

Microsoft Intune/365/Entra ID Home Lab

Table of Contents

Page 3-7 Preliminary Lab Environment Setup

Page 8-18 Join Devices to Entra ID and Intune

Page 19-25 Implementing Identity and Compliance

Page 26-34 Deploying/Upgrading Windows Clients Using Autopilot

Page 35-39 Implementing Device Configuration

Page 40-46 Implementing Intune Suite Add-on Capabilities

Page 47-48 Performing Remote Actions on Devices via Intune

Page 49-53 Deploying and Updating Apps

Page 54-58 App Protection and App Configuration Policies

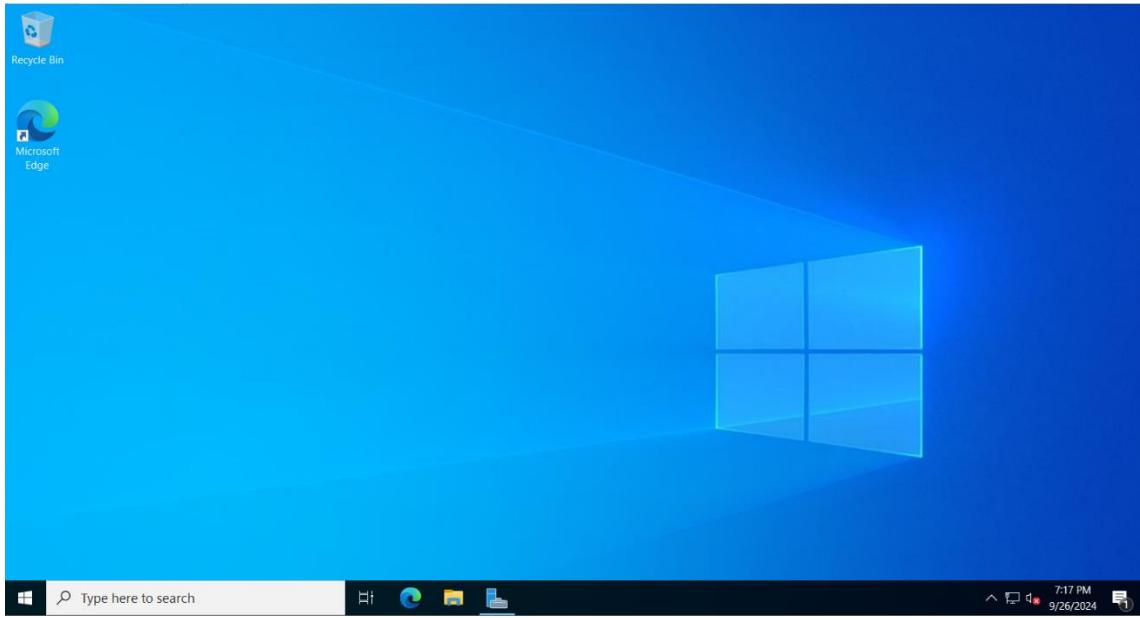
Page 59-62 Configuring Endpoint Security

Page 63-68 Managing Device Updates by Using Intune

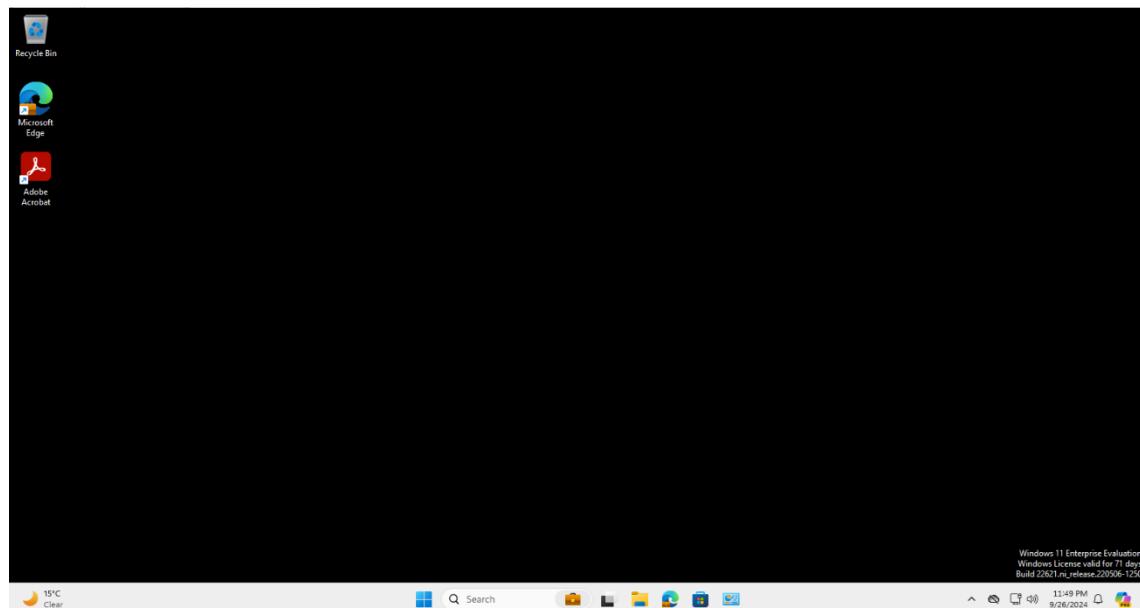
Page 69 Sources

Preliminary Lab Environment Setup

The first objective of this lab was to setup the virtual machines necessary for the client machine and the server (Windows 11 Enterprise and Windows Server 2022 Data Evaluation respectively). The first step was to download the images and install them as virtual machines using VMware Workstation.

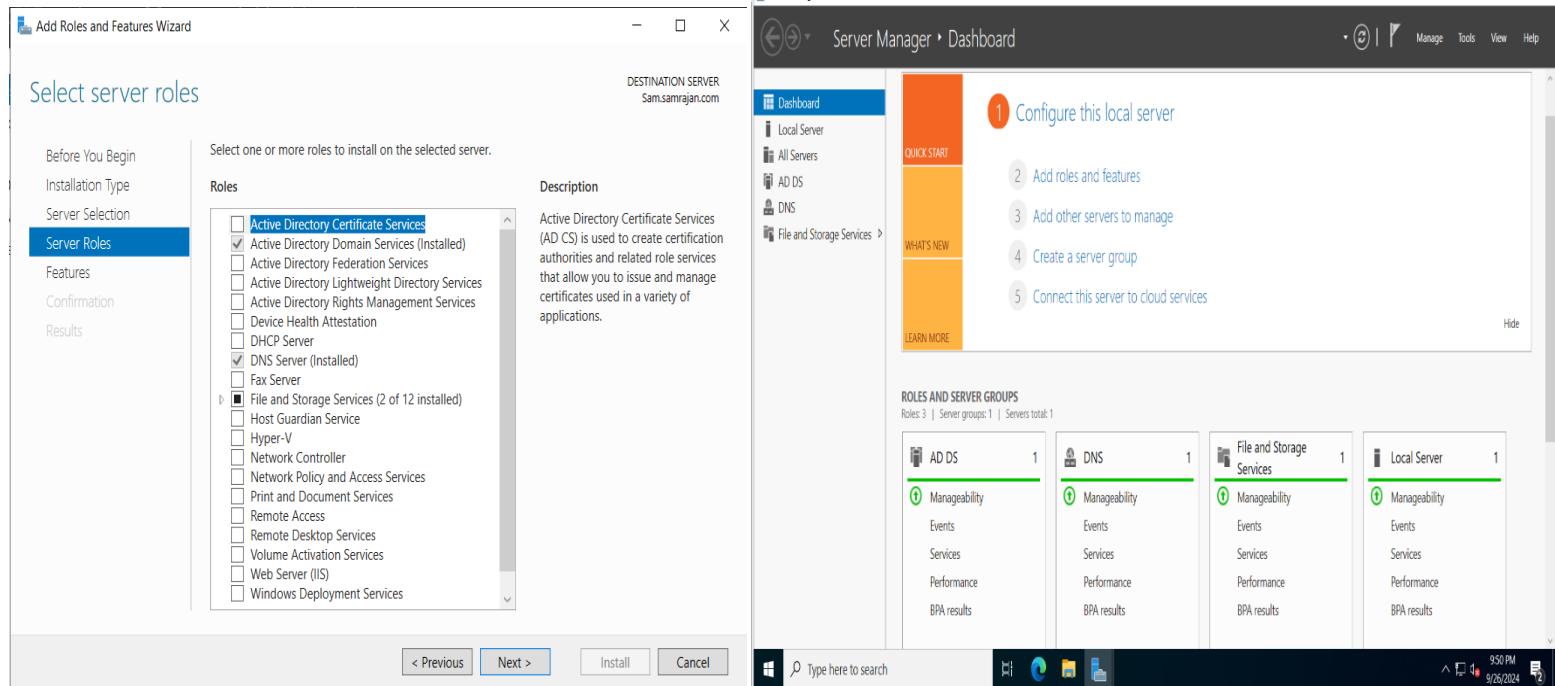


Windows Server 2022 virtual machine

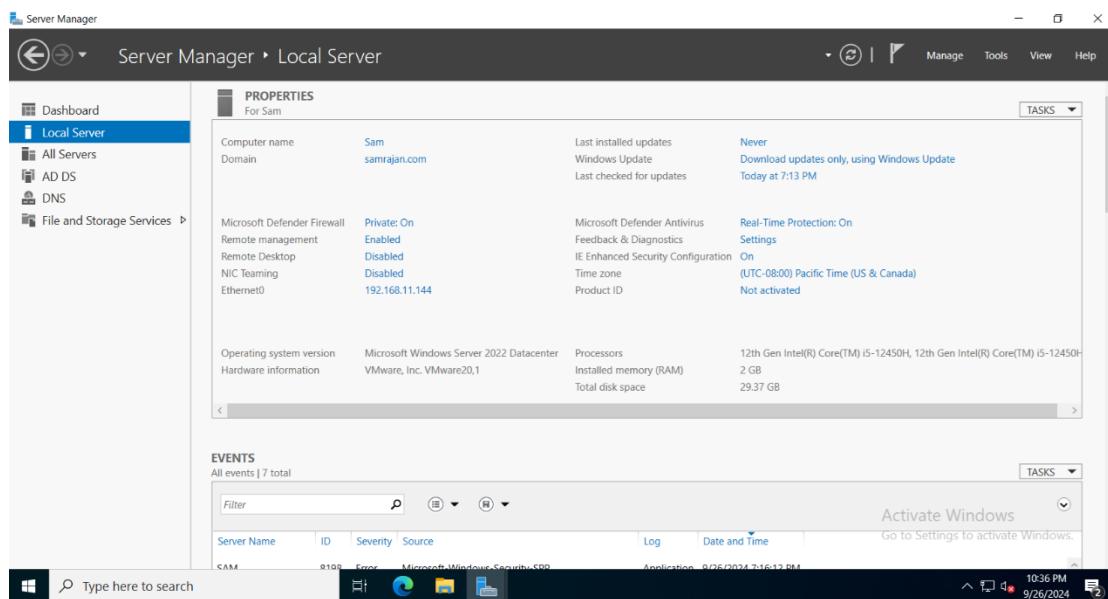


Windows 11 virtual machine

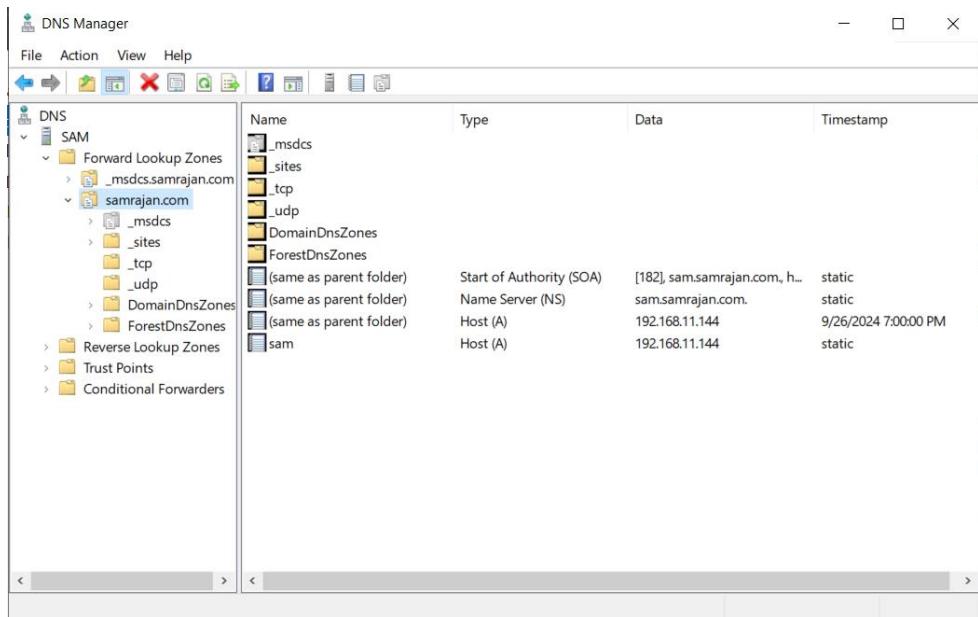
After setting up both virtual machines successfully, the server would need to be configured as a domain controller. To do this, Active Directory Domain Services and DNS capabilities needed to be activated on the server.



As can be seen in the left image, the Active Directory Domain Services and DNS Server roles have been selected and successfully installed. In the right image, the AD DS (Active Directory Domain Services) and DNS server groups appear in the Server Manager dashboard.



After running the Active Directory Domain Services configuration wizard, the domain name was configured to be "samrajan.com".



The DNS database (samrajan.com) has been successfully created and populated.

Following the domain controller setup, the next step is to join the Windows 11 device to the domain.

```
C:\Users\Administrator>ipconfig /all

Windows IP Configuration

Host Name . . . . . : Sam
Primary Dns Suffix . . . . . : samrajan.com
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : samrajan.com

Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) 82574L Gigabit Network Connection
Physical Address. . . . . : 00-0C-29-A1-1D-15
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . . : Yes
IPv4 Address. . . . . : 192.168.11.144(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.11.2
DNS Servers . . . . . : 127.0.0.1
                                         192.168.11.2
NetBIOS over Tcpip. . . . . : Enabled

C:\Users\Administrator>
```

The IP address configured on the server is 192.168.11.144 (manually configured) and in addition it's loopback address (127.0.0.1) is configured to be its DNS server.

The screenshot shows two windows side-by-side. On the left is the 'Edit DNS settings' dialog, which includes sections for IPv4 (Preferred DNS set to 192.168.11.144), Alternate DNS, and IPv6 (disabled). On the right is a Command Prompt window running 'ipconfig /all', showing network configuration details for the Ethernet adapter (IP: 192.168.11.128, Subnet Mask: 255.255.255.0, Default Gateway: 192.168.11.254, Primary WINS Server: 192.168.11.144) and the Bluetooth Network Connection.

```
C:\Users\SamRajan>ipconfig /all

Windows IP Configuration

Host Name . . . . . : SR-CL1
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : localdomain

Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . . . . . : localdomain
Description . . . . . : Intel(R) 82574L Gigabit Network Connection
Physical Address . . . . . : 00-0C-29-AC-8E-67
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
IPv4 Address . . . . . : 192.168.11.128(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Saturday, September 28, 2024 8:37:22 PM
Lease Expires . . . . . : Saturday, September 28, 2024 9:37:22 PM
Default Gateway . . . . . : 192.168.11.254
DHCP Server . . . . . : 192.168.11.254
DNS Servers . . . . . : 192.168.11.144
Primary WINS Server . . . . . : 192.168.11.144
NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter Bluetooth Network Connection:
```

The client must be configured to use the server as the DNS server. As can be seen above, the client's preferred DNS has been manually configured to be 192.168.11.144 which is the server's IP address. In addition, the client's host name has been manually renamed to "SR-CL1".

The screenshot shows two overlapping windows. The foreground window is 'Computer Name/Domain Changes', where the computer name is set to 'SR-CL1' and it is joined to the domain 'samrajan.com'. The background window is 'Windows Security' for 'Computer Name/Domain Changes', prompting for a user account ('samrajan\administrator') and password to complete the domain join process.

To register the device to the domain, the device needs to be declared a member of the domain by going to Settings > System > About > Domain or workgroup > Change. A username and password of an account that is permitted to join the domain must then be entered in.

Your products

These are products owned by your organization that were bought from Microsoft or 3rd-party providers. Select a product to manage product and billing settings or assign licenses.

Product name ↑	Assigned licenses	Purchased quantity	Subscription status	Purchase date
Microsoft 365 E3 (no Teams)	3	25	Active: Renews on 10/10/2024 with 1 paid license	Commercial
Microsoft Intune Advanced Analytics Trial	1	250	Active: Expires on 12/13/2024	Commercial
Microsoft Intune Suite for FLW	2	25	Active: Renews on 10/14/2024 with 1 paid license	Commercial

The final step is to register for a free Microsoft 365/Azure account. The default domain name assigned was `samrajan659.onmicrosoft.com` and the Microsoft 365 license chosen was Microsoft 365 E3 (no Teams) as this was the latest license available which offered a free trial.

Microsoft 365 E3 (no Teams)

You own at least 1 subscription for this product. [Manage subscription details](#)

Licenses

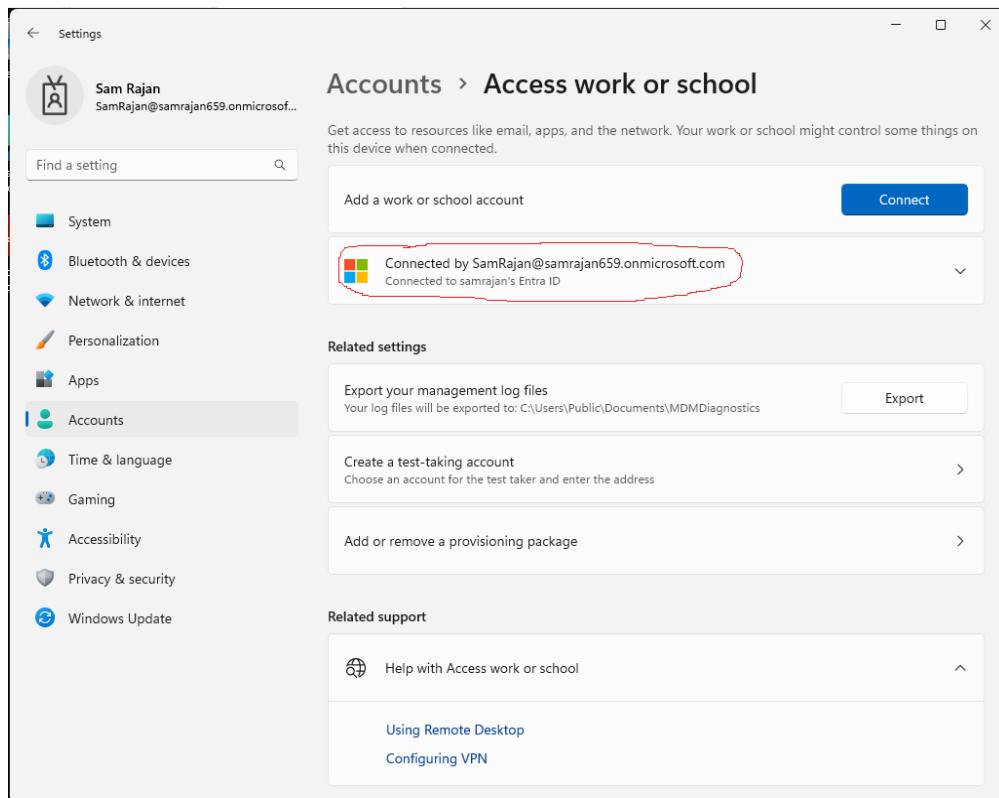
Licenses assigned 3/25

Name	Email
Jimmy McGill	jimmymcgill@samrajan659.onmicrosoft.com
Kim Wexler	kimwexler@samrajan659.onmicrosoft.com
Sam Rajan	SamRajan@samrajan659.onmicrosoft.com

The Microsoft 365 E3 (no Teams) license must be assigned to the global administrator (SamRajan@samrajan659.onmicrosoft.com) in order to access all features of Microsoft 365 such as Intune, Entra ID, etc. Other users can be assigned licences as well (e.g Kim Wexler and Jimmy McGill).

Join Devices to Entra ID and Intune

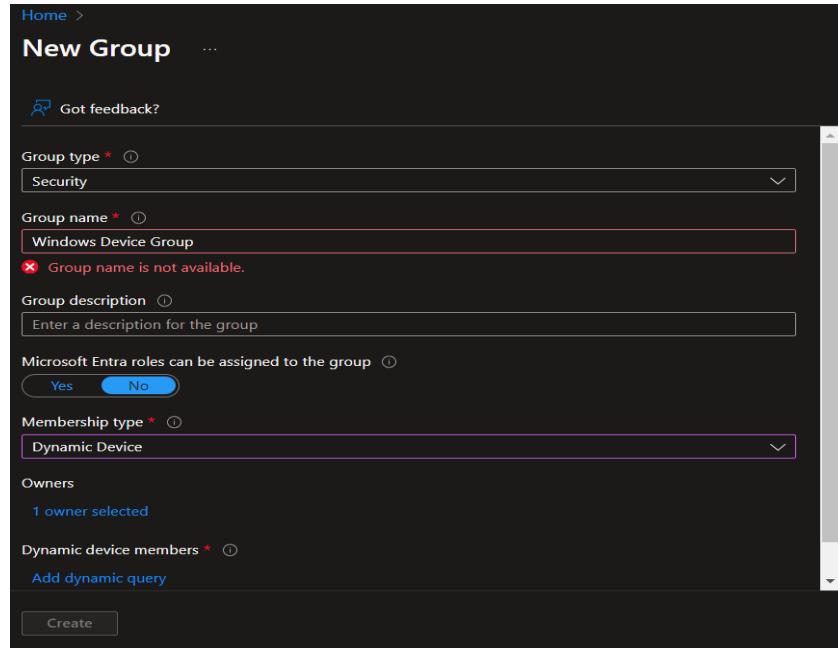
To enroll Windows devices into Entra ID, the device was registered as a work/school account in System > Accounts > Access work or school in order to join the device to Entra ID.



The device join can then be confirmed by accessing portal.azure.com, logging into the global administrator account and navigating to Entra ID > Devices > All devices. The joined device name and its associated information (OS type, Owner, Join type, etc) was then displayed in the table below.

A screenshot of the Microsoft Azure portal, specifically the 'Devices > All devices' page. The top navigation bar includes 'Microsoft Azure', 'Upgrade', 'Search resources, services, and docs (G+)', 'Copilot', and a user profile. The main content area shows a table with one device entry. The table columns are: Name, Enabled, OS, Version, Join type, Owner, MDM, Security settings m..., Compliant, Registered, and Activity. The single device listed is 'SR-CLI' with the following details: Enabled (Yes), OS (Windows), Version (10.0.22631.4169), Join type (Microsoft Entra jo...), Owner (Sam Rajan), MDM (Microsoft Intune), Security settings m... (Microsoft Intune), Compliant (Yes), Registered (9/11/2024, 7:50 PM), and Activity (9/26/2024, 10:1...).

Furthermore, a device group was created by logging in to the Azure portal (portal.azure.com) using the global administrator account and navigating to Show portal menu > Entra ID > Groups > New group. The group characteristics were then configured as follows:



The group was configured as a security group with a dynamic device membership type. Entra roles couldn't be assigned to the group. Note that the group name is not available since it was already created.

A screenshot of the 'Dynamic membership rules' configuration page in the Azure portal. The page has a dark theme. At the top, it says 'Home > New Group > Dynamic membership rules'. The interface includes: 'Save' and 'Discard' buttons; 'Got feedback?' link; 'Configure Rules' (selected) and 'Validate Rules' tabs; a note about using the rule builder or rule syntax text box; a table for building rules ('And/Or', 'Property', 'Operator', 'Value'); a 'Role syntax' text area containing '(device.deviceOSType -eq "Windows")'; and a 'Edit' button next to the role syntax.

The dynamic membership rules under Dynamic device members > Add dynamic query.

The screenshot shows the 'Windows Device Group' blade in Microsoft Intune. At the top left, there are buttons for 'Edit properties', 'Delete', and 'Got feedback?'. Below these are tabs for 'Overview' (which is selected) and 'Properties'. Under 'Basic information', there's a large orange button labeled 'WD' and 'Windows Device Group'. A sub-section says 'All Windows devices are in this group'. Below this are sections for 'Membership type' (Dynamic), 'Source' (Cloud), 'Type' (Security), 'Object ID' (aeb0432d-56fb-42e6-b491-9c15c358f545), 'Created on' (9/10/2024, 11:40 PM), and 'Pause processing' (with a toggle switch). On the right, the 'Members' section shows a table with one direct member: 'SR-011' (Device). The table has columns for Name, Type, Email, and User type.

The successfully created group and joined device.

When enrolling devices into Intune, enrollment settings must be configured first. The first objective is to validate the CNAME navigating to Devices > Enrollment > CNAME Validation in Intune.

The screenshot shows the 'CNAME Validation' blade. At the top, it says 'CNAME Validation' and 'Windows enrollment'. Below this is a descriptive text: 'Configuring a CNAME in your DNS saves your users from having to enter the address of the MDM server when enrolling their Windows devices.' It includes a link to 'Learn more'. Below this is a 'Domain' input field containing 'samrajan659.onmicrosoft.com' with a green checkmark. There is a 'Test' button below the input field. At the bottom, a message says 'CNAME for samrajan659.onmicrosoft.com is configured correctly.' with a green checkmark icon.

The CNAME has been validated successfully.

Microsoft Intune supports configuring device enrollment settings for Windows, Apple, and Android devices. To enroll Apple devices, an Apple MDM Push Certificate needs to be created and uploaded to Intune first. This requires having a valid Apple ID.

Navigating to Devices > Enrollment > Apple > Apple MDM Push Certificate will open the MDM Push Certificate blade. From here the Certificate Signing Request (CSR) had to be downloaded and then the Apple Push Certificate Portal had to be logged into to create the push certificate.

Finally, the certificate was then uploaded to the MDM Push Certificate blade in Intune and the associated Apple ID (obfuscated for privacy) was entered in as well.

Configure MDM Push Certificate

You need an Apple MDM push certificate to manage Apple devices with Intune.

Steps:

1. I grant Microsoft permission to send both user and device information to Apple. [More information on Microsoft permission.](#)
 I agree.
2. Download the Intune certificate signing request required to create an Apple MDM push certificate.
[Download your CSR](#) 4.
3. Create an Apple MDM push certificate. [More information on Apple MDM push certificate.](#)
[Create your MDM push Certificate](#) 2.
4. Enter the Apple ID used to create your Apple MDM push certificate.
Apple ID * ✓

Apple Push Certificates Portal

Certificates for Third-Party Servers

Service	Vendor	Expiration Date*	Status	Actions
Mobile Device Management	Microsoft Corporation	Oct 1, 2025	Active	<input type="button" value="Remove"/> <input type="button" value="Download"/> <input type="button" value="Revoke"/>
Mobile Device Management	Microsoft Corporation	Oct 1, 2025	Active	<input type="button" value="Remove"/> <input type="button" value="Download"/> <input type="button" value="Revoke"/>

*Revoking or allowing this certificate to expire will require existing devices to be re-enrolled with a new push certificate.

About Apple Push Certificates Portal

Create and manage push certificates that enable your third-party server to work with the Apple Push Notification Service and your Apple devices.
[Learn more about Mobile Device Management](#)

MDM push certificates created in the iOS Developer Enterprise Program have been migrated to the Apple Push Certificate Portal.
[Learn more about MDM push certificate migration](#)

Contact Apple for assistance with the Apple Push Certificates Portal.
Enterprise-level customers with an AppleCare OS Support plan: 1-866-752-7753
General inquiries and requests for assistance are handled by Deployment Programs Support.

The Apple Push Certificates Portal.

Apple Push Certificates Portal

Create a New Push Certificate

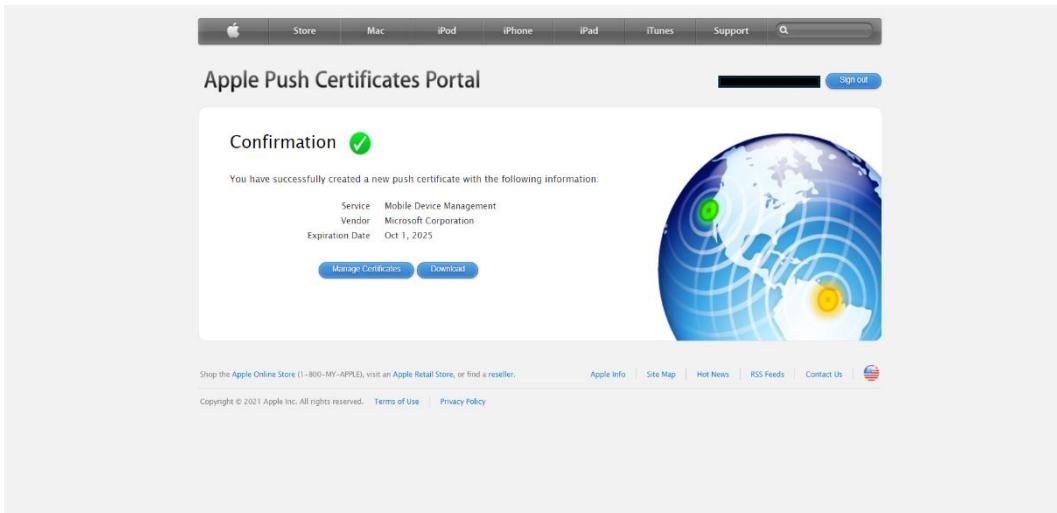
Upload your Certificate Signing Request signed by your third-party server vendor to create a new push certificate.

Notes

Vendor-Signed Certificate Signing Request

[IntuneCSR \(2\).csr](#)

Here the push certificate is created using the CSR created in Intune.



The confirmation screen showing the successful creation of the push certificate.

Configure MDM Push Certificate

[Delete](#)

Download the MDM certificate signing request required to create an Apple MDM push certificate.

[Download your CSR](#)

3. Create an Apple MDM push certificate. [More information on Apple MDM push certificate.](#)
[Create your MDM push Certificate](#)

4. Enter the Apple ID used to create your Apple MDM push certificate.
Apple ID *

[Upload](#)

5. Browse to your Apple MDM push certificate to upload
Apple MDM push certificate *
 [Upload](#)

The Apple MDM push certificate has been uploaded.

Configure MDM Push Certificate

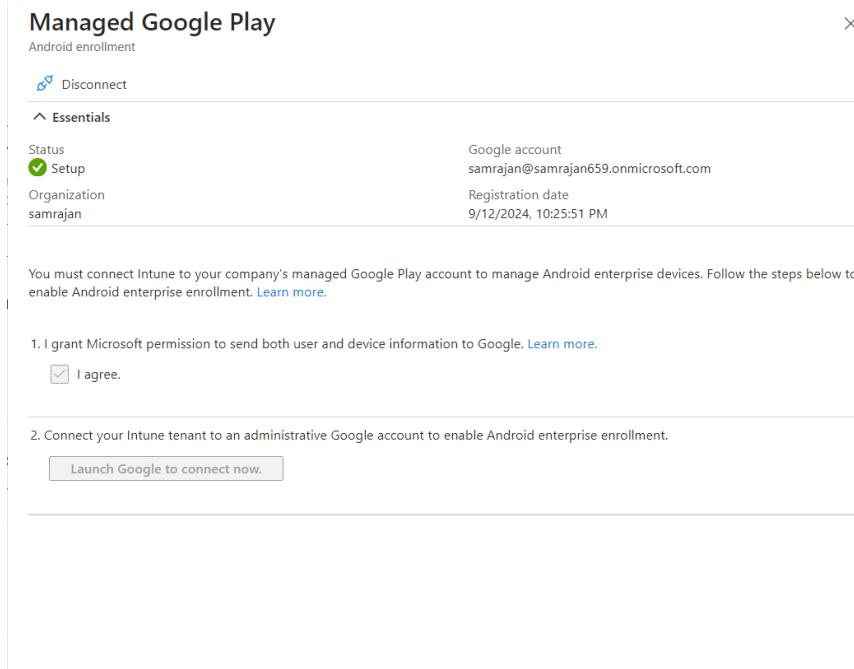
[Delete](#)

[^ Essentials](#)

Status	Active	Days until expiration	365
Last updated	9/30/2024	Expiration	9/30/2025
Apple ID	<input type="text" value="████████████████"/>	Subject ID	com.apple.mgmt.External.d8ffe4e5-8734-4dde-809c-ff053e...
Serial number	3ABCA07AF67614BD		

The Apple MDM Push Certificate has been successfully configured.

To configure enrollment settings for Android devices, a valid Google Play account is required. This process is much simpler than configuring the enrollment settings for Apple devices as the only requirement is to connect the Intune tenant to an administrative Google account. Navigating to Devices > Enrollment > Android > Managed Google Play will open the Managed Google Play blade. Next, the Google Play Connect prompt opened and requested the Domain name or business name (samrajan.com was entered). Following this, the information for the Data Protection Officer and EU Representative was entered in (personal information). After this, the registration was completed. Note that pictures of the process couldn't be shown since this can only be done once.



The checkmark and “Setup” status indicates that Intune was successfully connected to the desired managed Google Play account.

A device enrollment limit restriction was implemented to configure the maximum number of devices that can enroll. The default enrollment restriction configures the maximum number of devices to be 5 but a new device limit restriction was created to increase this number to 15.

Name	Description
Device limit	15

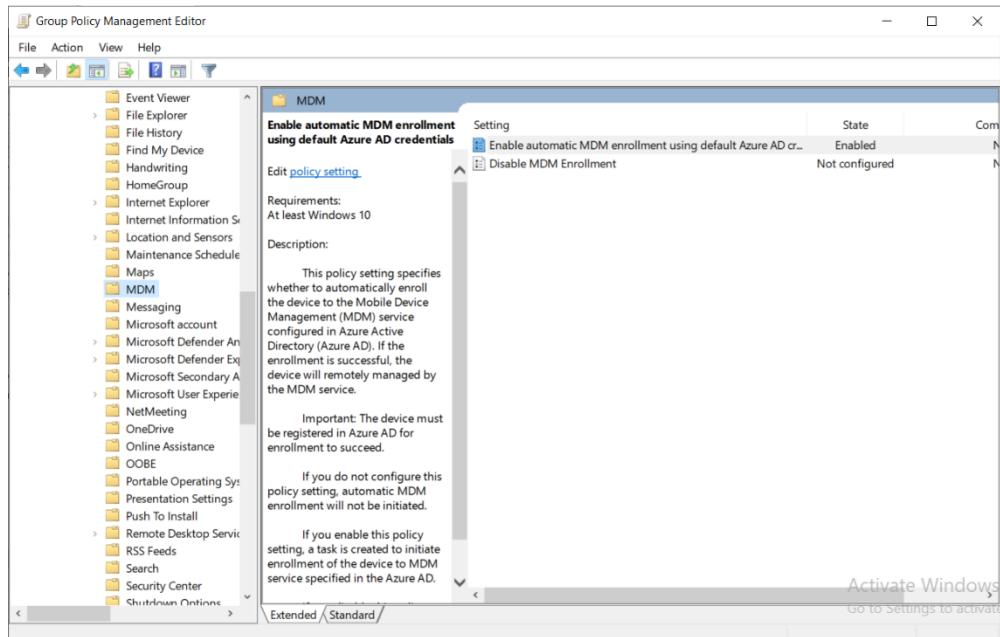
Included groups: Company Users and Devices

This was achieved by navigating to Devices > Enrollment > Device limit restriction > Create restriction and editing the device limit to 15. A device enrollment manager was added by navigating to Devices > Enrollment > Device enrollment managers > Add and simply entering in the user name (SamRajan@samrajan659.onmicrosoft.com).

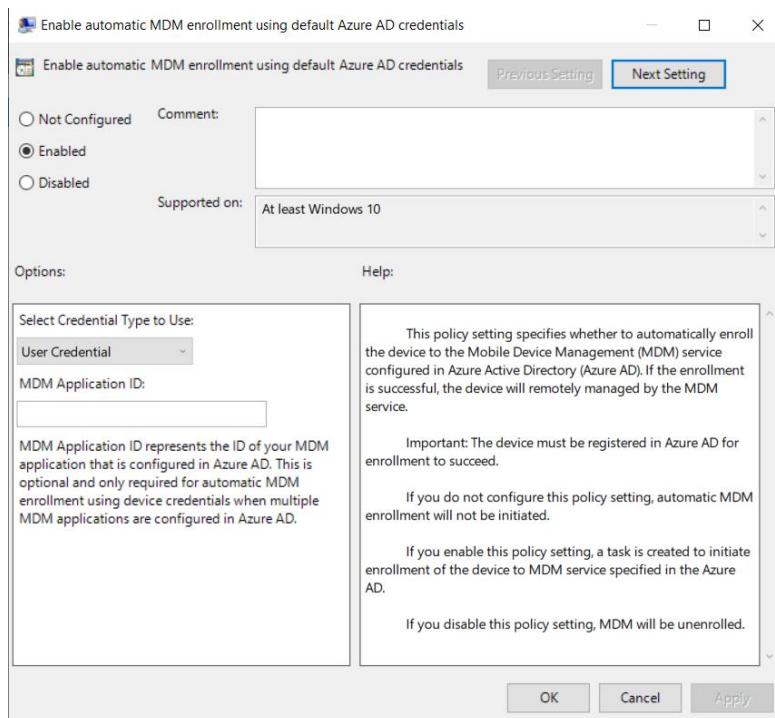
The screenshot shows the Microsoft Intune portal's 'Devices | Enrollment' section. On the left, there's a navigation menu with options like Home, Dashboard, All services, Devices, Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main area shows a search bar and tabs for Windows, Apple, Android, Corporate device identifiers, and Device enrollment managers (which is selected). Below these tabs is a message: 'Add or remove device enrollment managers to allow certain users to enroll larger quantities of devices.' There are buttons for Add, Refresh, Export, and Delete. A list of users is shown, with 'SamRajan@samrajan659.onmicrosoft.com' listed. A modal window titled 'Add User' is open on the right, containing a 'User name' input field with the value 'SamRajan@samrajan659.onmicrosoft.com' and an 'Add' button at the bottom.

To configure automatic enrollment, the automatic MDM enrollment policy needs to be enabled via Server Manager in Windows Server. After navigating to Tools > Group Policy Management in Server Manager, a group policy object called Autoenrollment was edited to enable the “enable automatic MDM enrollment using default Azure AD credentials” setting.

The screenshot shows the Windows Server 2024 Group Policy Management console. The left pane shows the navigation tree with 'Group Policy Management' selected under 'Forest: samrajan.com'. The right pane displays a table titled 'Group Policy Objects in samrajan.com' with columns for Name, QPO Status, WMI Filter, Modified, and Owner. The table lists four GPOs: 'Autoenrollment' (Enabled), 'Default Domain Controller...', 'Default Domain Policy' (Enabled), and 'Microsoft 365 App Settings' (Enabled). The 'Autoenrollment' GPO is selected, and a context menu is open over it, listing options such as Edit, GPO Status, Back Up..., Restore from Backup..., Import Settings..., Save Report..., Copy, Delete, Rename, and Refresh.



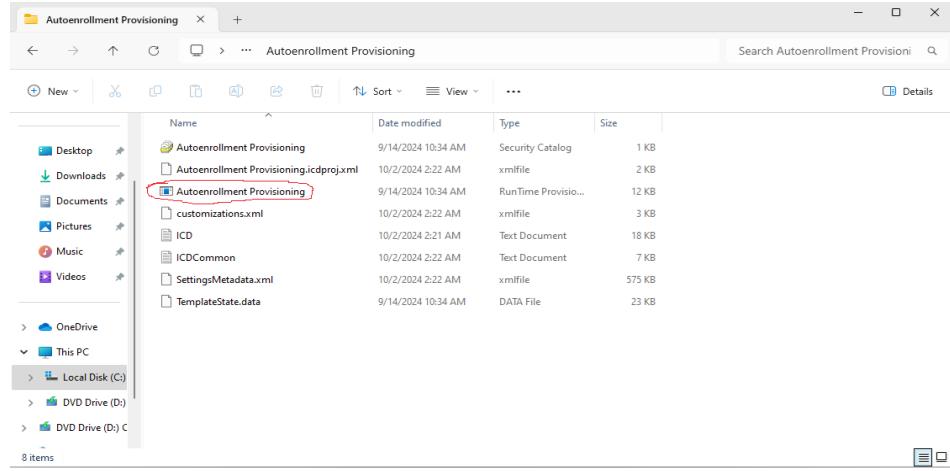
This screen was shown after clicking "Edit" and navigating to Computer Configuration > Policies > Administrative Templates > Windows Components > MDM.



The policy was enabled by double-clicking it and selecting the "Enabled" option.

The edited Autoenrollment GPO was then dragged and dropped into the domain (samrajan.com) in the Group Policy Management screen.

Bulk enrollment can be configured by using Windows Configuration Designer to create a provisioning package. This application must be downloaded and installed from the Microsoft App Store. Once the package has been successfully created, it can be readily provisioned to all desired devices.



Another way to enroll devices into Intune is to use Autopilot. A deployment profile was created along with an enrollment status page. The client device being used for this lab was enrolled via Autopilot.

Assignment	Value
Included groups	AutopilotManaged
Excluded groups	No Excluded groups

Group	Policy Set	Mode
Company Users and Devices	Company Policy Set	Included groups

These are the configured settings for the deployment profile.

Client | Properties ...

X

Search X <>

Basics Edit

Overview

Name	Client
Description	No Description

Manage

Properties

Settings Edit

Show app and profile configuration progress	Yes
Show an error when installation takes longer than specified number of minutes	60
Show custom message when time limit or error occurs	Yes
Error message	Setup could not be completed. Please try again or contact your support person for help.
Turn on log collection and diagnostics page for end users	Yes
Only show page to devices provisioned by out-of-box experience (OOBE)	Yes
Block device use until all apps and profiles are installed	Yes
Allow users to reset device if installation error occurs	Yes
Allow users to use device if installation error occurs	Yes
Block device use until required apps are installed if they are assigned to the user/device	All

Assignments Edit

Included groups

Group	Filter	Filter mode
AutopilotManaged	None	None

Assignment via Policy sets

This object exists in one or more Policy sets and is assigned to the following groups. To edit these assignments, go to Policy sets.

Group	Policy Set
Company Users and Devices	Company Policy Set

Scope tags Edit

Default

These are the settings configured for the enrollment status page.

Windows Autopilot devices ...

X

Windows enrollment

Refresh Export Columns Sync Import Assign user Delete Unblock device 1 items loaded

Search Add filters

Windows Autopilot lets you customize the out-of-box experience (OOBE) for your users.

Last successful sync

10/02/2024, 12:42 AM

Last sync request

10/02/2024, 12:42 AM

<input type="checkbox"/>	Serial number	Manufacturer	Model	Group tag	Profile status	Purchase order	Userless Enrollment Sta...
<input type="checkbox"/>	VMware-56 4d 31 c0 31 50 2a 29-4a b4 40 d9 19 ...	VMware, Inc.	VMware20.1		Assigned	Allowed	...

The device has been successfully enrolled into Intune via Windows Autopilot.

Multiple apps, policies, and other management objects can be assigned at once to devices using policy sets. One policy set was created with the pictured properties.

Home > Devices | Policy sets > Policy sets (Preview) | Policy sets >

Company Policy Set - properties

X

Summary

Basics [Edit](#)

Name	Company Policy Set
Description	No Description

Application management [Edit](#)

Apps

No results.

App configuration policies

No results.

App protection policies

No results.

Device management [Edit](#)

Device configuration profiles

No results.

Device compliance policies

No results.

Device enrollment [Edit](#)

Windows autopilot deployment profiles (1)

Name	Join Type
Autopilot Demo	Microsoft Entra joined

Enrollment status pages (1)

Name	Priority
Client	1

Assignments [Edit](#)

Included groups	Company Users and Devices
Excluded groups	No Excluded groups

Implementing Identity and Compliance

Compliance and identity measures are implemented so that only devices which meet certain criteria are allowed to be enrolled into Intune/Entra ID. Among the criteria are firewall, antivirus, and antispyware activation.

The screenshot shows the 'Properties' tab of a 'Company Windows Compliance' policy. It includes sections for Basics (Name: Company Windows Compliance, Description: --, Platform: Windows 10 and later, Profile type: Windows 10/11 compliance policy), Compliance settings (Edit), System Security (Firewall: Required, Antivirus: Required, Antispyware: Required), Actions for noncompliance (Edit), Scope tags (Edit), Assignments (Edit), Included groups (Group: Company Users and Devices, Filter: None, Filter mode: None), and Excluded groups (Group: No results).

The screenshot shows the 'All devices' page in the Microsoft Intune portal. The left sidebar shows navigation options like Overview, All devices (selected), Monitor, By platform (Windows, iOS/iPadOS, macOS, Android, Linux), Device onboarding (Windows 365, Enrollment), Manage devices (Configuration, Compliance, Conditional access). The main area displays a table of devices:

Device name	Managed by	Ownership	Compliance	OS	OS version	Primary user U...	Last check-in
SR-CL1	Intune	Corporate	Compliant (highlighted)	Windows	10.0.22631.4169	SamRajan@sa...	10/01/2024, 10:16 ...

The device has been marked as compliant. In addition, a security baseline (will be discussed in a later section) has been implemented which enforces the same criteria for compliance.

Conditional access policies are a form of access control that requires a user to have fulfilled certain actions to be able to access company resources. One of these policies was configured for Android devices such that they needed to be marked as compliant to access Windows 365 and Office 365.

The screenshot displays four main sections of a Conditional Access policy configuration:

- Policy Overview:** Shows the policy name "Android/Win 365" and its status as a "Conditional Access policy". It includes sections for "Assignments" (specific users included), "Target resources" (2 apps included), "Network" (Not configured), "Conditions" (1 condition selected), and "Access controls". The "Enable policy" switch is set to "On".
- Assignments:** Details the users assigned to the policy, including "Specific users included" (Kim Wexler, kimwexler@samrajan659.on...).
- Target resources:** Lists the target resources: "2 apps included" (Windows 365 and 1 more, Office 365, and Windows 365).
- Conditions:** Shows the single condition selected: "1 condition selected".
- Access controls:** Shows the grant configuration: "Grant access" selected, with "Require device to be marked as compliant" checked. Other options like "Block access" and "Require multifactor authentication" are available but unchecked.
- Device platforms:** A modal window showing the selected device platform: "Android" (checked). Other options like "iOS", "Windows Phone", "Windows", "macOS", and "Linux" are listed but unchecked.
- Grant:** A detailed view of the access enforcement settings, including "Grant access" selected, "Require device to be marked as compliant" checked, and a note about not locking自己 out if the device is compliant. Other options like "Block access", "Require multifactor authentication", and "Require authentication strength" are listed but unchecked.

The conditional access policy configurations for Android devices relating to Windows 365 and Office 365 access.

Furthermore, there was another conditional access policy configured which required App Protection to be enabled for Android and iOS users. This was part of a later procedure in the lab.

Require App Protection

Name: Require App Protection

Assignments:

- Users: Specific users included
- Target resources: No target resources selected
- Network: Not configured
- Conditions: 1 condition selected

Access controls:

Enable policy: Report-only (On)

Device platforms

Device platforms: 2 included

Locations: Not configured

Client apps: Not configured

Filter for devices: Not configured

Authentication flows (Preview): Not configured

Grant

Control access enforcement to block or grant access. Learn more

- Block access
- Grant access (selected)

- Require multifactor authentication
- Require authentication strength
- Require device to be marked as compliant
- Require Microsoft Entra hybrid joined device
- Require approved client app
- Require app protection policy (selected)

The configuration of the conditional access policy which requires Android and iOS devices to enable App Protection.

Notifications for compliance policies can be configured in Intune. These notifications function via email to notify a user if they are noncompliant. One such notification has been configured with the pictured settings.

Home > Devices | Compliance >

Email Company User

[Send preview email](#)

[Edit](#)

Name: Email Company User

Header and footer settings [Edit](#)

Email Header

Show company logo: Disable

Email Footer

Show device details	Enable
Show company name	Enable
Show contact information	Enable
Show company portal website link	Disable

Notification message templates [Edit](#)

Locale	Subject	Message	Is Default
English (United States)	Compliance	You're not compliant!	true

Home > Devices | Compliance >

Company Windows Compliance

Compliance policy - Windows 10 and later

[Edit](#)

Actions for noncompliance

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

Scope tags [Edit](#)

Default

Assignments [Edit](#)

Included groups

Group	Filter	Filter mode
Company Users and Devices	None	None

Excluded groups

Group

The email has been configured in Intune to be sent immediately to the user once their device has been found noncompliant.

Device compliance can be monitored by navigating to Reports > Device Compliance.

Implementing Local Administrative Password Settings (LAPS) for Entra ID provides management for the local account passwords of domain joined computers. The passwords are stored in Entra ID and protected by access control list, so only eligible users can read it or request its reset. LAPS was enabled and configured in this lab. The first step in setting it up was to navigate to Microsoft Entra ID > Devices > Device Settings at portal.azure.com and enable Microsoft Entra Local Administrator Password Solution (LAPS).

Following this, the LAPS policy would be created in Intune at Endpoint Security > Account Protection > Create Policy.

Force LAPS on Windows clients

Local admin password solution (Windows LAPS)

[Delete](#)**Properties****Basics** [Edit](#)

Name	Force LAPS on Windows clients
Description	No Description
Platform	Windows

Assignments [Edit](#)

Included groups	All Devices
Excluded groups	No Excluded groups

Scope tags [Edit](#)

Selected tags	Default
---------------	---------

Configuration settings [Edit](#)

^ LAPS

Backup Directory ⓘ Backup the password to Azure AD only

Password Age Days ⓘ 30

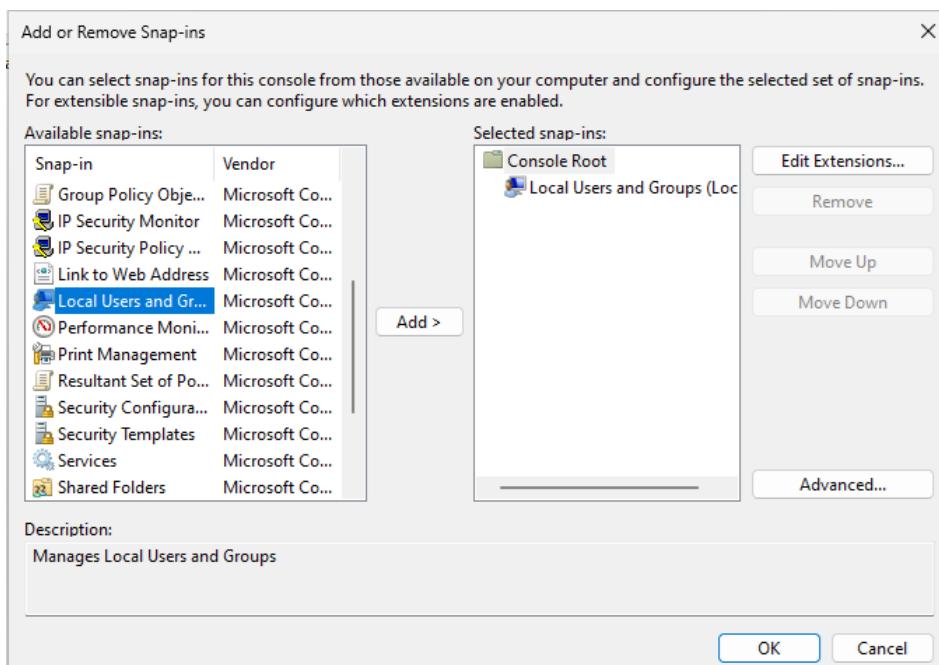
Administrator Account Name ⓘ Admin

Password Complexity ⓘ Large letters + small letters + numbers + special characters

Password Length ⓘ 8

Post Authentication Actions ⓘ Reset the password and logoff the managed account: upon expiry of the grace period, the managed account password will be reset and any interactive logon sessions using the managed account will terminate.

Following this, mmc.exe was ran on the Windows 11 client machine and the “Add or Remove Snap-ins” screen was opened via File > Add or Remove Snap-ins. From here, Local Users and Groups was added as a selected snap-in.



To ensure that the LAPS policy has been applied to the selected device(s), the verification was found at Devices > Windows Devices > Clicking on the device name (SR-CL1) > Device Configuration > Force LAPS on Windows Clients (Logged in user: System account).

Home > Devices | Overview > Windows | Windows devices > SR-CL1 | Device configuration >

SR-CL1 - Policy Settings ...

Recently updated information can take up to 20 minutes to be available in this report.

Refresh Columns

Search Add filters

Name	Status	Error code
Administrator Account Name	Succeeded	
Backup Directory	Succeeded	
Password Age Days	Succeeded	
Password Complexity	Succeeded	
Password Length	Succeeded	
Post Authentication Actions	Succeeded	

Furthermore, navigating to Devices > Windows Devices > Clicking on the device name (SR-CL1) > Local admin password confirmed that an admin password was created.

Home > Devices | Overview > Windows | Windows devices > SR-CL1

SR-CL1 | Local admin password ...

Search Refresh Got feedback?

Learn more about Local Administrator Password Solution (LAPS) →

Local administrator password	Last password rotation
Show local administrator password	9/12/2024, 9:56:07 PM

Local administrator password x

Account name
Administrator

Security ID
S-1-5-21-187137864-2174204526-2595731369-500

Local administrator password
***** Show Local administrator password

Last password rotation
9/12/2024, 9:56:07 PM

Next password rotation
10/12/2024, 9:56:07 PM

Deploying/Upgrading Windows Clients Using Autopilot

Windows Autopilot is a collection of technologies mainly used to set up and pre-configure new devices but can also be used to reset, repurpose, and recover devices. The first step in using Autopilot to deploy and set-up the Windows 11 device in this lab was to download the CSV file using Windows PowerShell prompts.

The screenshot shows two windows side-by-side. On the left is the 'Windows Autopilot devices' list, showing a single device entry for a VMware virtual machine. On the right is the 'Add Autopilot devices' blade, which includes a file selection input field and an 'Import' button.

Windows Autopilot devices

Last successful sync: 10/05/2024, 02:35 PM
Last sync request: 10/05/2024, 02:35 PM

Serial number	Manufacturer	Model	Group tag	Profile
VMware-56 4d 31 c0 31 50 2a 29-4a b4 40 d9 19 ...	VMware, Inc.	VMware20.1	Assigned	

Add Autopilot devices

Import Windows Autopilot devices from a .CSV file. When assigning users in the .CSV, make sure that you are assigning correct UPNs. [Learn more about formatting requirements here.](#)

Select a file

Import

This blade where the CSV file gets uploaded was accessed by navigating to Devices > Enrollment > Devices (in the Windows Autopilot section) > Import. Note that the Windows 11 device appears in the table as a VMware 20.1 model device as the serial number in the CSV file correctly identifies it as a VMware virtual machine.

The first step in creating the CSV file using PowerShell was to reset the execution policy status from restricted to unrestricted (i.e allowing scripts to be ran on the machine).

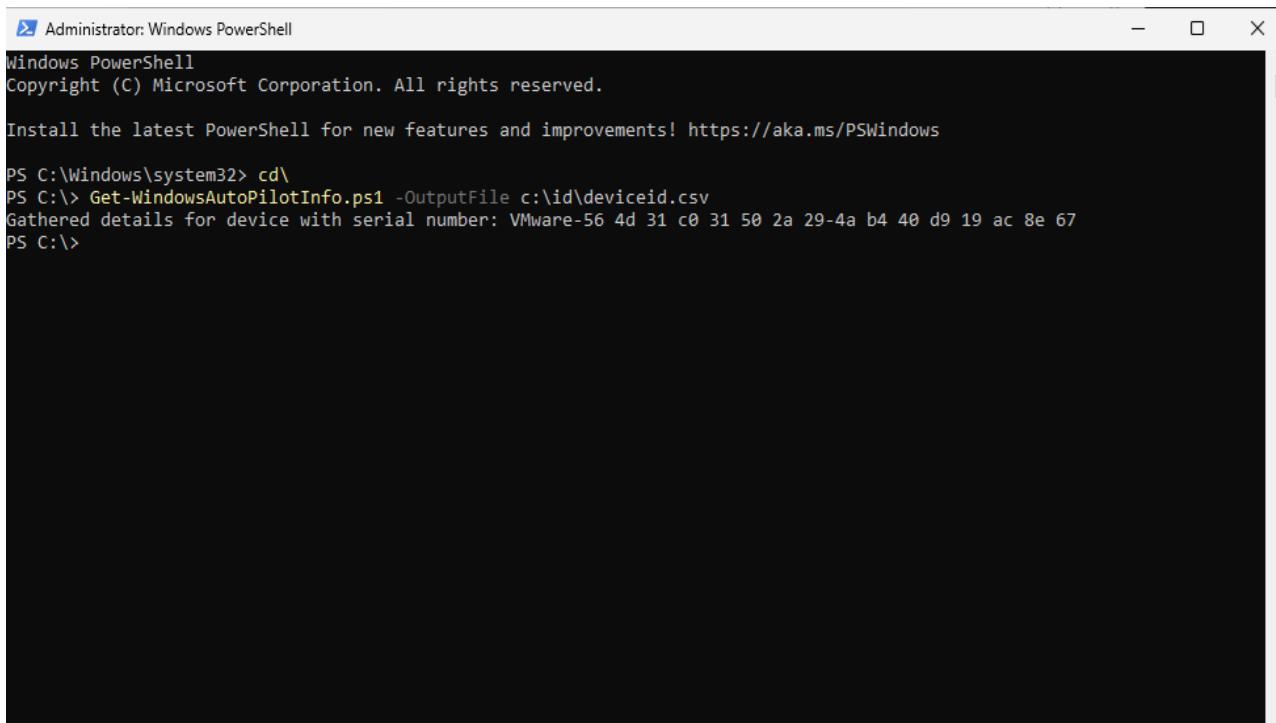
```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Windows\system32> Get-ExecutionPolicy
Unrestricted
PS C:\Windows\system32> Set-ExecutionPolicy -ExecutionPolicy Unrestricted (This was the script needed to change the policy to unrestricted.)
```

It was not possible to enter all the commands as they first were due to Autopilot already being configured and installed. Therefore, a list of those PowerShell commands/scripts that were used will be provided instead.

- Get-ExecutionPolicy (to verify the status change)
- Install-Script -Name Get-WindowsAutoPilotInfo
- *PATH Environment Variable Change Y/N prompt* Answer: Y
- *NuGet provider is required to continue prompt* Answer: Y
- *Untrusted repository prompt* Answer: Y
- cd\ (change directory from C:\Users\administrator to C:\)
- mkdir ID



The screenshot shows a Windows PowerShell window titled "Administrator: Windows PowerShell". The window contains the following command history:

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Windows\system32> cd\
PS C:\> Get-WindowsAutoPilotInfo.ps1 -OutputFile c:\id\deviceid.csv
Gathered details for device with serial number: VMware-56 4d 31 c0 31 50 2a 29-4a b4 40 d9 19 ac 8e 67
PS C:\>
```

Issuing the pictured command caused the CSV file named “deviceid.csv” to be sent to the “ID” folder created using the mkdir command.

The contents of the CSV file. Encircled in red is the serial number.

The final step required to add the device into Intune as an Autopilot device was to login to intune.microsoft.com on the Windows 11 client, navigate to Devices > Enrollment > Devices (in the Windows Autopilot section) > Import, select the deviceid.csv file from C:\ID and click the Import button.

The screenshot shows a Microsoft Intune Admin Center window titled "Windows Autopilot devices". The left sidebar includes links for Home, Dashboard, All services, Devices, Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main content area displays a table of Windows Autopilot devices. The table has columns for Serial number, Manufacturer, Model, Group tag, and Profile. One device entry is visible: "VMware-56 4d 31 c0 31 50 2a 29-4a b4 40 d9 19 ...". Below the table, a message states: "Windows Autopilot lets you customize the out-of-box experience (OOBE) for your users. Last successful sync: 10/05/2024, 09:15 PM. Last sync request: 10/05/2024, 09:15 PM." On the right, a modal dialog titled "Add Autopilot devices" is open, prompting the user to "Import Windows Autopilot devices from a .CSV file. When assigning users in the CSV, make sure that you are assigning correct UPNs. Learn more about formatting requirements here." It contains a text input field with the value "deviceid.csv", a "Formatting results" section showing "Total rows: 1" and "Rows formatted correctly: 1", and a button labeled "Import".

A group made for Autopilot-managed devices named “AutopilotManaged” was created.

Overview Properties

General

Display name: AutopilotManaged

Description:

Creation date/time: 9/11/2024, 1:25 AM

Object ID: 1587bda5-2239-47f3-89ae-f0c5cf36c22

Group type: Security

Membership type: Dynamic Device

Source: Cloud

Administrative unit:

Security enabled: True

Visibility: Private

Security identifier: S-1-12-1-361217445-1207116345-3320884873-577557455

Classification:

Assignable to role: False

License processing state:

Proxy address:

Mail enabled: False

Mail nickname: 0950acc7-1

Unique name:

Dynamic

Membership rule: (device.devicePhysicalIDs -any (_ -startsWith "[ZTDid]"))

Processing status:

Last membership change:

The membership rule configuration encircled in red defines the group as containing all Autopilot devices.

After this, a deployment profile which can be used to configure devices added to the “AutopilotManaged” was created.

Autopilot Demo | Properties ... X

Windows PC

Search X <<

Basics [Edit](#)

- Overview**
- Manage
- Properties**
- Assigned devices

Name	Autopilot Demo
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	Yes
Microsoft Software License Terms	Hide
Privacy settings	Hide
Hide change account options	Hide
User account type	Standard
Allow pre-provisioned deployment	No
Apply device name template	Yes
Enter a name	SR-CL1

Assignments [Edit](#)

Included groups	AutopilotManaged
Excluded groups	No Excluded groups

Assignment via Policy sets

This object exists in one or more Policy sets and is assigned to the following groups. To edit these assignments, go to Policy sets.

Group	Policy Set	Mode
Company Users and Devices	Company Policy Set	Included groups

Automatic enrollment needed to be enabled in Intune by navigating to Devices > Enrollment > Automatic Enrollment and setting the MDM user scope to “all”.

Home > Devices | Enrollment > **Microsoft Intune** ...

MDM user scope [\(i\)](#)

None Some All

MDM terms of use URL [\(i\)](#)

MDM discovery URL [\(i\)](#)

MDM compliance URL [\(i\)](#)

[Restore default MDM URLs](#)

Windows Information Protection (WIP) user scope [\(i\)](#)

None Some All

WIP terms of use URL [\(i\)](#)

WIP discovery URL [\(i\)](#)

WIP compliance URL [\(i\)](#)

[Save](#) [Discard](#) [Delete](#)

Company branding was configured in the Azure Portal by navigating to Microsoft Entra ID > Company Branding > Default sign-in.

Basics	
Favicon ⓘ	Not provided
Background image ⓘ	Not provided
Page background color ⓘ	
Layout	
Template ⓘ	Full-screen background
Header ⓘ	Hide header
Footer ⓘ	Show footer
Custom CSS ⓘ	Not provided
Header	
Header	Hidden
Footer	
Show 'Privacy & Cookies' ⓘ	Shown
Display text ⓘ	
URL ⓘ	
Show 'Terms of Use' ⓘ	Shown
Display text ⓘ	
URL ⓘ	
Sign-in form	
Banner logo ⓘ	Not provided
Square logo (light theme) ⓘ	Not provided
Square logo (dark theme) ⓘ	Not provided
Username hint text ⓘ	
Show self-service password reset ⓘ	Shown
Common URL ⓘ	
Account collection display text ⓘ	
Password collection display text ⓘ	
Sign-in page text ⓘ	Welcome to Sam Rajan's website!

The enrollment status page (ESP) was configured in Intune by navigating to Device > Enrollment > Enrollment Status Page > Create.

The screenshot shows the configuration page for an Enrollment Status Page (ESP) named "Client".

Basics Edit

Name	Client
Description	No Description

Settings Edit

Show app and profile configuration progress	Yes
Show an error when installation takes longer than specified number of minutes	60
Show custom message when time limit or error occurs	Yes
Error message	Setup could not be completed. Please try again or contact your support person for help.
Turn on log collection and diagnostics page for end users	Yes
Only show page to devices provisioned by out-of-box experience (OOBE)	Yes
Block device use until all apps and profiles are installed	Yes
Allow users to reset device if installation error occurs	Yes
Allow users to use device if installation error occurs	Yes
Allow users to use device if installation error occurs	Yes
Block device use until required apps are installed if they are assigned to the user/device	All

Assignments Edit

Included groups

Group	Filter	Filter mode
AutopilotManaged	None	None

Assignment via Policy sets

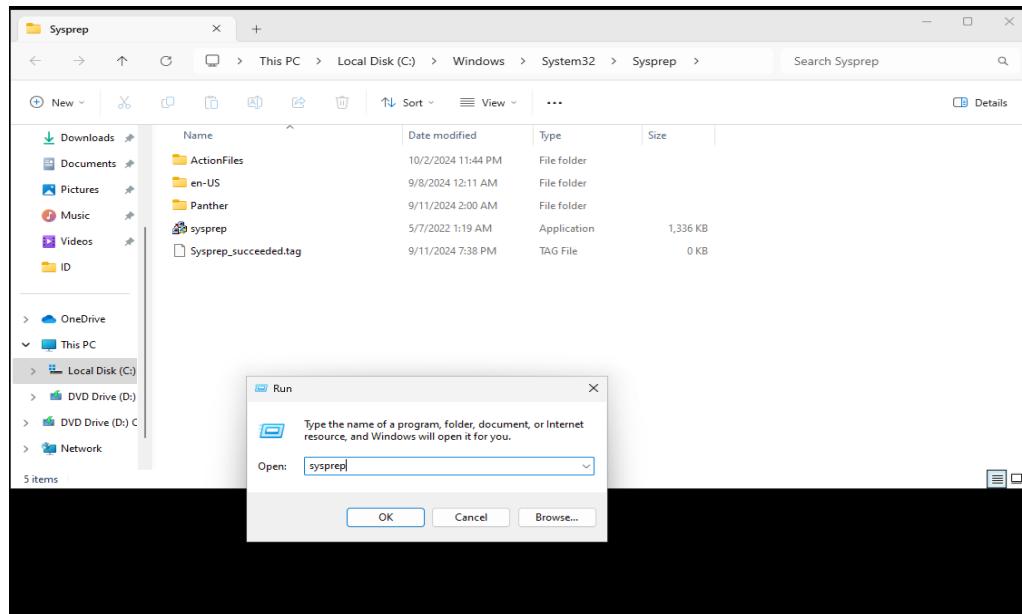
This object exists in one or more Policy sets and is assigned to the following groups. To edit these assignments, go to Policy sets.

Group	Policy Set
Company Users and Devices	Company Policy Set

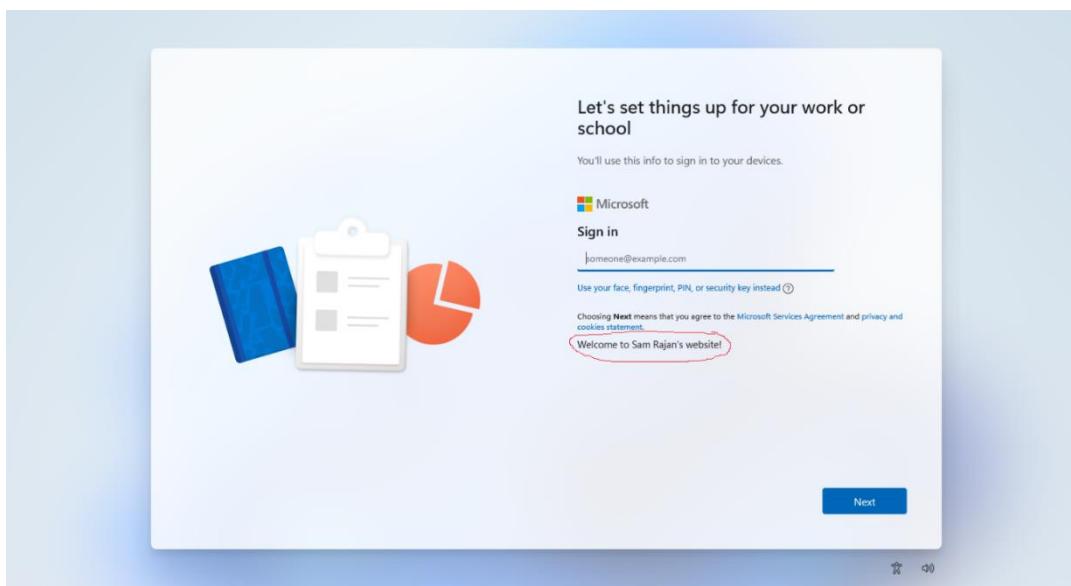
Scope tags Edit

Default

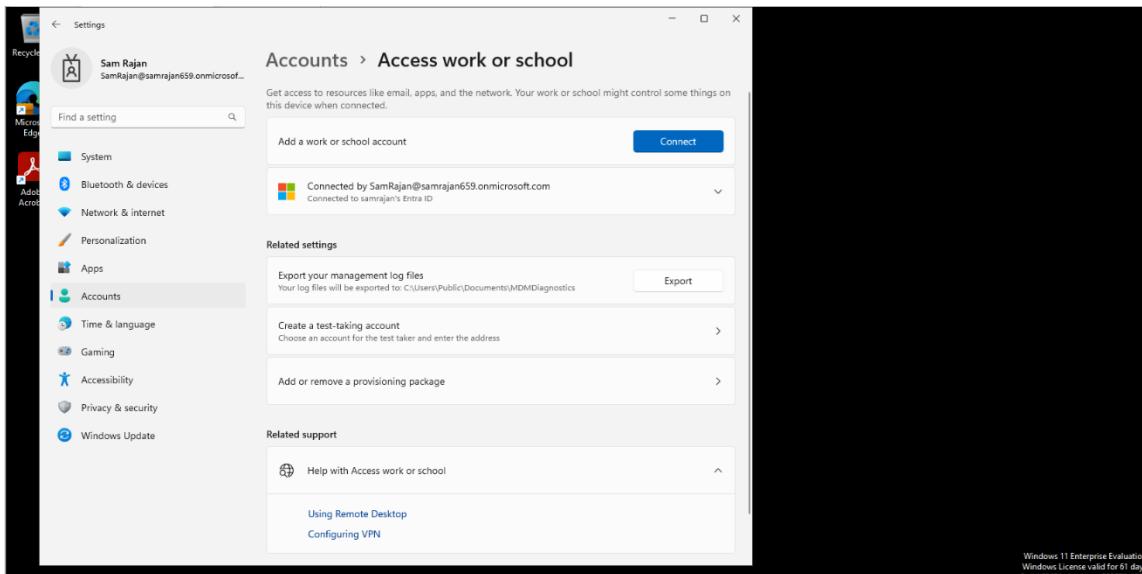
To test whether the enrollment status page settings would appear during the out-of-box-experience (OOBE), the sysprep tool was accessed and ran on the Windows 11 client. This was accessed via Start > Run > sysprep.exe



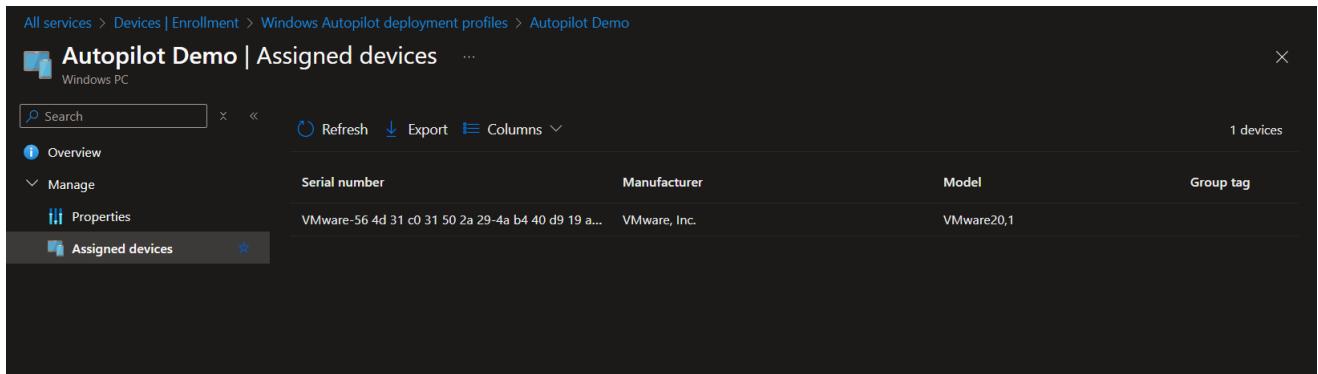
After the device rebooted, the OOBE began, and the welcome message configured in the enrollment status page was displayed.



The OOBE was completed successfully and the enterprise account (SamRajan@samrajan659.onmicrosoft.com) used to sign in previously was able to sign into the device again.



By navigating to Devices > Enrollment > Deployment Profiles > Autopilot Demo > Assigned Devices, the Windows 11 client device could be seen.

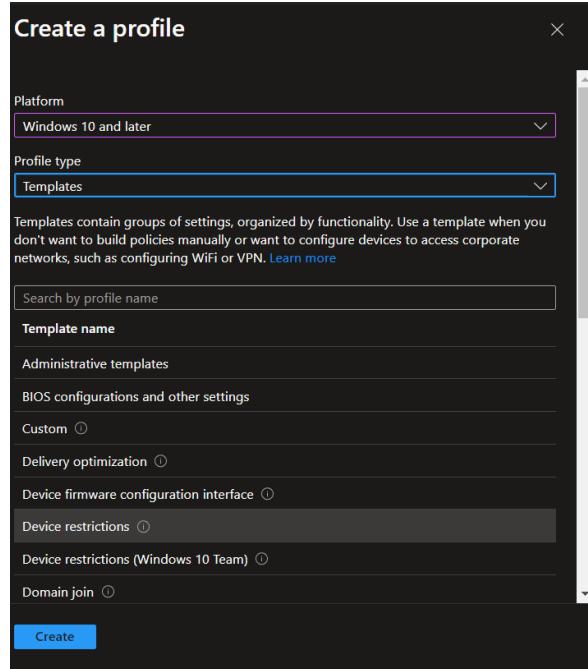


The screenshot shows the Microsoft Intune interface for managing assigned devices. The top navigation bar includes 'All services', 'Devices | Enrollment', 'Windows Autopilot deployment profiles', and 'Autopilot Demo'. The main title is 'Autopilot Demo | Assigned devices' with a subtitle 'Windows PC'. Below the title are buttons for 'Search', 'Refresh', 'Export', and 'Columns'. A status message indicates '1 devices'. On the left, a sidebar menu has 'Overview' selected, while 'Manage', 'Properties', and 'Assigned devices' are also listed. The main content area displays a table with columns: 'Serial number', 'Manufacturer', 'Model', and 'Group tag'. One row is shown, representing a VMware PC with serial number 'VMware-56 4d 31 c0 31 50 2a 29-4a b4 40 d9 19 a...', manufacturer 'VMware, Inc.', model 'VMware20.1', and group tag 'VMware20.1'.

Serial number	Manufacturer	Model	Group tag
VMware-56 4d 31 c0 31 50 2a 29-4a b4 40 d9 19 a...	VMware, Inc.	VMware20.1	VMware20.1

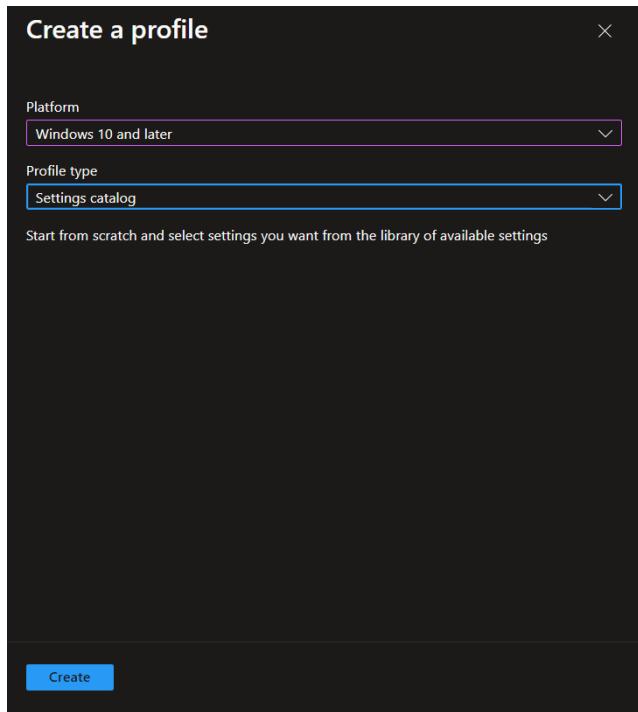
Implementing Device Configuration Profiles

Device configuration profiles are settings used to configure devices upon initial set-up. Device configuration profiles have two different profile types: templates and settings catalog. Device configuration profile creation was accessed at Devices > Configuration > Policies > Create.



This device configuration profile was created using the templates profile type to configure device restrictions for Windows 10 and later devices using the device restrictions template.

A screenshot of the 'Properties' page for a device configuration profile. The profile is named 'Company Device Config' and is described as 'No Description'. It is set for 'Windows 10 and later' and uses the 'Device restrictions' profile type. Under the 'Assignments' section, 'Company Users and Devices' is listed under 'Included groups' with 'None' filter and 'None' filter mode. There are no results in the 'Excluded groups' section. Under 'Scope tags', there is a single entry 'Default'. The 'Configuration settings' section contains several items: 'Camera' (Block), 'USB connection' (Block), 'Cortana' (Block), 'Windows Spotlight' (Block), and 'Windows Spotlight' (Block). The 'Applicability Rules' section is currently empty. The table at the bottom lists 'Rule', 'Property', and 'Value' columns.



This device configuration profile was created for Windows 10 and later devices using the settings catalog profile type.

Properties

Basics [Edit](#)

Name	Company Config from Settings Catalog
Description	No Description
Platform	Windows

Assignments [Edit](#)

Included groups

Group	Filter	Filter mode
Company Users and Devices	None	None

Excluded groups

Group
No results.

Scope tags [Edit](#)

Selected tags	Default
---------------	---------

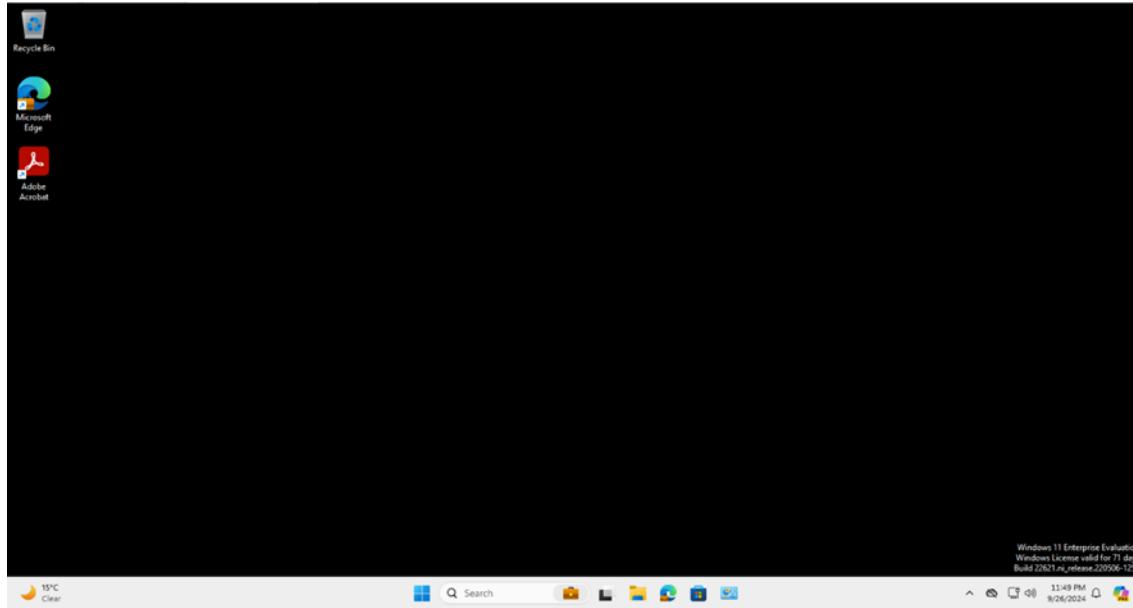
Configuration settings [Edit](#)

Administrative Templates

Desktop > Desktop

Wallpaper Name: (User)	blank.jpg
Wallpaper Style: (User)	Stretch

Desktop Wallpaper (User) ⓘ	Enabled
----------------------------	---------



The background image on the client is a black screen because the wallpaper location was unspecified in the settings catalog configuration profile.

Configuration profiles were also created for Android and iOS devices.

Properties

Basics [Edit](#)

Name	Company Android Config
Description	No Description
Platform	Android Enterprise
Profile type	Device restrictions

Assignments [Edit](#)

Included groups

Group	Filter	Filter mode
Company Users and Devices	None	None

Excluded groups

Group
No results.

Scope tags [Edit](#)

Default

Configuration settings [Edit](#)

General

Screen capture (work profile-level)	Block
Camera (work profile-level)	Block

System security

Threat scan on apps	Require
---------------------	---------

Android configuration profile.

Properties

Basics [Edit](#)

Name	Company iOS/iPadOS Config
Description	No Description
Platform	iOS/iPadOS
Profile type	Device restrictions

Assignments [Edit](#)

Included groups

Group	Filter	Filter mode
Company Users and Devices	None	None

Excluded groups

Group
No results.

Scope tags [Edit](#)

Default

Configuration settings [Edit](#)

- ^ App Store, Doc Viewing, Gaming

Block in-app purchases	Yes
Block App store	Yes

iOS configuration profile.

Kiosk mode is a feature in Windows operating systems (OS) that allow a device to run only specified applications and settings. A group for kiosk devices (Groups > New group) was first configured.

[Overview](#) **Properties**

General

	Display name	Kiosk Devices Edit
Description		
Creation date/time		
9/14/2024, 12:59 PM		
Object ID		
330d86cc-072a-49e3-8467-624b1acbbf9a Edit		
Group type		
Security		
Membership type		
Assigned		
Source		
Cloud		
Administrative unit		
Security enabled		
True		
Visibility		
Private		
Security identifier		
S-1-12-1-856524492-1239615274-1264740228-2596260634		
Classification		
Assignable to role		
False		
License processing state		
Proxy address		
Mail enabled		
False		
Mail nickname		
324c2ccf-b		
Unique name		

Then, a configuration profile was created (Devices > Configuration > Policies > Create) using the templates profile type and a kiosk mode template.

Properties

Basics [Edit](#)

Name	Kiosk Demo Profile
Description	No Description
Platform	Windows 10 and later
Profile type	Kiosk

Assignments [Edit](#)

Included groups

Group	Filter	Filter mode
Kiosk Devices	None	None

Excluded groups

Group
No results.

Scope tags [Edit](#)

Default

Configuration settings [Edit](#)

^Kiosk

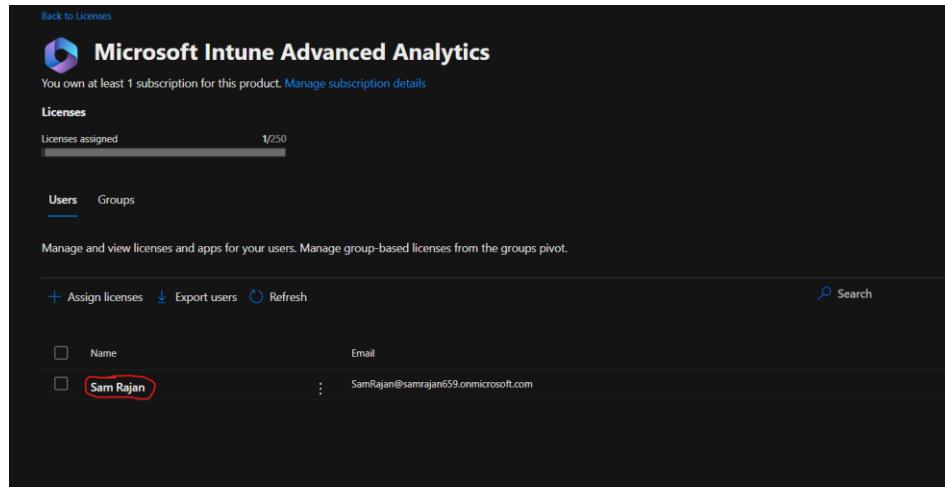
Select a kiosk mode	Single app, full-screen kiosk
User logon type	Auto logon (Windows 10, version 1803 and later, or Windows 11)
Application type	Add Microsoft Edge browser
Edge Kiosk URL	https://bing.com
Microsoft Edge kiosk mode type	Public Browsing (InPrivate)
Refresh browser after idle time	
Maintenance Window Recurrence	Daily (recommended)

Applicability Rules [Edit](#)

Rule	Property	Value	Rule Details
------	----------	-------	--------------

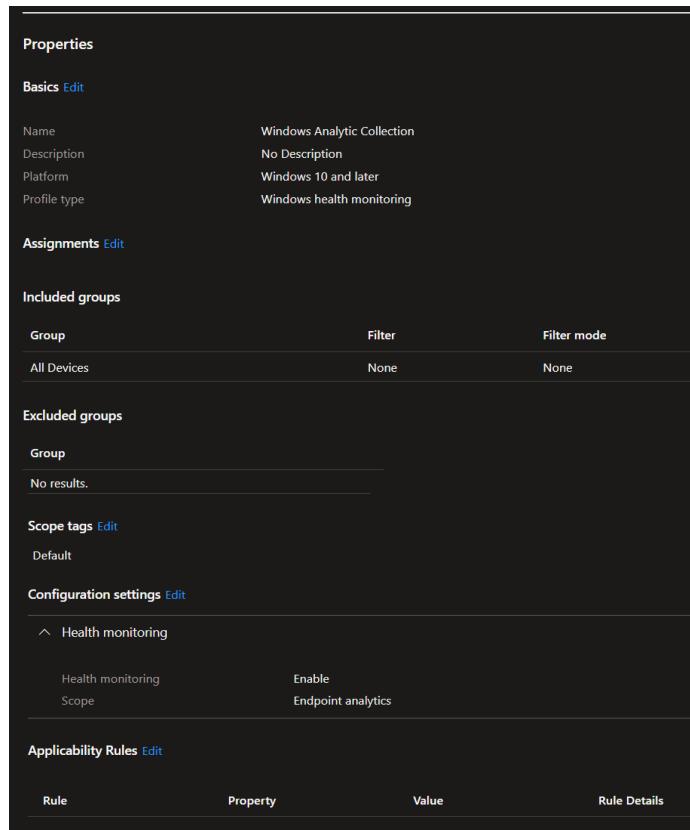
Implementing Intune Suite Add-on Capabilities

One of the Intune Suite add-ons that was implemented is Intune Advanced Analytics. Intune Advanced Analytics is used to proactively detect and resolve endpoint issues, streamline troubleshooting process, and improve users' technology experience. The product (trial) was first obtained, and a license was assigned to the global administrator (Sam Rajan) at admin.microsoft.com

A screenshot of the Microsoft Intune Advanced Analytics interface. At the top, it says "Microsoft Intune Advanced Analytics" and "You own at least 1 subscription for this product. Manage subscription details". Below that is a "Licenses" section showing "Licenses assigned" with a progress bar at 1/250. Under "Users" (which is selected), there's a table with one row for "Sam Rajan". The "Name" column shows "Sam Rajan" with a red box around it, and the "Email" column shows "SamRajan@samrajan659.onmicrosoft.com". There are buttons for "+ Assign licenses", "Export users", and "Refresh". A "Search" bar is also present.

The Intune Advanced Analytics license was assigned to Sam Rajan (Billing > Licenses > Microsoft Intune Advanced Analytics > Assign licenses).

One service of Intune Advanced Analytics that was set up was Windows Health Monitoring. Firstly, a templates-based configuration profile was created in Intune (Devices > Configuration > Policies > Create) to enable health monitoring.

A screenshot of the Windows Health Monitoring configuration profile settings in Intune. It shows the following sections: "Properties", "Basics" (with Name: Windows Analytic Collection, Description: No Description, Platform: Windows 10 and later, Profile type: Windows health monitoring), "Assignments", "Included groups" (Group: All Devices, Filter: None, Filter mode: None), "Excluded groups" (Group: No results.), "Scope tags" (Default), "Configuration settings" (Health monitoring: Scope: Endpoint analytics, Status: Enable), and "Applicability Rules".

Navigating to Reports > Endpoint Analytics > Settings provided confirmation that the Intune data collection policy is connected. This was required for endpoint analytic data to be collected.

The screenshot shows the 'Endpoint analytics | Settings' page. The 'General' tab is selected. Under 'Intune data collection policy', it says 'Connected'. Under 'Configuration Manager data collection', it says 'Not connected'. Under 'Consent to share data', there is a checked checkbox for 'I consent to share anonymized and aggregated metrics to see updated Endpoint analytics scores and insights.'

The screenshot shows the 'Endpoint analytics | Overview' page. The 'Overview' tab is selected. It displays the 'Endpoint analytics score' as 47, comparing it to a baseline of 37. Below the score, a chart shows 'Score categories' for various metrics: Startup performance (35), Application reliability (0), Resource performance (53), Work from anywhere (100), and Battery health (0). A note indicates that the preview reports do not contribute to the score.

Endpoint Analytic data has been collected (Reports > Endpoint Analytics > Overview).

Remote Help is an Intune add-on which allows permitted users to connect to other users' devices and provide helpdesk support. Remote Help was configured in this lab. Before configuring Remote Help, a user named "Help Operator" was added in the Microsoft 365 admin centre (admin.microsoft.com). This account was to be given permission to use Remote Help for helpdesk support.

The screenshot shows the Microsoft 365 Admin Center user profile for "Help Operator". Key details include:

- Username:** helpoperator@samrajan659.onmicrosoft.com
- Last sign-in:** View last 30 days
- Sign-out:** Sign this user out of all Microsoft 365 sessions, or Sign out of all sessions
- Groups:** Remote Help Operators, samrajan
- Roles:** No administrator access, Manage roles
- Contact information:** Display name: Help Operator, First name: Help, Last name: Operator
- Microsoft 365 activations:** View Microsoft 365 activations
- Multifactor authentication:** Manage multifactor authentication

Remote Help had to be obtained via a trial subscription for Microsoft Intune Suite for FLW as a trial subscription for Remote Help doesn't exist. The license was assigned to "Help Operator" and the global administrator (Sam Rajan).

The screenshot shows the Microsoft Intune Suite for FLW License details page. Key features include:

- Licenses:** Licenses assigned: 2/25
- Users:** Manage and view licenses and apps for your users. Assign licenses, Export users, Refresh, Search, and Give Feedback.
- Table:** Shows assigned licenses for users "Help Operator" and "Sam Rajan".

Name	Email
Help Operator	helpoperator@samrajan659.onmicrosoft.com
Sam Rajan	Samrajan@samrajan659.onmicrosoft.com

Remote Help needed to be enabled in Intune by navigating to Tenant administration > Settings > Configure.

The screenshot shows the Microsoft Intune Tenant admin interface. On the left, there's a sidebar with various navigation options like Tenant status, Remote Help, Microsoft Tunnel Gateway, Cloud PKI, Connectors and tokens, Filters, Roles, Microsoft Entra Privileged Identity Management, Diagnostics settings, Audit logs, Device diagnostics, Multi Admin Approval, Intune add-ons, Copilot (preview), End user experiences, and Customization. The 'Remote Help' option is selected. The main area has tabs for Monitor, Settings (which is selected), and Remote Help sessions. Under Settings, there are sections for Remote Help requirements (which says 'Enabled'), Remote Help to unenrolled devices (set to 'Allowed'), and Disable Chat (set to 'No'). A red circle highlights the 'Enabled' dropdown under 'Remote Help requirements'. Another red circle highlights the 'Enabled' status under 'Remote Help requirements'.

Next, a group for the help desk operators called “Remote Help Operators” was created (Groups > New group).

The screenshot shows the 'General' settings page for a group named 'Remote Help Operators'. The page includes fields for Display name (Remote Help Operators), Description, Creation date/time (9/15/2024, 1:07 AM), Object ID (9f289512-9674-407c-9979-fd31f7cf347f), Group type (Security), Membership type (Assigned), Source (Cloud), Administrative unit, Security enabled (True), Visibility (Private), Security identifier (S-1-12-1-2670236946-1081906804-838695321-2134167543), Classification, Assignable to role (False), License processing state, Proxy address, Mail enabled (False), Mail nickname (44aec036-e), and Unique name.

The screenshot shows a list of members for a group named 'Remote Help Operators'. There are two entries: 'Help Operator' (User) and 'Sam Rajan' (User). Both entries have a small circular icon next to their names.

Name	Type	Email	User type
HO Help Operator	User		Member
SR Sam Rajan	User	SamRajan@samrajan659.onmicrosoft.com	Member

Members of the group.

The help desk operator role was assigned to this group by navigating to Tenant administration > Roles > Help Desk Operator > Assignments > Assign.

The screenshot shows the 'Properties' tab for a group named 'Help Operators for Remote Help Permissions'. In the 'Members' section, the 'Remote Help Operators' group is listed and highlighted with a red oval.

The role was assigned to the Remote Help Operators group.

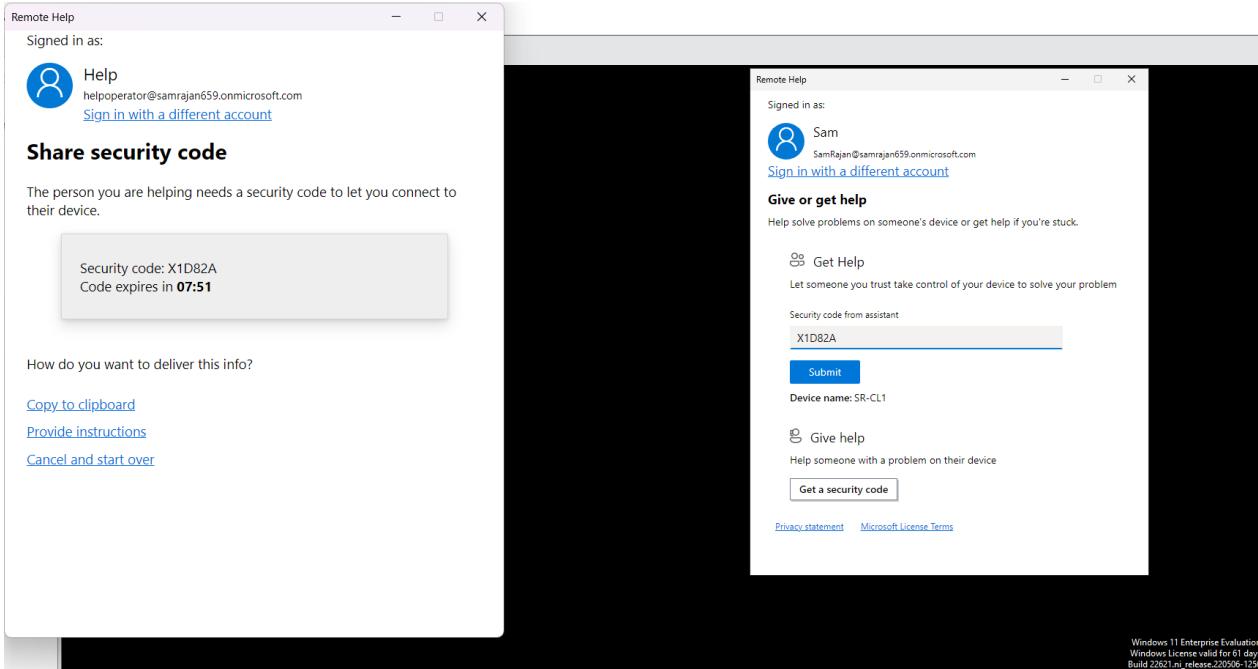
Remote Help was downloaded on the host machine and Windows 11 client and was used to start a session. The help operator account was used to sign in on the host machine. Clicking on "Get a security code" while signed in on Remote Help will provide a code that a user in need used to initiate a remote helpdesk session.

Left Screenshot: Give or get help

- Signed in as: Help (helpoperator@samrajan659.onmicrosoft.com)
- [Sign in with a different account](#)
- Give or get help**
 - Help solve problems on someone's device or get help if you're stuck.
 - Get Help**: Let someone you trust take control of your device to solve your problem.
 - Security code from assistant
 - Enter code:
 - Submit
- Device name: MSI
- Give help**: Help someone with a problem on their device.
- [Get a security code](#)

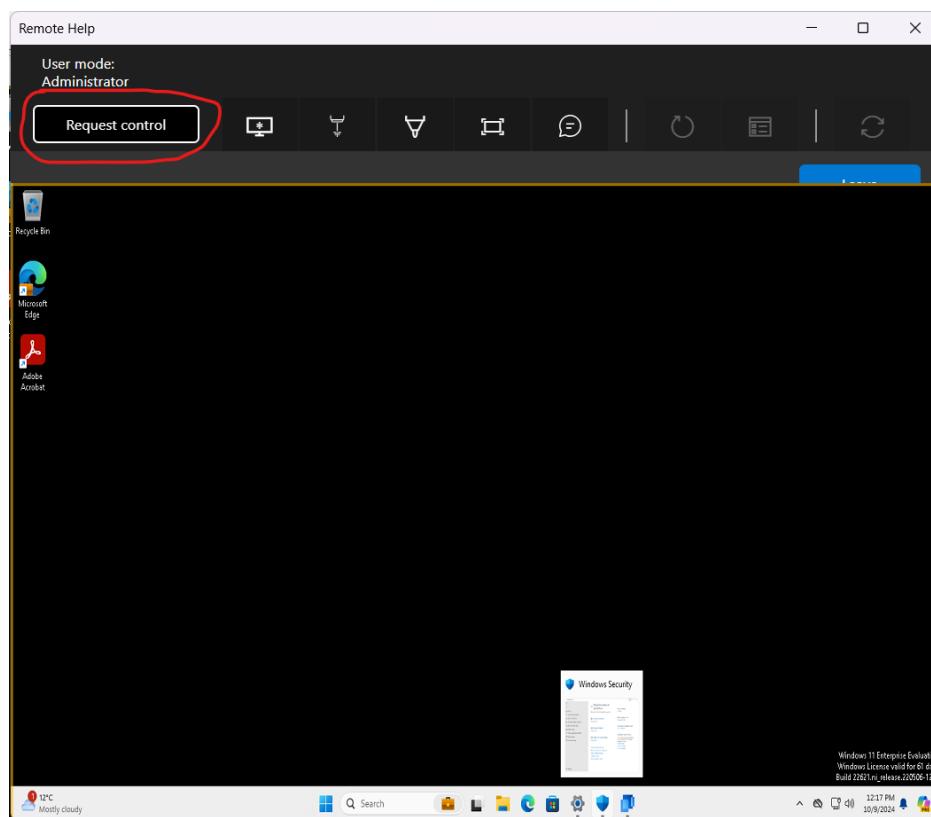
Right Screenshot: Share security code

- Signed in as: Help (helpoperator@samrajan659.onmicrosoft.com)
- [Sign in with a different account](#)
- Share security code**: The person you are helping needs a security code to let you connect to their device.
- Security code: X1D82A
Code expires in 09:58
- How do you want to deliver this info?
 - [Copy to clipboard](#)
 - [Provide instructions](#)
 - [Cancel and start over](#)

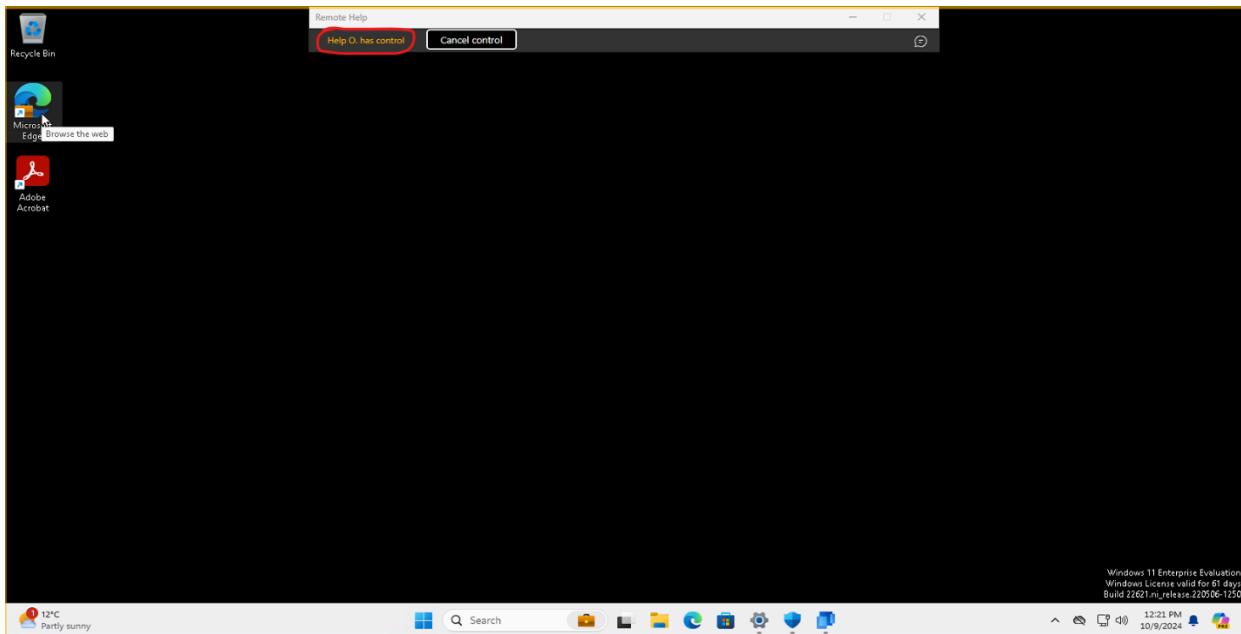


The user must enter the code given from the helpdesk operator.

Once screen-sharing permission was granted to the operator, the operator could then request control of the user's device.



Once the help desk operator was given permission to control the device by the user, the help desk operator was able to freely move the user's cursor and give support.



Performing Remote Actions on Devices via Intune

The first remote action performed was updating the Windows Antivirus settings. This was done by configuring a policy by navigating to Endpoint Security > Antivirus > Create Policy.

The screenshot shows the 'Properties' section of a policy named 'Defender Antivirus'. It includes fields for Name (Defender Antivirus), Description (No Description), and Platform (Windows). Under 'Assignments', it lists 'Included groups' (Windows Device Group) and 'Excluded groups' (No Excluded groups). In the 'Configuration settings' section, under the 'Defender' category, there are three settings: 'Allow Email Scanning' (Allowed), 'Allow Realtime Monitoring' (Allowed), and 'Allow Script Scanning' (Allowed).

Another remote action performed was rotating the BitLocker recovery keys. BitLocker is a full-volume disk encryption software that helps protect the entire operating system drive against offline attacks. When BitLocker sees a new device in the boot list or an attached external storage device, it prompts the user for a recovery key as a security measure.

The screenshot shows the 'Overview' tab for a device named 'SR-CL1'. The 'More' menu is open, and the 'BitLocker key rotation' option is highlighted with a red box. Other options in the menu include Autopilot Reset, Quick scan, Full scan, Update Windows Defender security intelligence, Rotate local admin password, Rename device, New remote assistance session, Locate device, Pause config refresh, Run remediation (preview), and Remote Help.

Bitlocker Key Rotation was accessed at Devices > Windows > SR-CL1 > More > Bitlocker key rotation.

Home > Devices | Windows > Windows | Windows devices >

SR-CL1

Search X Retire Wipe Delete Remote lock Sync Reset passcode Restart Collect diagnostics Fresh Start ...

Overview

Manage Properties Monitor Hardware Discovered apps Device compliance Device configuration App configuration Local admin password Recovery keys User experience Device diagnostics Group membership Managed Apps Filter evaluation

BitLocker key rotation - SR-CL1

If you rotate the encryption keys on this device, you'll remove all keys on the device. A single key will be escrowed to your identity provider (Microsoft Entra ID or Active Directory) after you restart the device. If multiple recovery keys exist, old keys will be automatically deleted. Rotate keys anyway?

Yes **No**

Management name: SamRajan_Windows_10/7/2024_2:10 AM
Enrolled by: Sam Rajan
Ownership: Corporate
Compliance: Compliant
Serial number: VMware-564d31c031502a29-4ab440d919ac8e67
Operating system: Windows
Phone number: ---
Device manufacturer: VMware, Inc.
Last check-in time: 10/9/2024, 4:37:43 PM
Device model: VMware20.1
Remote assistance: Remote Help

Device actions status

Action	Status	Date/Time	Error
Collect diagnostics	Complete	10/6/2024, 11:08:40 PM	

Home > Devices | Windows > Windows | Windows devices >

SR-CL1

Search X Retire Wipe Delete Remote lock Sync Reset passcode Restart Collect diagnostics Fresh Start ...

Overview

Manage Properties Monitor Hardware Discovered apps Device compliance Device configuration App configuration Local admin password Recovery keys User experience Device diagnostics Group membership Managed Apps Filter evaluation

BitLocker key rotation pending...

Essentials

Device name: SR-CL1
Management name: SamRajan_Windows_10/7/2024_2:10 AM
Enrolled by: Sam Rajan
Ownership: Corporate
Compliance: Compliant
Serial number: VMware-564d31c031502a29-4ab440d919ac8e67
Operating system: Windows
Phone number: ---
Device manufacturer: VMware, Inc.
Last check-in time: 10/9/2024, 4:37:43 PM
Device model: VMware20.1
Remote assistance: Remote Help

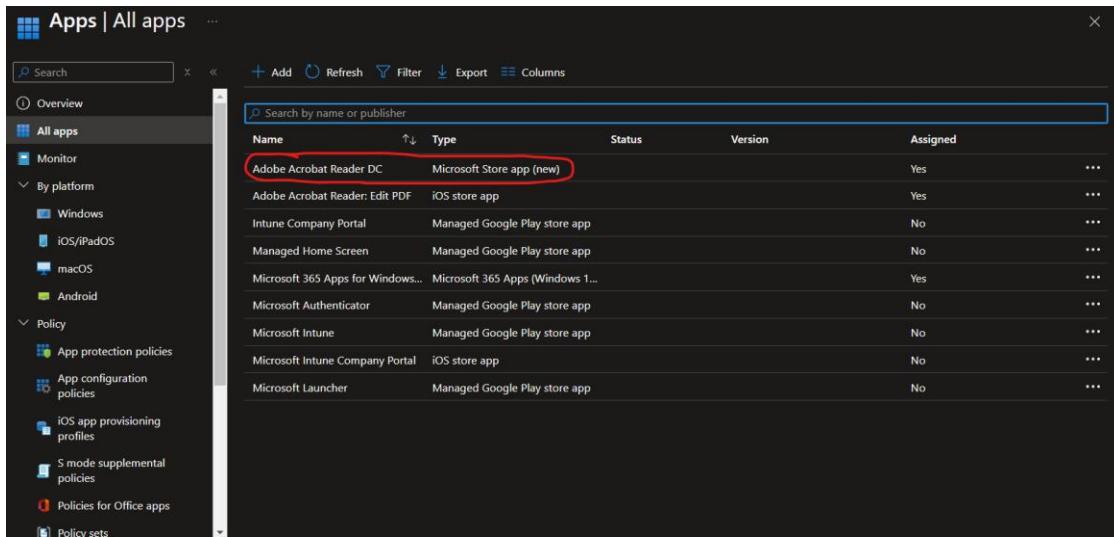
Device actions status

Action	Status	Date/Time	Error
BitLocker key rotation	Pending	10/9/2024, 7:58:09 PM	

The Bitlocker key rotation has been initiated.

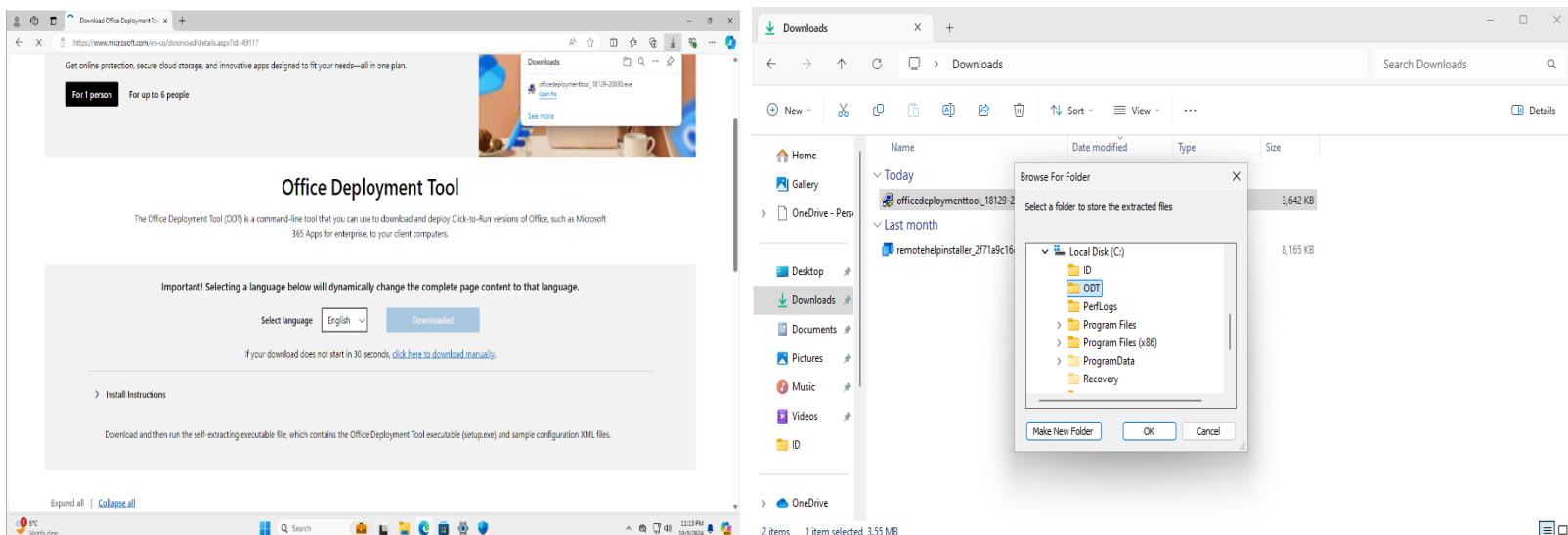
Deploying and Updating Apps

Intune can be used (and was used) to deploy apps to devices. One such app that was deployed using Intune was Adobe Acrobat Reader DC. It was deployed by navigating to Apps > All apps > Add and was installed directly from the Microsoft Store.



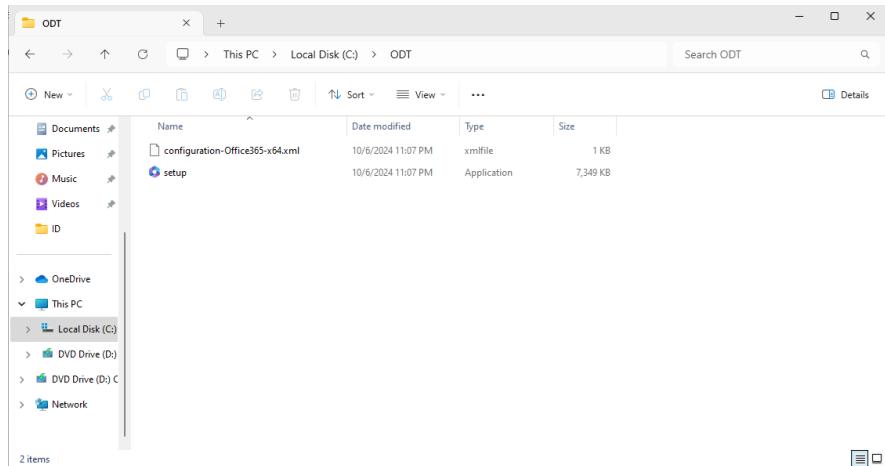
The screenshot shows the Microsoft Intune interface for managing apps. On the left, there's a navigation pane with sections like Overview, All apps, Monitor, By platform (Windows, iOS/iPadOS, macOS, Android), Policy (App protection policies, App configuration policies, iOS app provisioning profiles, S mode supplemental policies, Policies for Office apps), and Policy sets. The main area is titled 'Apps | All apps' and contains a table of apps. The table has columns for Name, Type, Status, Version, and Assigned. A row for 'Adobe Acrobat Reader DC' is highlighted with a red box around the 'Type' column, which shows 'Microsoft Store app (new)'. Other rows include 'Adobe Acrobat Reader: Edit PDF' (iOS store app), 'Intune Company Portal' (Managed Google Play store app), 'Managed Home Screen' (Managed Google Play store app), 'Microsoft 365 Apps for Windows...' (Microsoft 365 Apps (Windows 1...)), 'Microsoft Authenticator' (Managed Google Play store app), 'Microsoft Intune' (Managed Google Play store app), 'Microsoft Intune Company Portal' (iOS store app), and 'Microsoft Launcher' (Managed Google Play store app). The status column shows 'Yes' for the Adobe app and 'No' for others.

Microsoft 365 apps were deployed using the Office Deployment Tool (ODT) and Office Customization Tool (OCT). The Office Deployment Tool is a command-line tool used to download and deploy Click-to-Run versions of Office to client computers while the Office Customization Tool creates the configuration files that are used to deploy Office. The first step in using the ODT to install Microsoft 365 on the Windows 11 client was to download and install the Office Deployment Tool on the client.



The screenshot shows two windows. On the left is a web browser displaying the Microsoft Office Deployment Tool download page at <https://www.microsoft.com/en-us/download/details.aspx?id=8117>. The page shows a download link for 'Office Deployment Tool' (version 18129-20000.exe, 3,642 KB) and instructions for installing it for up to 6 people. On the right is a Windows File Explorer window titled 'Downloads' showing the extracted contents of the downloaded file. A 'Browse For Folder' dialog box is open, prompting the user to 'Select a folder to store the extracted files'. The extracted files are listed in a tree view under 'Local Disk (C:)': 'ODT', 'PerfLogs', 'Program Files', 'Program Files (x86)', 'ProgramData', and 'Recovery'. The total size of the extracted files is 8,165 KB.

The ODT files were installed and stored in the "ODT" folder on the client's C:\ drive.



The files have successfully been extracted.

The configuration-Office365-x64.xml file was edited from it's original version to remove Microsoft Viso, auto-activate, and accept the EULA.

```
<Configuration>
    <Add OfficeClientEdition="64" Channel="Current">
        <Product ID="0365ProPlusRetail">
            <Language ID="en-us" />
        </Product>
    </Add>
    <!-- <Updates Enabled="TRUE" Channel="Current" / -->
    <Display Level="None" AcceptEULA="TRUE" />
    <Property Name="AUTOACTIVATE" Value="1" />
</Configuration>
```

Ln 7, Col 3 | 334 characters

Next, the configuration-Office365-x64.xml file was ran via the command prompt.

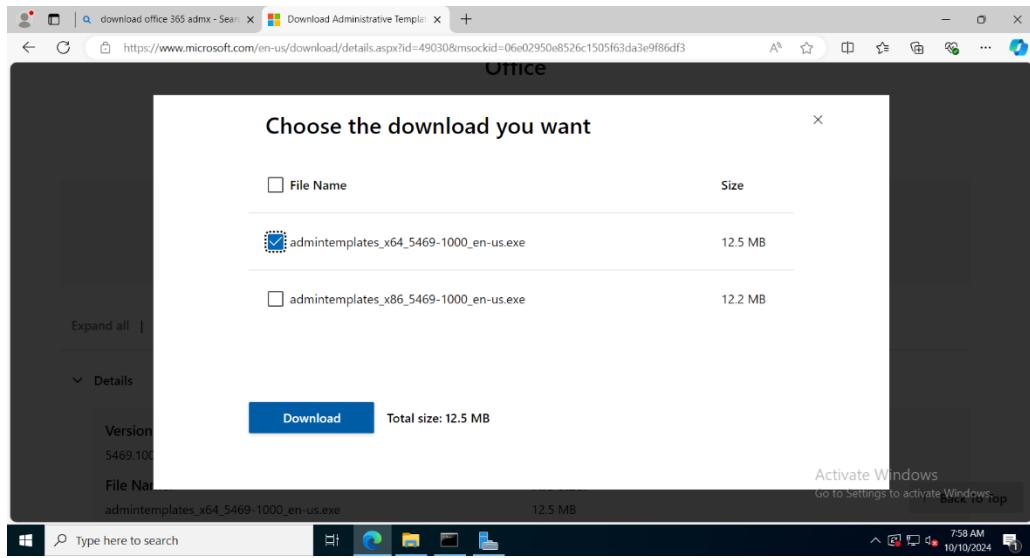
```
Command Prompt - setup /d
Microsoft Windows [Version 10.0.22631.4169]
(c) Microsoft Corporation. All rights reserved.

C:\Users\SamRajan>cd odt
The system cannot find the path specified.

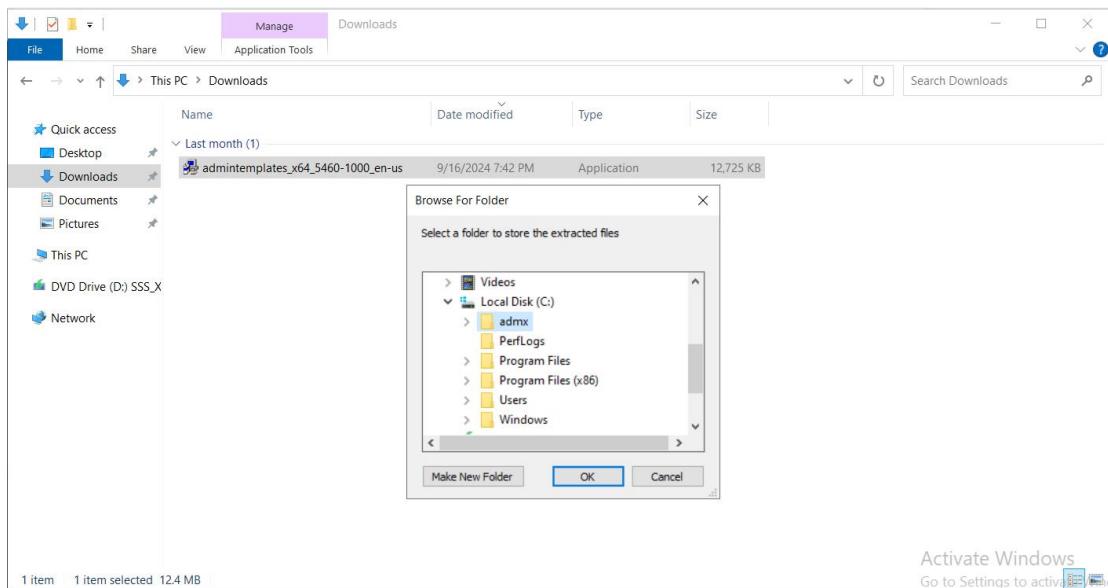
C:\Users\SamRajan>cd\
C:\>cd odt
C:\ODT>setup /download configuration-Office365-x64.xml
```

After this point, the Click-to-Run versions of the 365 apps will download onto the client.

Policies for Office apps can be implemented by using Group Policy. The first step in doing this was to download the Administrative Template (ADMX/ADML) files onto the Windows Server 2022 machine.

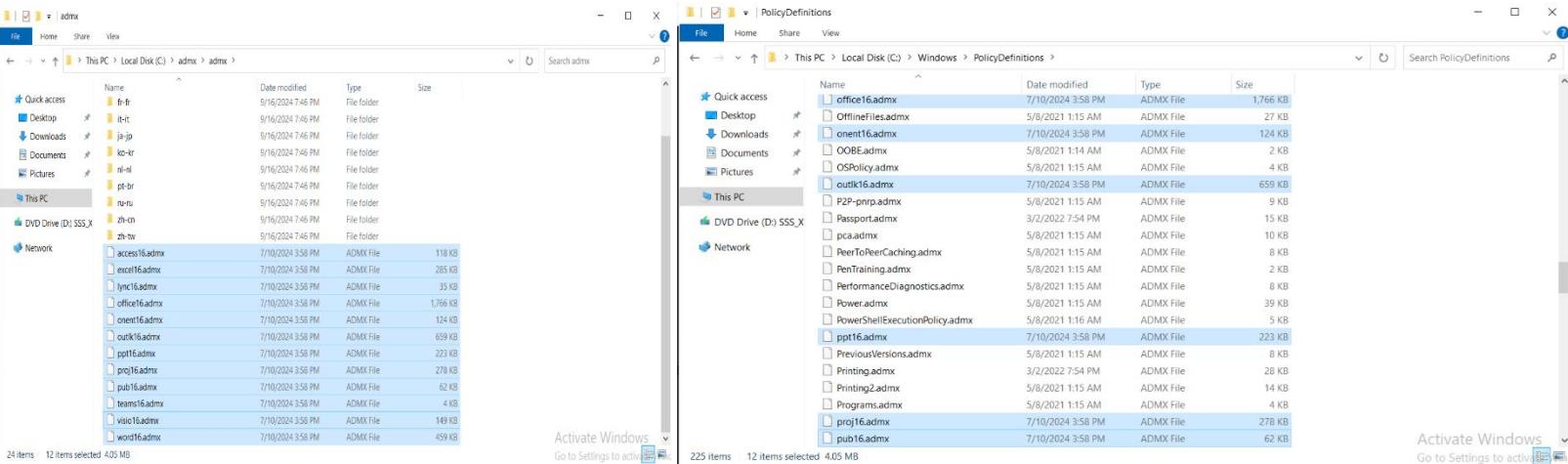


After navigating to <https://www.microsoft.com/en-us/download/details.aspx?id=49030&msockid=06e02950e8526c1505f63da3e9f86df3>, the 64-bit version of the ADMX/ADML files were downloaded.



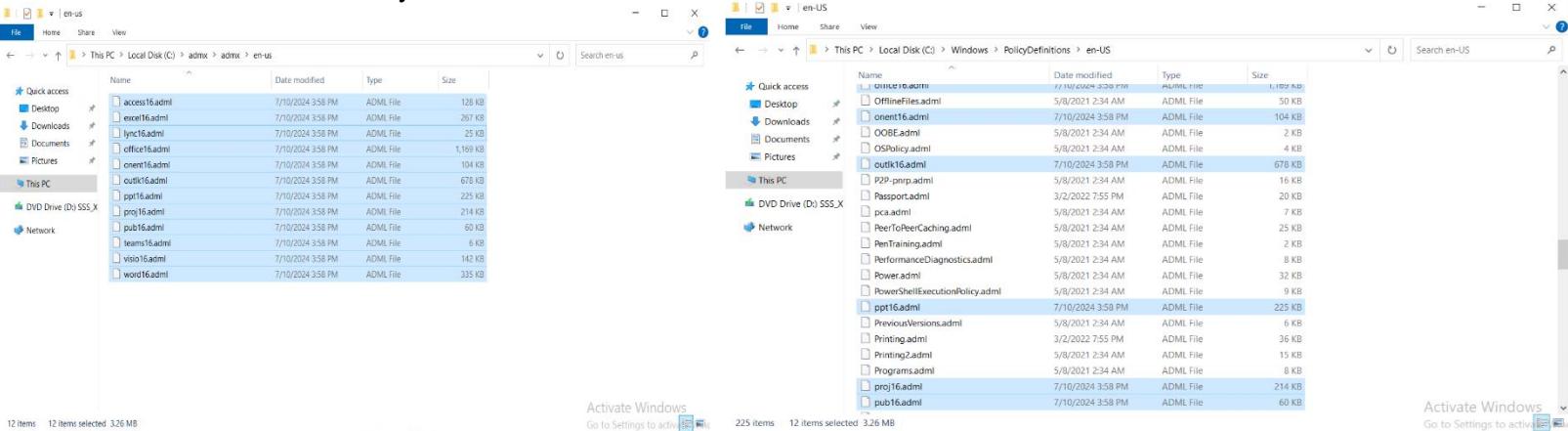
The setup file was run, and the files were extracted to a folder called "admx" on the C:\ drive.

After navigating to C:\admx\admx, the ADMX files were copied and transferred to C:\Windows\PolicyDefinitions.



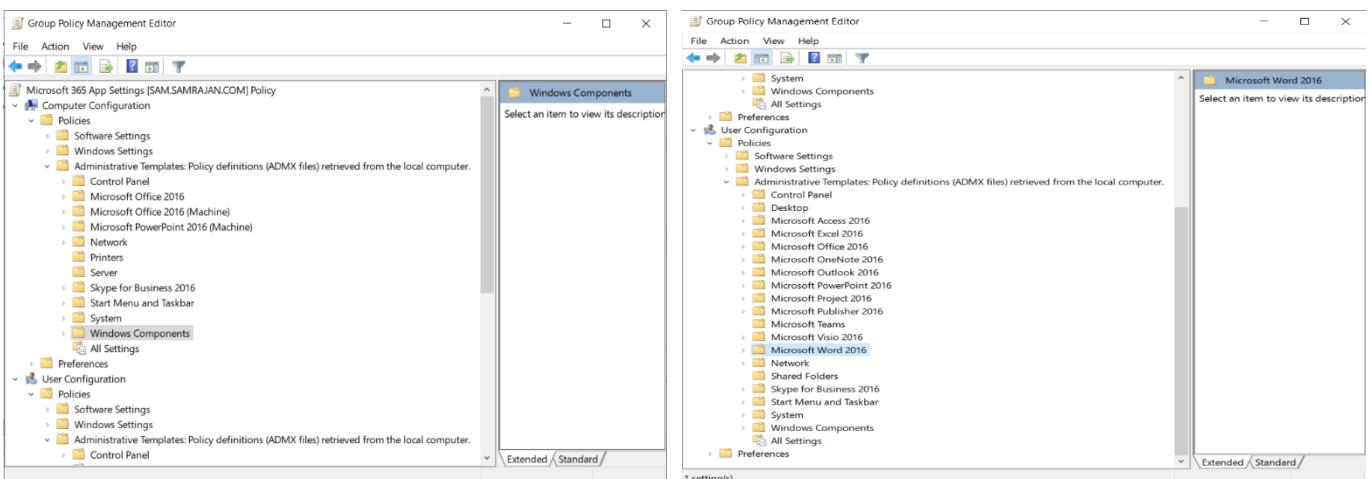
The files were copied and transferred.

Next, the ADML files were copied and transferred from C:\admx\admx\en-us to C:\Windows\PolicyDefinitions\en-US.

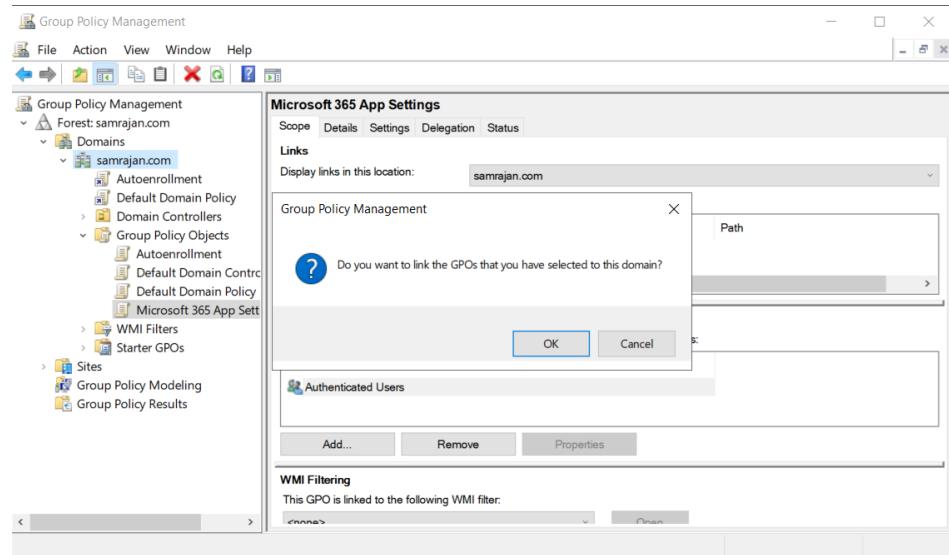


The files were copied and transferred.

Then, a Group Policy Object (GPO) was created in Server Manager (Tools > Group Policy Management). It was named Microsoft 365 App Settings. Upon right-clicking the group policy and clicking Edit, the policies could be seen under Computer Configuration > Policies > Administrative Templates. More policies could also be seen under User Configuration > Policies > Administrative Templates.



The Microsoft 365 App Settings GPO could then be dragged and dropped over the company domain (samrajan.com).



The dragged and dropped GPO was linked after clicking the OK button.

Apps were also deployed using platform-specific app stores. For example, Adobe Acrobat Reader DC was deployed as a Microsoft Store app and Adobe Acrobat Reader: Edit PDF was deployed as an iOS store app.

A screenshot of the Microsoft Intune 'Apps | All apps' page. The left sidebar shows a navigation tree with 'All apps' selected. The main area displays a table of deployed apps. The columns are 'Name', 'Type', 'Status', 'Version', and 'Assigned'. The table includes rows for 'Adobe Acrobat Reader DC' (Microsoft Store app), 'Adobe Acrobat Reader: Edit PDF' (iOS store app), 'Intune Company Portal' (Managed Google Play store app), 'Managed Home Screen' (Managed Google Play store app), 'Microsoft 365 Apps for Windows...' (Microsoft 365 Apps (Windows 1...)), 'Microsoft Authenticator' (Managed Google Play store app), 'Microsoft Intune' (Managed Google Play store app), 'Microsoft Intune Company Portal' (iOS store app), and 'Microsoft Launcher' (Managed Google Play store app). Each row has a '...' button for more options.

App Protection and App Configuration Policies

App protection policies (APP) in Intune are rules which keep an organization's data safe or contained in a managed app. These policies allow control over how data is accessed and shared by apps on mobile devices. APPs were configured for both iOS and Android devices by navigating to Apps > App protection policies > Create policy.

The screenshot shows the configuration interface for an App Protection Policy (APP). It is divided into several sections:

- Basics Edit**:
 - Name: iOS App Protection Settings
 - Description: No Description
 - Platform: iOS/iPadOS
- Apps Edit**:
 - Target to apps on all device types: Yes
 - Device types: No Device types
 - Public apps: Adobe Acrobat Reader
 - Custom apps: No Custom apps
- Data protection Edit**:
 - Prevent backups: Block
 - Send org data to other apps: All Apps
 - Select apps to exempt:
 - Select universal links to exempt:
 - http://facetime.apple.com
 - http://maps.apple.com
 - https://facetime.apple.com
 - https://maps.apple.com
 - http://*.appsplatform.us/*
 - http://*.onedrive.com/*
 - http://*.powerapps.cn/*
 - http://*.powerapps.us/*
 - http://*.powerbi.com/*
 - http://*.service-now.com/*
 - http://*.sharepoint-df.com/*
 - http://*.sharepoint.com/*
 - http://*.yammer.com/*
 - http://*.zoom.us/*
 - http://collab.apps.mil/l/*
 - http://devspaces.skype.com/l/*
 - http://teams-fl.microsoft.com/l/*
 - http://teams.live.com/l/*
 - http://teams.microsoft.com/l/*
 - http://teams.microsoft.us/l/*
 - http://app.powerbi.cn/*
 - http://app.powerbi.de/*
 - http://app.powerbigov.us/*
 - http://msit.microsoftstream.com/video/*
 - http://tasks.office.com/*
 - http://to-do.microsoft.com/sharing/*
 - http://web.microsoftstream.com/video/*
 - http://zoom.us/*
 - https://*.appsplatform.us/*
 - https://*.onedrive.com/*
 - https://*.powerapps.cn/*
 - https://*.powerapps.com/*
 - https://*.powerbi.us/*
 - https://*.powerbi.com/*
 - https://*.service-now.com/*
 - https://*.sharepoint-df.com/*
 - https://*.sharepoint.com/*
 - https://*.yammer.com/*
 - https://*.zoom.us/*
 - https://collab.apps.mil/l/*
 - https://devspaces.skype.com/l/*
 - https://teams-fl.microsoft.com/l/*
 - https://teams.live.com/l/*
 - https://teams.microsoft.com/l/*
 - https://teams.microsoft.us/l/*
 - https://app.powerbi.cn/*
 - https://app.powerbi.de/*
 - https://app.powerbigov.us/*
 - https://msit.microsoftstream.com/video/*
 - https://tasks.office.com/*
 - https://to-do.microsoft.com/sharing/*
 - https://web.microsoftstream.com/video/*
 - https://zoom.us/*
 - Select managed universal links:
 - http://*.appsplatform.us/*
 - https://*.onedrive.com/*
 - https://*.powerapps.cn/*
 - https://*.powerapps.com/*
 - https://*.powerbi.us/*
 - https://*.powerbi.com/*
 - https://*.service-now.com/*
 - https://*.sharepoint-df.com/*
 - https://*.sharepoint.com/*
 - https://*.yammer.com/*
 - https://*.zoom.us/*
 - https://collab.apps.mil/l/*
 - https://devspaces.skype.com/l/*
 - https://teams-fl.microsoft.com/l/*
 - https://teams.live.com/l/*
 - https://teams.microsoft.com/l/*
 - https://teams.microsoft.us/l/*
 - https://app.powerbi.cn/*
 - https://app.powerbi.de/*
 - https://app.powerbigov.us/*
 - https://msit.microsoftstream.com/video/*
 - https://tasks.office.com/*
 - https://to-do.microsoft.com/sharing/*
 - https://web.microsoftstream.com/video/*
 - https://zoom.us/*
 - Save copies of org data: Allow
 - Allow user to save copies to selected services: No Allow user to save copies to selected services
 - Transfer telecommunication data to:
 - Any dialer app
 - No Dialer App URL Scheme
 - Transfer messaging data to:
 - Any messaging app
 - No Messaging App URL Scheme
 - Receive data from other apps: All Apps
 - Open data into Org documents: Allow

Allow users to open data from selected services	OneDrive for Business SharePoint Camera Photo Library	
Restrict cut, copy, and paste between other apps	Blocked	
Cut and copy character limit for any app	0	
Third party keyboards	Allow	
Encrypt org data	Require	
Sync policy managed app data with native apps or add-ins	Allow	
Printing org data	Allow	
Restrict web content transfer with other apps	Any app	
Unmanaged browser protocol	No Unmanaged browser protocol	
Org data notifications	Allow	
Access requirements Edit		
PIN for access	Require	
PIN type	Numeric	
Simple PIN	Allow	
Select minimum PIN length	6	
Touch ID instead of PIN for access (iOS 8+ /iPadOS)	Allow	
Override biometrics with PIN after timeout	Require	
Timeout (minutes of inactivity)	30	
Face ID instead of PIN for access (iOS 11+ /iPadOS)	Allow	
PIN reset after number of days	No	
Number of days	0	
App PIN when device PIN is set	Require	
Work or school account credentials for access	Not required	
Recheck the access requirements after (minutes of inactivity)	30	
Conditional launch Edit		
Setting	Value	Action
Max PIN attempts	5	Reset PIN
Offline grace period	720	Block access (minutes)
Offline grace period	90	Wipe data (days)
Jailbroken/rooted devices		Block access
Assignments Edit		
Included groups		
Group	Filter	Filter mode
Company Users and Devices	None	None
Excluded groups		
Group		
No results.		
Scope tags Edit		
Default		

The APP for iOS devices.

Basics [Edit](#)

Name	Android Device App Restrictions
Description	No Description
Platform	Android

Apps [Edit](#)

Target to apps on all device types	Yes
Device types	No Device types
Public apps	Adobe Acrobat Reader
Custom apps	No Custom apps

Data protection [Edit](#)

Prevent backups	Block
Send org data to other apps	All Apps
Select apps to exempt	No Select apps to exempt
Save copies of org data	Allow
Allow user to save copies to selected services	No Allow user to save copies to selected services
Transfer telecommunication data to	Any dialer app
Dialer App Package ID	No Dialer App Package ID
Dialer App Name	No Dialer App Name
Transfer messaging data to	Any messaging app
Messaging App Package ID	No Messaging App Package ID
Messaging App Name	No Messaging App Name
Receive data from other apps	All Apps
Open data into Org documents	Allow
Allow users to open data from selected services	OneDrive for Business SharePoint Camera Photo Library
Restrict cut, copy, and paste between other apps	Blocked
Cut and copy character limit for any app	0
Screen capture and Google Assistant	Enable
Approved keyboards	Not required
Select keyboards to approve	No Select keyboards to approve
Encrypt org data	Require
Encrypt org data on enrolled devices	Require
Sync policy managed app data with native apps or add-ins	Allow
Printing org data	Allow
Restrict web content transfer with other apps	Any app
Unmanaged Browser ID	No Unmanaged Browser ID
Unmanaged Browser Name	No Unmanaged Browser Name
Org data notifications	Allow
Start Microsoft Tunnel connection on app-launch	No

Access requirements [Edit](#)

PIN for access	Require
PIN type	Numeric
Simple PIN	Allow
Select minimum PIN length	6
Biometrics instead of PIN for access	Allow
Override biometrics with PIN after timeout	Require
Timeout (minutes of inactivity)	30
Class 3 Biometrics (Android 9.0+)	Not required
Override Biometrics with PIN after biometric updates	Not required
PIN reset after number of days	No
Number of days	0
Select number of previous PIN values to maintain	0
App PIN when device PIN is set	Require
Work or school account credentials for access	Not required

Recheck the access requirements after 30 minutes of inactivity

Conditional launch [Edit](#)

Setting	Value	Action
Max PIN attempts	5	Reset PIN
Offline grace period	720	Block access (minutes)
Offline grace period	90	Wipe data (days)
Jailbroken/rooted devices		Block access

Assignments [Edit](#)

Included groups

Group	Filter	Filter mode
Company Users and Devices	None	None

Excluded groups

Group
No results.

Scope tags [Edit](#)

Default

APP for Android devices. This APP specifically outlines app restrictions.

App protection policies can have conditional access policies configured for them. In this case, a conditional access policy which makes app protection a requirement was configured.

Require App Protection

Conditional Access policy

[Delete](#) [View policy information](#)

Name *
Require App Protection

Assignments

Users [\(1\)](#)
Specific users included

Target resources [\(1\)](#)
No target resources selected

Network [\(1\)](#)
Not configured

Conditions [\(1\)](#)
1 condition selected

Access controls

Enable policy
[Report-only](#) [On](#) [Off](#)

Include **Exclude**

- None
- All users
- Select users and groups
 - Guest or external users [\(1\)](#)
 - Directory roles [\(1\)](#)
 - Users and groups

Select
1 user

KW Kim Wexler
kimwexler@samrajan659.on...

Require App Protection

Conditional Access policy

[Delete](#) [View policy information](#)
decisions, and enforce organizational policies.
[Learn more](#) [Edit](#)

Name *
Require App Protection

Assignments

Users [\(1\)](#)
Specific users included

Target resources [\(1\)](#)
No target resources selected

Network [\(1\)](#)
Not configured

Conditions [\(1\)](#)
1 condition selected

device state [Learn more](#) [Edit](#)

Device platforms [\(1\)](#)
2 included

Locations [\(1\)](#)
Not configured

Client apps [\(1\)](#)
Not configured

Filter for devices [\(1\)](#)
Not configured

Authentication flows (Preview) [\(1\)](#)
Not configured

Apply policy to selected device platforms. [Learn more](#) [Edit](#)

Configure [\(1\)](#)
[Yes](#) [No](#)

Include **Exclude**

- Any device
- Select device platforms
 - Android
 - iOS
 - Windows Phone
 - Windows
 - macOS
 - Linux

Require App Protection ...

Conditional Access policy

[Delete](#) [View policy information](#)

Target resources ⓘ

No target resources selected

Network NEW ⓘ

Not configured

Conditions ⓘ

1 condition selected

Access controls

Grant ⓘ

1 control selected

Session ⓘ

0 controls selected

Enable policy

Report-only **On** Off

Save **Select**

Control access enforcement to block or grant access. [Learn more](#) ⓘ

Block access

Grant access

Require multifactor authentication ⓘ

Require authentication strength ⓘ

Require device to be marked as compliant ⓘ

Require Microsoft Entra hybrid joined device ⓘ

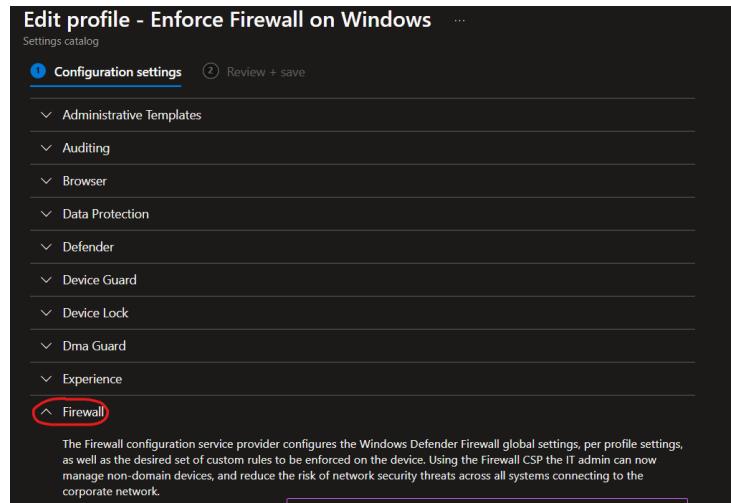
Require approved client app
[See list of approved client apps](#) ⓘ

Require app protection policy
[See list of policy protected client apps](#) ⓘ

This conditional access policy was configured for both iOS and Android devices to require app protection.

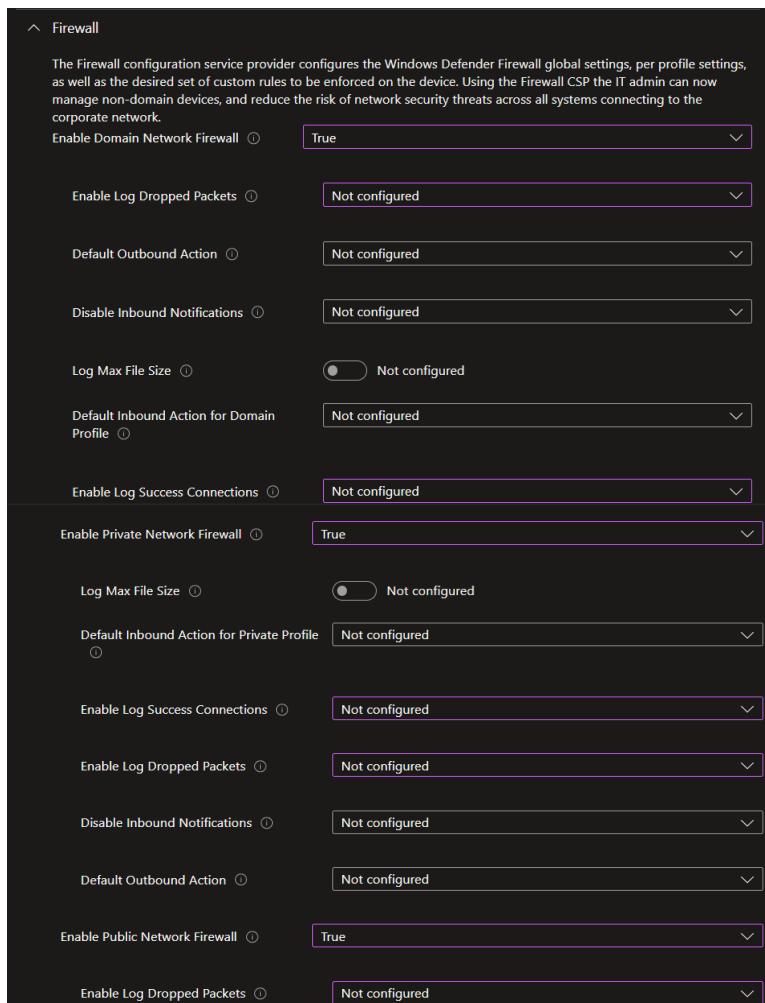
Configuring Endpoint Security

Security baselines are a group of preconfigured Windows settings that can be customized to help protect users and Windows devices. One of these baselines configured was used to enforce firewall for Windows 10 and later devices. This was accomplished by navigating to Endpoint Security > Security baselines > Security Baseline for Windows 10 and later > Create profile.

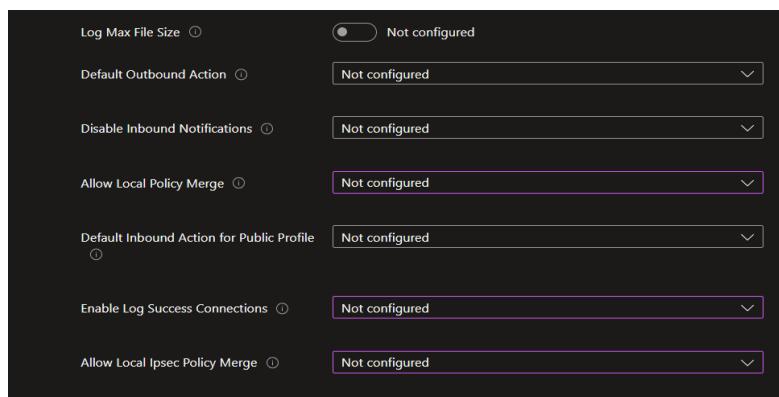


The screenshot shows the 'Edit profile - Enforce Firewall on Windows' configuration settings page. The 'Configuration settings' tab is selected. On the left, there's a tree view with categories like Administrative Templates, Auditing, Browser, Data Protection, Defender, Device Guard, Device Lock, Dma Guard, Experience, and Firewall. The 'Firewall' category is highlighted with a red oval. Below the tree view, there's a descriptive text about the Firewall configuration service provider. At the top right, there's a 'Review + save' button.

All settings except for the firewall settings were set to “Not configured”. This was done to remove any default recommended settings and ensure only the firewall settings were configured.



The screenshot shows the 'Edit profile - Enforce Firewall on Windows' configuration settings page. The 'Firewall' section is expanded. Under 'Firewall', there are several settings listed with their current values: 'Enable Domain Network Firewall' is set to 'True'; 'Enable Log Dropped Packets' and 'Default Outbound Action' are both set to 'Not configured'; 'Disable Inbound Notifications' is also set to 'Not configured'; 'Log Max File Size' has a toggle switch set to 'Not configured'; 'Default Inbound Action for Domain Profile' is set to 'Not configured'; 'Enable Log Success Connections' is set to 'Not configured'; 'Enable Private Network Firewall' is set to 'True'; 'Log Max File Size' for Private Profile has a toggle switch set to 'Not configured'; 'Default Inbound Action for Private Profile' is set to 'Not configured'; 'Enable Log Success Connections' for Private Profile is set to 'Not configured'; 'Enable Log Dropped Packets' for Private Profile is set to 'Not configured'; 'Disable Inbound Notifications' for Private Profile is set to 'Not configured'; 'Default Outbound Action' for Private Profile is set to 'Not configured'; 'Enable Public Network Firewall' is set to 'True'; and 'Enable Log Dropped Packets' for Public Network is set to 'Not configured'.



By navigating to Endpoint Security > Security baselines > Security Baseline for Windows 10 and later > Enforce Firewall on Windows > View report, it was confirmed that the baseline was successfully applied to the Windows 11 client (SR-CL1).

Success	Conflict	Error	Pending	Not applicable	Total
1	0	0	0	0	1

Report generated on: 10/14/2024, 12:33:02 AM

Showing 1 to 1 of 1 records

Device name	Last active user	Assignment status	Last report modification time
SR-CL1	SamRajan@samrajan659.onmicrosoft.com	Success	Sun Oct 13 2024 23:43:59 GMT-0400 (Eastern Daylight Time)

An antivirus policy was configured by navigating to Endpoint Security > Antivirus > Create Policy.

The policy covers settings for the Engine, Platform, and Security Intelligence update channels.

Devices can be onboarded to Microsoft Defender for Endpoint which is an endpoint security platform designed to help prevent, detect, investigate, and respond to advanced threats. The first step in doing this was to go to security.microsoft.com and navigate to System > Settings > Endpoints > Advanced Features and enable a Microsoft Intune connection.

Endpoints

General

Advanced features

Licenses

Email notifications

Permissions

Roles

Device groups

APIs

SIEM

Rules

Microsoft Intune connection

Authenticated telemetry

Preview features

Save preferences

After this, there was verification in Intune (Endpoint Security > Microsoft Defender for Endpoint) that the connection status displayed as "Enabled". Settings for Microsoft Defender for Endpoint were also configured here.

Connection status

Last synchronized

Enabled

Endpoint Security Profile Settings

Allow Microsoft Defender for Endpoint to enforce Endpoint Security Configurations

Off On

Compliance policy evaluation

Connect Android devices version 6.0.0 and above to Microsoft Defender for Endpoint

Off On

Connect iOS/iPadOS devices version 13.0 and above to Microsoft Defender for Endpoint

Off On

Connect Windows devices version 10.0.15063 and above to Microsoft Defender for Endpoint

Off On

Enable App Sync (sending application inventory) for iOS/iPadOS devices

Off On

Send full application inventory data on personally owned iOS/iPadOS devices

Off On

Block unsupported OS versions

Off On

App protection policy evaluation

Connect Android devices to Microsoft Defender for Endpoint

Off On

Connect iOS/iPadOS devices to Microsoft Defender for Endpoint

Off On

Shared settings

Number of days until partner is unresponsive

7

Then, a policy for endpoint detection and response which specified an automatic response was configured. This was accomplished by navigating to Endpoint Security > Endpoint detection and response > Create policy.

The screenshot shows the 'Properties' screen for a new policy. It includes sections for 'Basics', 'Assignments', 'Scope tags', and 'Configuration settings'.

Basics

Name	Company Onboard Devices for Defender for Endpoint
Description	No Description
Platform	Windows

Assignments

Included groups

Group	Filter	Filter mode
Company Users and Devices	None	None

Excluded groups

Group
No results.

Scope tags

Selected tags	Default
---------------	---------

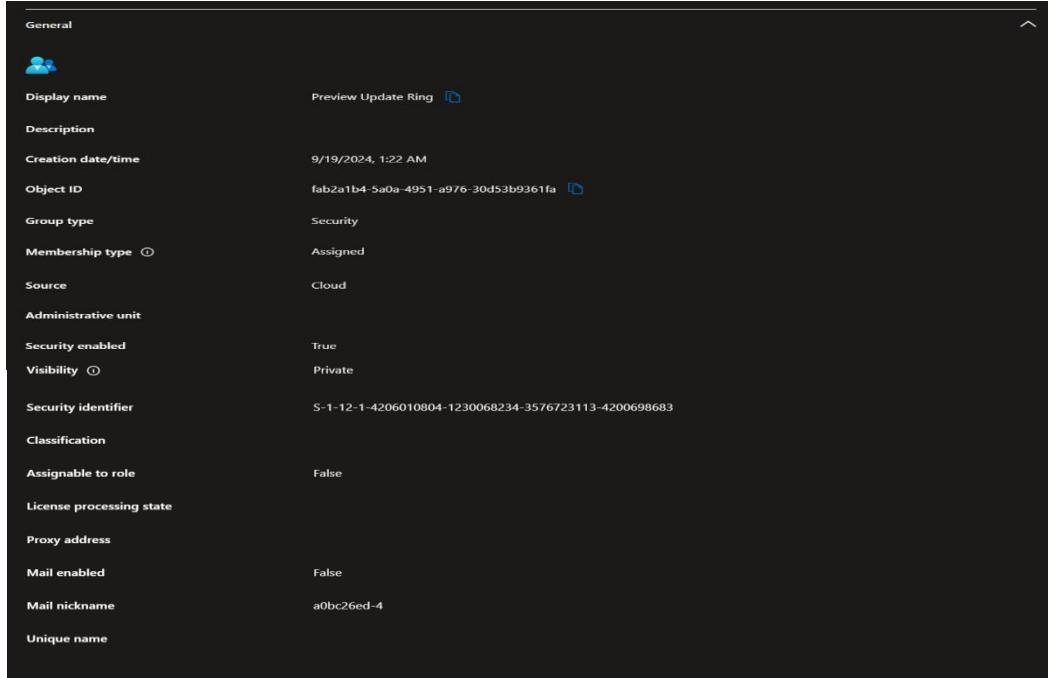
Configuration settings

Microsoft Defender for Endpoint

Microsoft Defender for Endpoint client configuration package type	Auto from connector
---	---------------------

Managing Device Updates by Using Intune

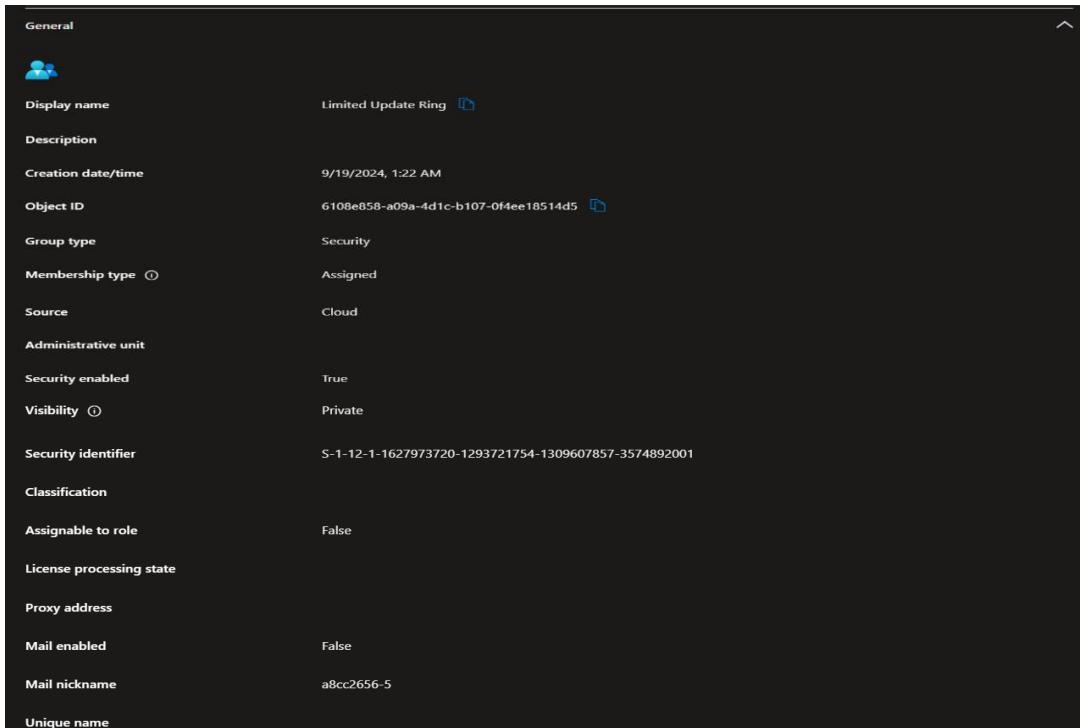
Update rings in Intune are used to specify how and when Windows as a Service updates Windows 10/11 devices with feature and quality updates. Firstly, three groups were created in Intune (Groups > New group) for different update ring types.



The screenshot shows the 'General' settings for a group named 'Preview Update Ring'. The group type is set to 'Security' and 'Assigned' membership type. It has a 'Cloud' source and is part of the 'Administrative unit'. Security is enabled, and visibility is set to 'Private'. The security identifier is S-1-12-1-4206010804-1230068234-3576723113-4200698683. The unique name is a0bc26ed-4.

Setting	Value
Display name	Preview Update Ring
Description	
Creation date/time	9/19/2024, 1:22 AM
Object ID	fab2a1b4-5a0a-4951-a976-30d53b9361fa
Group type	Security
Membership type	Assigned
Source	Cloud
Administrative unit	
Security enabled	True
Visibility	Private
Security identifier	S-1-12-1-4206010804-1230068234-3576723113-4200698683
Classification	
Assignable to role	False
License processing state	
Proxy address	
Mail enabled	False
Mail nickname	a0bc26ed-4
Unique name	

The “Preview” update ring group.



The screenshot shows the 'General' settings for a group named 'Limited Update Ring'. The group type is set to 'Security' and 'Assigned' membership type. It has a 'Cloud' source and is part of the 'Administrative unit'. Security is enabled, and visibility is set to 'Private'. The security identifier is S-1-12-1-1627973720-1293721754-1309607857-3574892001. The unique name is a8cc2656-5.

Setting	Value
Display name	Limited Update Ring
Description	
Creation date/time	9/19/2024, 1:22 AM
Object ID	6108e858-a09a-4d1c-b107-0f4ee18514d5
Group type	Security
Membership type	Assigned
Source	Cloud
Administrative unit	
Security enabled	True
Visibility	Private
Security identifier	S-1-12-1-1627973720-1293721754-1309607857-3574892001
Classification	
Assignable to role	False
License processing state	
Proxy address	
Mail enabled	False
Mail nickname	a8cc2656-5
Unique name	

Limited” update ring group.

General	
Display name	Broad Update Ring
Description	
Creation date/time	9/19/2024, 1:24 AM
Object ID	cf69c0f0-2487-4057-b7cc-05e0d4578703
Group type	Security
Membership type	Assigned
Source	Cloud
Administrative unit	
Security enabled	True
Visibility	Private
Security identifier	S-1-12-1-3479814384-1079452807-3758476471-59201492
Classification	
Assignable to role	False
License processing state	
Proxy address	
Mail enabled	False
Mail nickname	f8cf87f-8
Unique name	

The “Broad” update ring group.

The policy settings for Windows feature updates were configured by navigating to Devices > Windows Updates > Feature updates > Create profile.

The screenshot shows the 'Production for Windows 11 | Properties' window. The left sidebar has a 'Manage' section with 'Properties' selected. The main area displays deployment settings and assignments.

Deployment settings

- Name: Production for Windows 11
- Description: No Description
- Feature deployment settings:
 - Name: Windows 11, version 23H2
 - Rollout options: ImmediateStart
 - Required or optional update: Required
 - Install Windows 10 on devices not eligible to run Windows 11: Enabled

Scope tags

- Default

Assignments

- Included groups: Company Users and Devices
- Excluded groups: No Excluded groups

The feature update policy settings.

The policy settings for Windows quality updates were configured by navigating to Devices > Windows Updates > Quality updates > Create profile.

The screenshot shows the 'Production Quality Updates' Properties window in the Microsoft Intune portal. The left sidebar has 'Overview', 'Manage', and 'Properties' sections, with 'Properties' selected. The main area shows the following configuration:

- Name:** Production Quality Updates
- Description:** No Description
- Expedite installation of quality updates if device OS version less than:** 09/10/2024 - 2024.09 B SecurityUpdate for Windows 10 and later
- Number of days to wait before restart is enforced:** 1 day
- Scope tags:** Default
- Assignments:** Company Users and Devices (Included groups), No Excluded groups (Excluded groups)

The quality update policy settings.

Upon opening the Settings app on the Windows 11 client machine and navigating to Accounts > Access Work or School > Managed by samrajan (under registered work/school account) > Info, updates were seen among the areas managed by samrajan (the domain). Thus, this confirmed that the policy settings were applied successfully.

The screenshot shows the Windows Settings app interface. The top bar includes a back arrow, the word 'Settings', and a search bar. The user profile 'Sam Rajan' is displayed. The main content area is titled 'Managed by samrajan' with the sub-instruction: 'Connecting to work or school allows your organization to control some things on this device, such as settings and applications.' Below this, there's a section titled 'Areas managed by samrajan' which lists several settings categories: System, Bluetooth & devices, Network & internet, Personalization, Apps, Accounts (which is highlighted in light blue), Time & language, Gaming, and Accessibility. To the right of this list, under 'Policies', is a bulleted list of managed items, including 'Update' (which is circled in red).

- ADMX_Desktop
- Camera
- DeliveryOptimization
- Experience
- Update**
- Defender
- DeviceLock
- DeviceHealthMonitoring
- Security
- System

Update settings for Android devices were configured by navigating to Devices > Configuration > Policies > Create.

The screenshot shows the 'Properties' screen for an Android update policy named 'Android Update Settings'. The 'Basics' tab is selected, showing details like Name, Description, Platform, and Profile type. The 'Assignments' tab is also visible. The 'Included groups' section lists 'Company Users and Devices' with a filter of 'None' and mode 'None'. The 'Excluded groups' section shows 'No results.'. The 'Scope tags' section has a single entry 'Default'. Under 'Configuration settings', there are sections for 'General' (System update set to 'Automatic') and 'System security' (Threat scan on apps set to 'Require').

Update settings for iOS/iPadOS devices were also configured by navigating to Devices > Apple Updates > iOS/iPadOS update policies > Create profile.

The screenshot shows the 'iOS/iPadOS Updates | Properties' screen. The 'Properties' tab is selected in the sidebar. The 'Overview' section shows the name 'iOS/iPadOS Updates' and 'No Description'. The 'Update policy settings' section includes 'Update to install' (set to 'Install iOS/iPadOS Latest update') and 'Schedule type' (set to 'Update at next check-in'). The 'Assignments' section lists 'Included groups' as 'Company Users and Devices' and 'Excluded groups' as 'No Excluded groups'.

Updates could be managed by navigating to Reports > Windows Updates > Summary.

The screenshot shows the Windows Updates Summary report interface. It displays three main sections:

- Windows Feature updates:** Shows a table with columns: Profile, Versions, In progress, Success, Error, Rollback initiated, and Cancelled. One row is visible: "Production for Wind..." with "Windows 11, version..." under Versions, "1" under In progress, "0" under Success, "0" under Error, "0" under Rollback initiated, and "0" under Cancelled.
- Windows Expedited Quality updates:** Shows a table with columns: Profile, Versions, In progress, Success, Error, and Cancelled. One row is visible: "Production Quality Upd..." with "2024-09-10T00:00:00Z" under Versions, "0" under In progress, "0" under Success, "0" under Error, and "0" under Cancelled.
- Windows Driver updates:** Shows a table with columns: Profile, In progress, Success, Error, Cancelled, Paused, and NeedsReview. A message "Refresh to see data" is displayed.

Each section includes a "Refresh" button and a timestamp indicating when it was last refreshed.

One feature update was in progress of being installed while one quality update was yet to begin installation.

Windows client Delivery Optimization was configured using Intune. Delivery Optimization is a HTTP downloader with a cloud-managed solution that allows Windows devices to download update packages from alternate sources in addition to internet-based servers. This was configured by navigating to Devices > Configuration > Policies > Create.

The screenshot shows the Properties page for a policy named "Company Peer-to-Peer Delivery Updating".

Basics

Name	Company Peer-to-Peer Delivery Updating
Description	No Description
Platform	Windows 10 and later
Profile type	Delivery Optimization

Assignments

Included groups

Group	Filter	Filter mode
Company Users and Devices	None	None

Excluded groups

Group
No results.

Scope tags [Edit](#)

Default

Configuration settings [Edit](#)

^ Delivery Optimization

Download mode	HTTP blended with peering behind same NAT (1)
Bandwidth optimization type	Percentage
Maximum foreground download bandwidth (in %)	20
Maximum background download bandwidth (in %)	30
Minimum RAM required for peer caching (in GB)	2
Minimum disk size required for peer caching (in GB)	2
Minimum content file size for peer caching (in MB)	10
Minimum battery level required to upload (in %)	40
Maximum cache age (in days)	7
Maximum cache size type	Percentage
Maximum cache size (in %)	20
VPN peer caching	Disabled

Applicability Rules [Edit](#)

Rule	Property	Value	Rule Details

Sources

1. Various learn.microsoft.com articles
2. *MD-102 Endpoint Administrator Associate course with SIMS!* by John Christopher (Udemy)