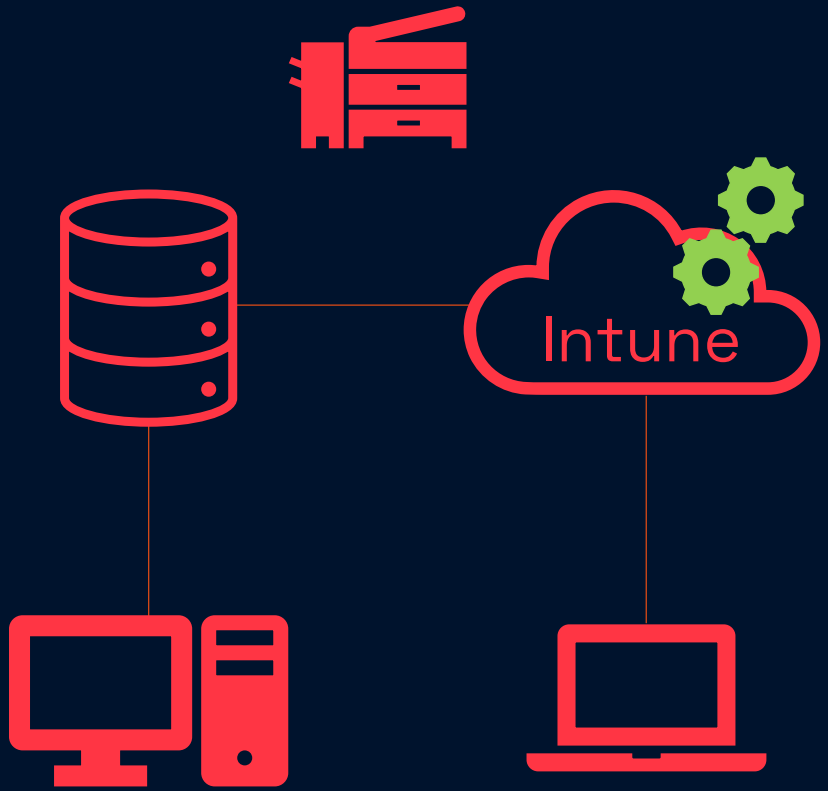

Intune

1. Hybrid

Group Policies?



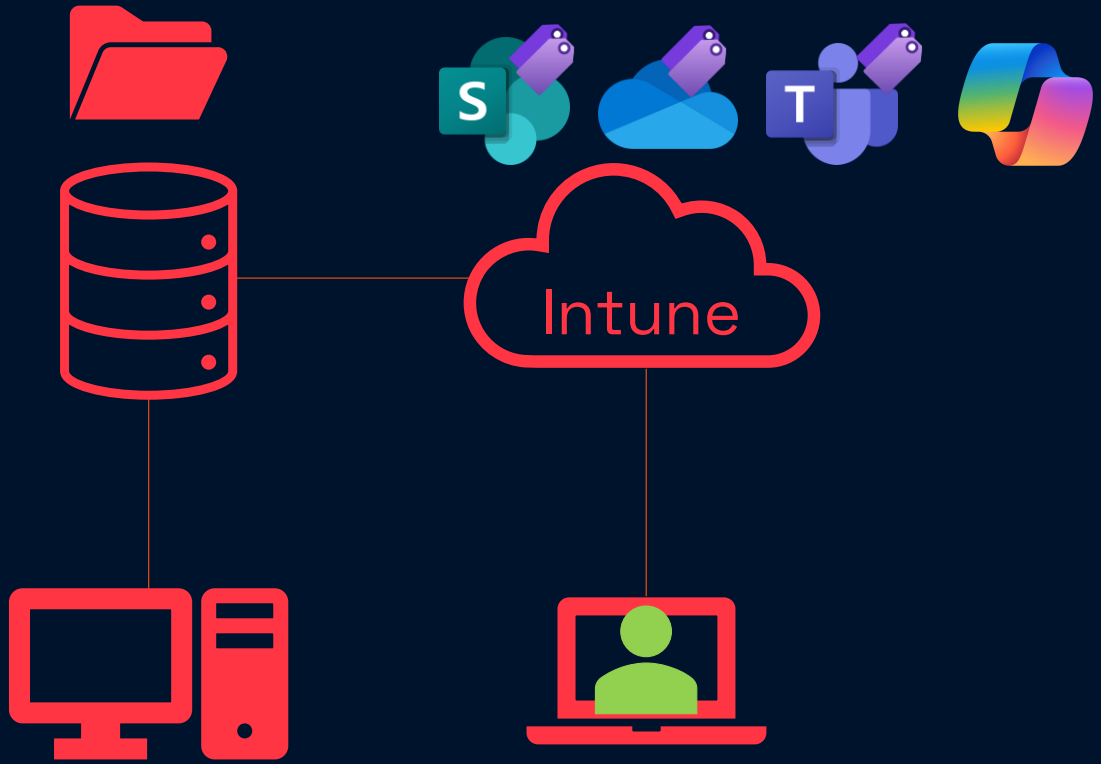
1. Hybrid



Group Policies

Printers?

1. Hybrid

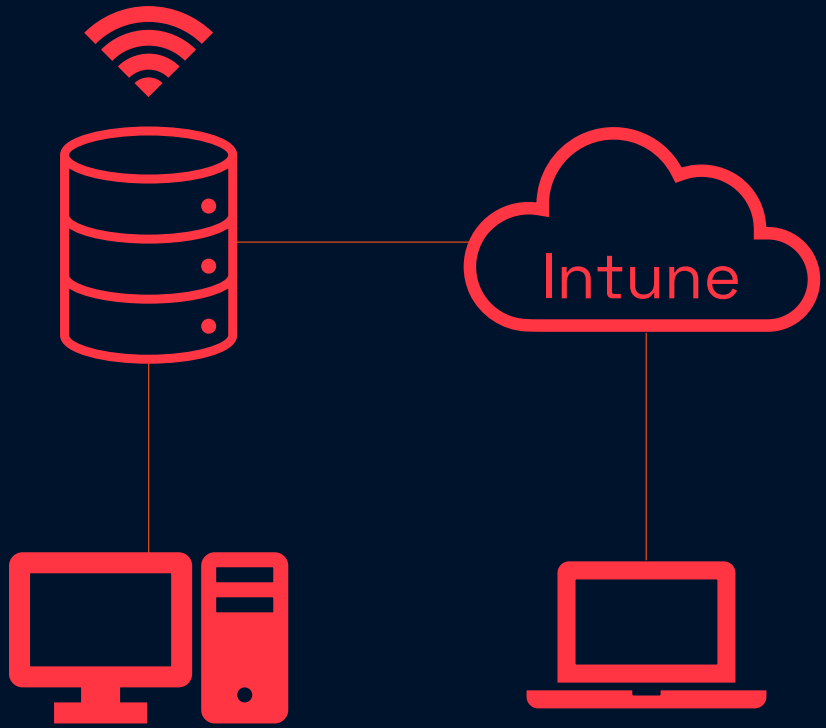


Group Policies

Printers

File Shares?

1. Hybrid



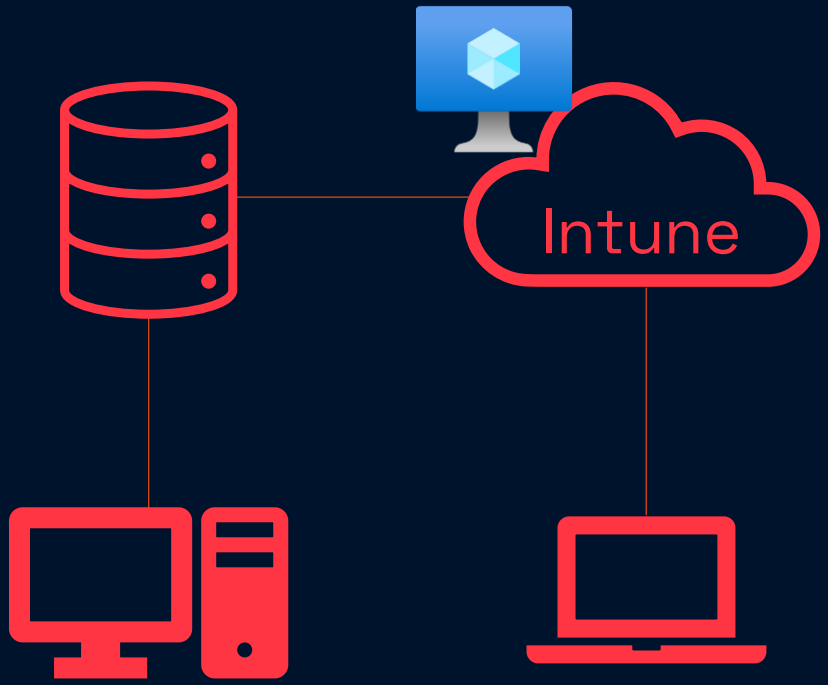
Group Policies

Printers

File Shares

PKI?

1. Hybrid



Group Policies

Printers

File Shares

PKI

3rd Party Solutions?

NIC Cloud Connect

Set up Intune

Add, configure, and protect apps

Use compliance and Conditional Access

Configure device features and settings

Enroll your devices

NIC Cloud Connect

Get ready for Microsoft 365 Copilot

Prerequisites for Microsoft 365 Copilot

Before you can access Copilot, you must meet the following requirements:

- **Microsoft 365 Apps for enterprise**. Microsoft 365 Copilot integration requires the core Word, Excel, PowerPoint, and Outlook. Organizations should deploy the latest cloud-co to all employee devices. They should keep apps updated to enable Copilot's full capab example, Copilot may suggest content edits directly within Word documents. Having C ensures tight integration. To get started with the implementation process, see Deployn Apps.
- **Microsoft Entra-based account**. Every employee using Copilot must have a Microsoft E This design ensures that all users sign in using Microsoft Entra credentials. Legacy local authenticate to the cloud limit Copilot functionality. To learn more, see Microsoft Entra
- **OneDrive accounts**. Copilot's integration with enterprise OneDrive accounts enables it You should consider provisioning 1-TB OneDrive to every user. For more information, s account for OneDrive.
- **New Outlook for Windows**. To get Copilot's interactive suggestions within Outlook em version of Outlook desktop. The new version enables Copilot integration as it evolves. Getting started with the new Outlook for Windows.
- **Microsoft Teams**. Use the Teams desktop or web app to enable Copilot within Teams c Mobile-only users have limited functionality. You can download the desktop client here app. Copilot supports both the current and the new version of Teams. For more infor in Teams.
- **Windows 11**. Windows 11 provides the best experience for Microsoft 365 Copilot. Orga organizations should ensure that all users have cloud-based Microsoft 365 licenses rat licenses. Cloud-connected licenses provide access to the company's latest features.

NIC Cloud Connect

Set up Intune

Add, configure, and protect apps

Use compliance and Conditional Access

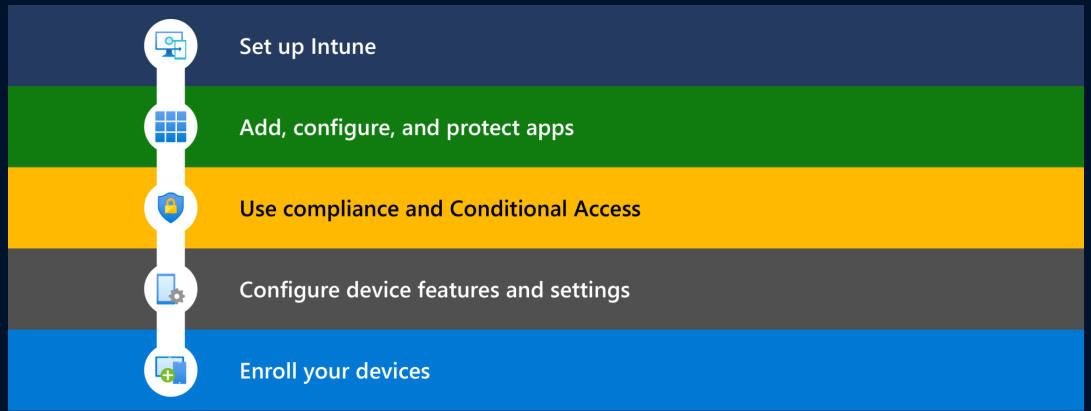
Configure device features and settings

Enroll your devices

Get ready for Microsoft 365 Copilot

Prerequisites for Microsoft 365 Copilot

- Microsoft 365 Apps for Enterprise (current channel)*
- Microsoft Entra-based account
- OneDrive
- Teams (either version)
- New Outlook for Windows
- Loop
- Windows 11 (preferred)
- Microsoft 365 E3 or E5 or Business Premium licences


Set up Intune
Add, configure, and protect apps
Use compliance and Conditional Access
Configure device features and settings
Enroll your devices

Thanks for attending

Secure productivity happens in the cloud

We will help you on your way

me

website

Simon.Skotheimsvik@TeamCloudWay.com

twitter

email