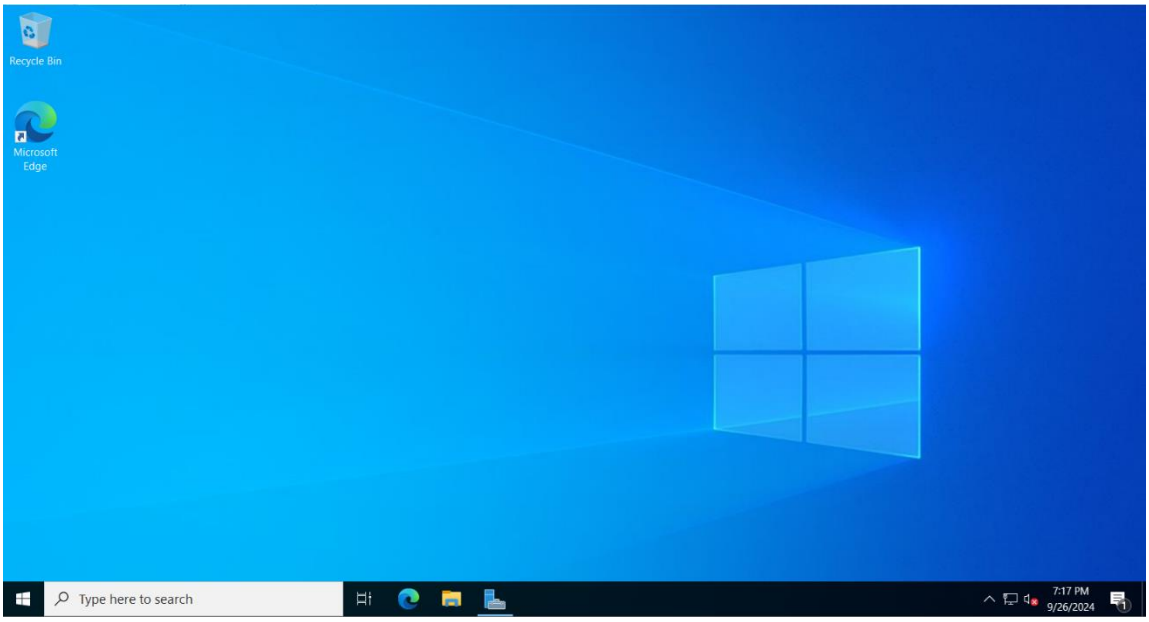
Microsoft Intune/365/Entra ID Home Lab

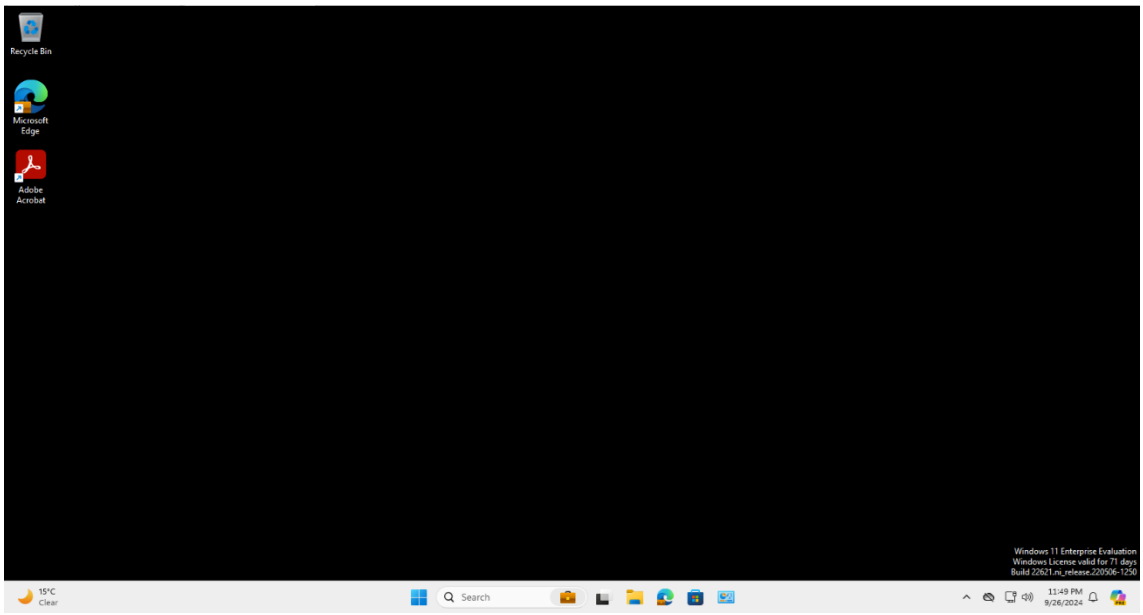
Table of Contents

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.

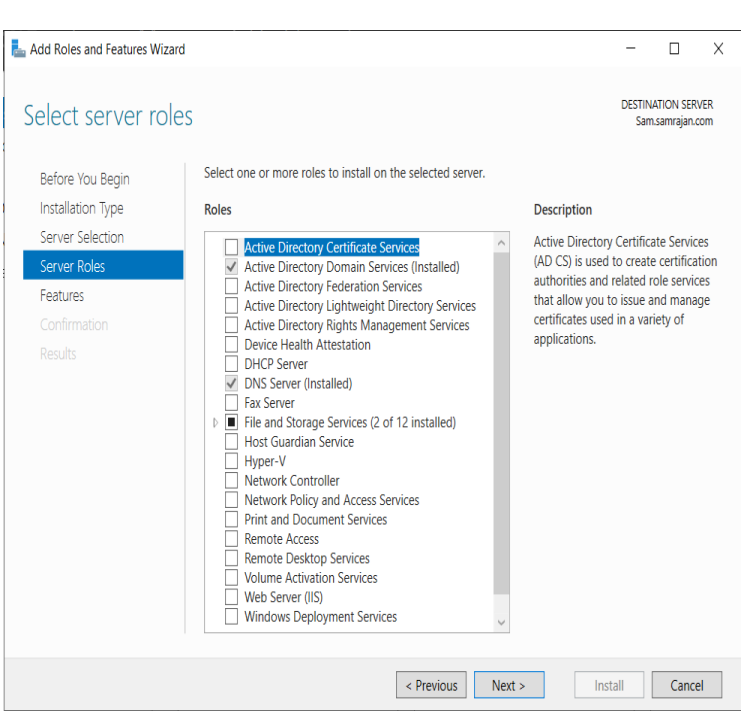


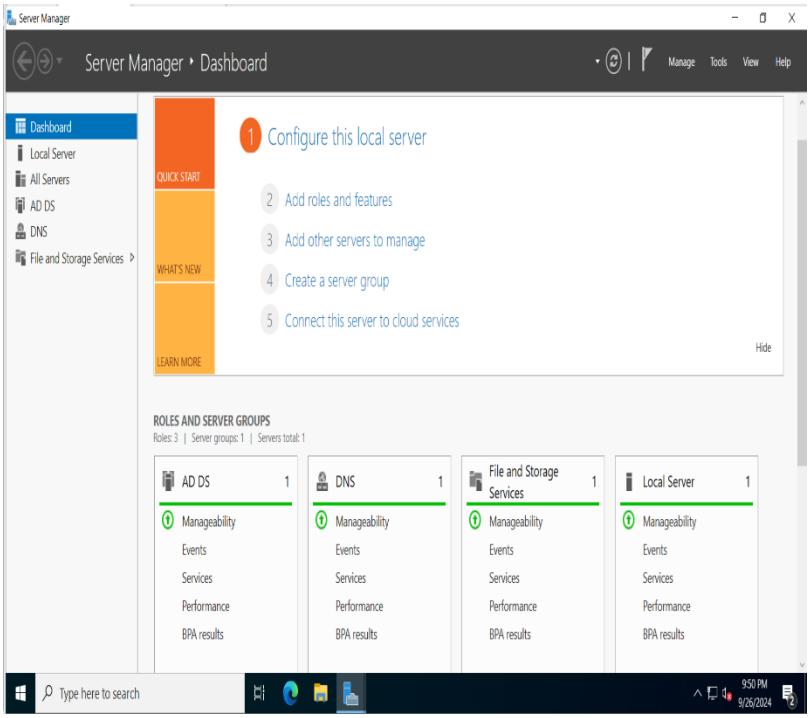
Windows Server 2022 virtual machine



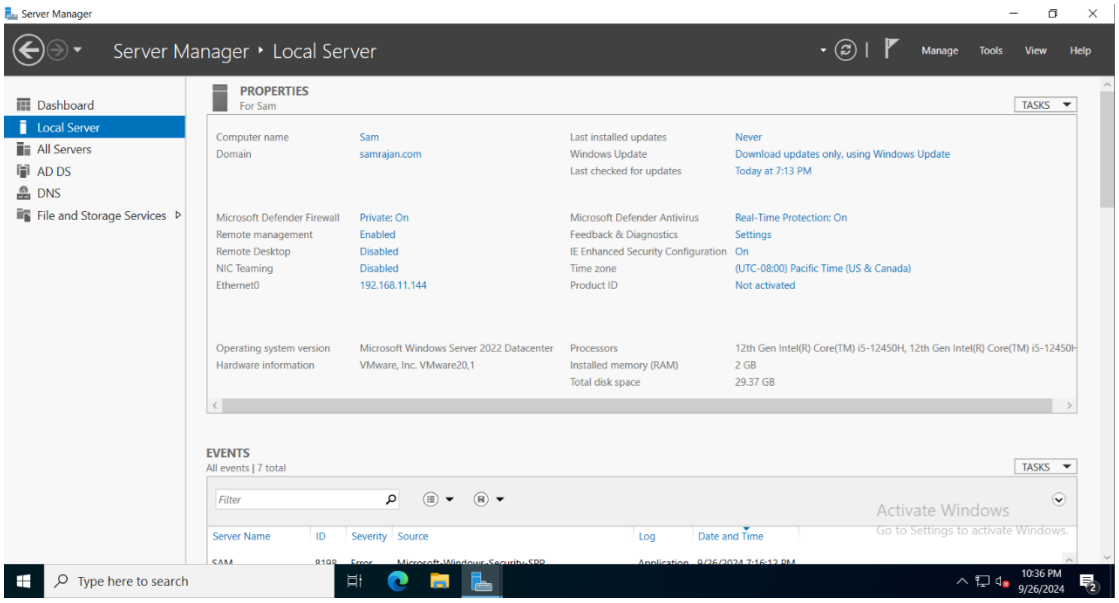
Windows 11 virtual machine

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.

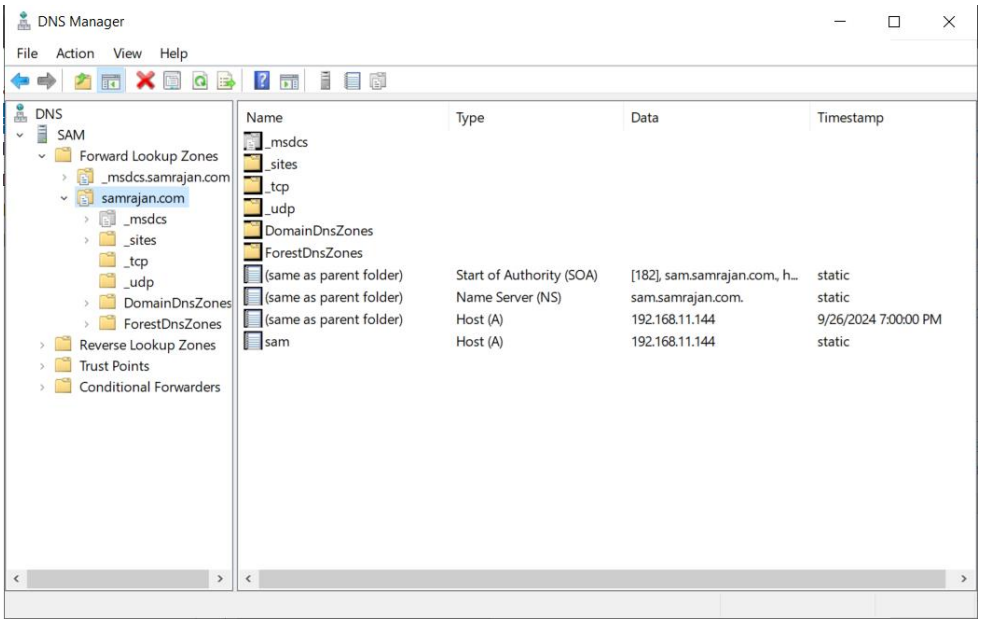




As can be seen in the left image, the Active Directory Domain Services and DNS Server roles have been selected and successfully installed. In the right image, the AD DS (Active Directory Domain Services) and DNS server groups appear in the Server Manager dashboard.

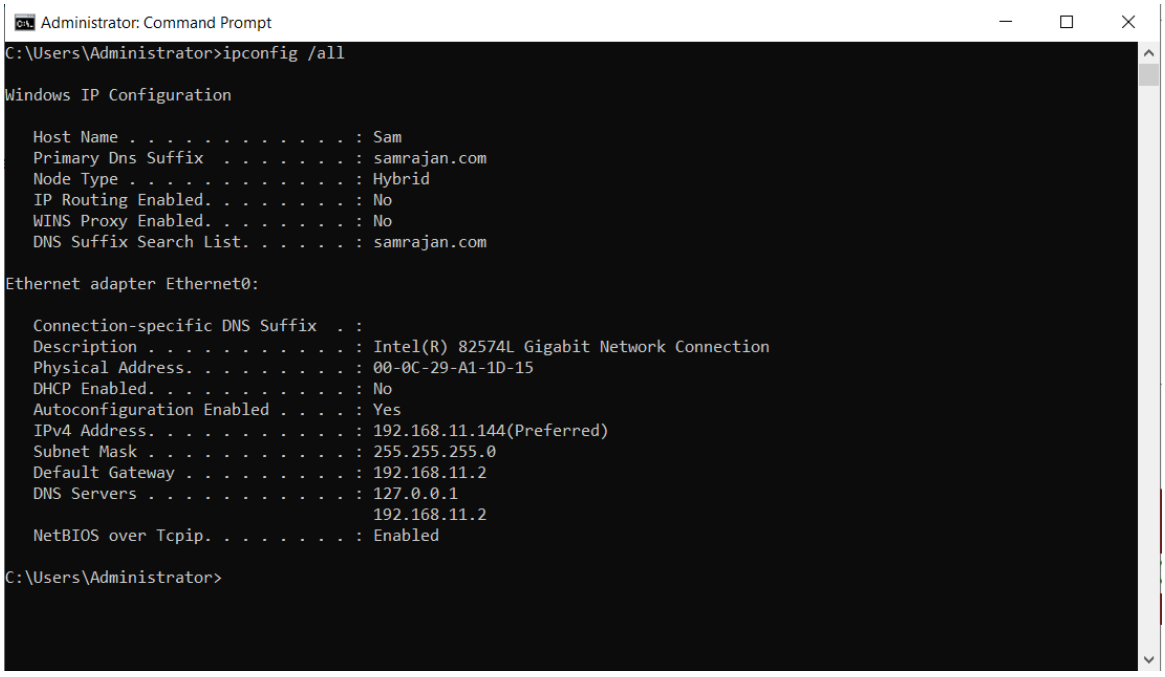


After running the Active Directory Domain Services configuration wizard, the domain name was configured to be “samrajan.com”.

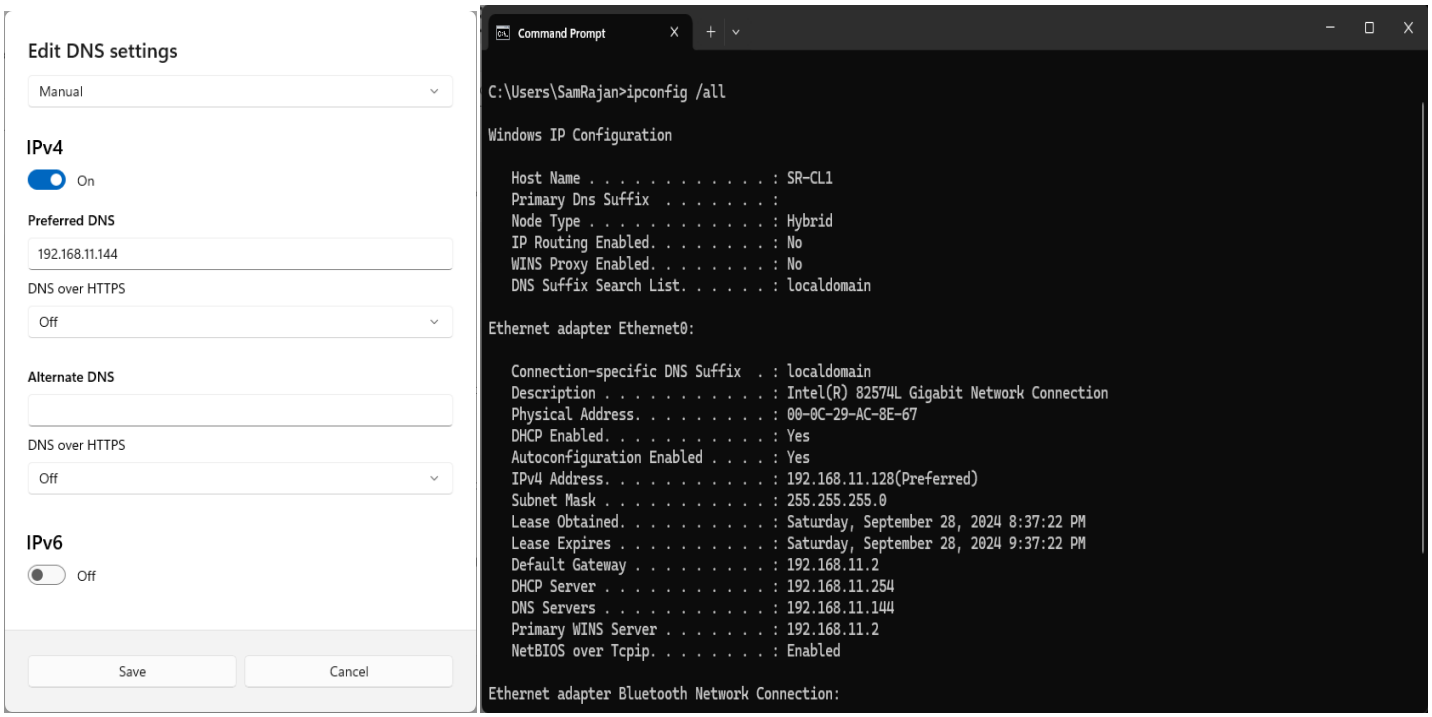


The DNS database (samrajan.com) has been successfully created and populated.

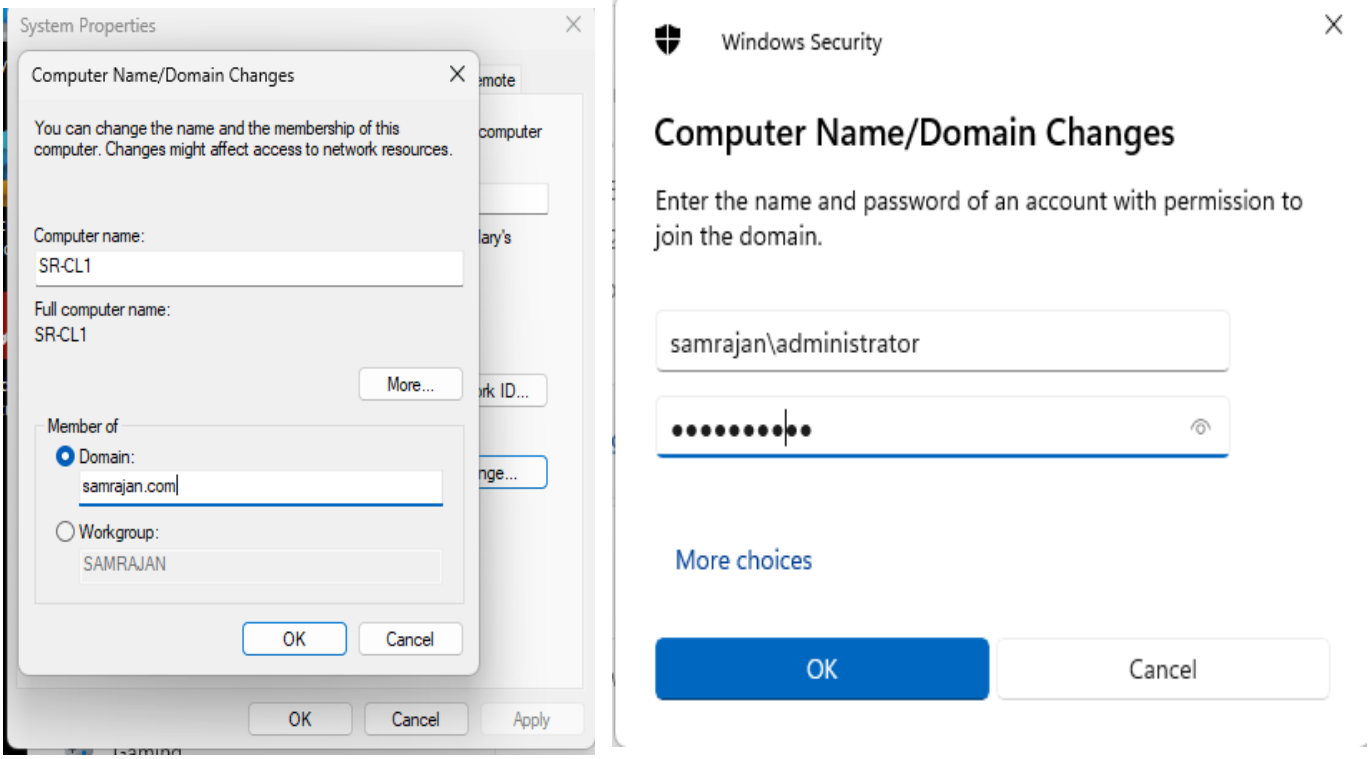
Following the domain controller setup, the next step is to join the Windows 11 device to the domain.



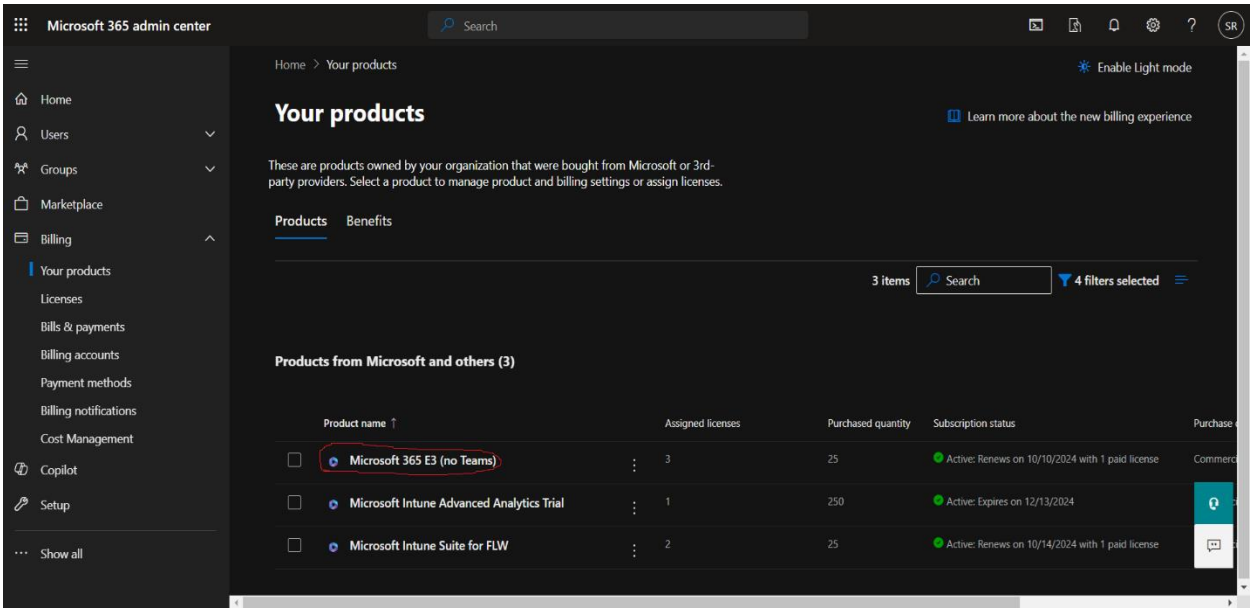
The IP address configured on the server is 192.168.11.144 (manually configured) and in addition it's loopback address (127.0.0.1) is configured to be it's DNS server.



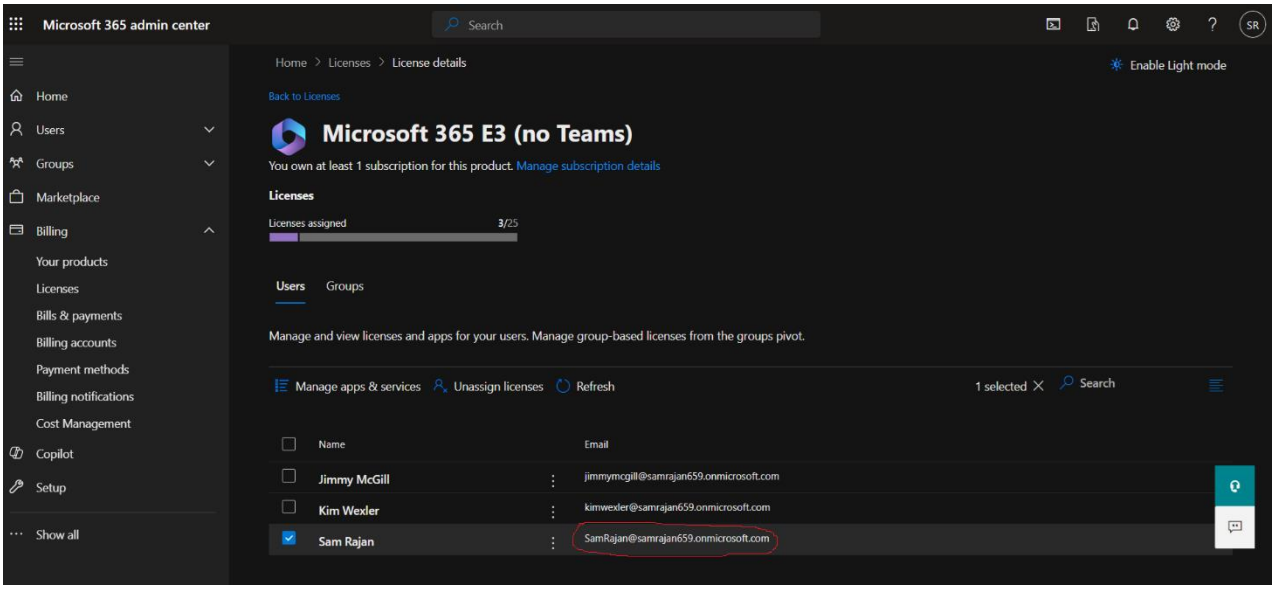
The client must be configured to use the server as the DNS server. As can be seen above, the client's preferred DNS has been manually configured to be 192.168.11.144 which is the server's IP address. In addition, the client's host name has been manually renamed to "SR-CL1".



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.



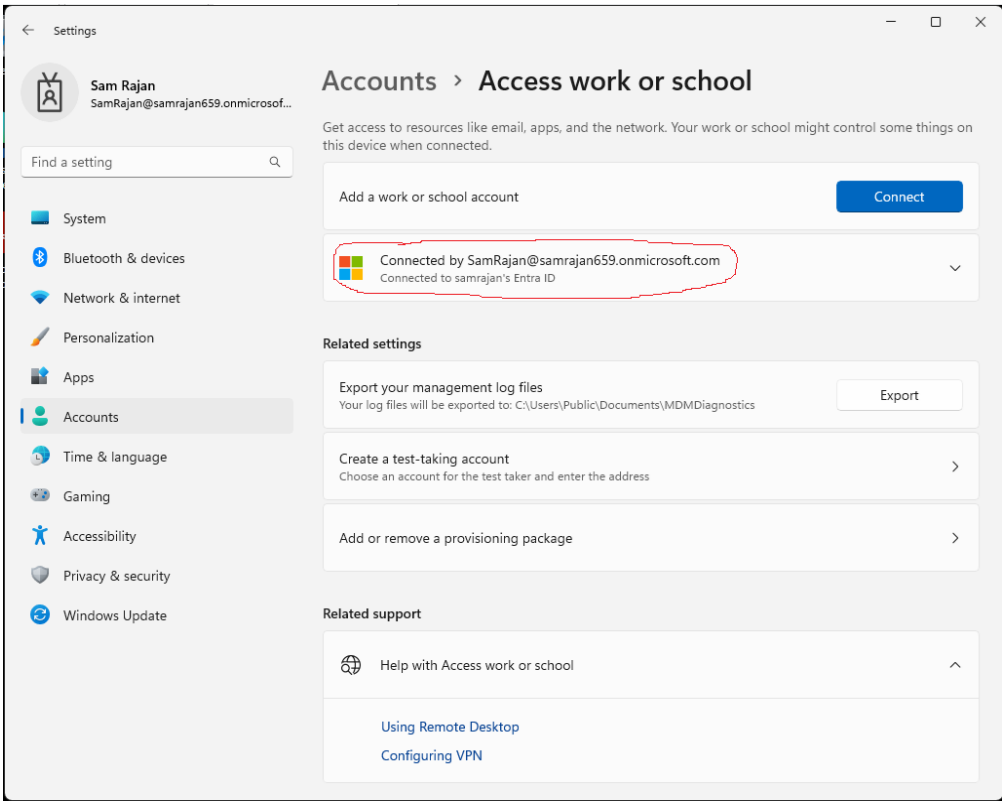
The final step is to register for a free Microsoft 365/Azure account. The default domain name assigned was samrajan659.onmicrosoft.com and the Microsoft 365 license chosen was Microsoft 365 E3 (no Teams) as this was the latest license available which offered a free trial.



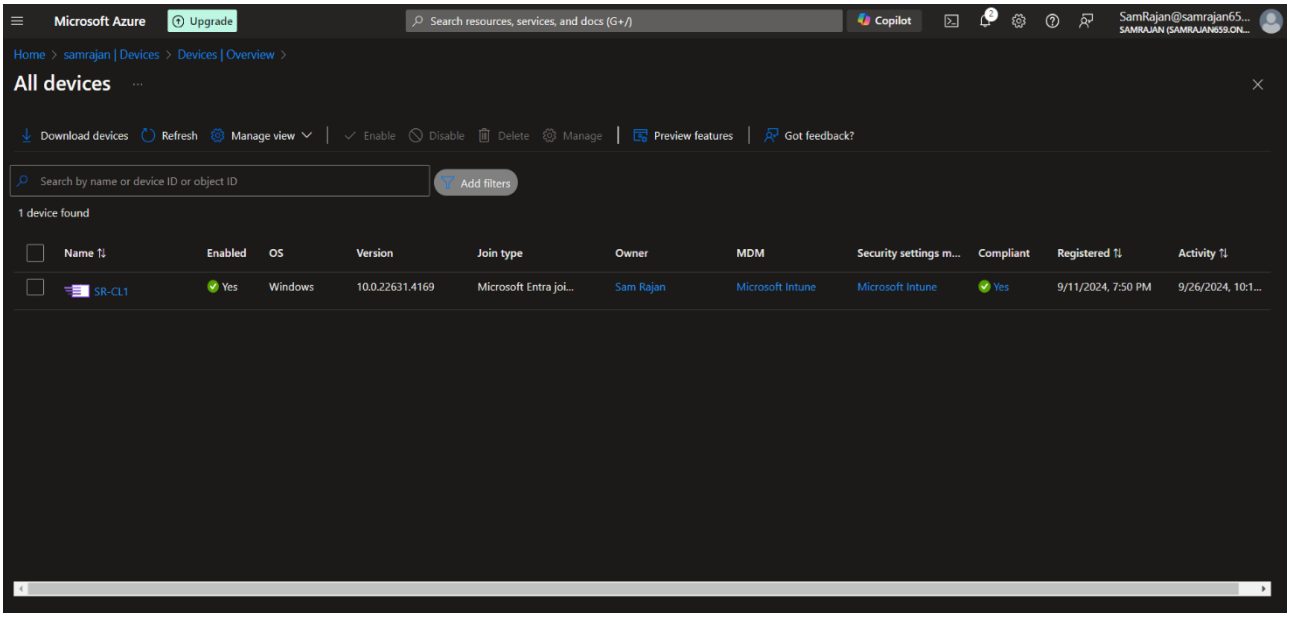
The Microsoft 365 E3 (no Teams) license must be assigned to the global administrator (SamRajan@samrajan659.onmicrosoft.com) in order to access all features of Microsoft 365 such as Intune, Entra ID, etc. Other users can be assigned licences as well (e.g Kim Wexler and Jimmy McGill).

Join Devices to Entra ID and Intune

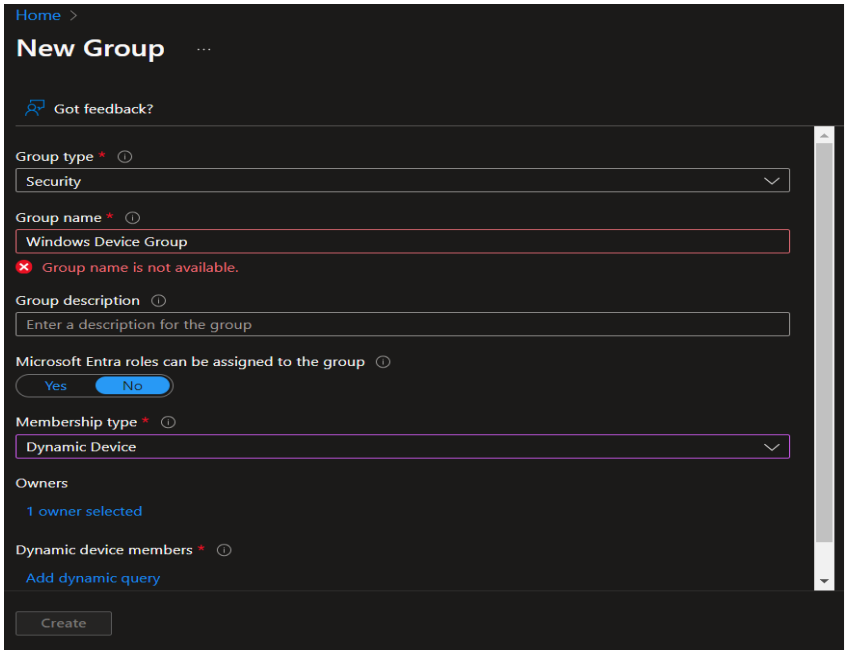
To enroll Windows devices into Entra ID, the device was registered as a work/school account in System > Accounts > Access work or school in order to join the device to Entra ID.



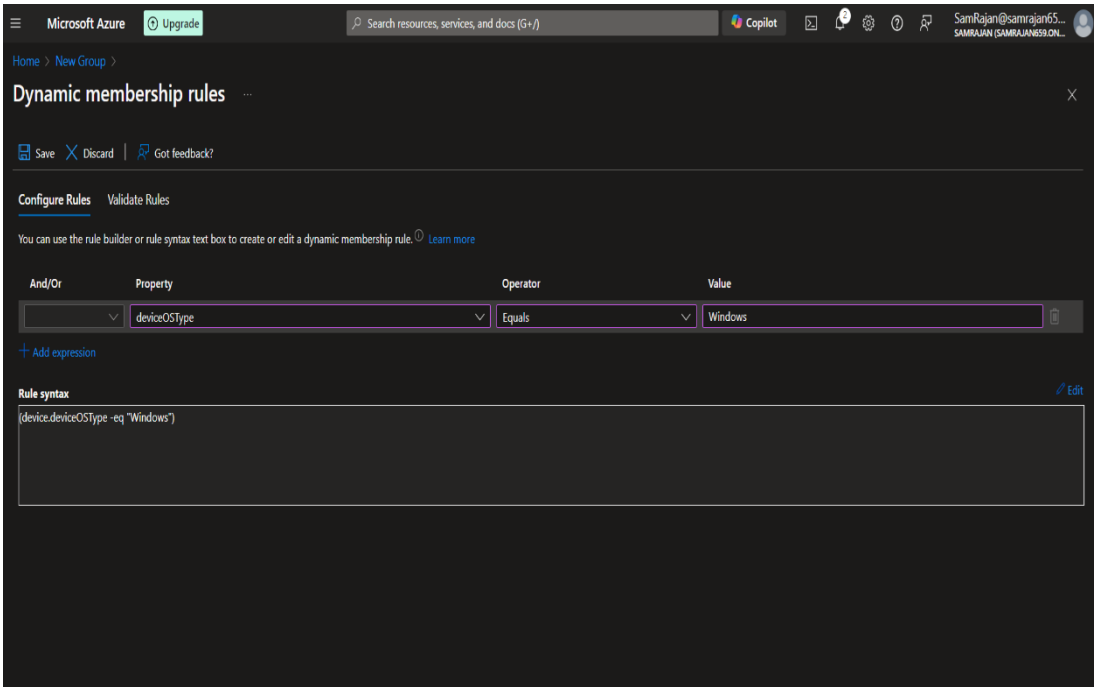
The device join can then be confirmed by accessing portal.azure.com, logging into the global administrator account and navigating to Entra ID > Devices > All devices. The joined device name and its associated information (OS type, Owner, Join type, etc) was then displayed in the table below.



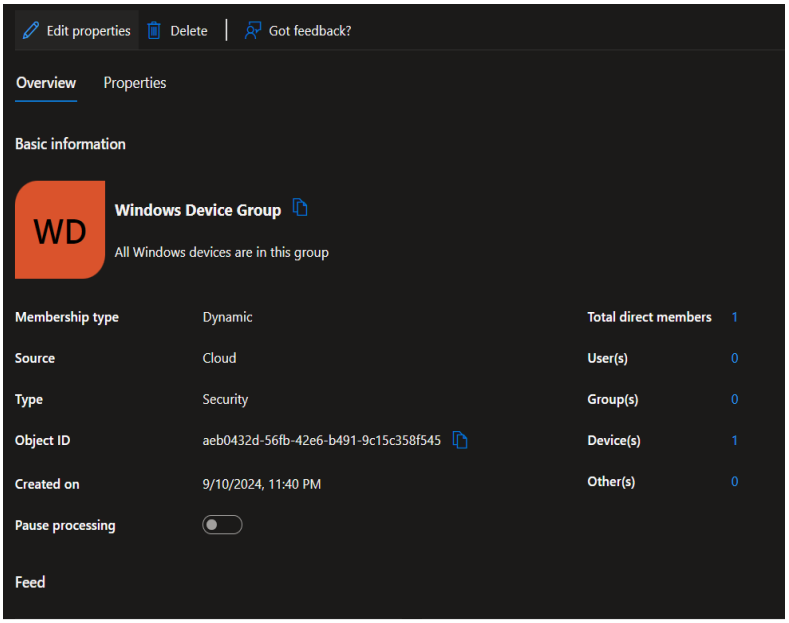
Furthermore, a device group was created by logging in to the Azure portal (portal.azure.com) using the global administrator account and navigating to Show portal menu > Entra ID > Groups > New group. The group characteristics were then configured as follows:

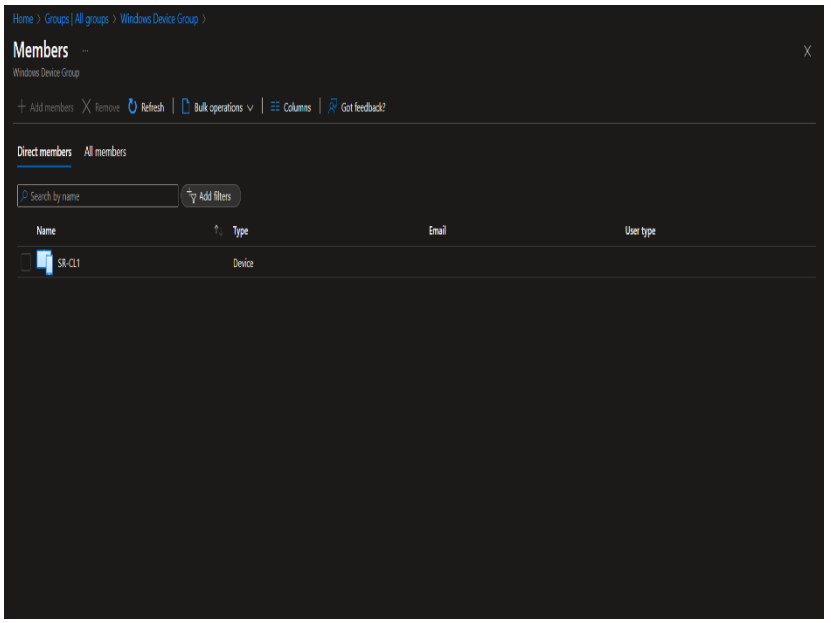


The group was configured as a security group with a dynamic device membership type. Entra roles couldn't be assigned to the group. Note that the group name is not available since it was already created.



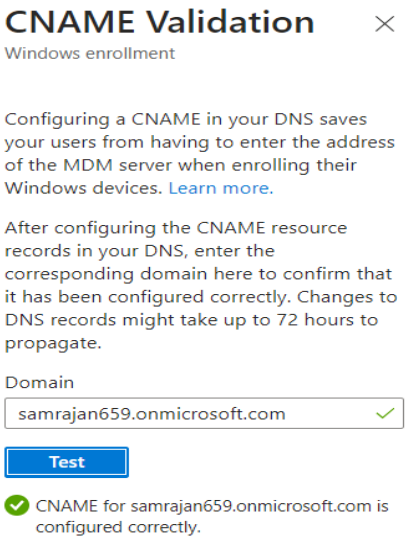
The dynamic membership rules under Dynamic device members > Add dynamic query.





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.

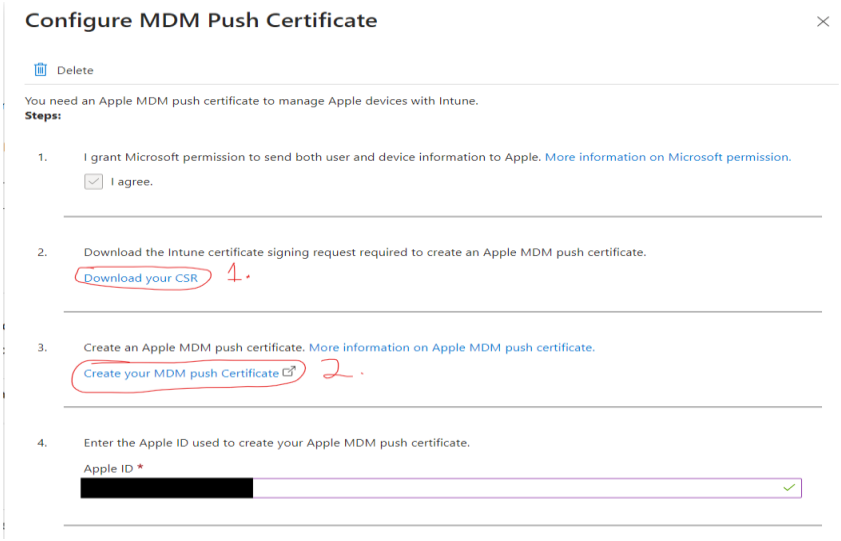


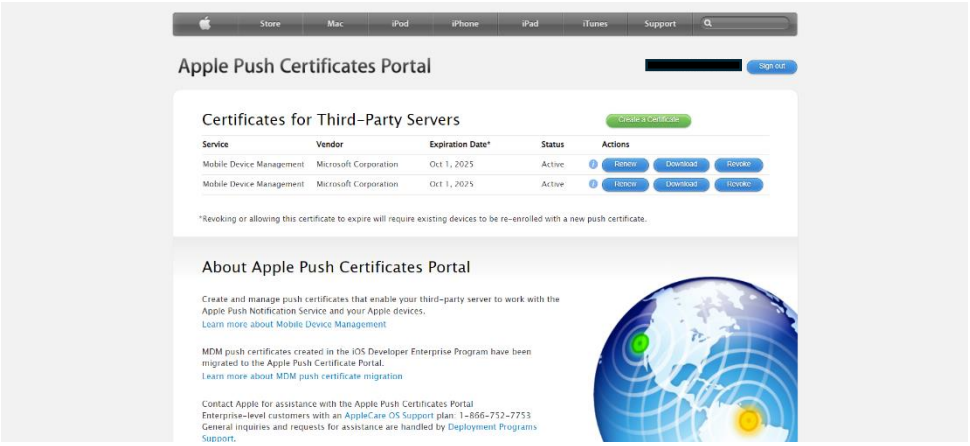
The CNAME has been validated successfully.

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.

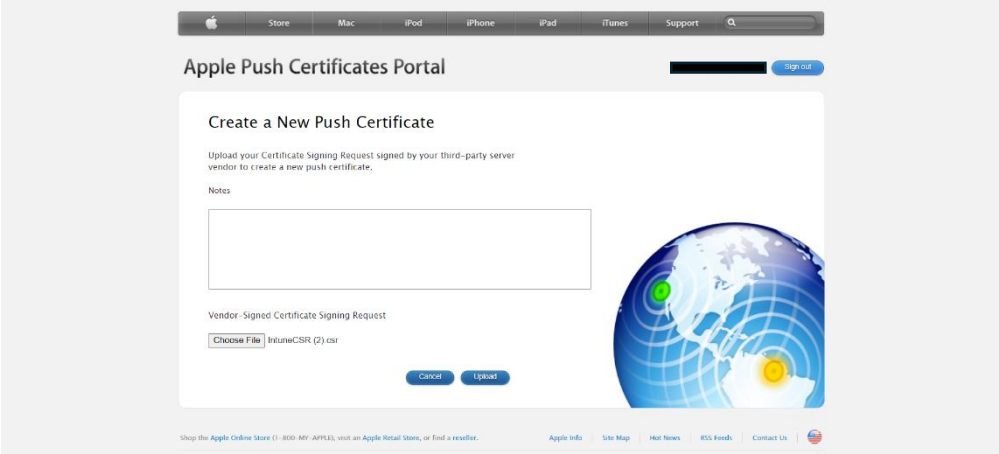
Navigating to Devices > Enrollment > Apple > Apple MDM Push Certificate will open the MDM Push Certificate blade. From here the Certificate Signing Request (CSR) had to be downloaded and then the Apple Push Certificate Portal had to be logged into to create the push certificate.

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.

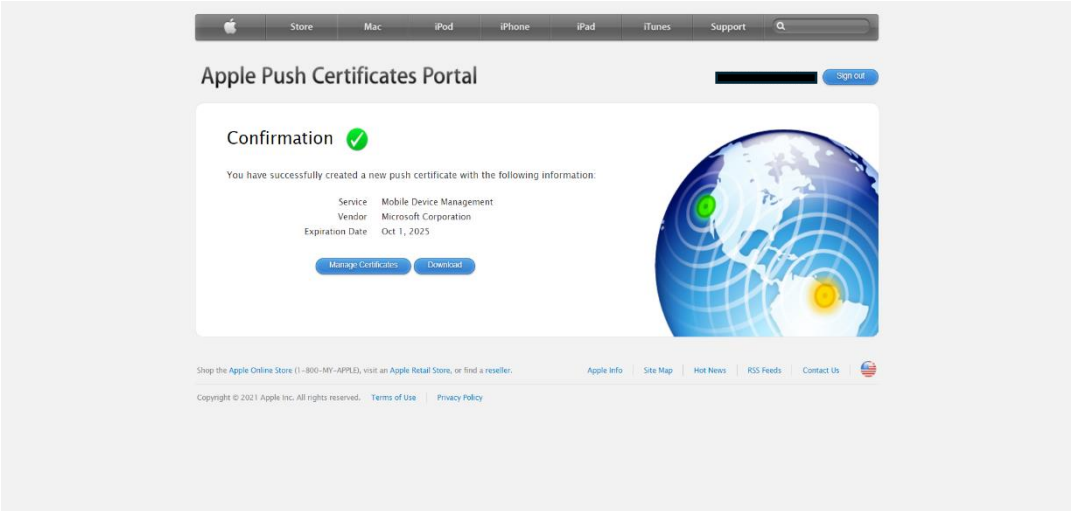




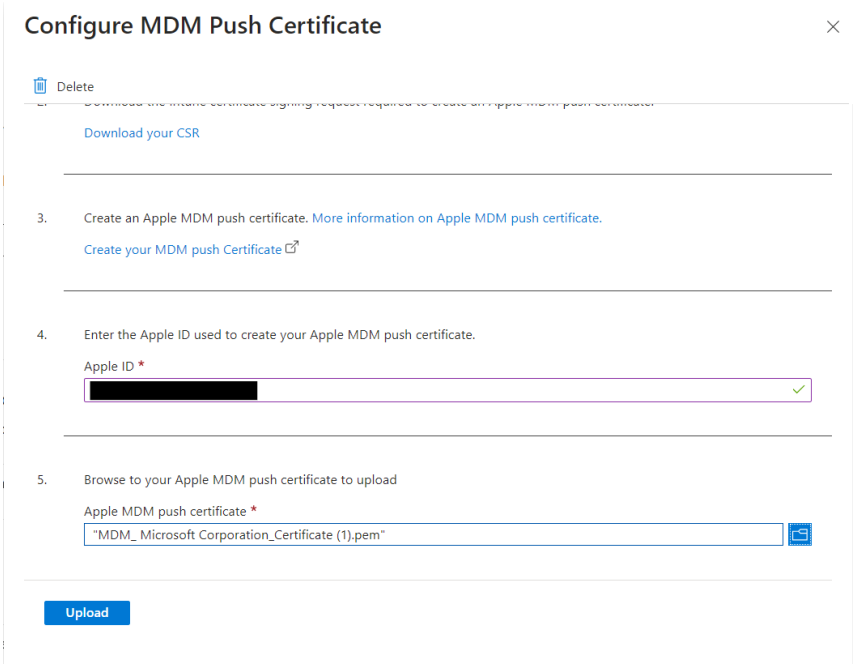
The Apple Push Certificates Portal.



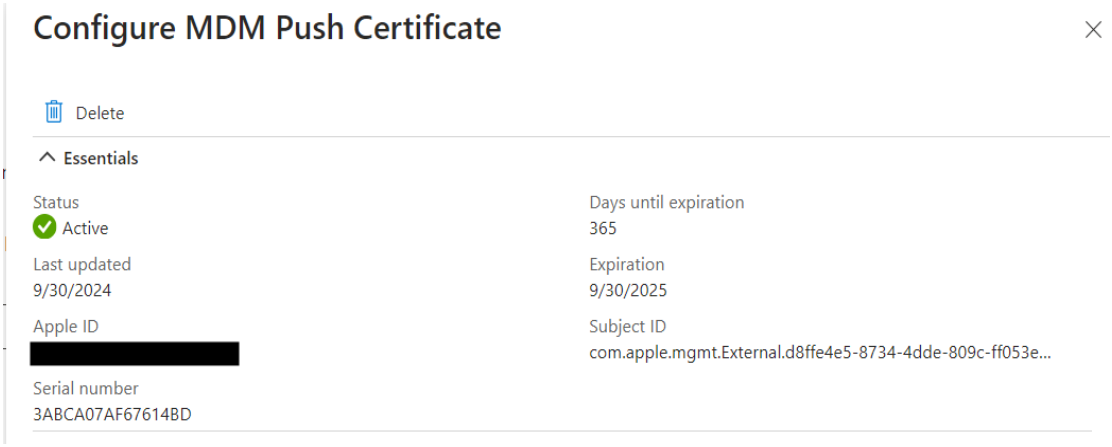
Here the push certificate is created using the CSR created in Intune.



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

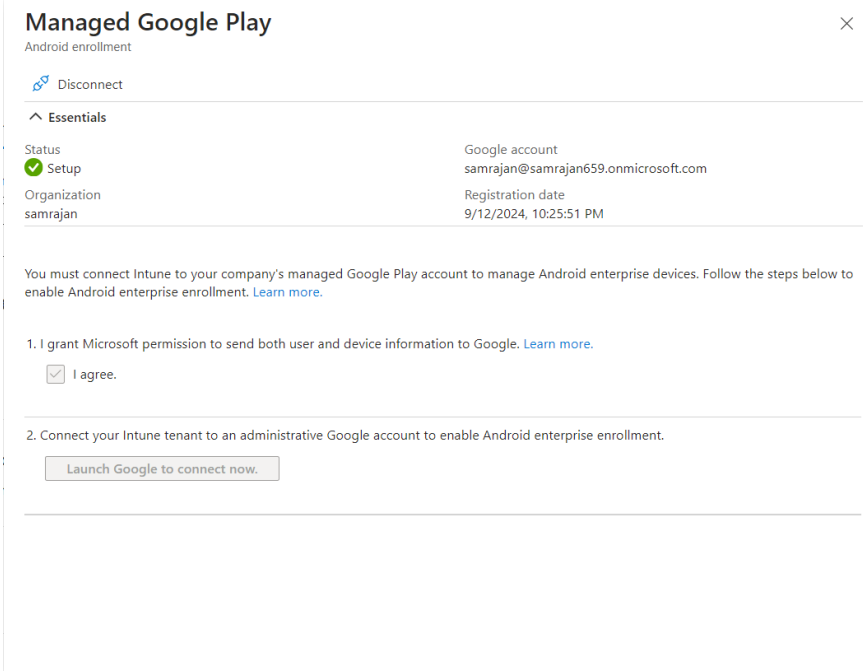


The Apple MDM push certificate has been uploaded.



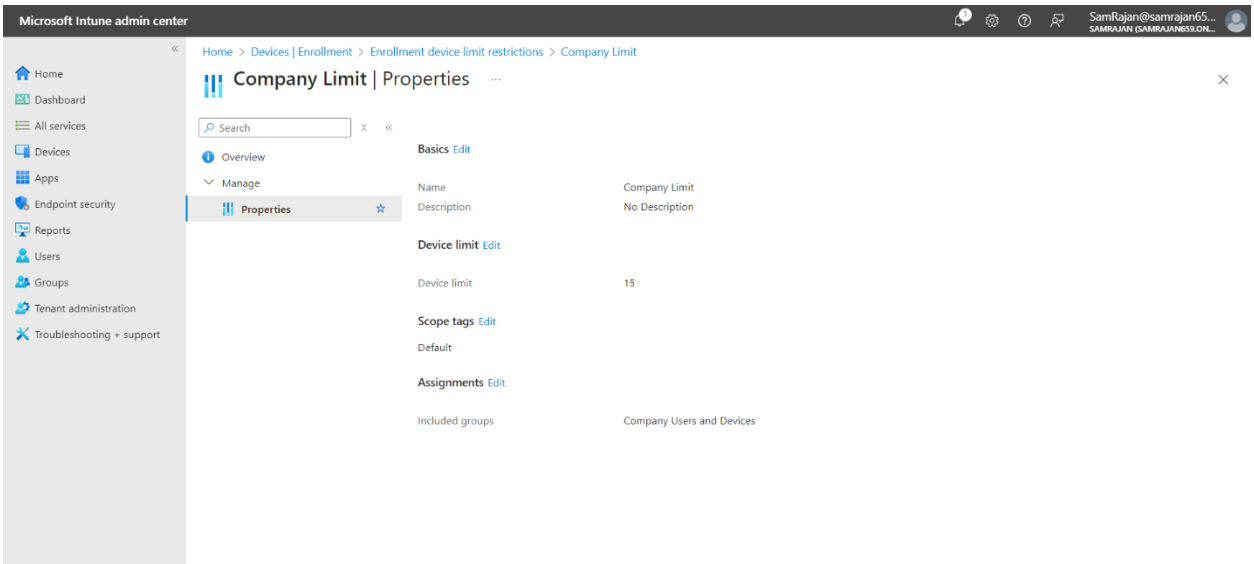
The Apple MDM Push Certificate has been successfully configured.

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.

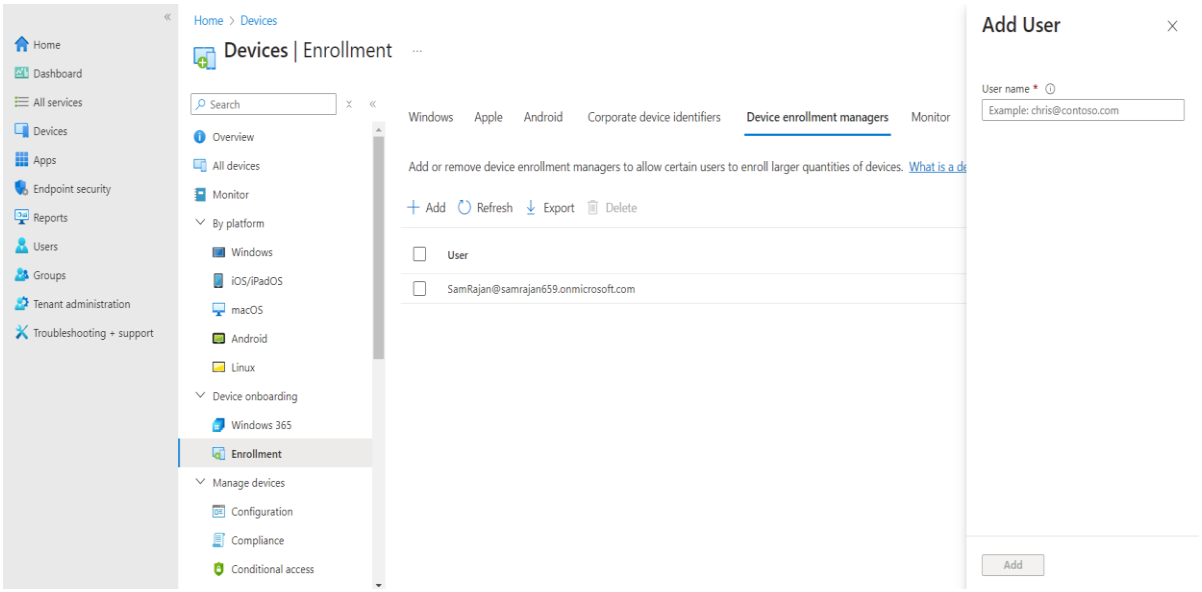


The checkmark and "Setup" status indicates that Intune was successfully connected to the desired managed Google Play account.

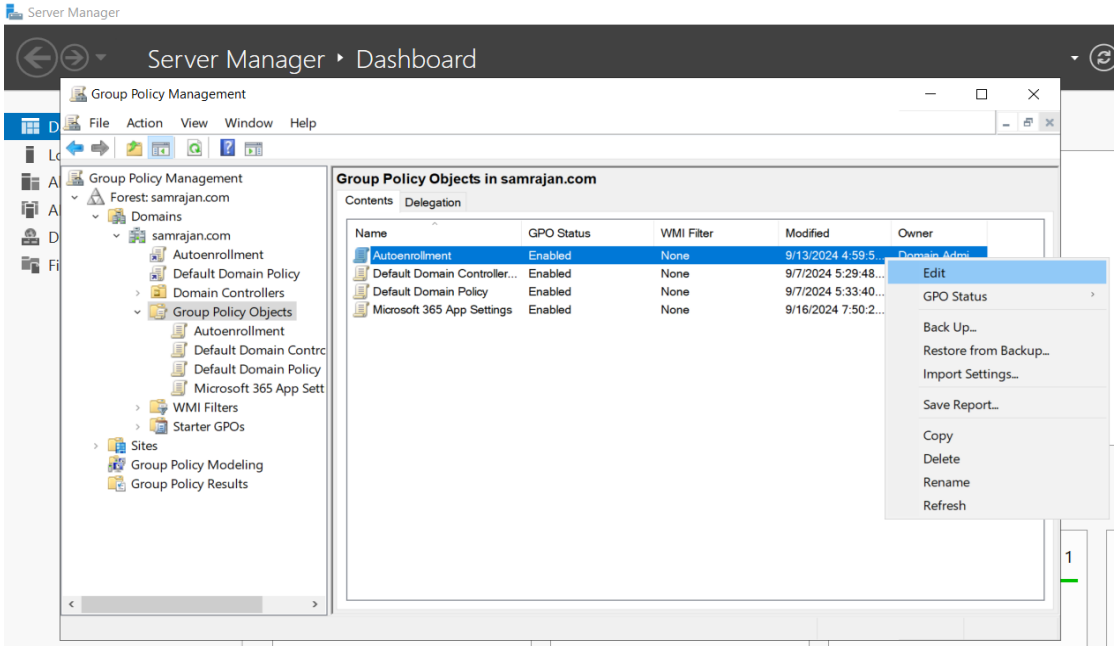
A device enrollment limit restriction was implemented to configure the maximum number of devices that can enroll. The default enrollment restriction configures the maximum number of devices to be 5 but a new device limit restriction was created to increase this number to 15.

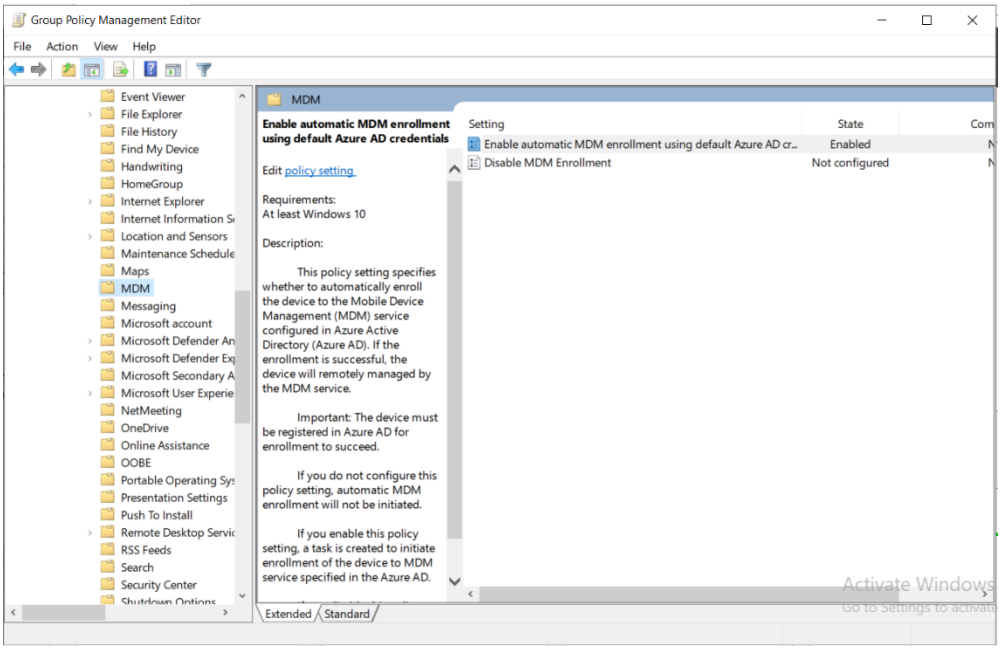


This was achieved by navigating to Devices > Enrollment > Device limit restriction > Create restriction and editing the device limit to 15. A device enrollment manager was added by navigating to Devices > Enrollment > Device enrollment managers > Add and simply entering in the user name (SamRajan@samrajan659.onmicrosoft.com).

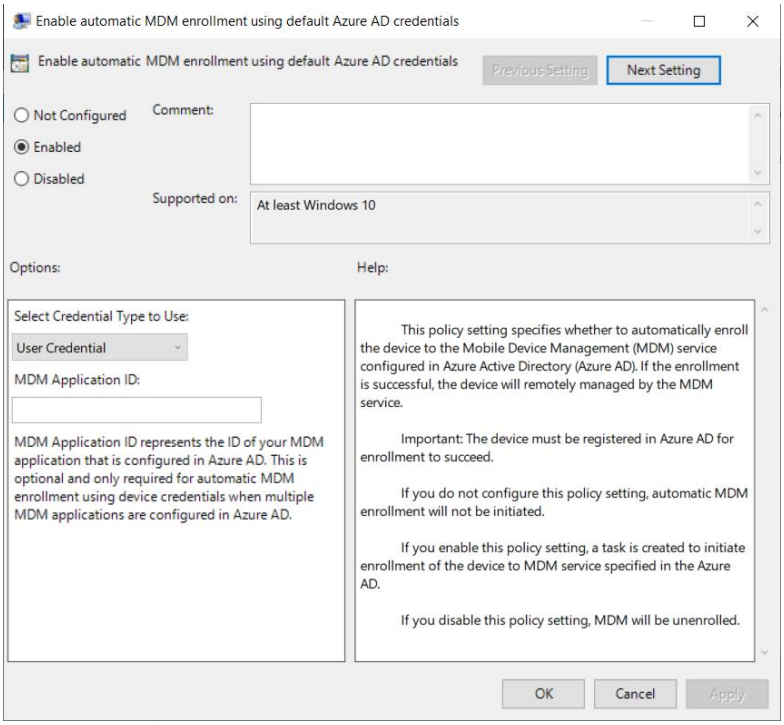


To configure automatic enrollment, the automatic MDM enrollment policy needs to be enabled via Server Manager in Windows Server. After navigating to Tools > Group Policy Management in Server Manager, a group policy object called Autoenrollment was edited to enable the “enable automatic MDM enrollment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





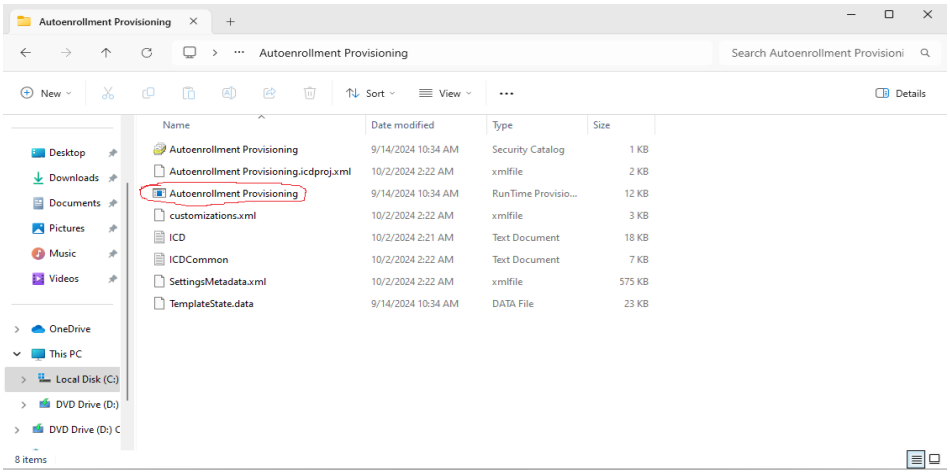
This screen was shown after clicking "Edit" and navigating to Computer Configuration > Policies > Administrative Templates > Windows Components > MDM.



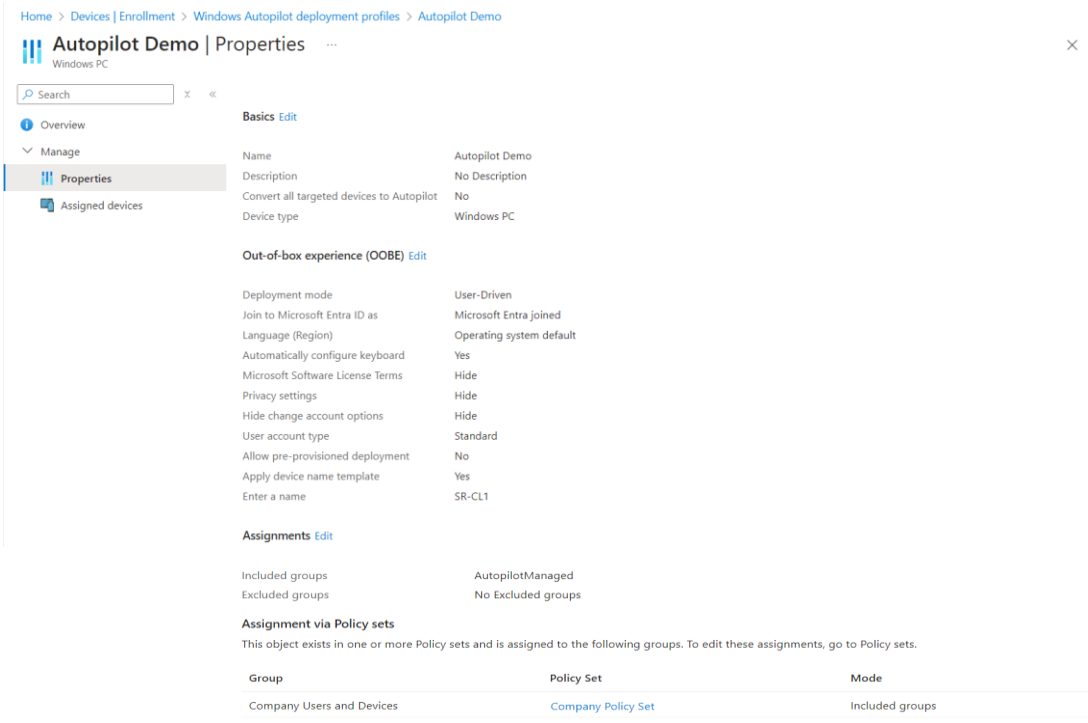
The policy was enabled by double-clicking it and selecting the "Enabled" option.

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

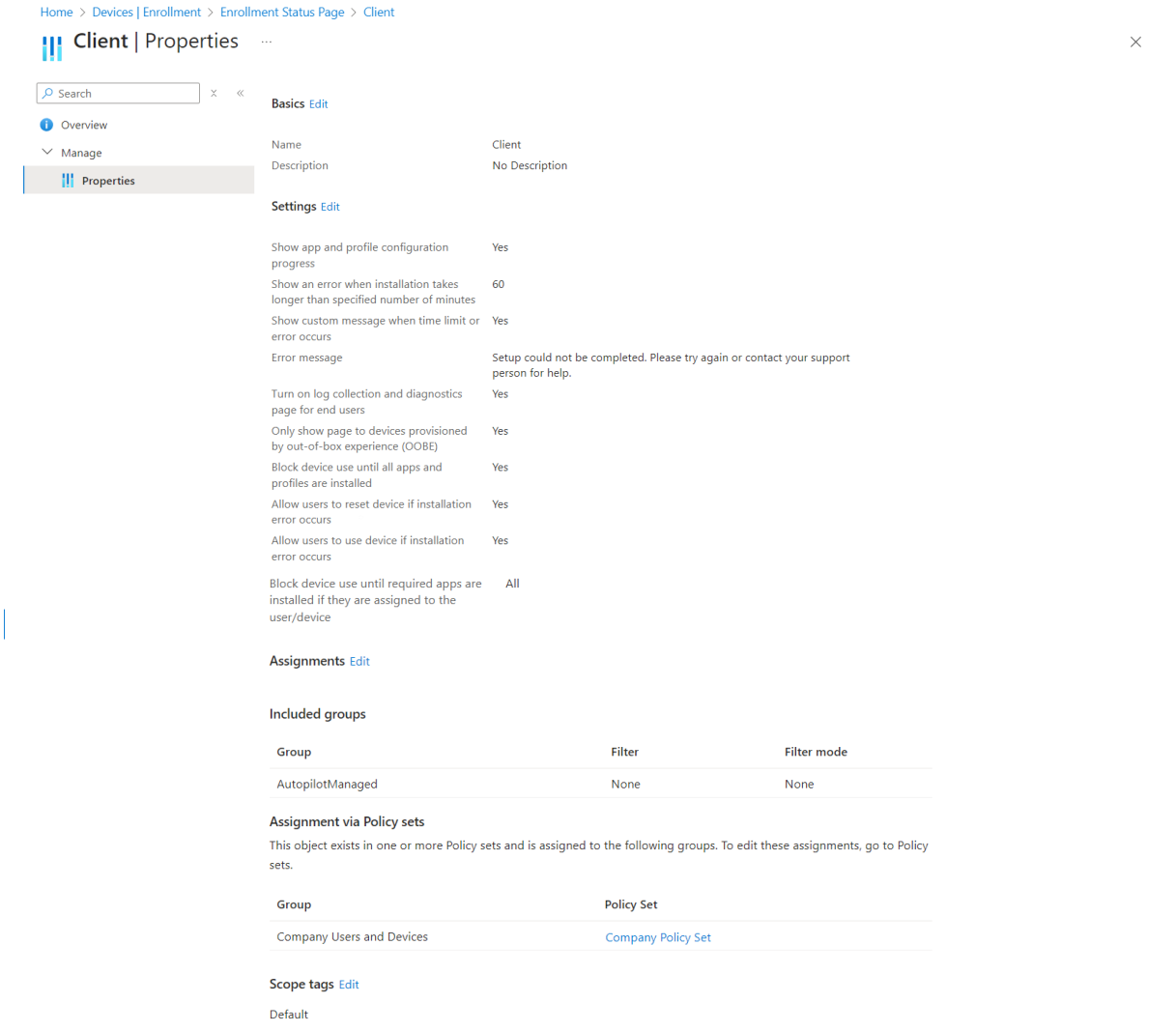
Bulk enrollment can be configured by using Windows Configuration Designer to create a provisioning package. This application must be downloaded and installed from the Microsoft App Store. Once the package has been successfully created, it can be readily provisioned to all desired devices.



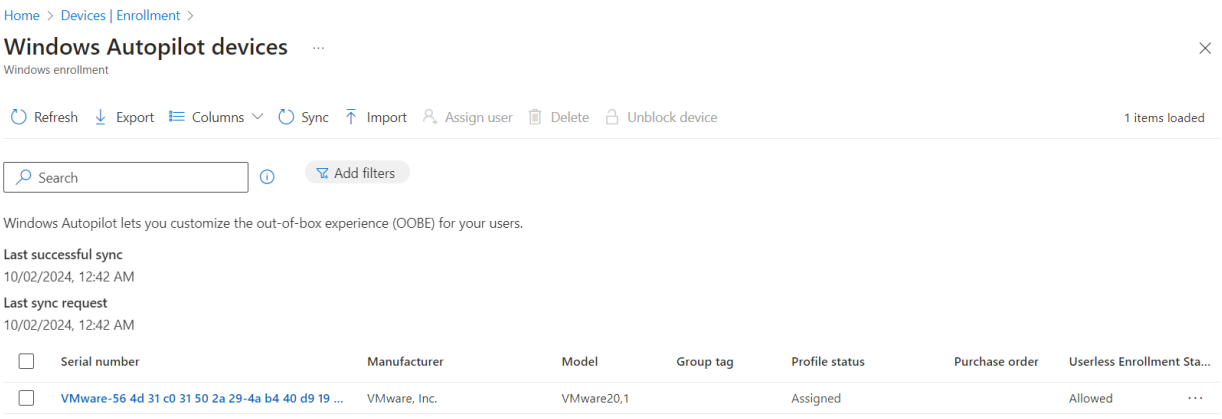
Another way to enroll devices into Intune is to use Autopilot. A deployment profile was created along with an enrollment status page. The client device being used for this lab was enrolled via Autopilot.



These are the configured settings for the deployment profile.

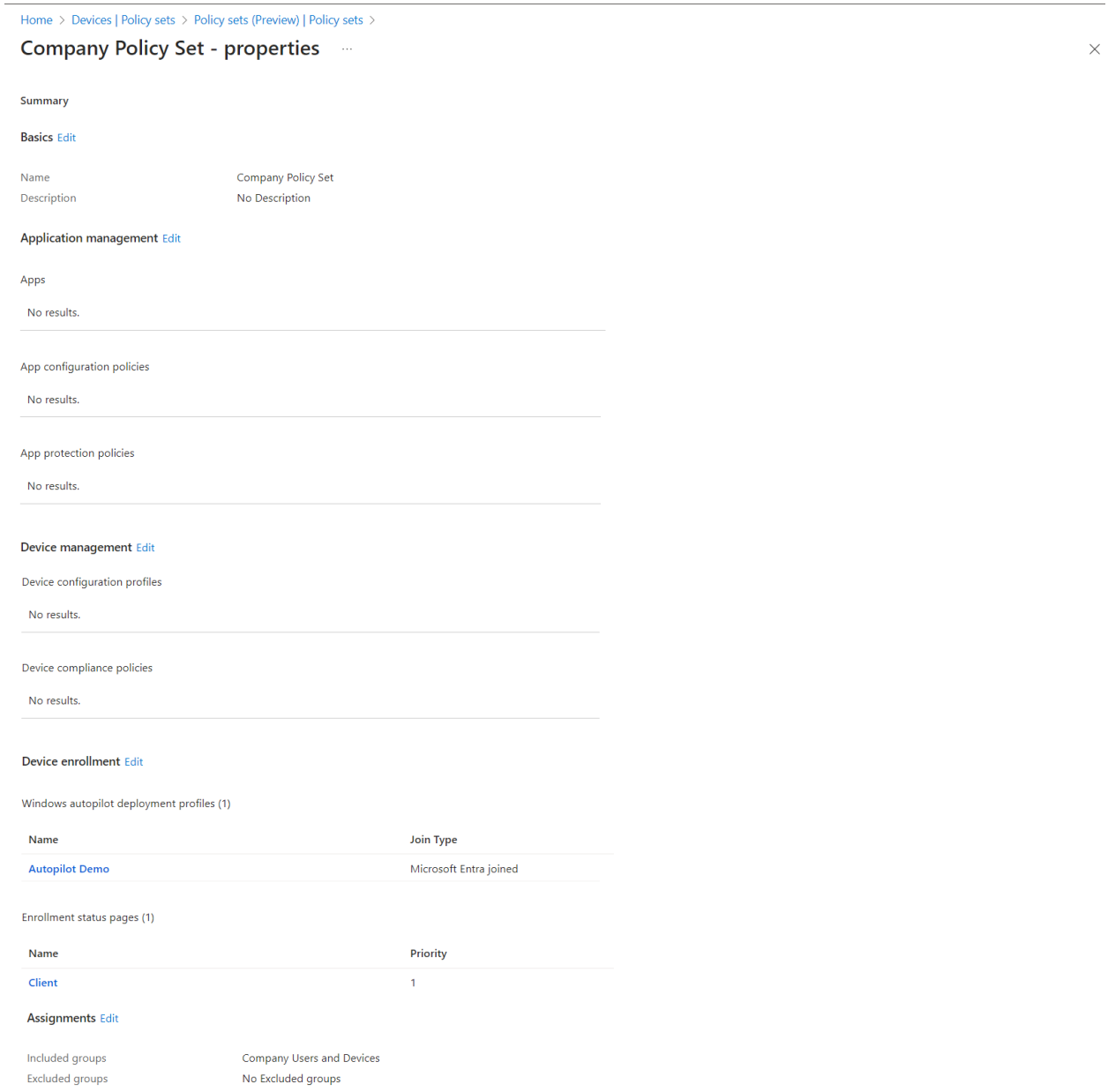


These are the settings configured for the enrollment status page.



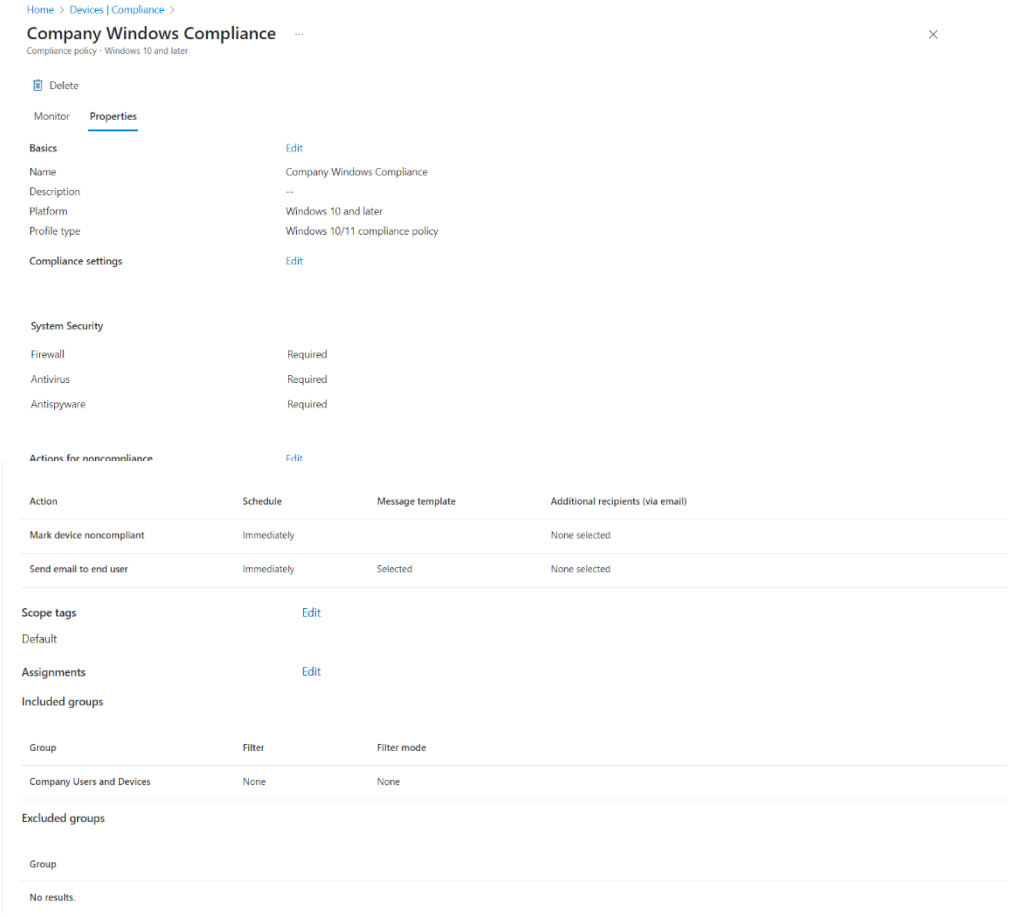
The device has been successfully enrolled into Intune via Windows Autopilot.

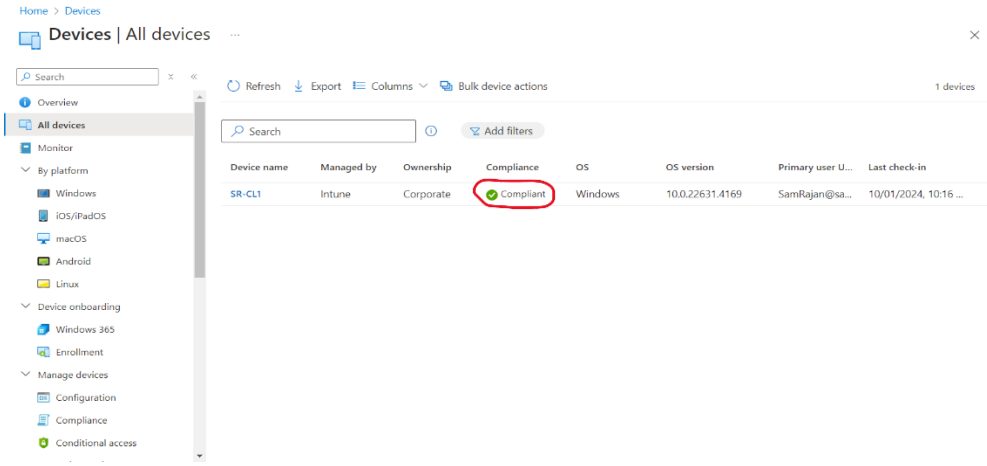
Multiple apps, policies, and other management objects can be assigned at once to devices using policy sets. One policy set was created with the pictured properties.



Implementing Identity and Compliance

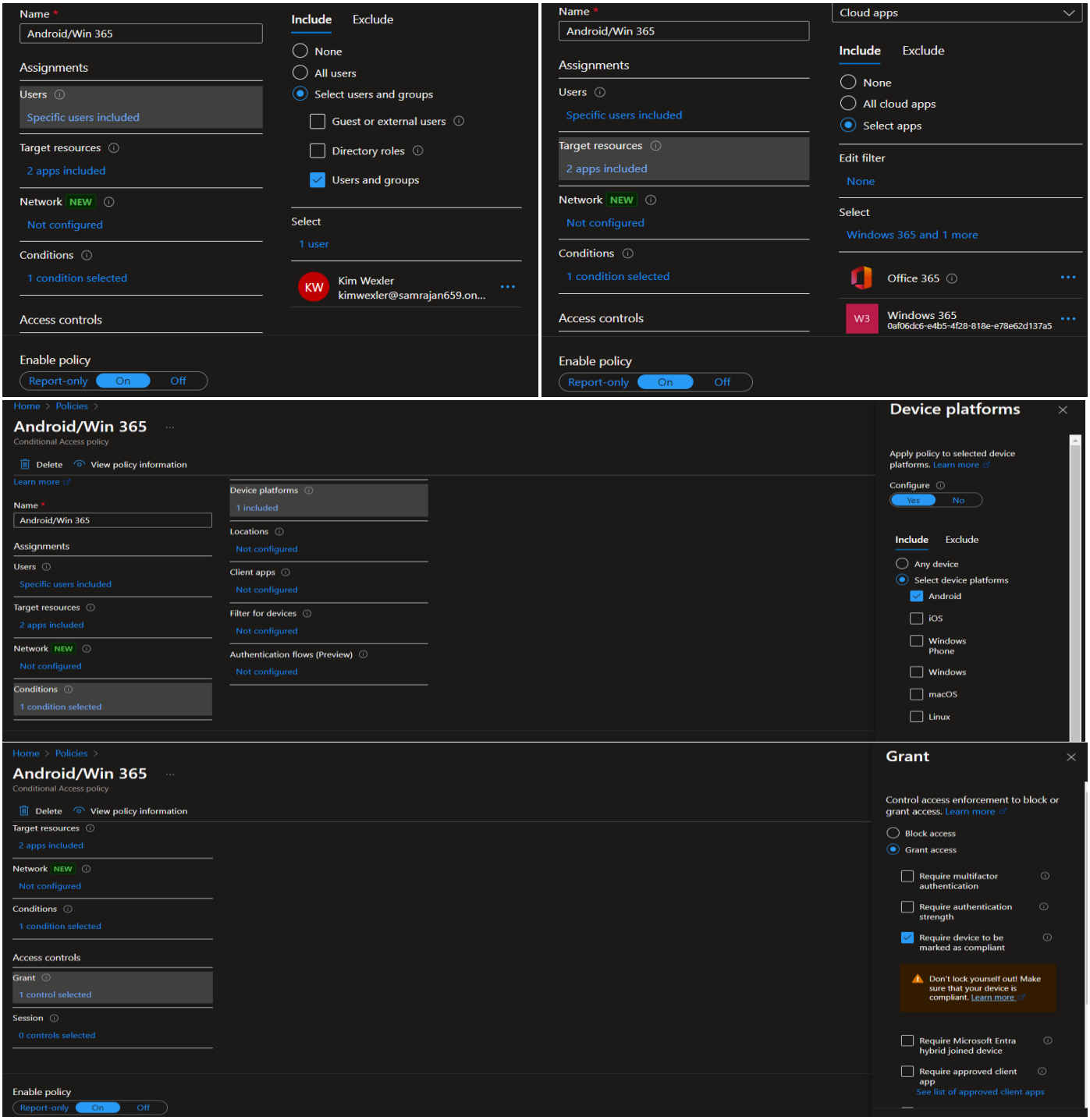
Compliance and identity measures are implemented so that only devices which meet certain criteria are allowed to be enrolled into Intune/Entra ID. Among the criteria are firewall, antivirus, and antispyware activation.





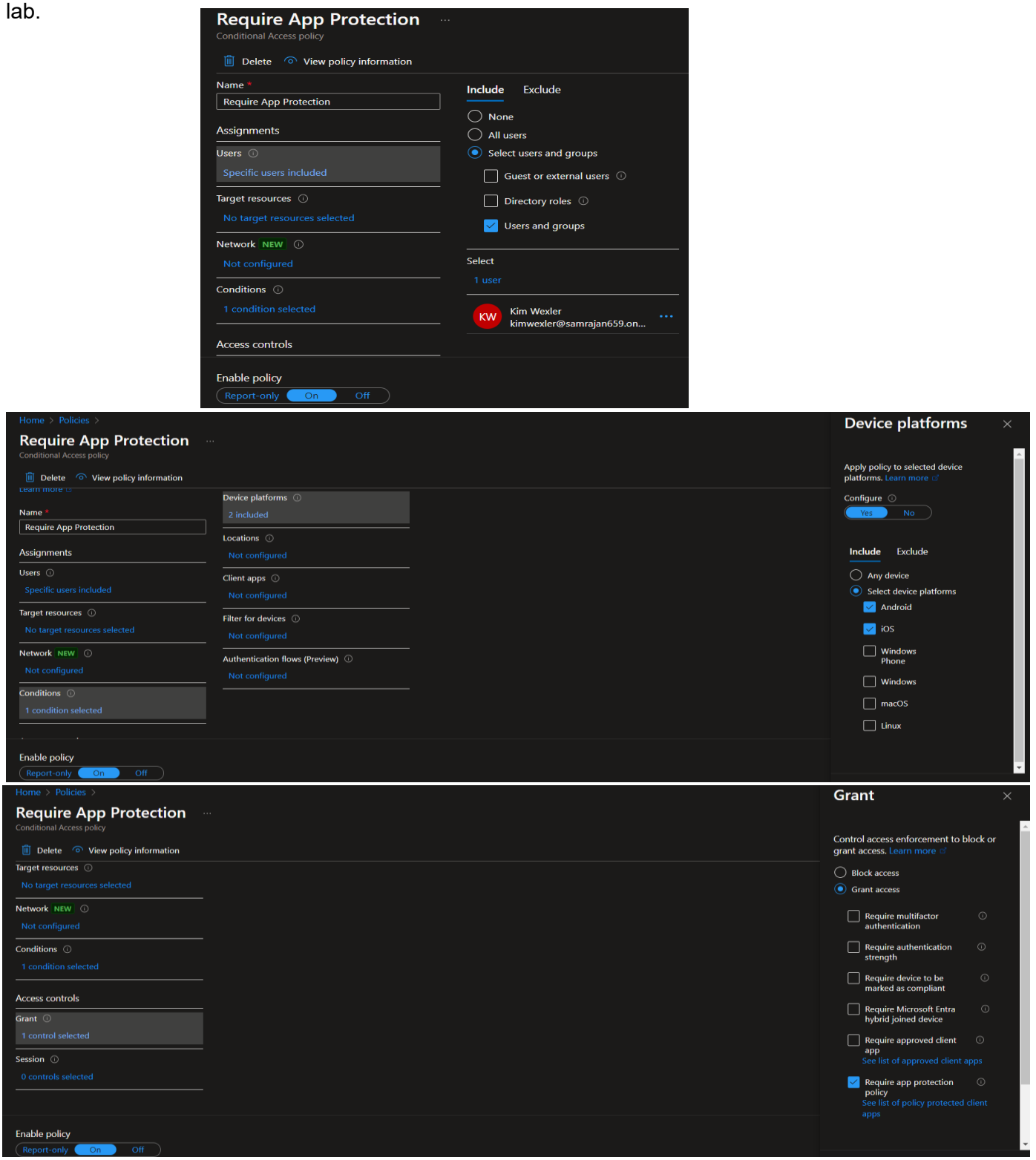
The device has been marked as compliant. In addition, a security baseline (will be discussed in a later section) has been implemented which enforces the same criteria for compliance.

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.



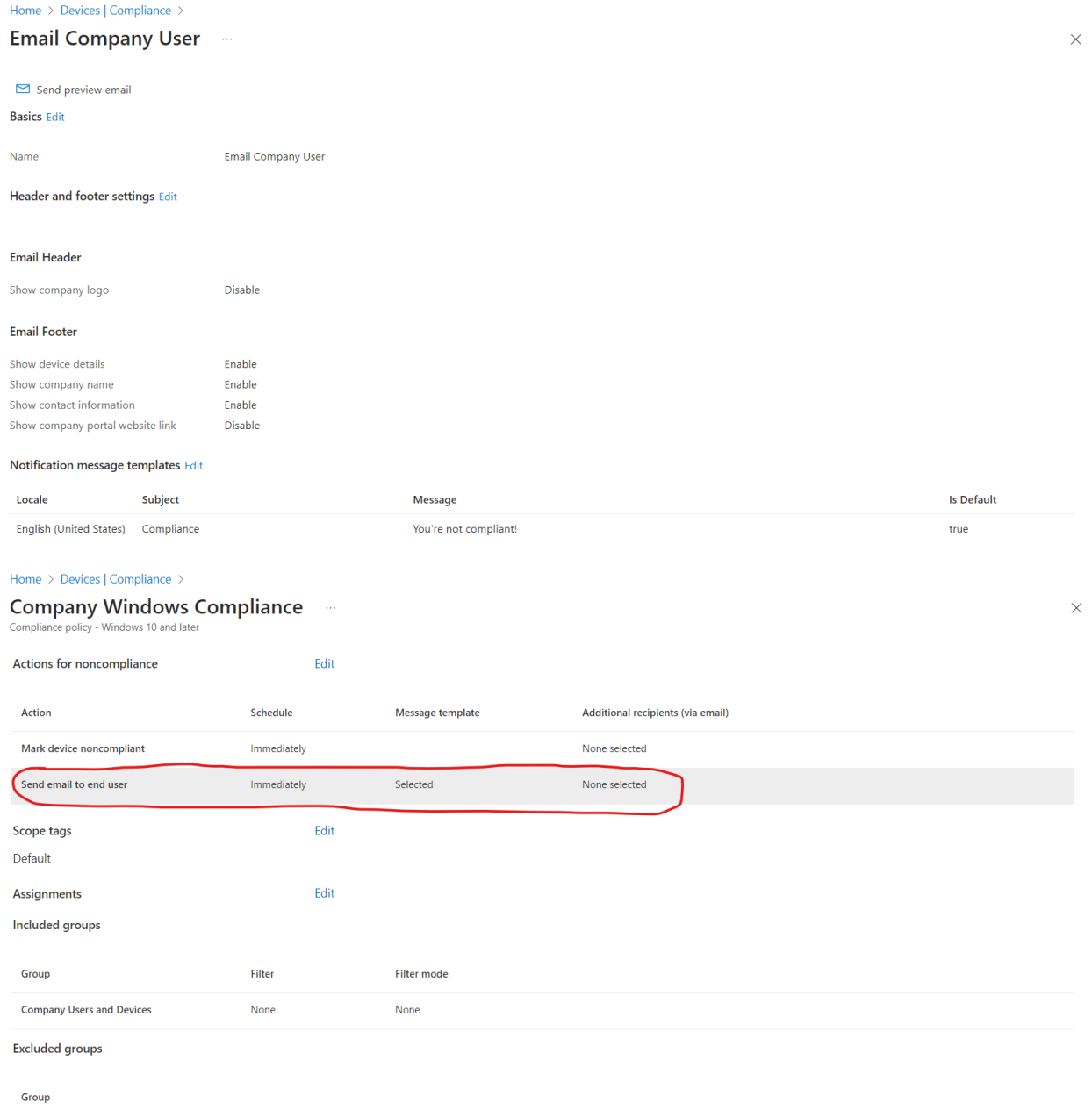
The conditional access policy configurations for Android devices relating to Windows 365 and Office 365 access.

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.



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

Basics 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

Actions for noncompliance Edit

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

Scope tags Edit

Default

Assignments Edit

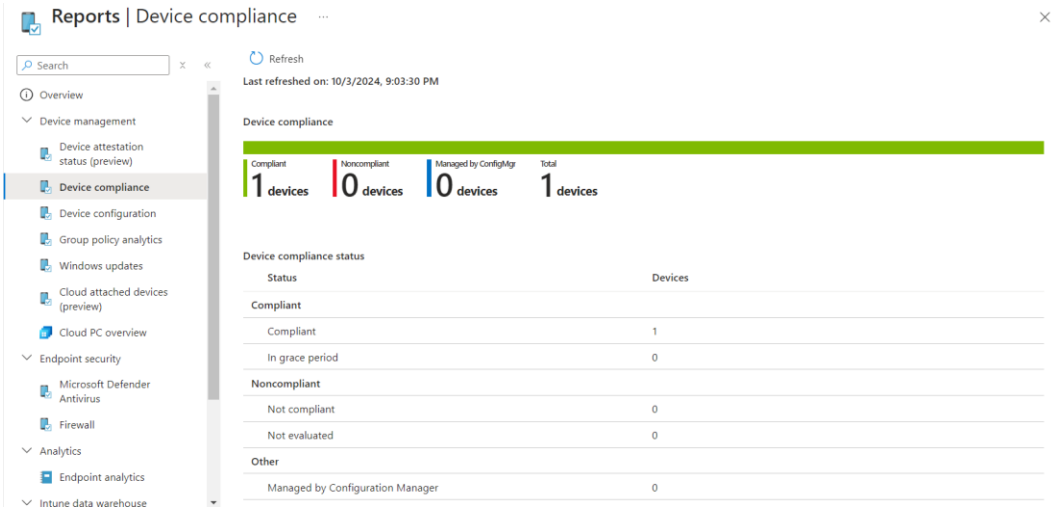
Included groups

Group	Filter	Filter mode
Company Users and Devices	None	None

Excluded groups

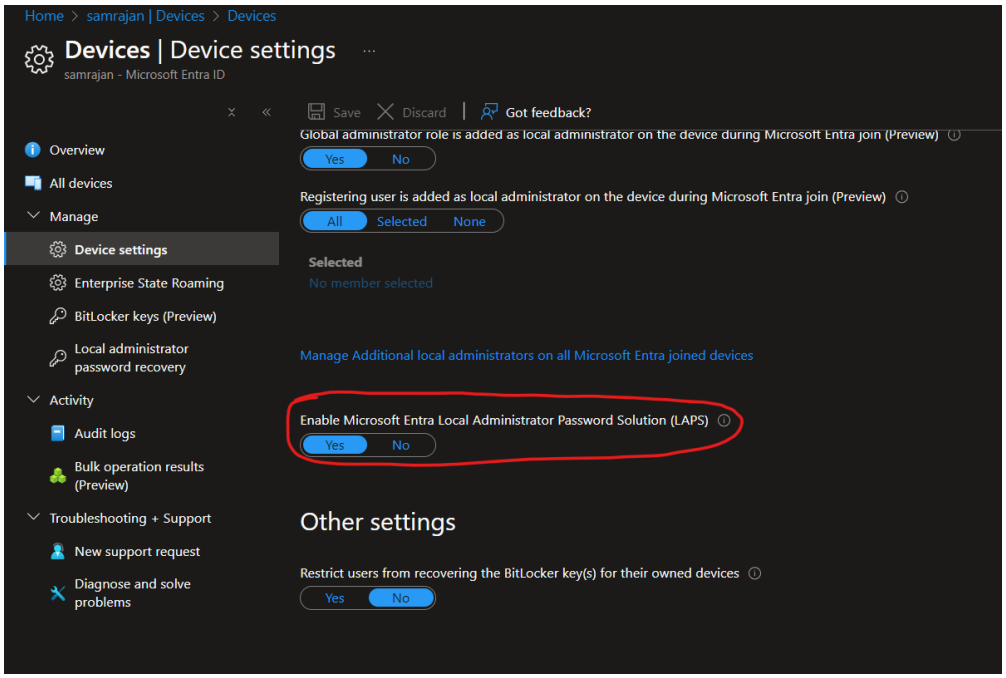
Group

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.

Home > Endpoint security | Account protection >

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

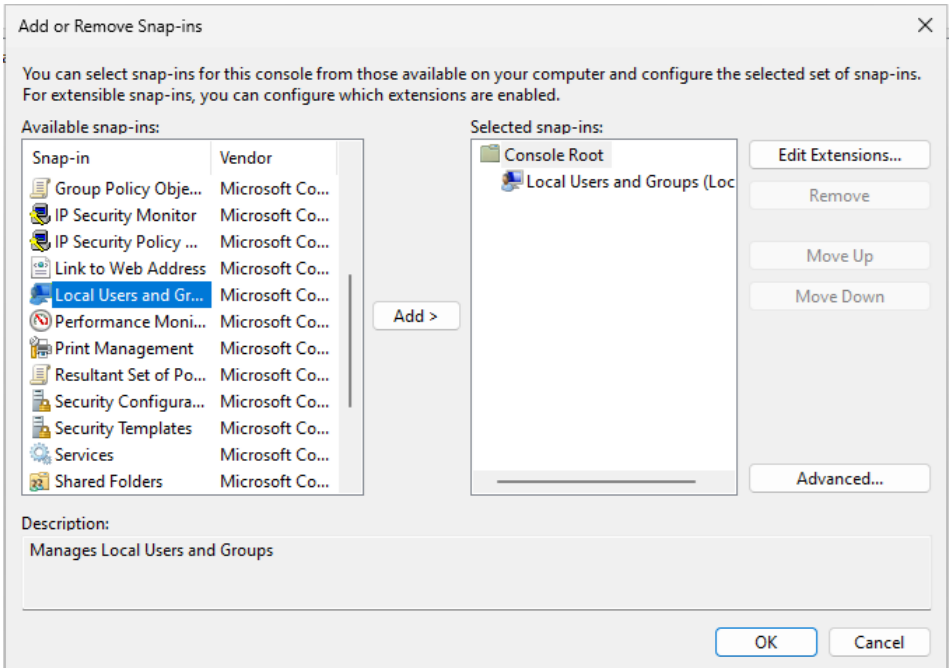
Selected tags	Default

Configuration settings Edit

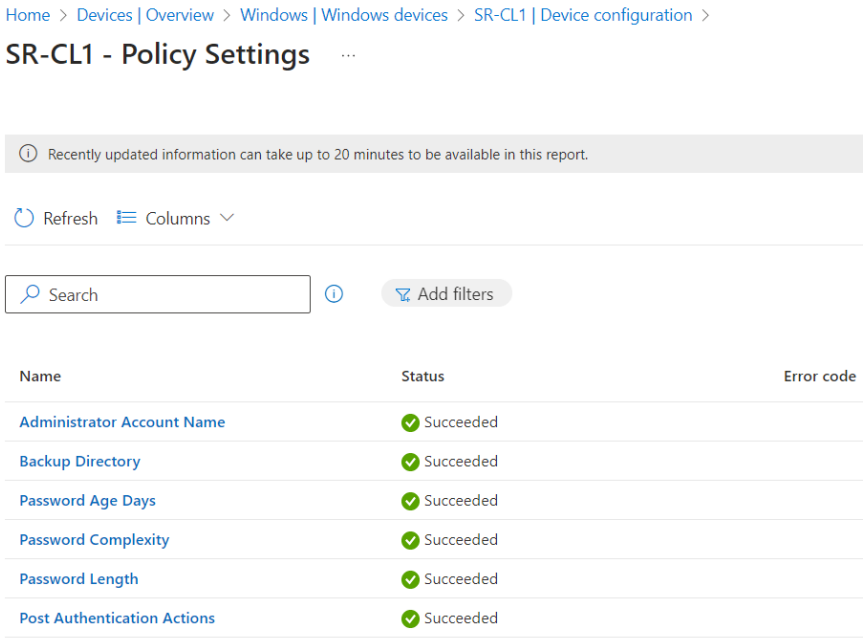
LAPS

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 terminated.

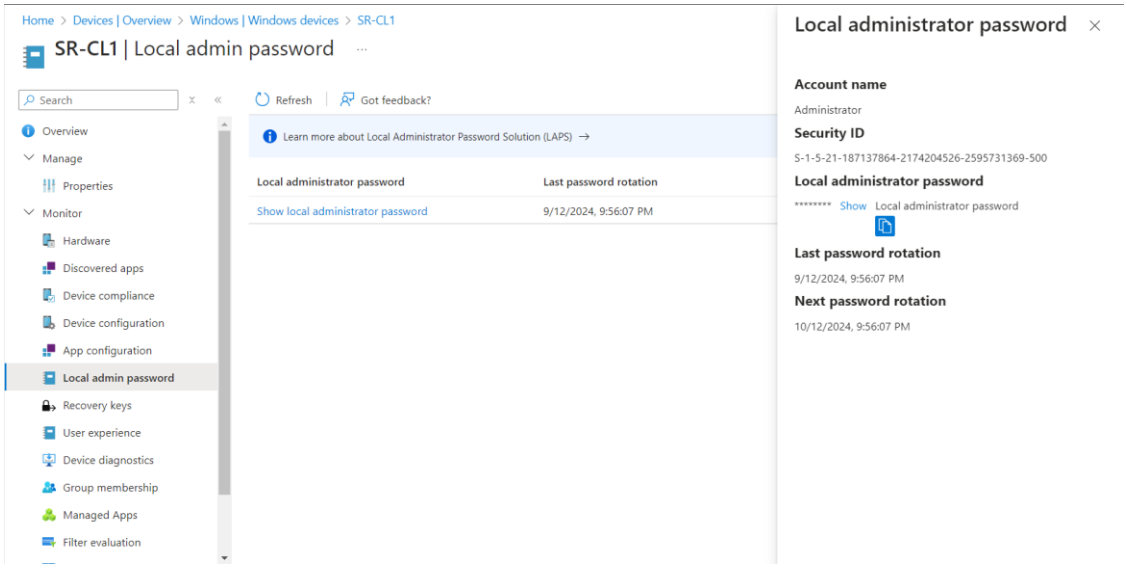
Following this, mmc.exe was ran on the Windows 11 client machine and the “Add or Remove Snap-ins” screen was opened via File > Add or Remove Snap-ins. From here, Local Users and Groups was added as a selected snap-in.



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).

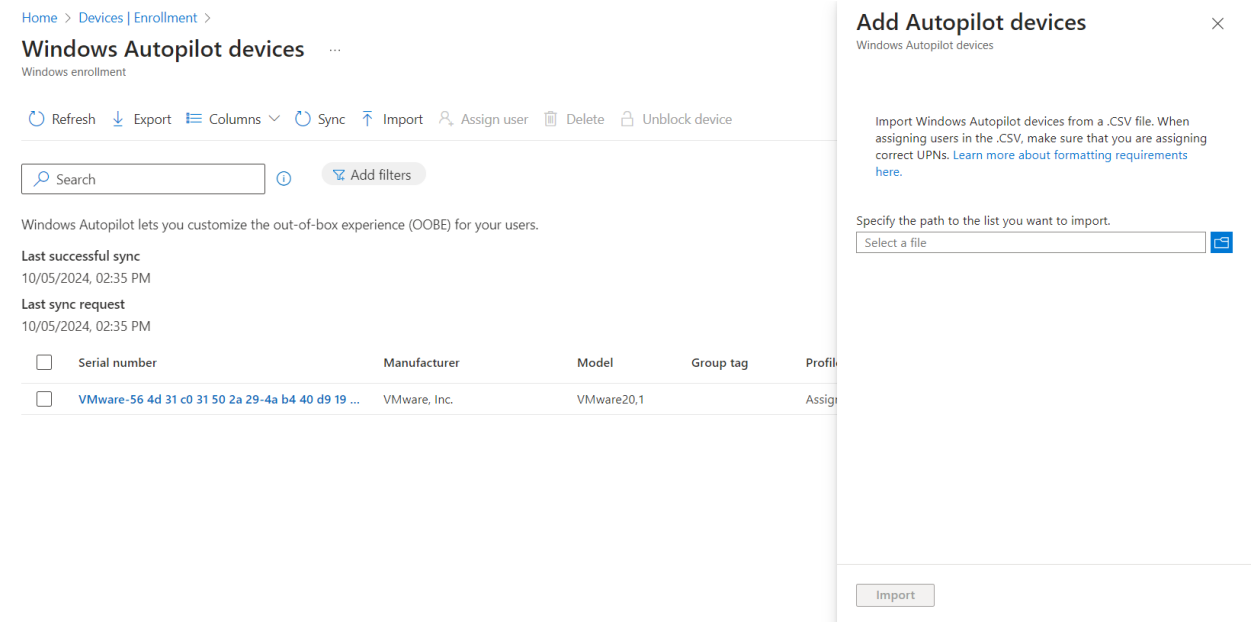


Furthermore, navigating to Devices > Windows Devices > Clicking on the device name (SR-CL1) > Local admin password confirmed that an admin password was created.



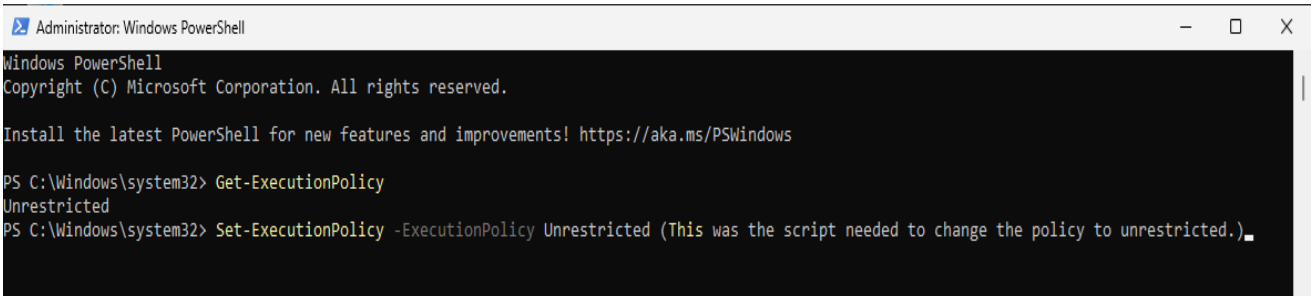
Deploying/Upgrading Windows Clients Using Autopilot

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.



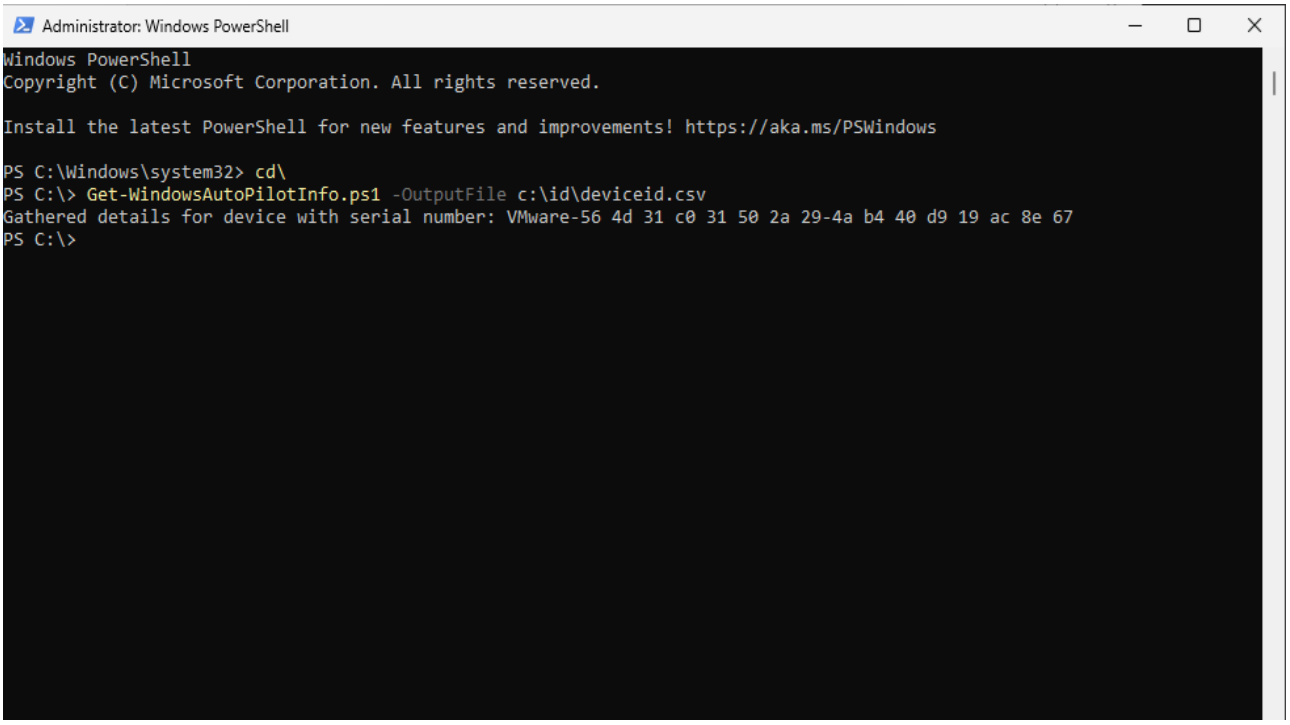
This blade where the CSV file gets uploaded was accessed by navigating to Devices > Enrollment > Devices (in the Windows Autopilot section) > Import. Note that the Windows 11 device appears in the table as a VMware 20.1 model device as the serial number in the CSV file correctly identifies it as a VMware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

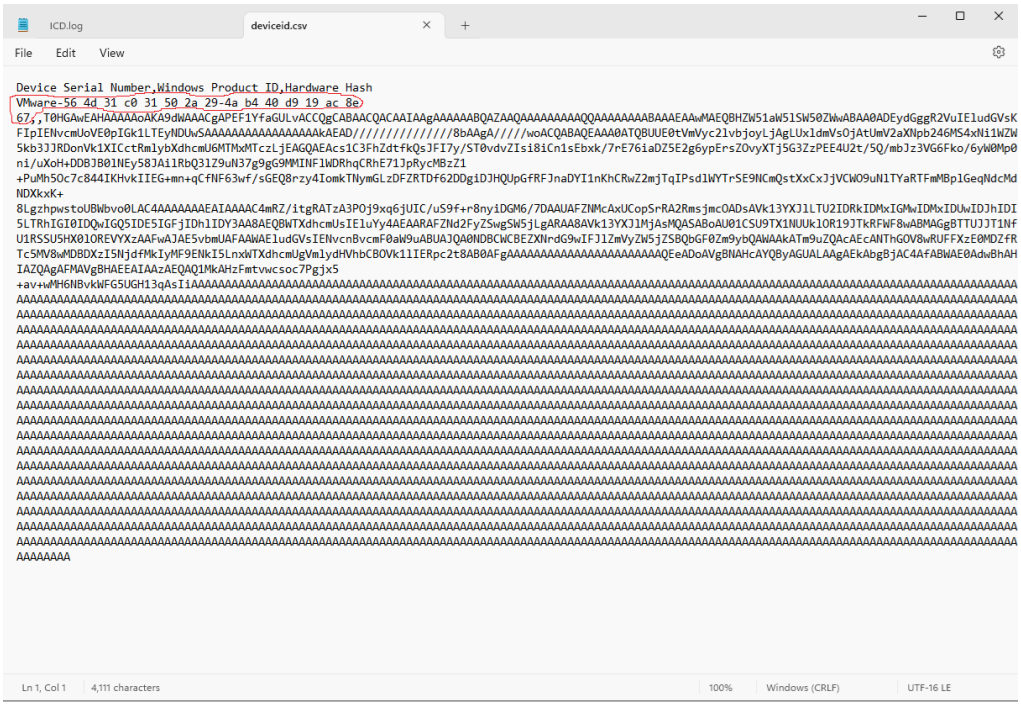


It was not possible to enter all the commands as they first were due to Autopilot already being configured and installed. Therefore, a list of those PowerShell commands/scripts that were used will be provided instead.

- 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

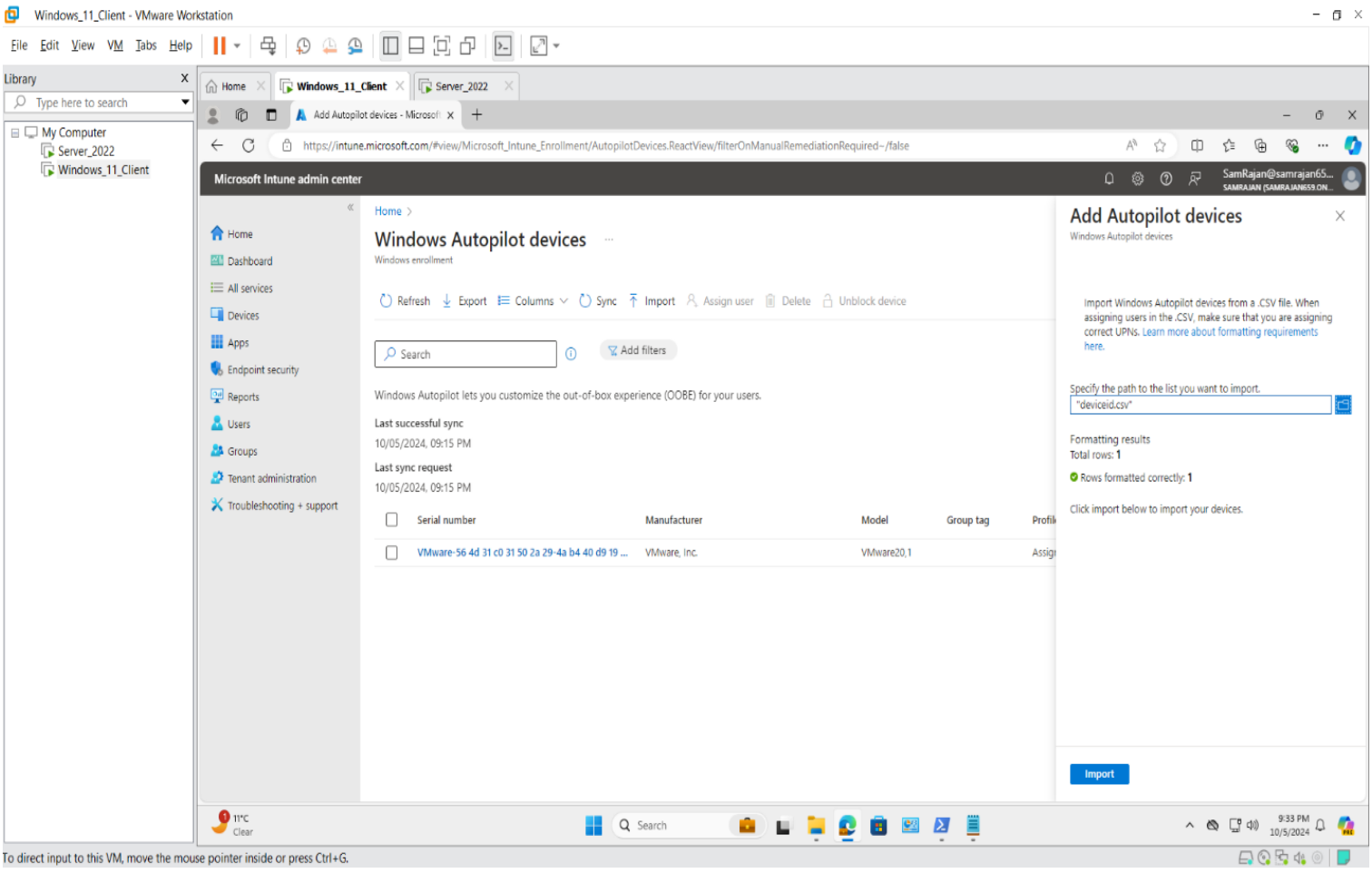


Issuing the pictured command caused the CSV file named "deviceid.csv" to be sent to the "ID" folder created using the mkdir command.

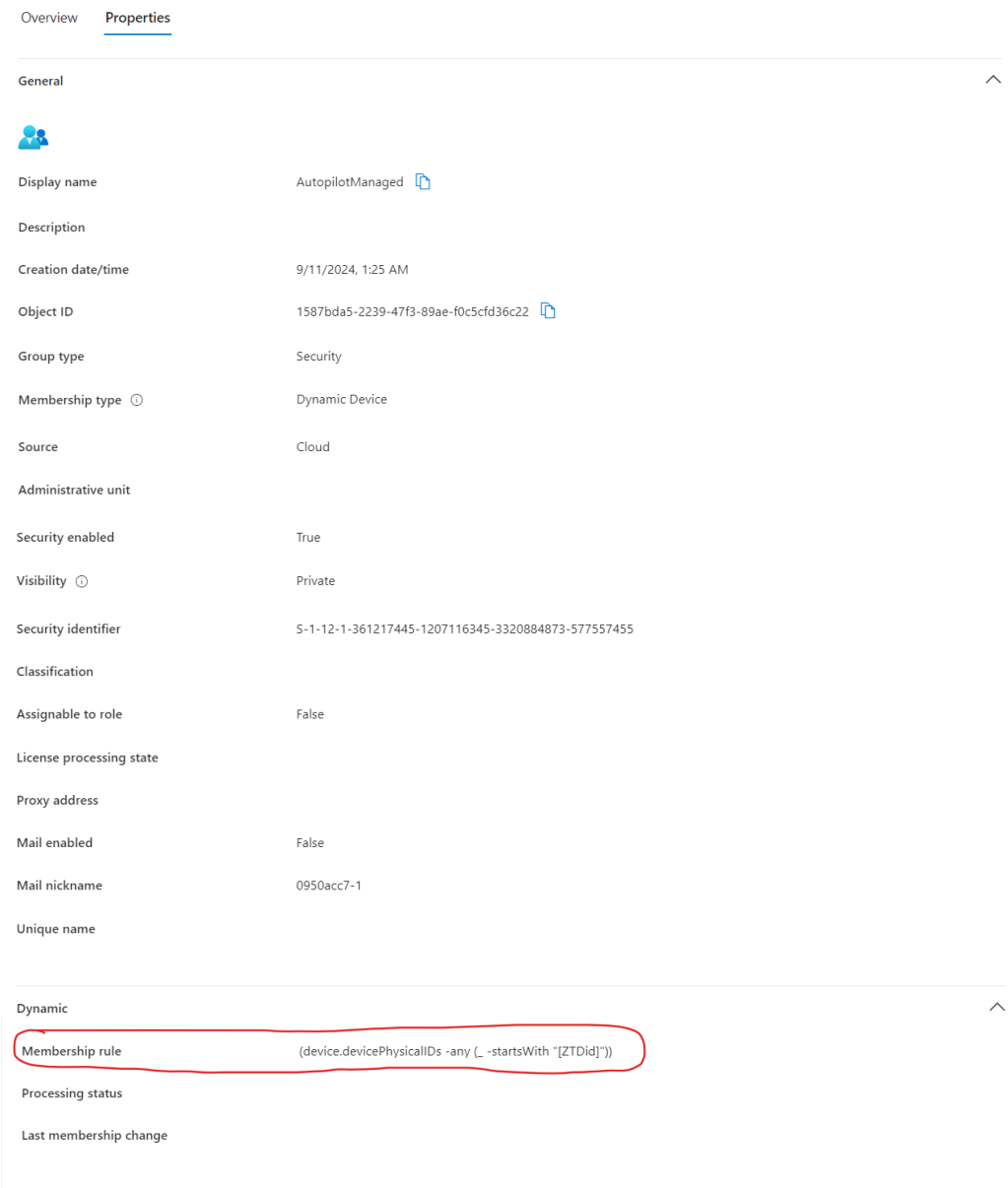


The contents of the CSV file. Encircled in red is the serial number.

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.

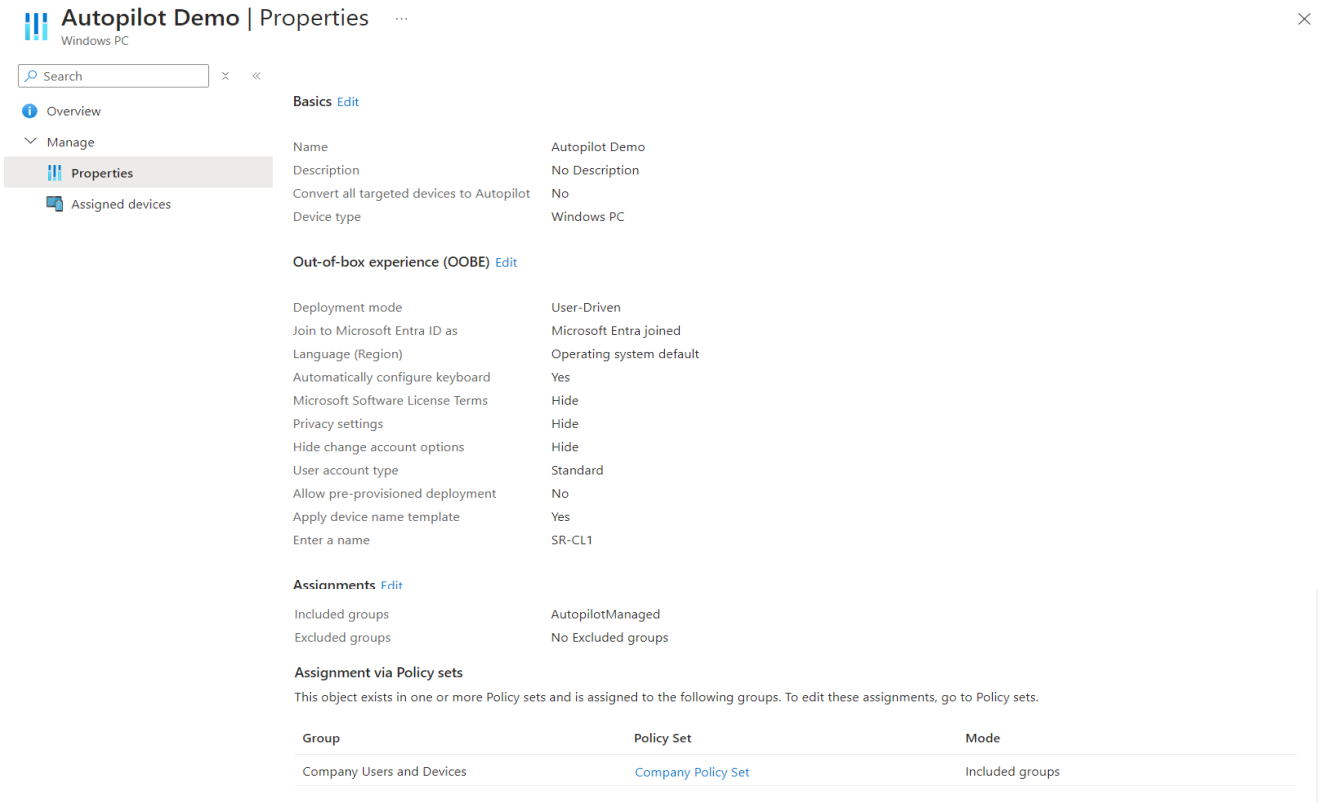


A group made for Autopilot-managed devices named “AutopilotManaged” was created.

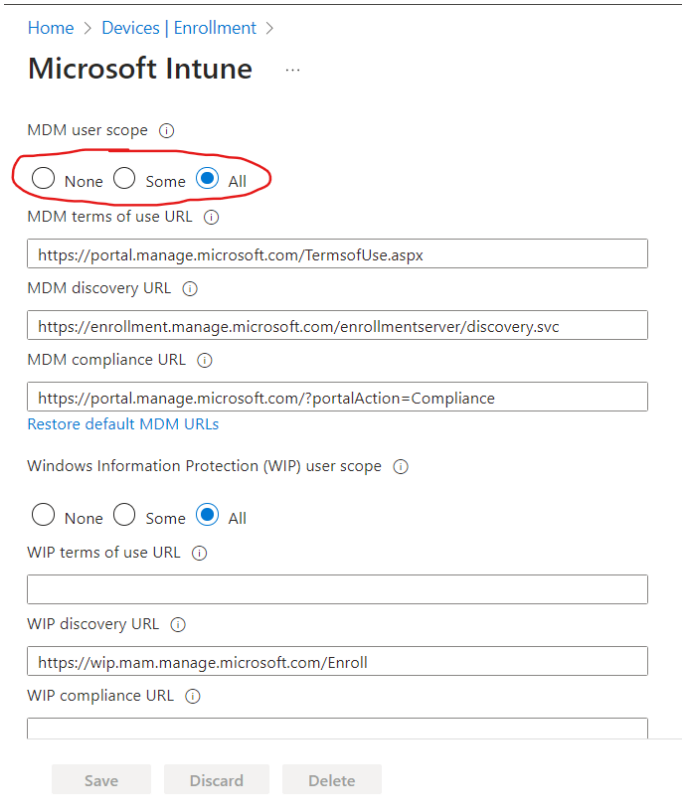


The membership rule configuration encircled in red defines the group as containing all Autopilot devices.

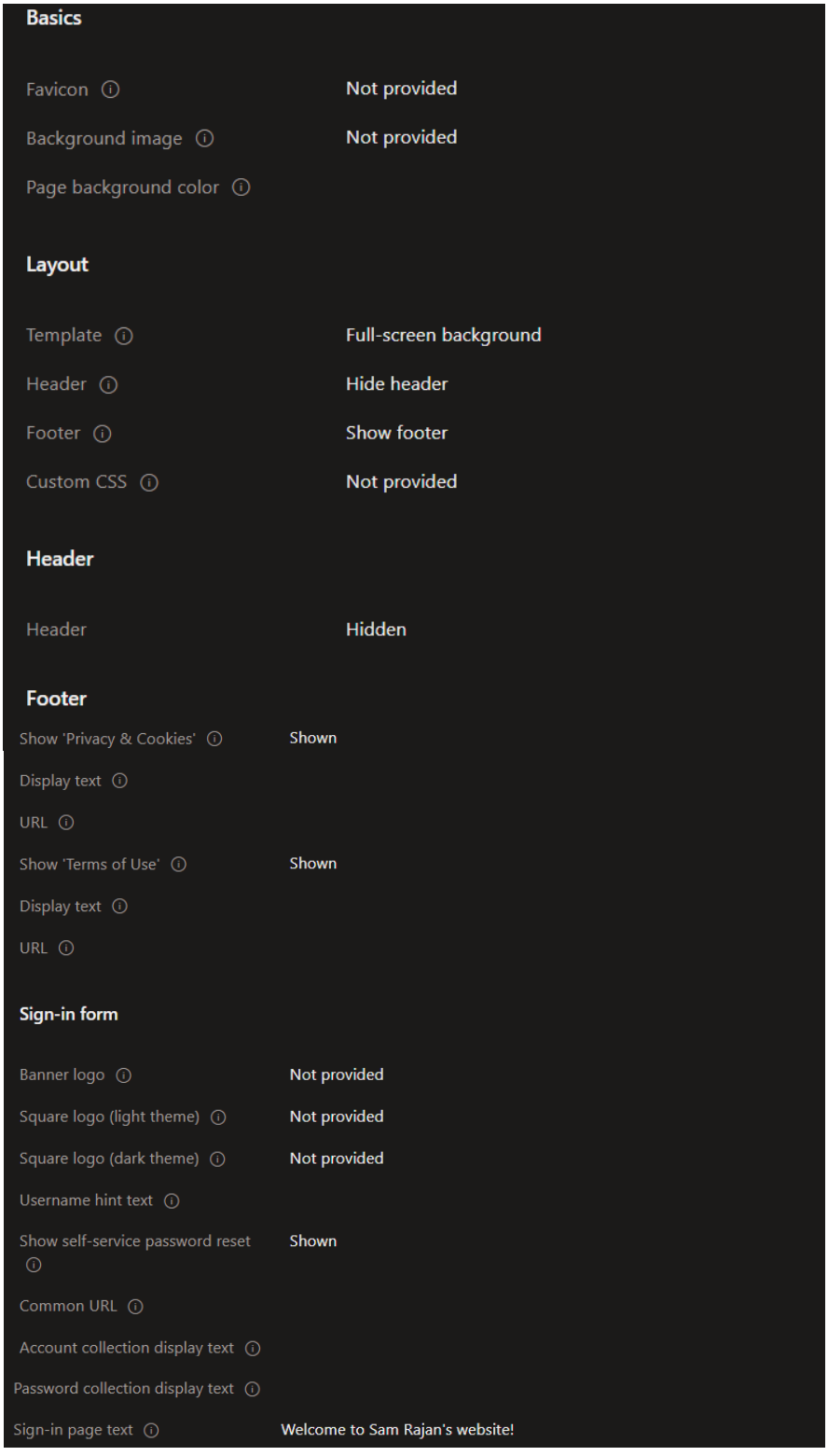
After this, a deployment profile which can be used to configure devices added to the “AutopilotManaged” was created.



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



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

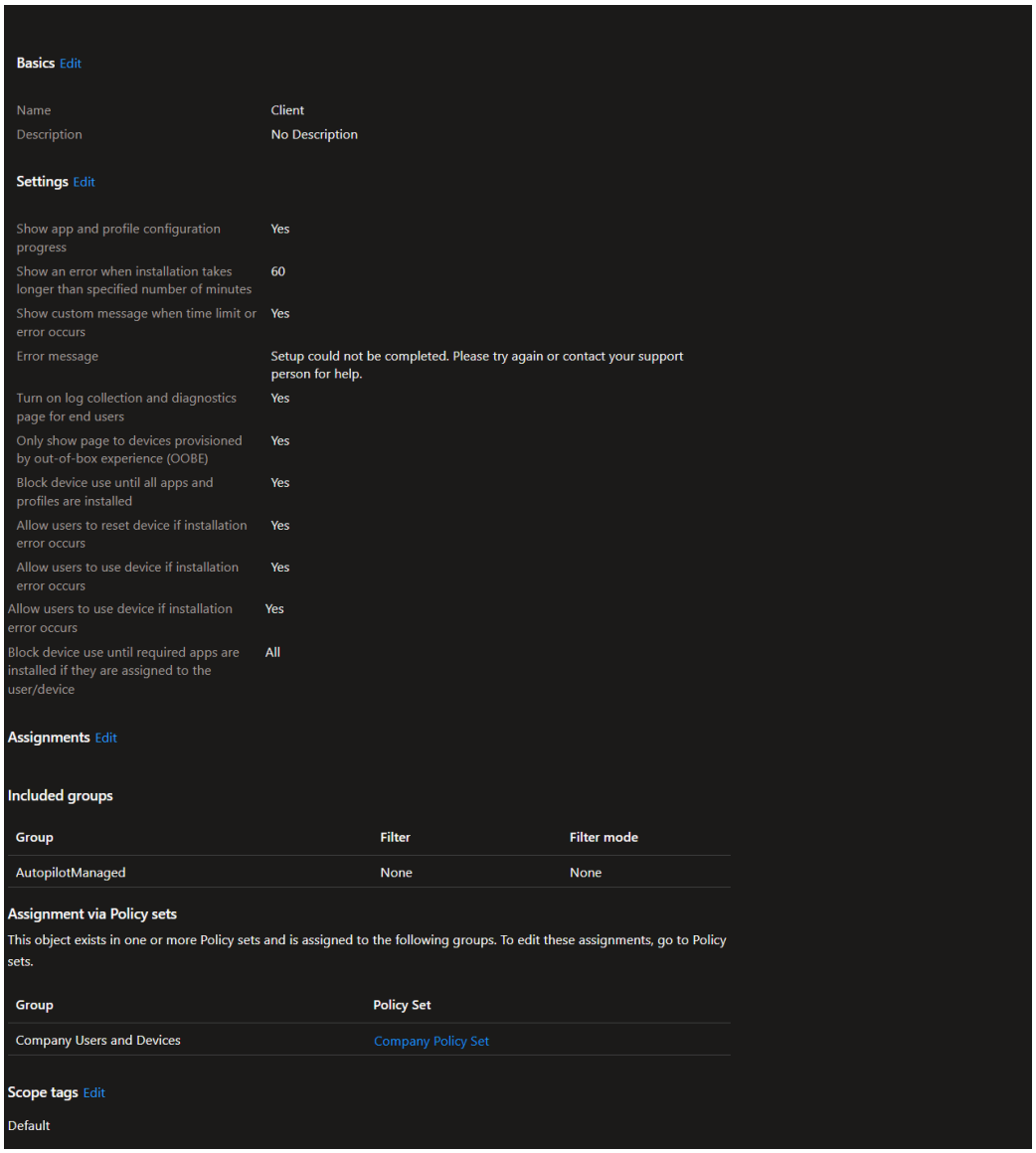
Footer

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.



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

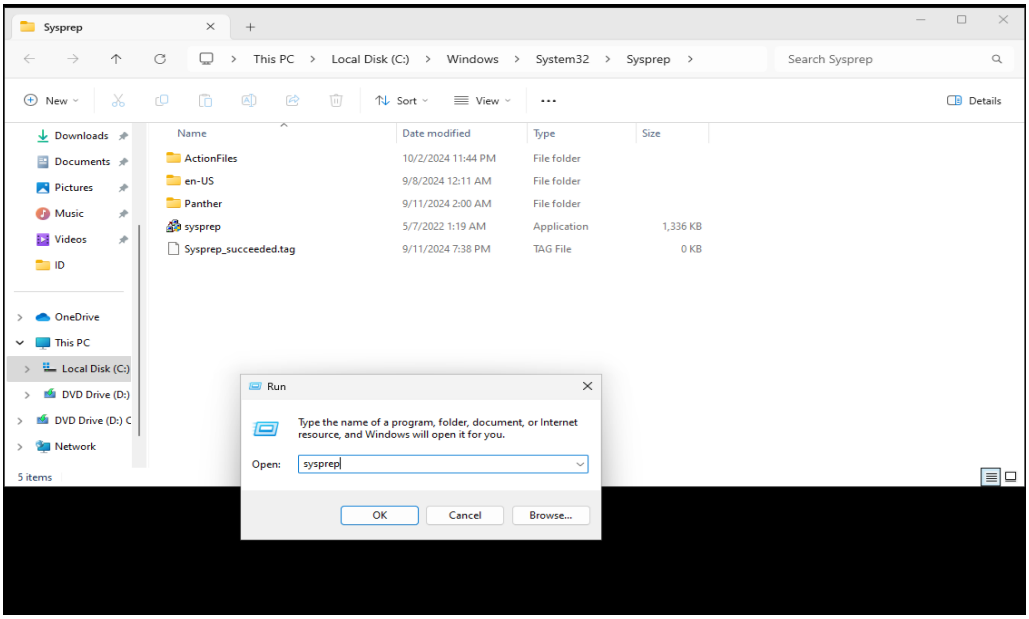
This object exists in one or more Policy sets and is assigned to the following groups. To edit these assignments, go to Policy sets.

Group	Policy Set
Company Users and Devices	Company Policy Set

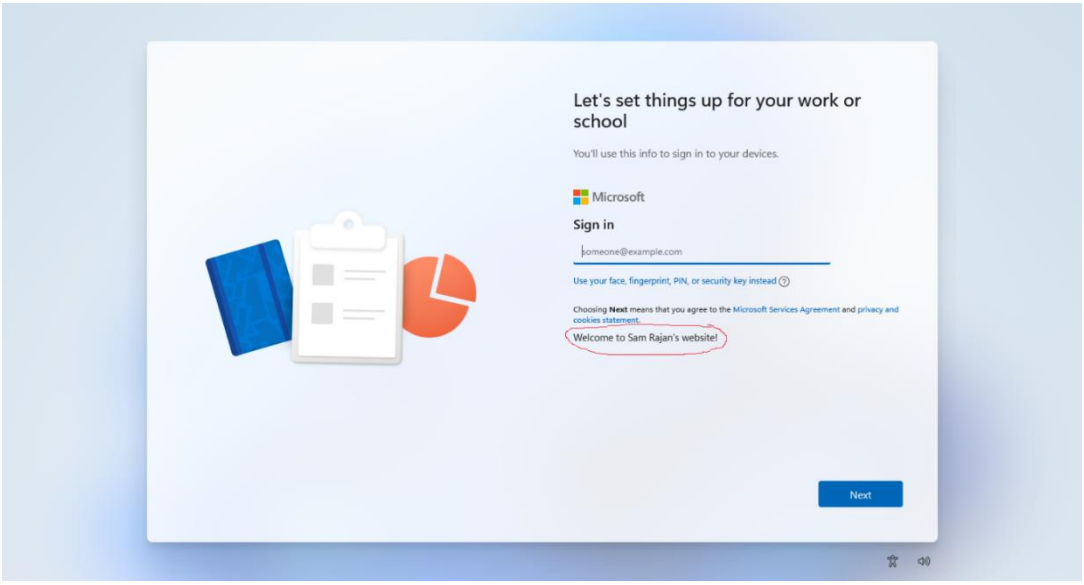
Scope tags Edit

Default

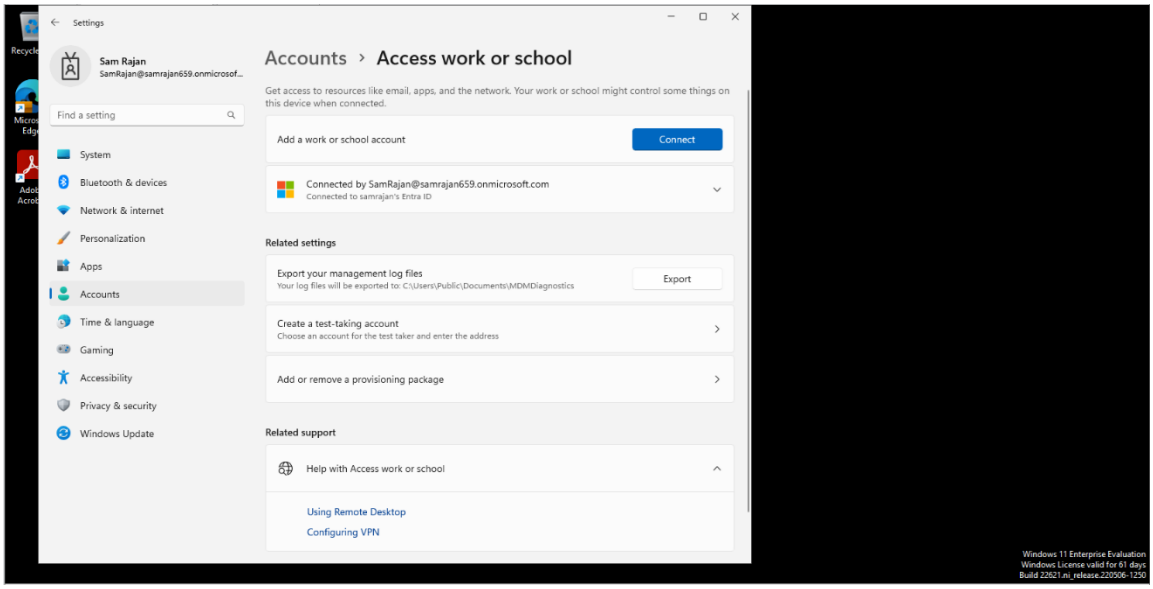
To test whether the enrollment status page settings would appear during the out-of-box-experience (OOBE), the sysprep tool was accessed and ran on the Windows 11 client. This was accessed via Start > Run > sysprep.exe



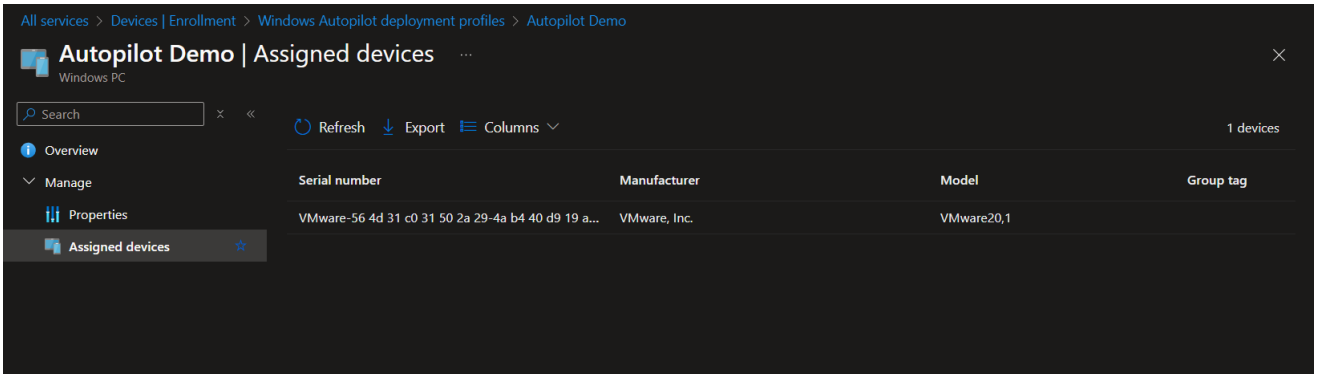
After the device rebooted, the OOBE began, and the welcome message configured in the enrollment status page was displayed.



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.

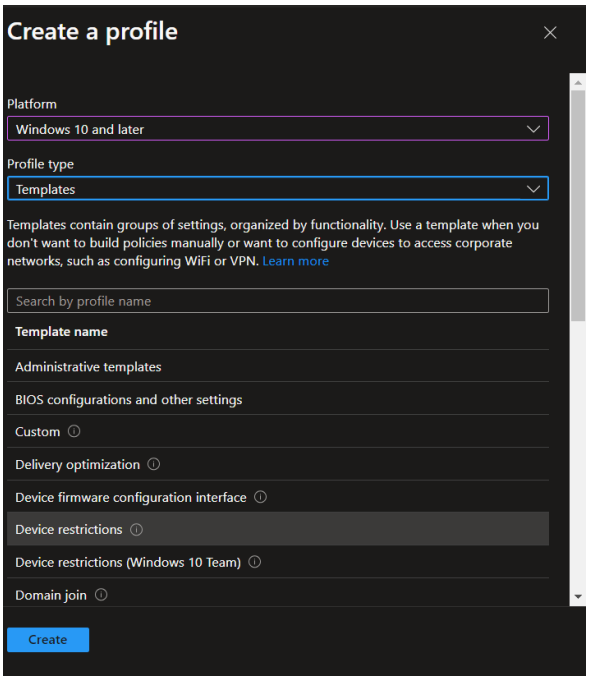


By navigating to Devices > Enrollment > Deployment Profiles > Autopilot Demo > Assigned Devices, the Windows 11 client device could be seen.

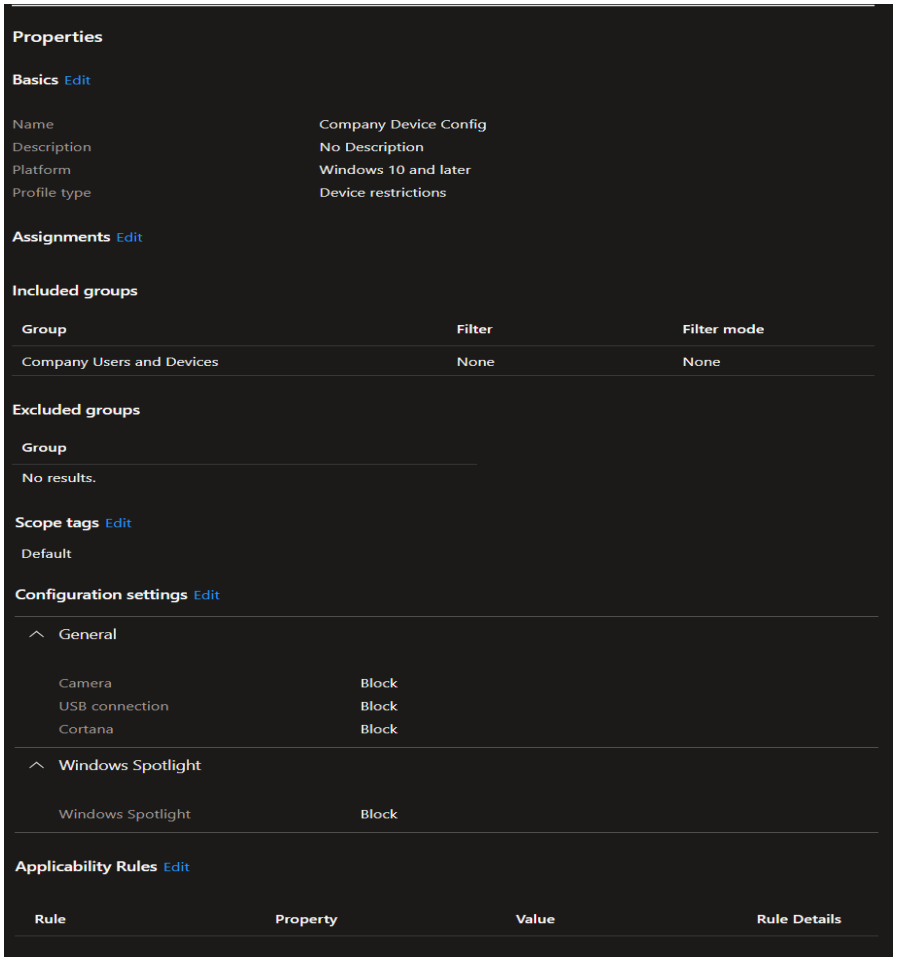


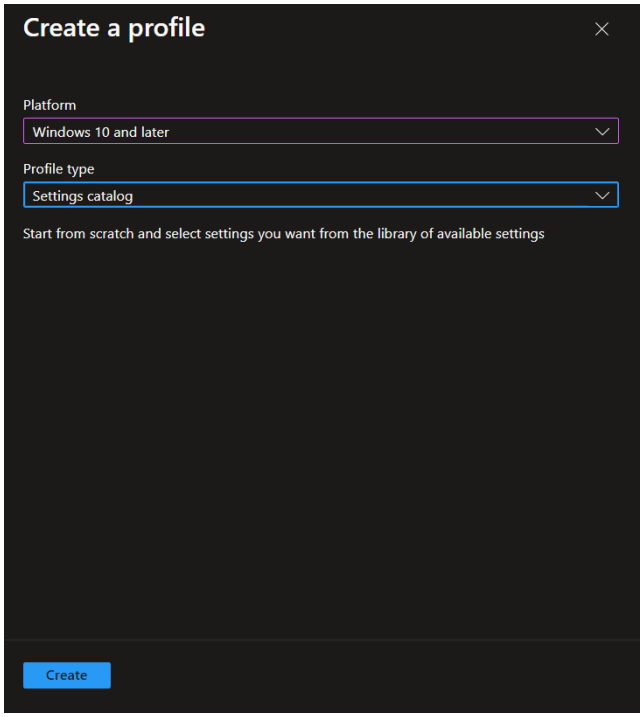
Implementing Device Configuration Profiles

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.

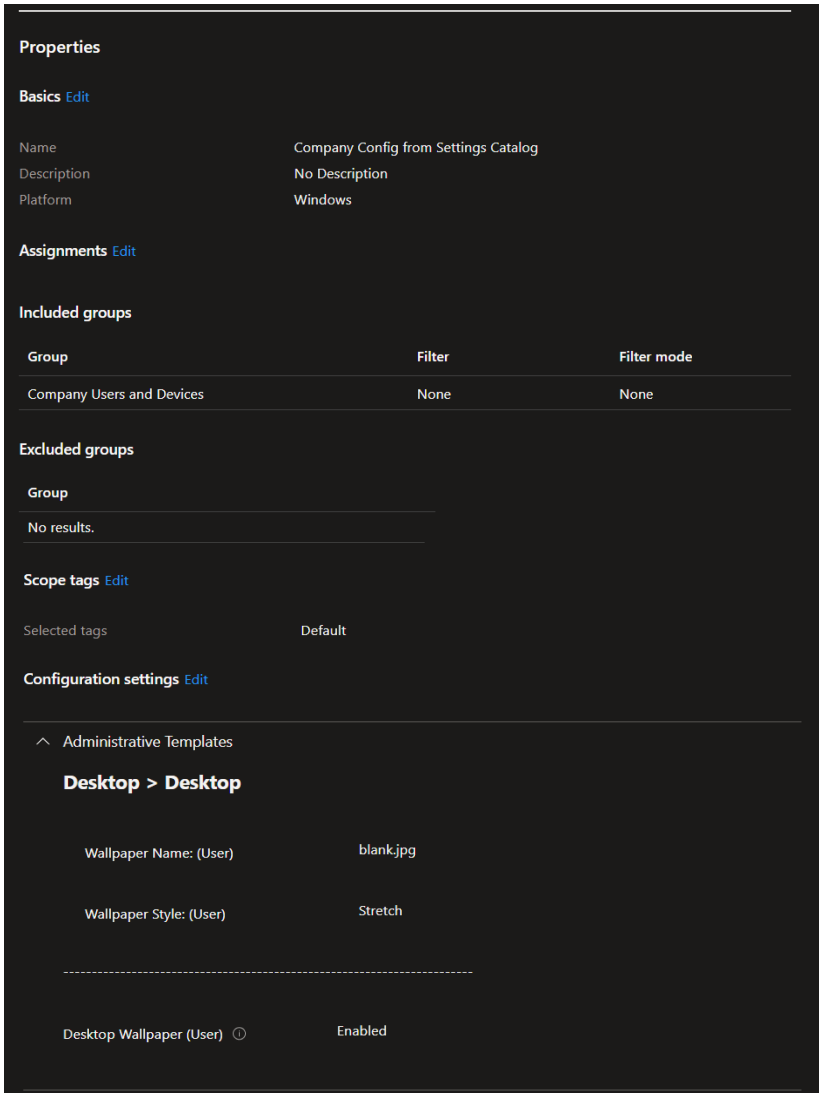


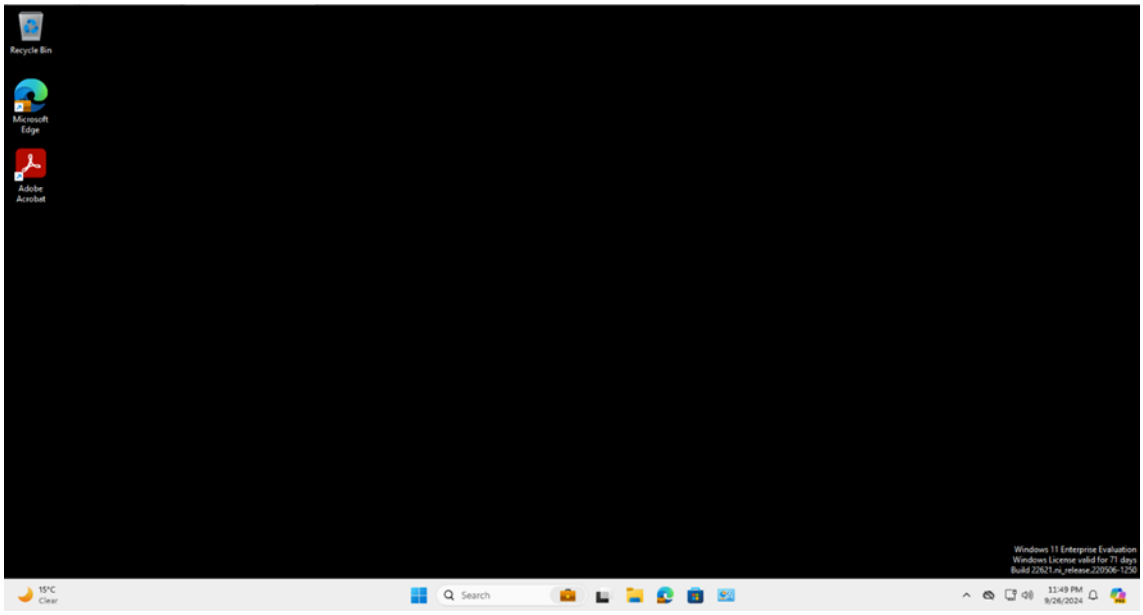
This device configuration profile was created using the templates profile type to configure device restrictions for Windows 10 and later devices using the device restrictions template.





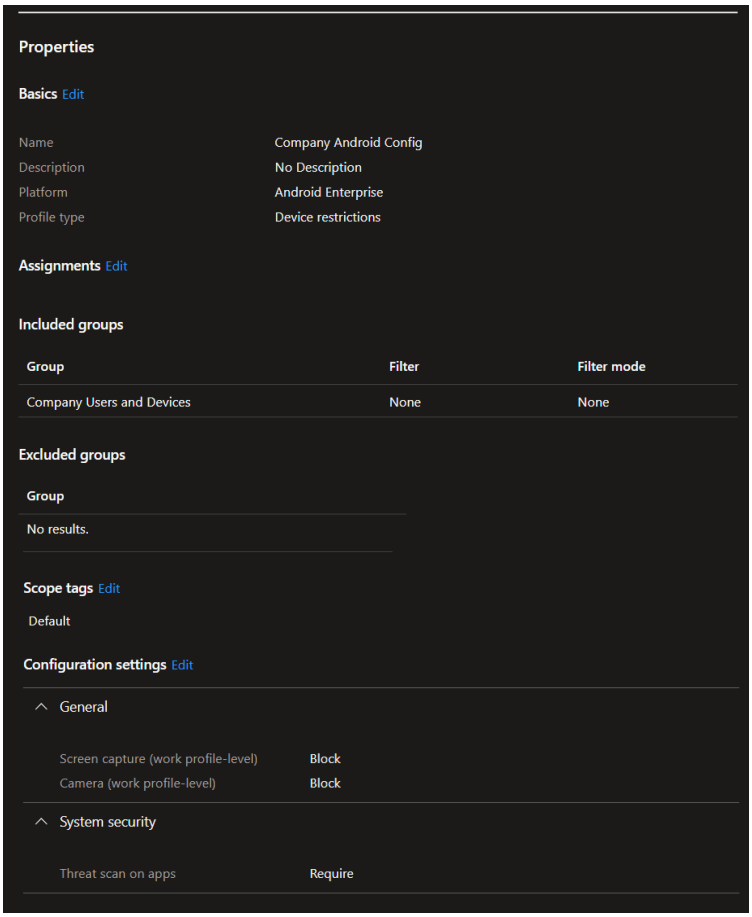
This device configuration profile was created for Windows 10 and later devices using the settings catalog profile type.



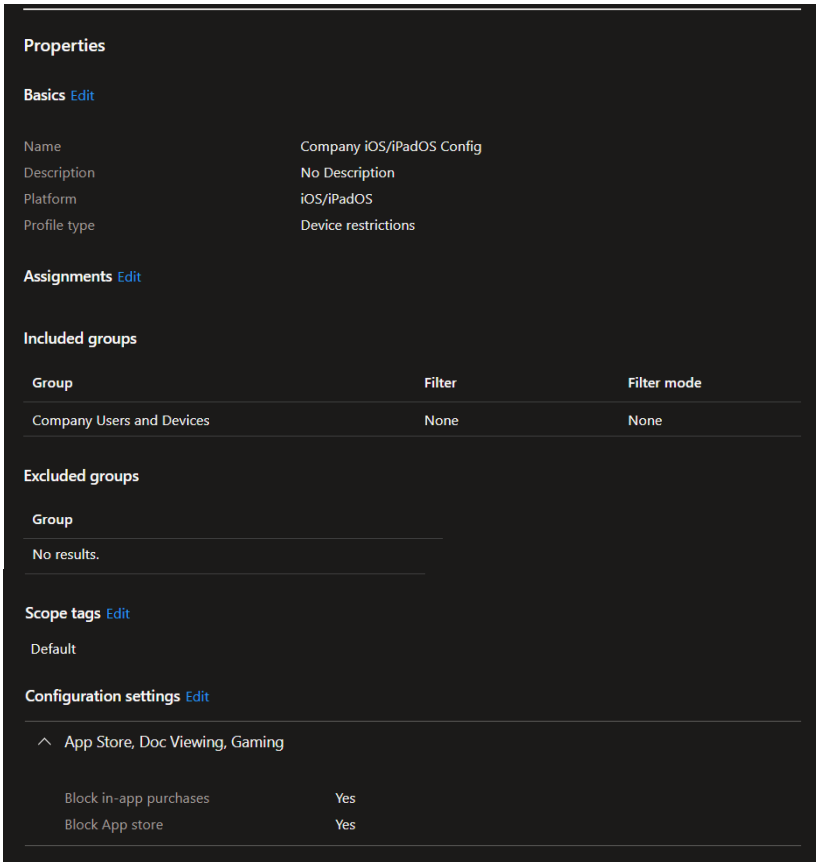


The background image on the client is a black screen because the wallpaper location was unspecified in the settings catalog configuration profile.

Configuration profiles were also created for Android and iOS devices.

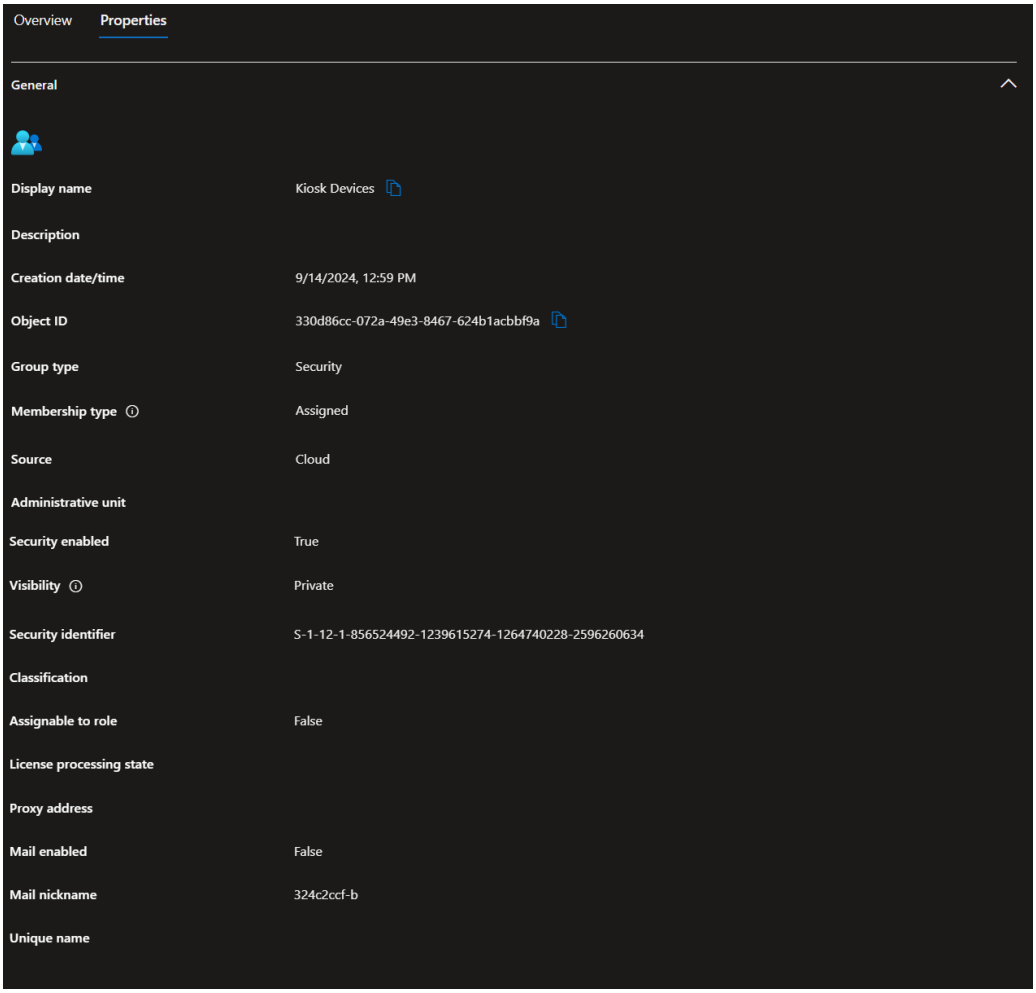


Android configuration profile.

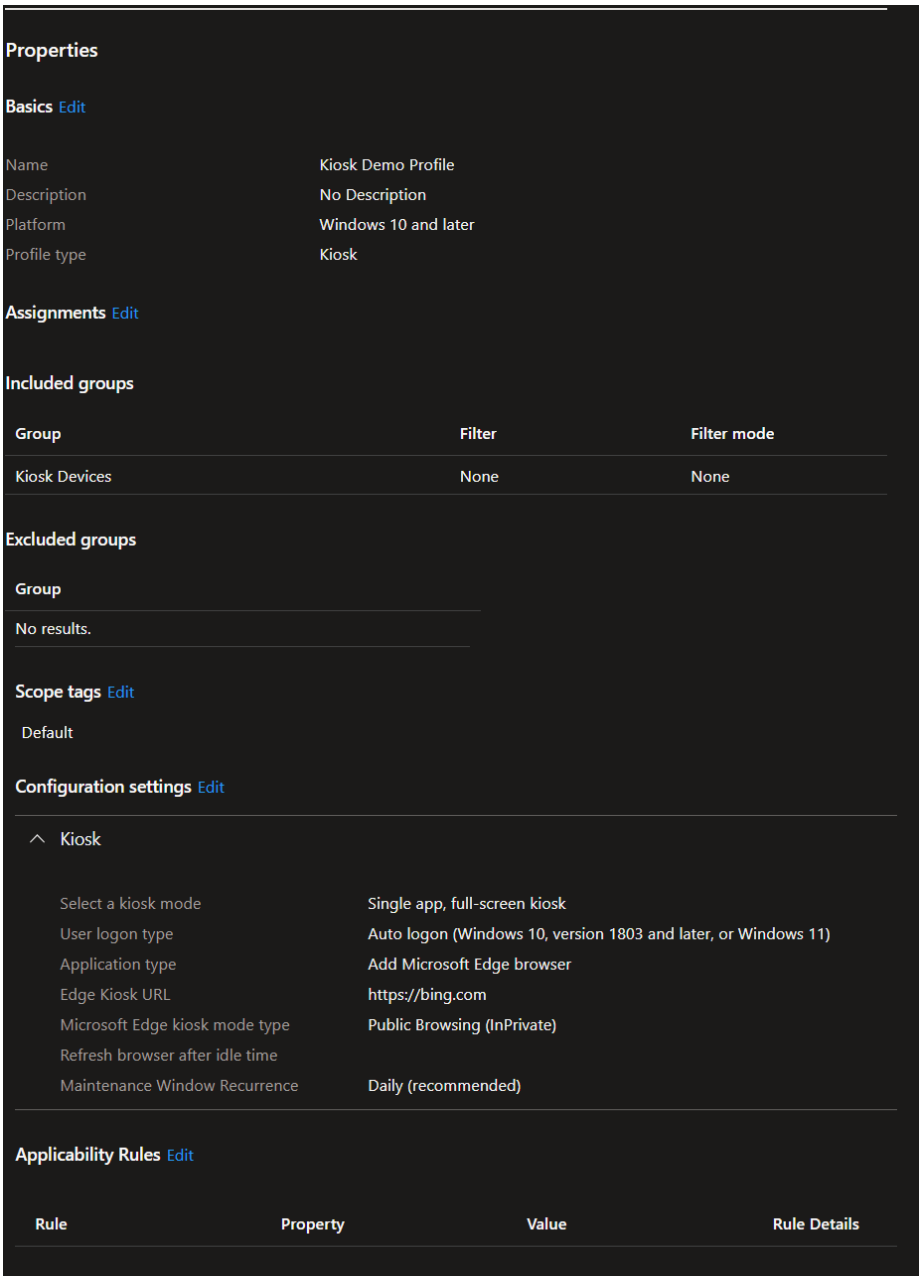


iOS configuration profile.

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.



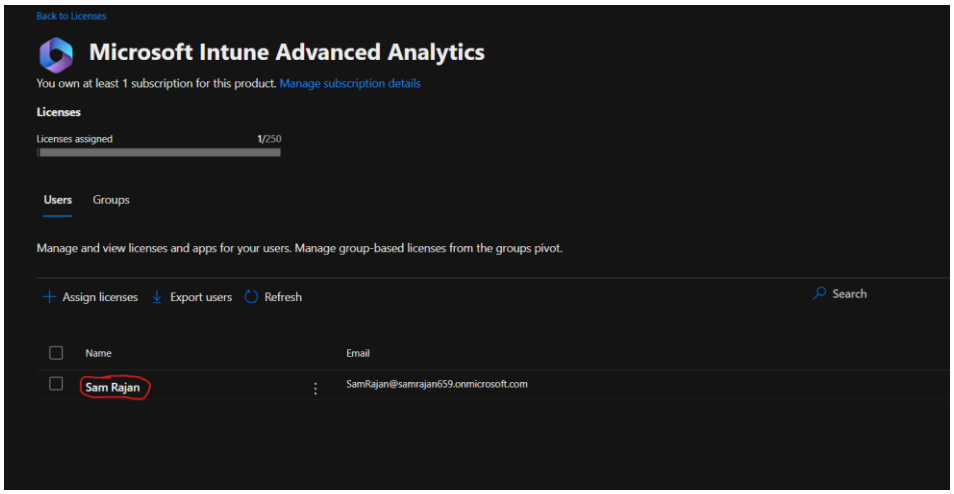
Then, a configuration profile was created (Devices > Configuration > Policies > Create) using the templates profile type and a kiosk mode template.



Implementing Intune Suite Add-on Capabilities

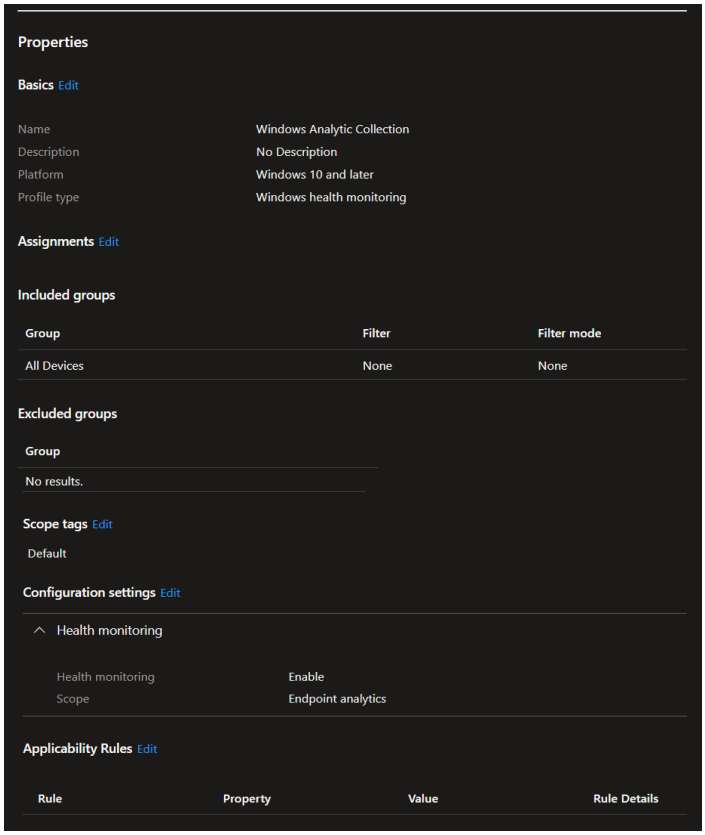
One of the Intune Suite add-ons that was implemented is Intune Advanced Analytics. Intune Advanced Analytics is used to proactively detect and resolve endpoint issues, streamline troubleshooting process, and improve users' technology experience. The product (trial) was first obtained, and a license was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

.

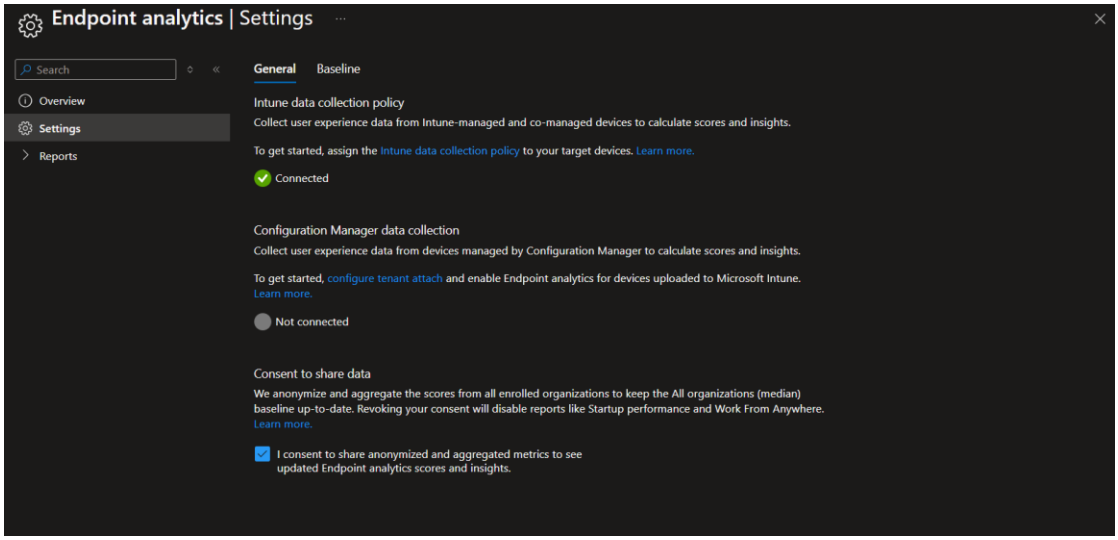


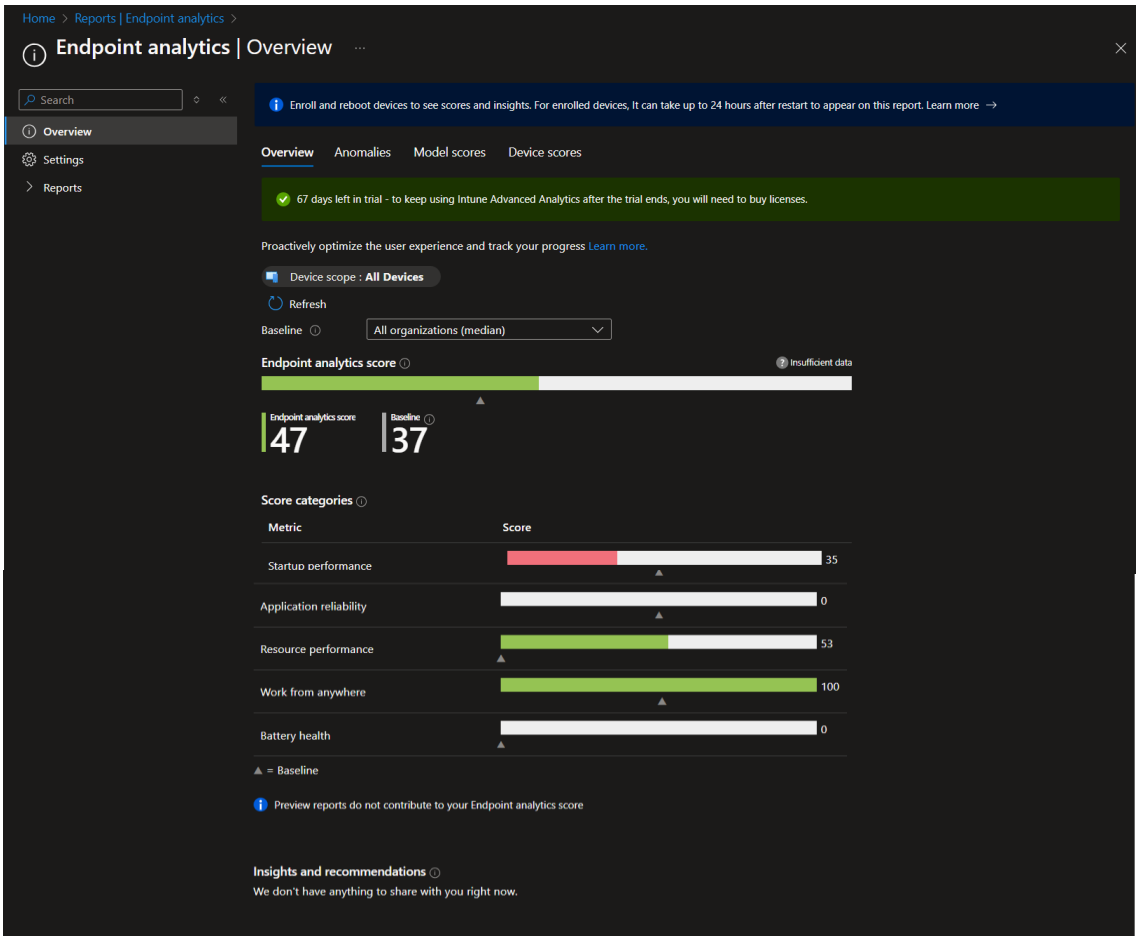
The Intune Advanced Analytics license was assigned to Sam Rajan (Billing > Licenses > Microsoft Intune Advanced Analytics > Assign licenses).

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.



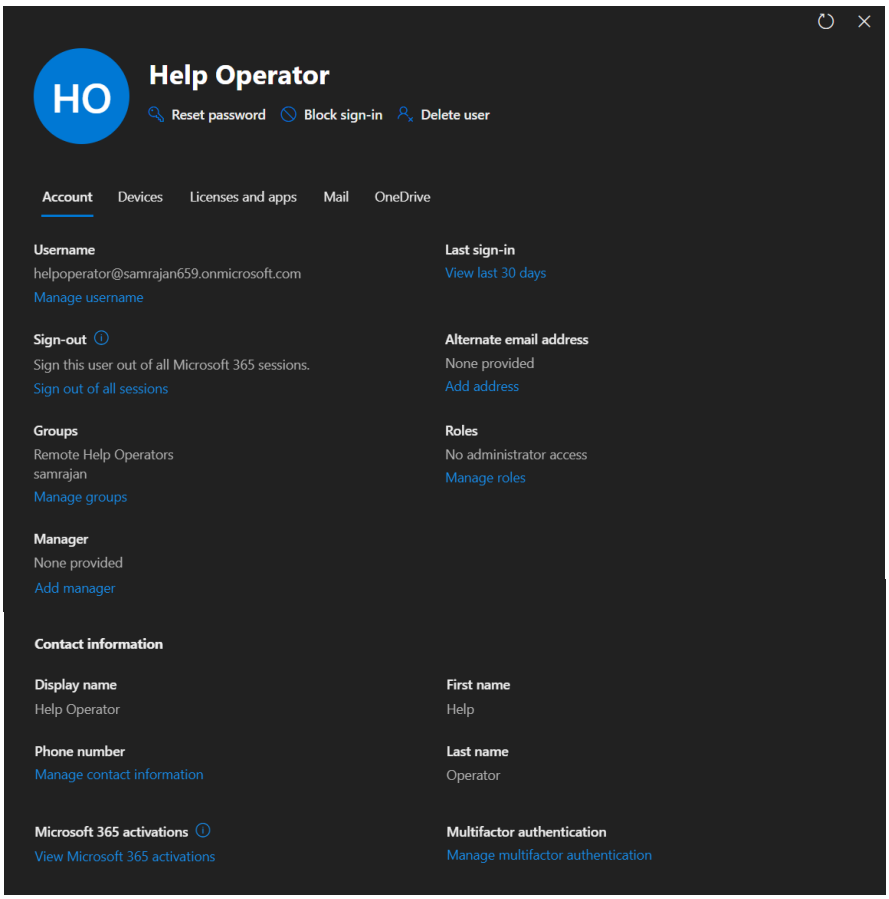
Navigating to Reports > Endpoint Analytics > Settings provided confirmation that the Intune data collection policy is connected. This was required for endpoint analytic data to be collected.



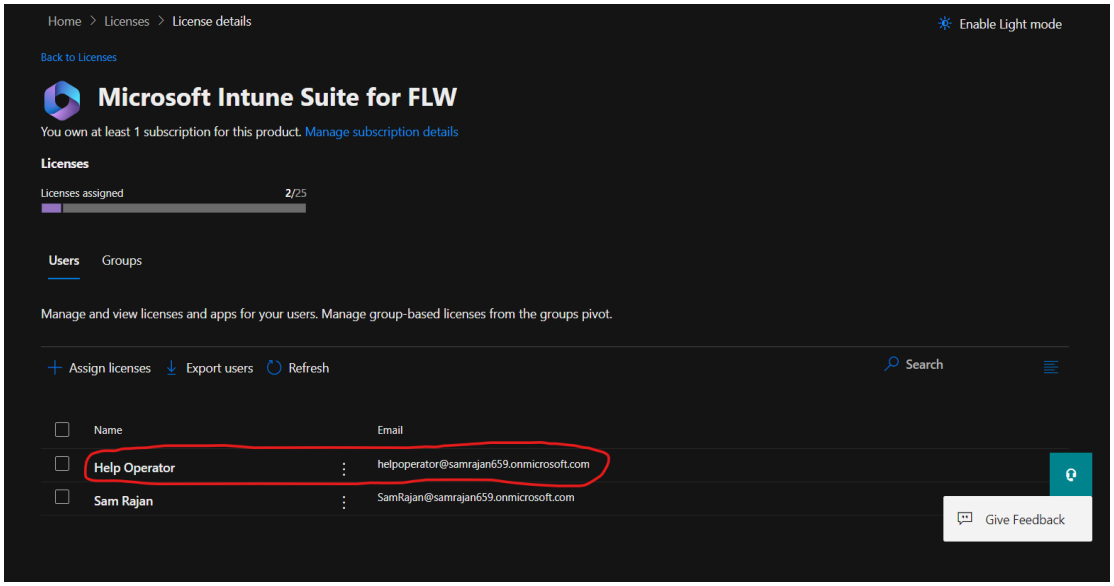


Endpoint Analytic data has been collected (Reports > Endpoint Analytics > Overview).

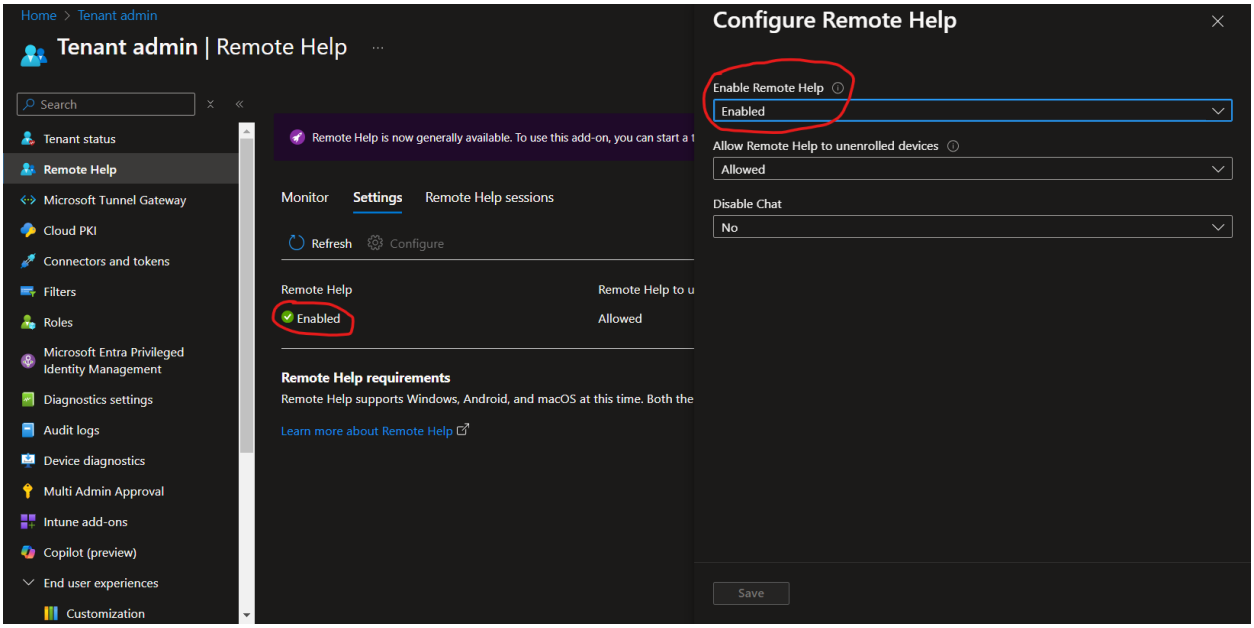
Remote Help is an Intune add-on which allows permitted users to connect to other users' devices and provide helpdesk support. Remote Help was configured in this lab. Before configuring Remote Help, a user named "Help Operator" was added in the Microsoft 365 admin centre (admin.microsoft.com). This account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



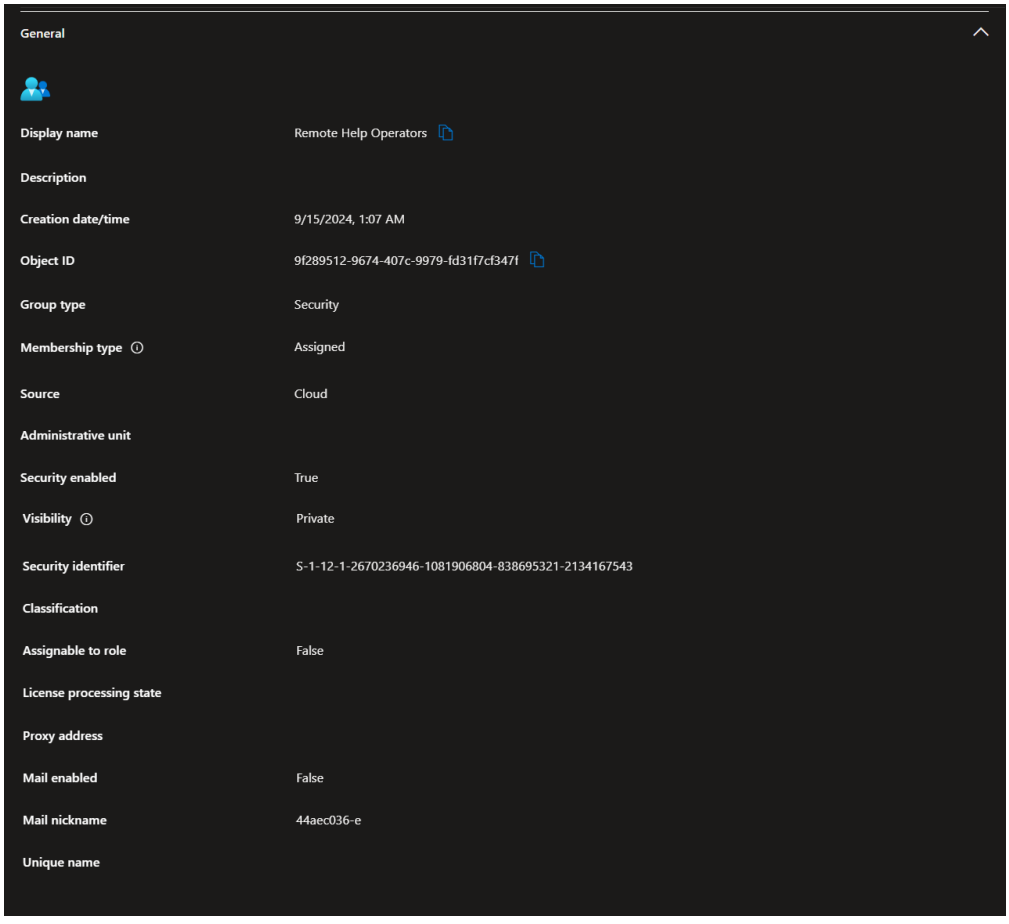
Remote Help had to be obtained via a trial subscription for Microsoft Intune Suite for FLW as a trial subscription for Remote Help doesn't exist. The license was assigned to "Help Operator" and the global administrator (Sam Rajan).

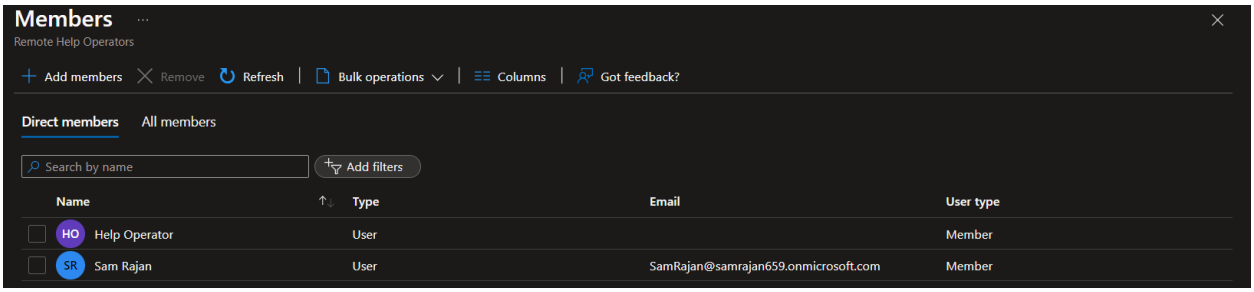


Remote Help needed to be enabled in Intune by navigating to Tenant administration > Settings > Configure.



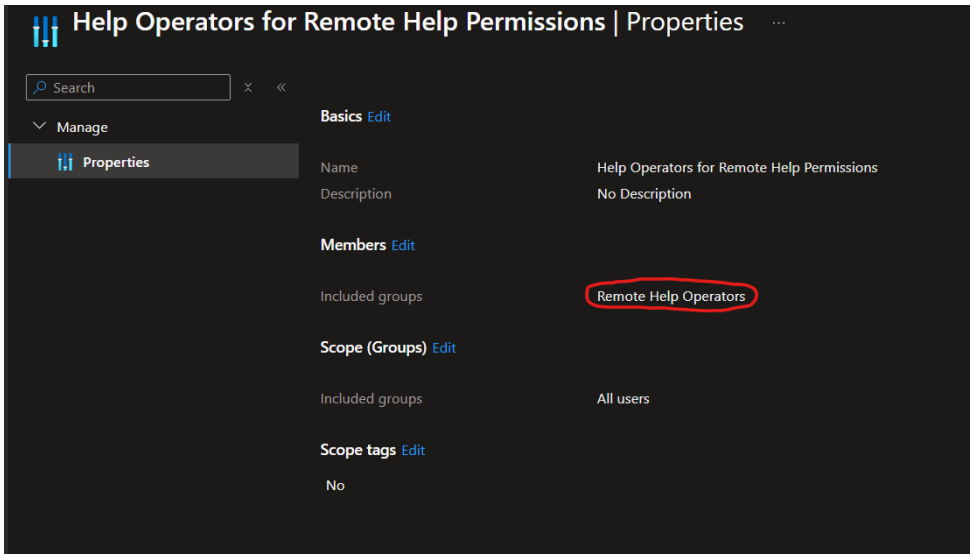
Next, a group for the help desk operators called “Remote Help Operators” was created (Groups > New group).





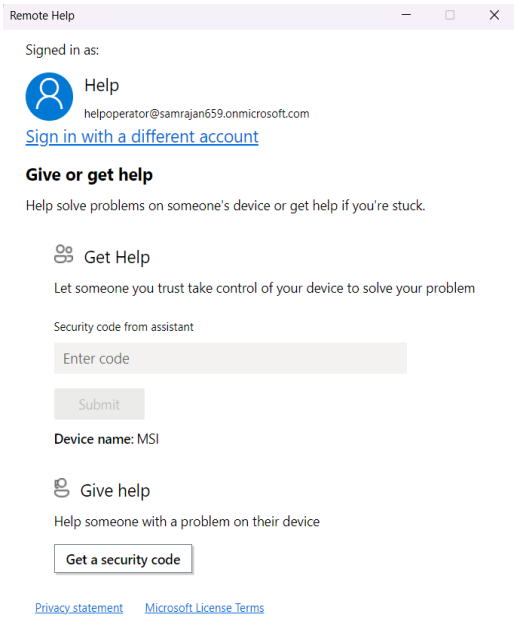
Members of the group.

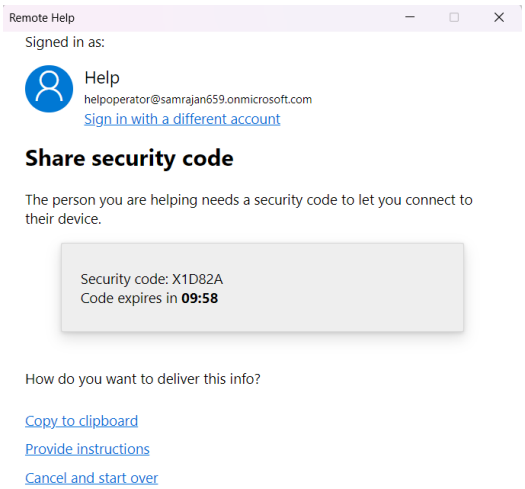
The help desk operator role was assigned to this group by navigating to Tenant administration > Roles > Help Desk Operator > Assignments > Assign.

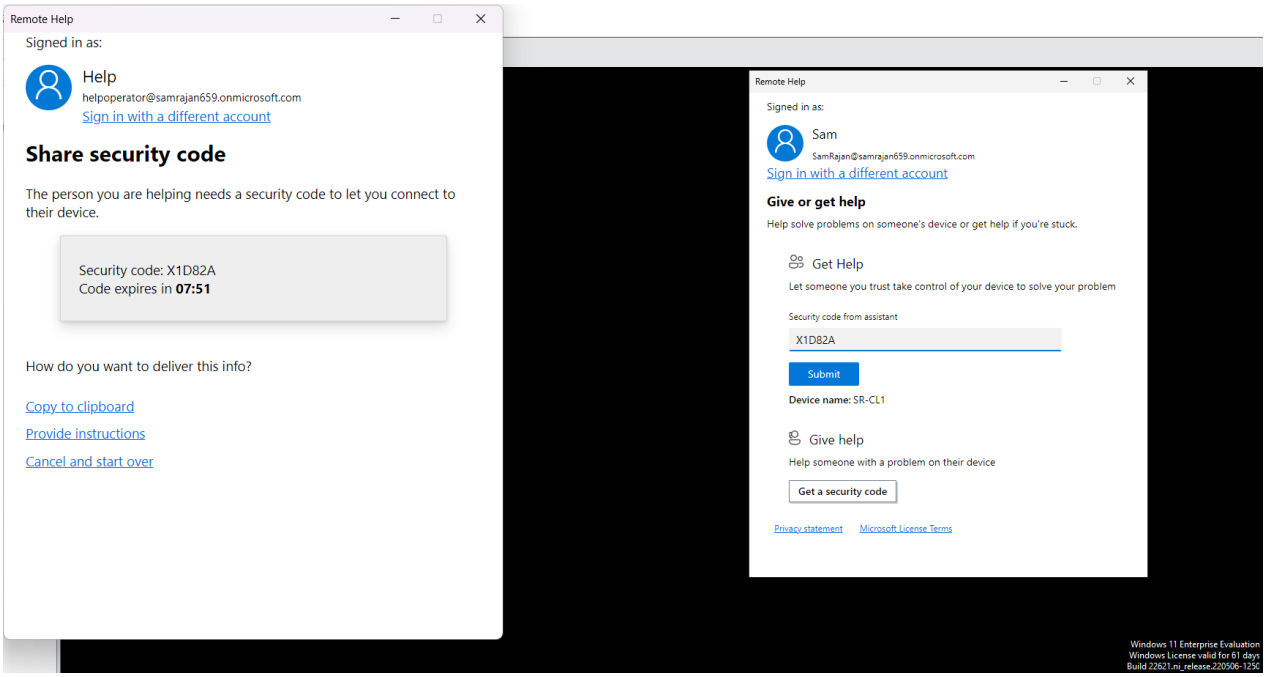


The role was assigned to the Remote Help Operators group.

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 provided a code that a user in need used to initiate a remote helpdesk session.

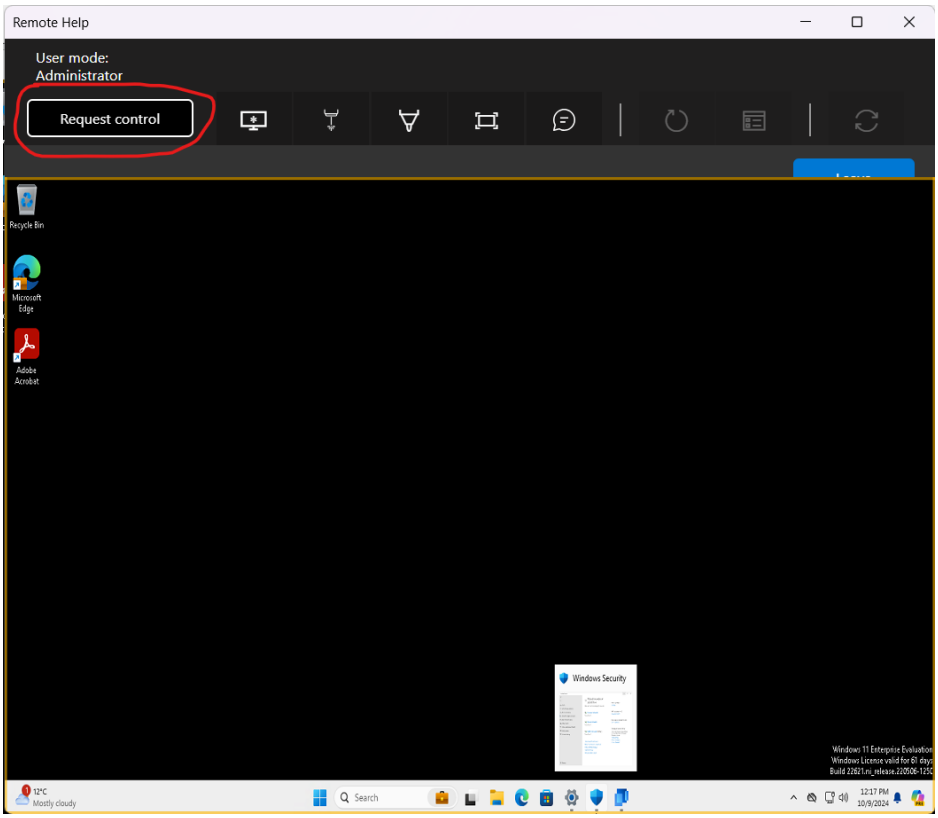




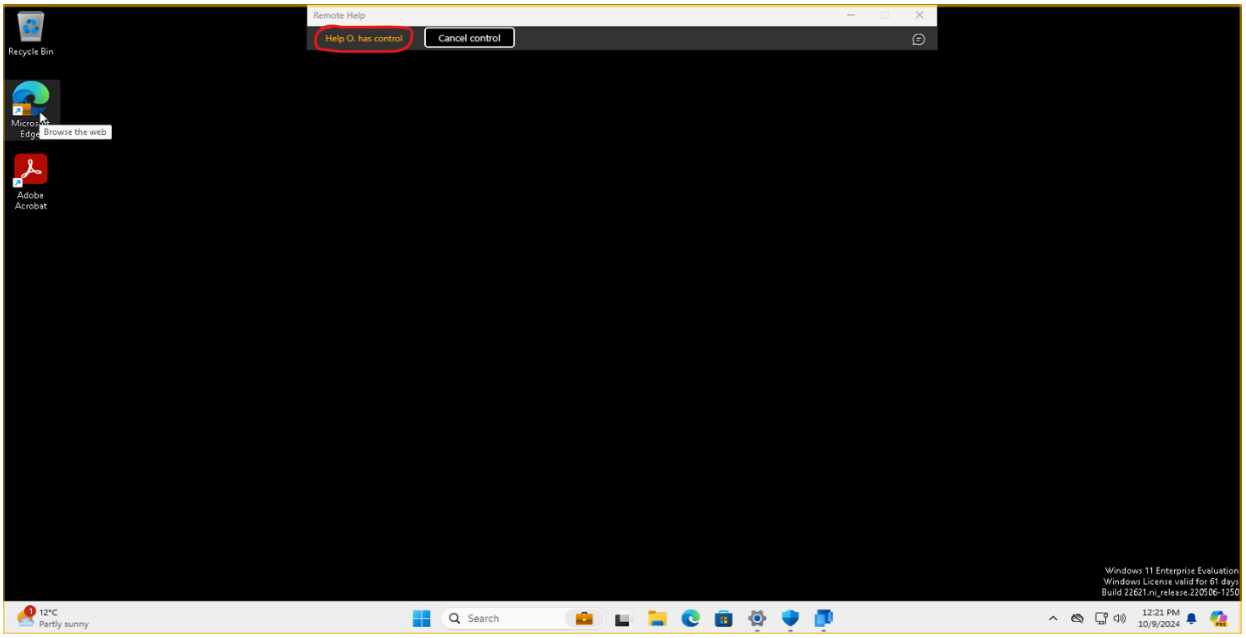


The user must enter the code given from the helpdesk operator.

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

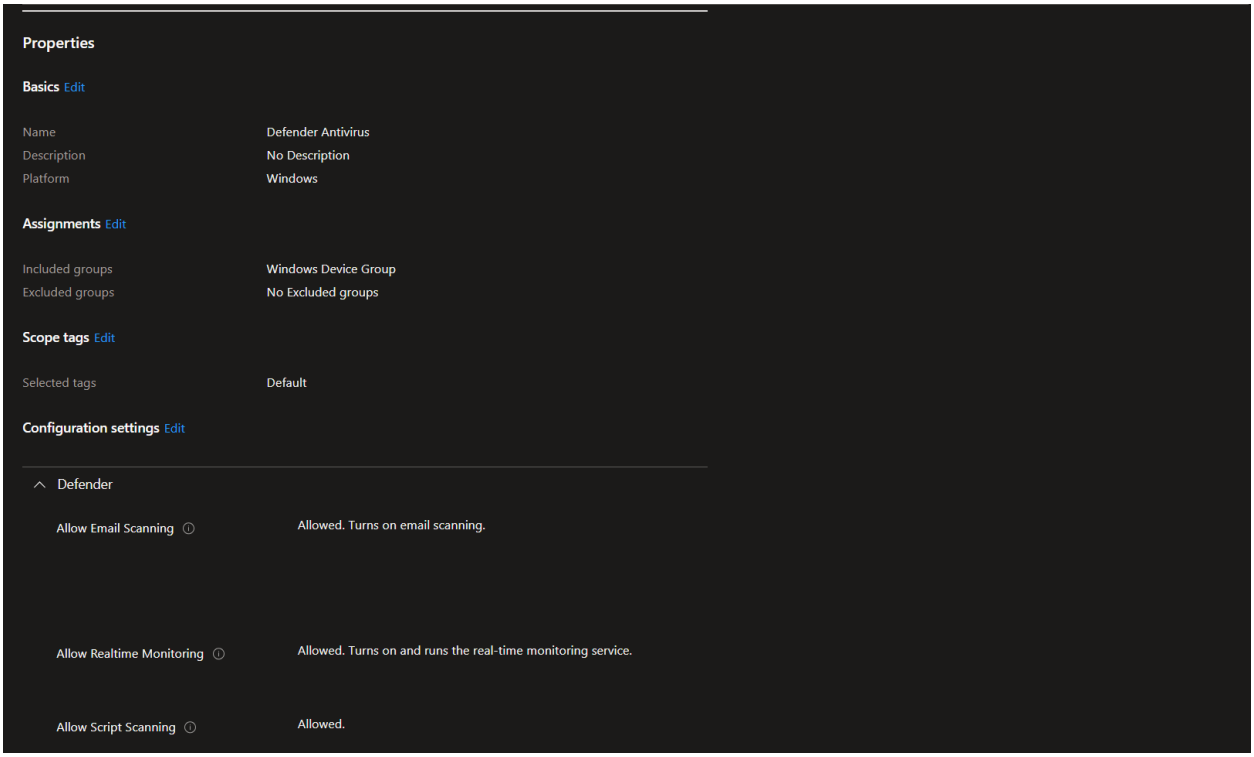


Once the help desk operator was given permission to control the device by the user, the help desk operator was able to freely move the user’s cursor and give support.

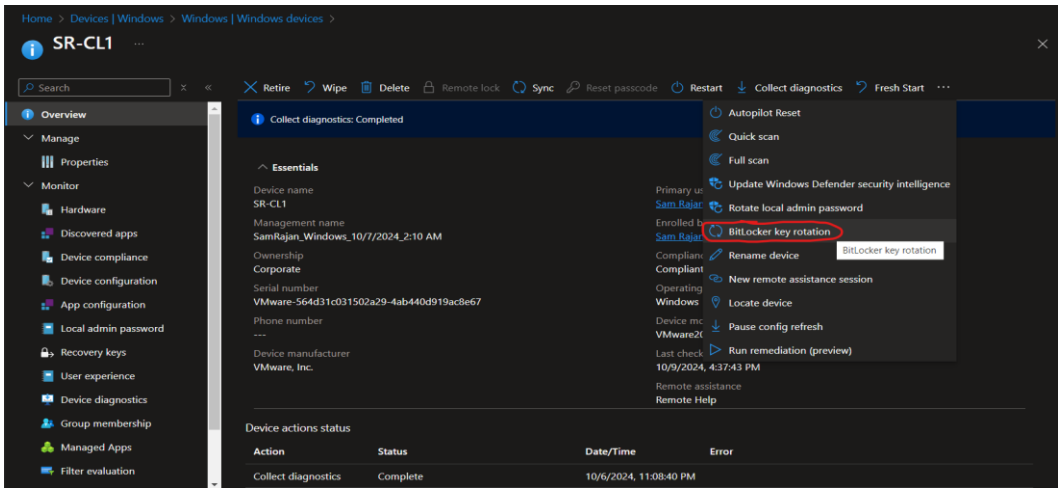


Performing Remote Actions on Devices via Intune

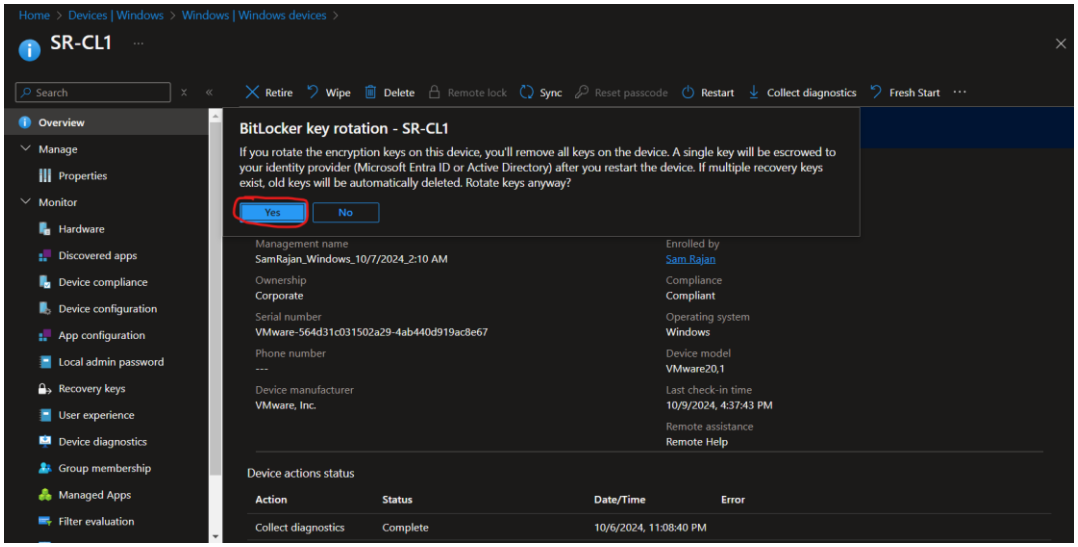
The first remote action performed was updating the Windows Antivirus settings. This was done by configuring a policy by navigating to Endpoint Security > Antivirus > Create Policy.

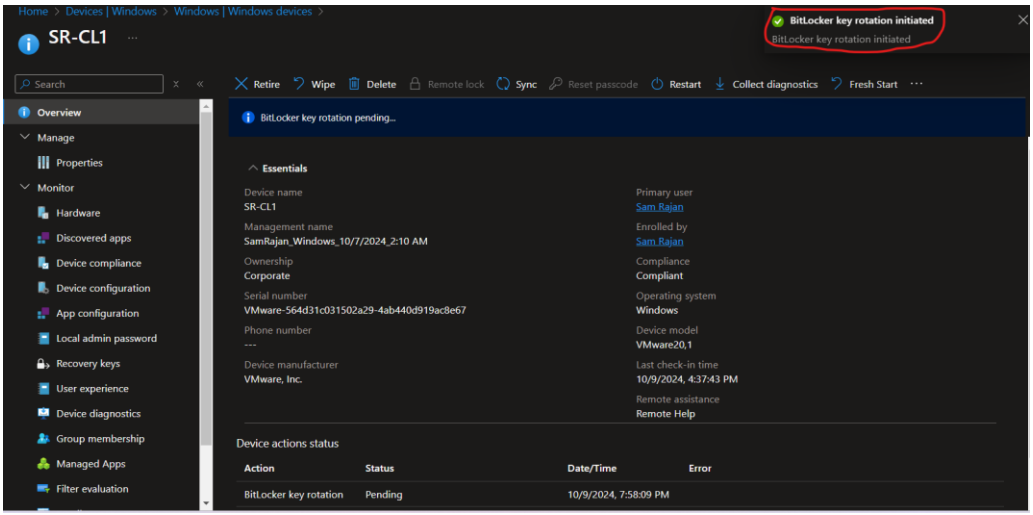


Another remote action performed was rotating the BitLocker recovery keys. BitLocker is a full-volume disk encryption software that helps protect the entire operating system drive against offline attacks. When BitLocker sees a new device in the boot list or an attached external storage device, it prompts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



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

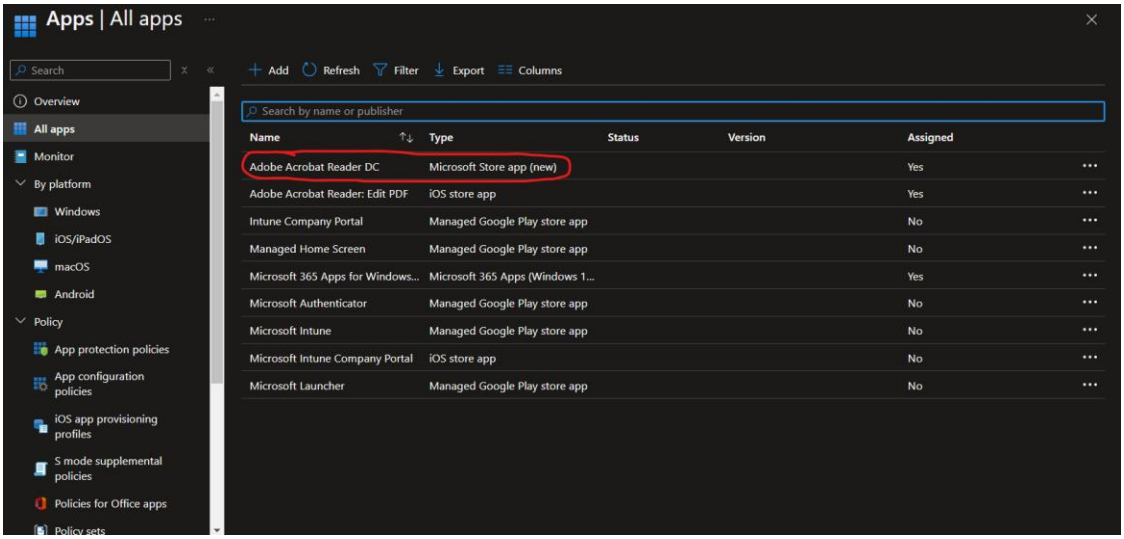




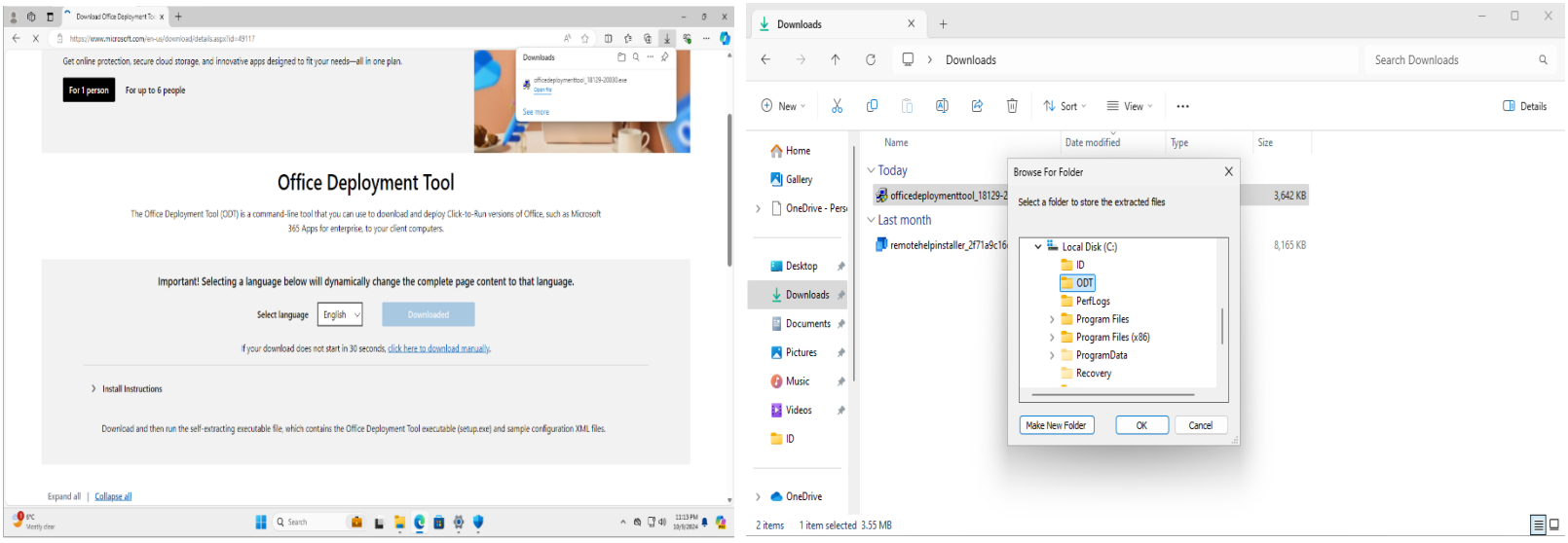
The Bitlocker key rotation has been initiated.

Deploying and Updating Apps

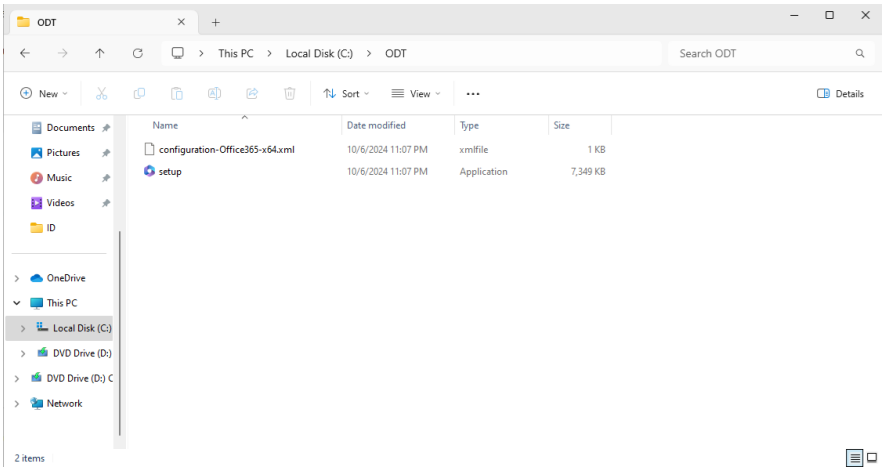
Intune can be used (and was used) to deploy apps to devices. One such app that was deployed using Intune was Adobe Acrobat Reader DC. It was deployed by navigating to Apps > All apps > Add and was installed directly from the Microsoft Store.



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.

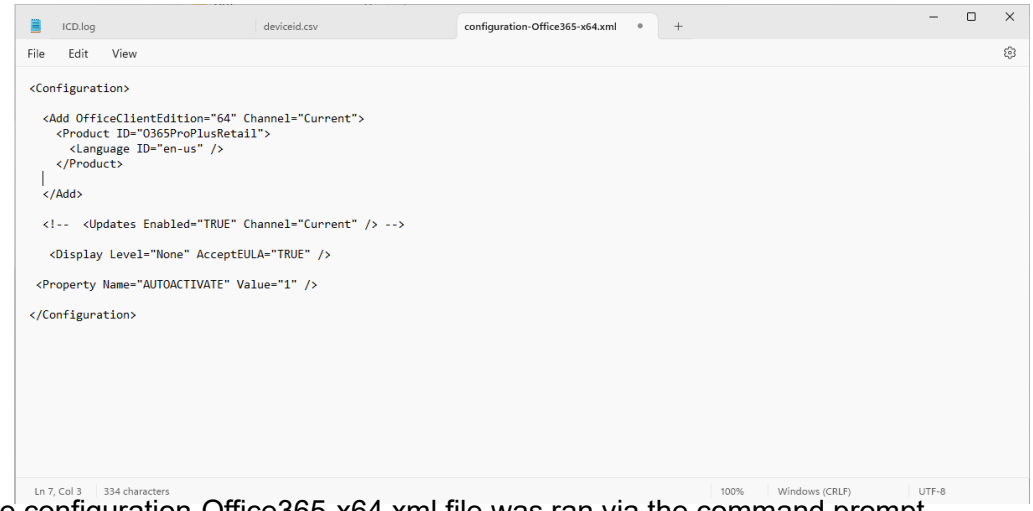


The ODT files were installed and stored in the "ODT" folder on the client's C:\ drive.

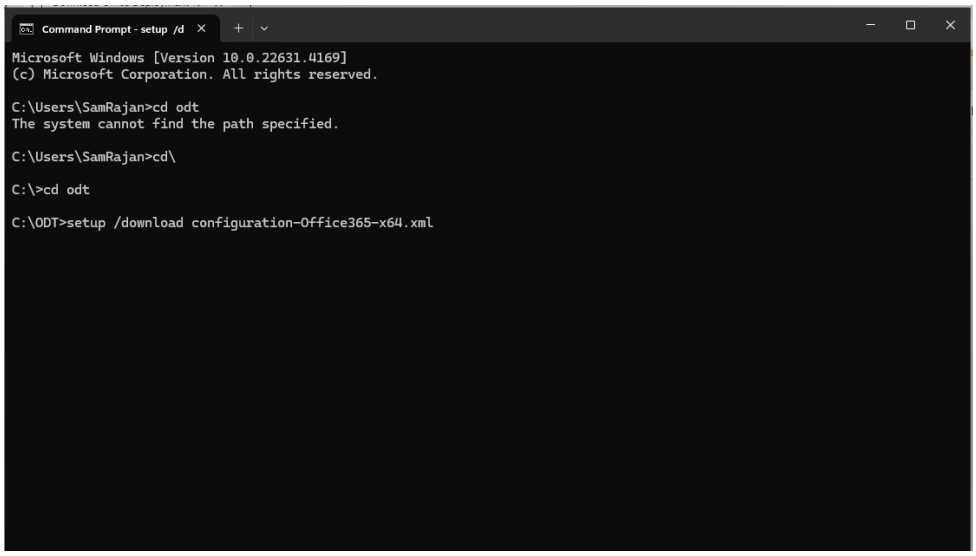


The files have successfully been extracted.

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

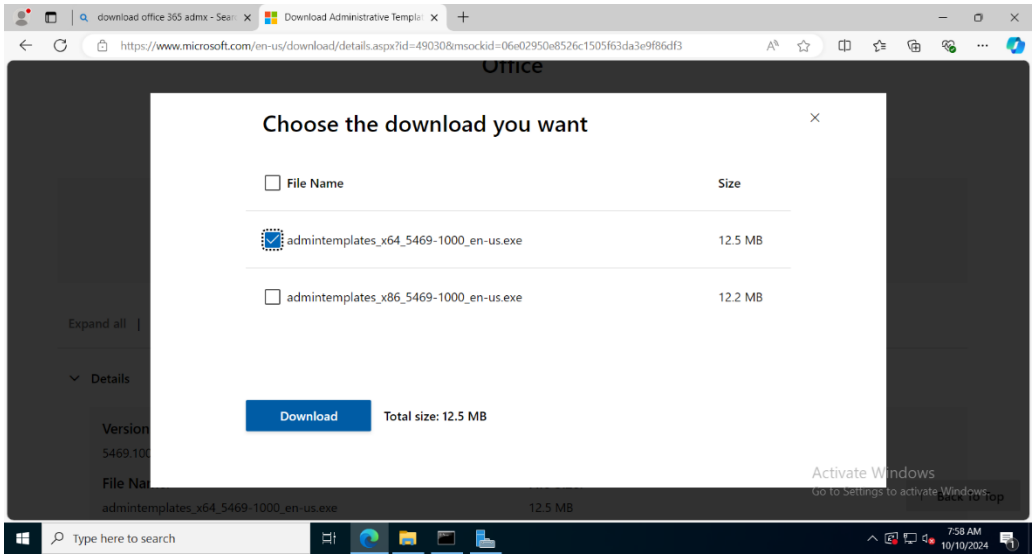


Next, the configuration-Office365-x64.xml file was ran via the command prompt.

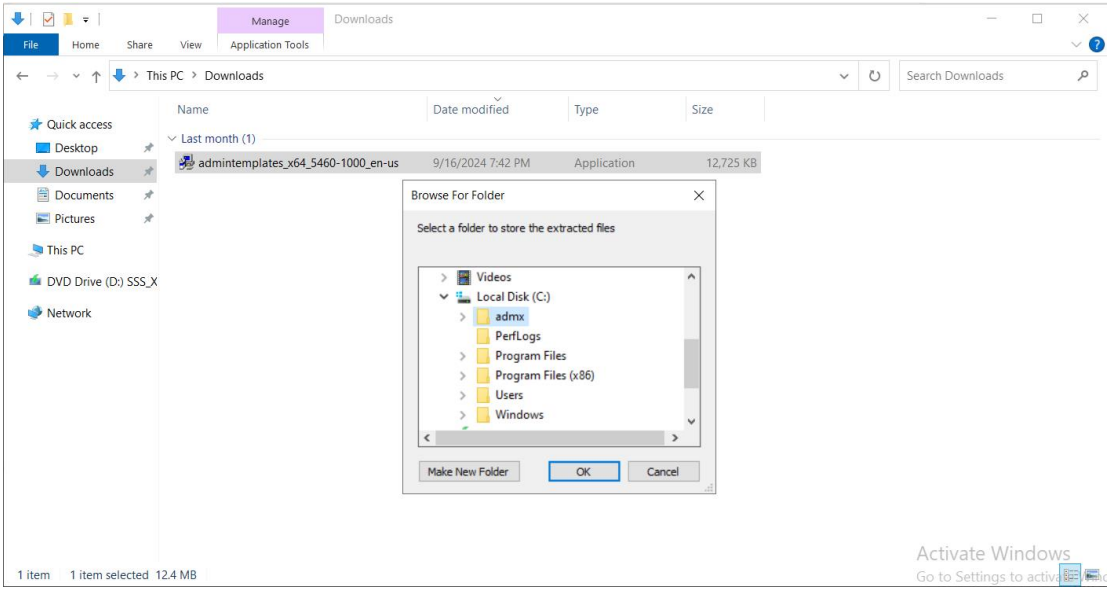


After this point, the Click-to-Run versions of the 365 apps will download onto the client.

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.

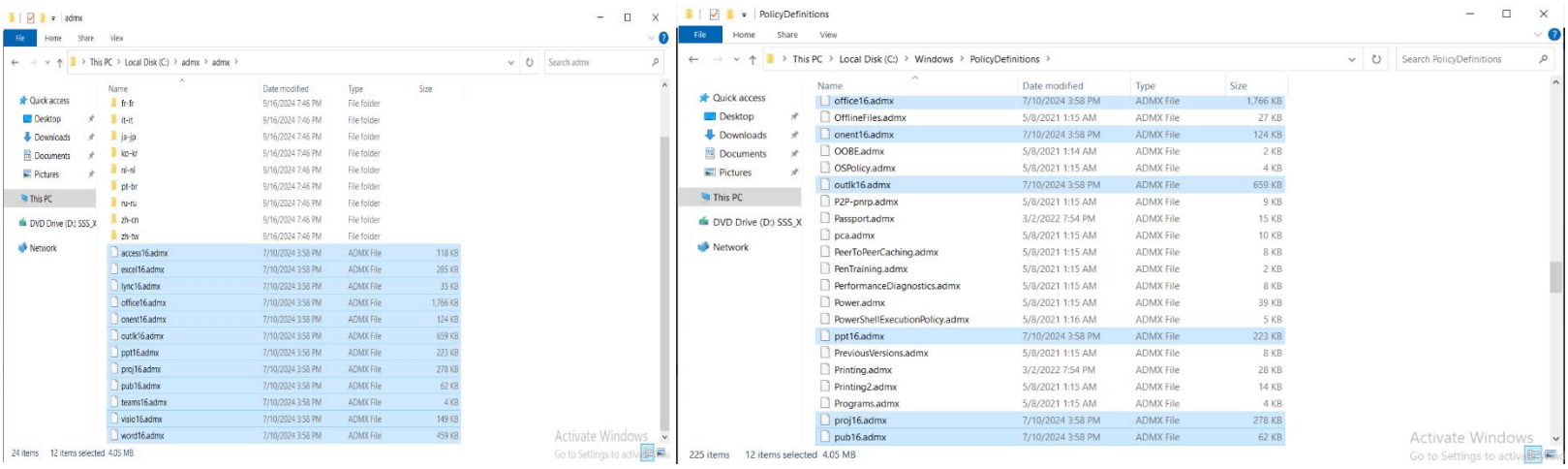


After navigating to https://www.microsoft.com/en-us/download/details.aspx?id=49030&msockid=06e02950e8526c1505f63da3e9f86df3, the 64-bit version of the ADMX/ADML files were downloaded.



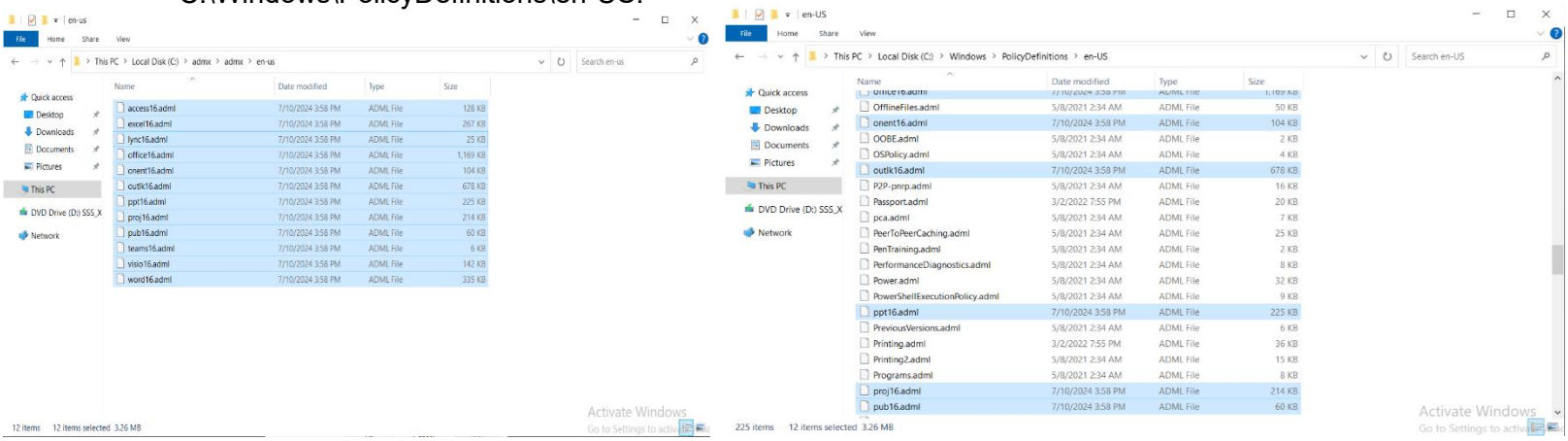
The setup file was run, and the files were extracted to a folder called “admx” on the C:\ drive.

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



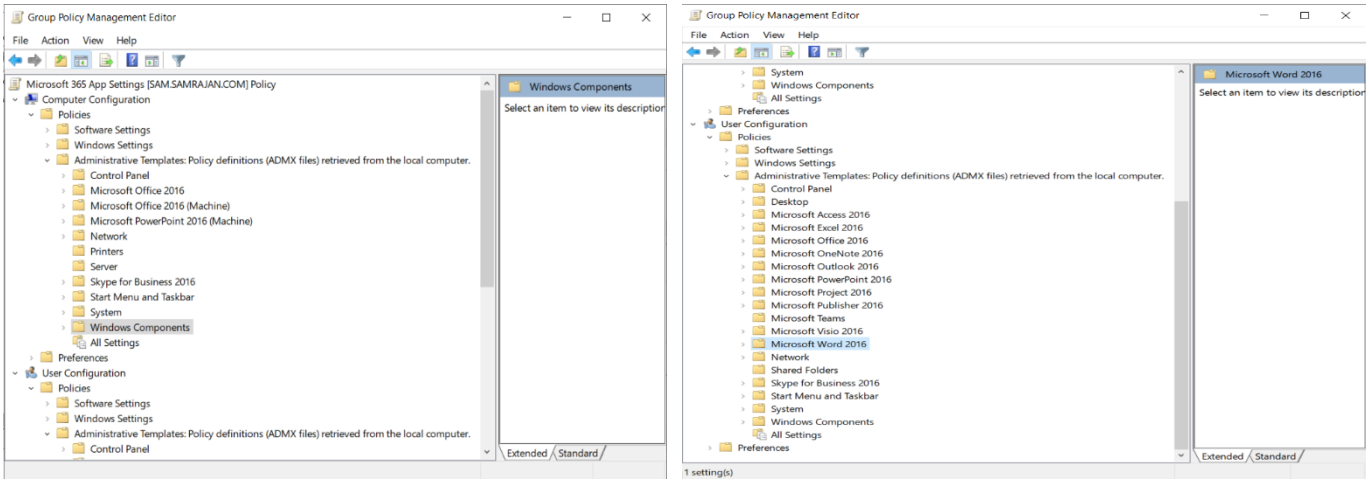
The files were copied and transferred.

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

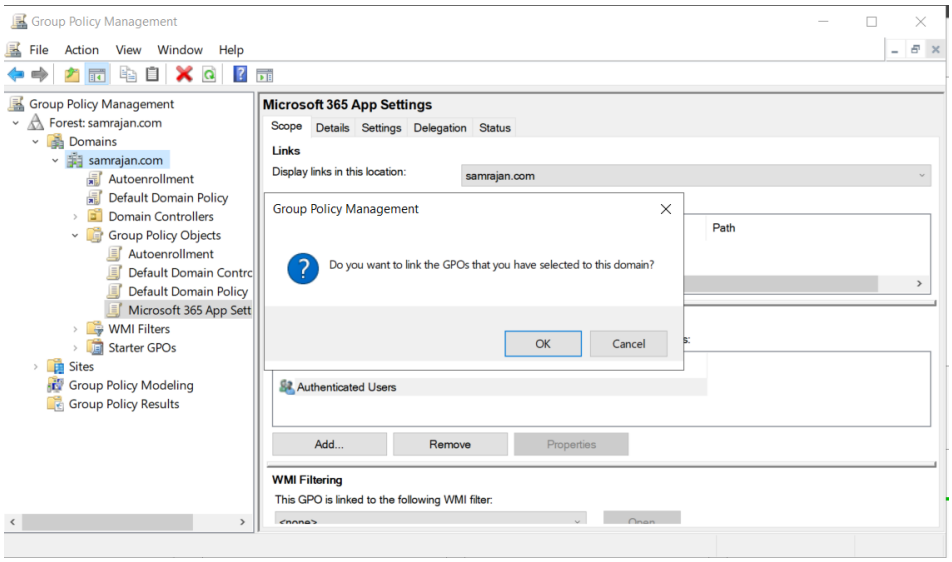


The files were copied and transferred.

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.

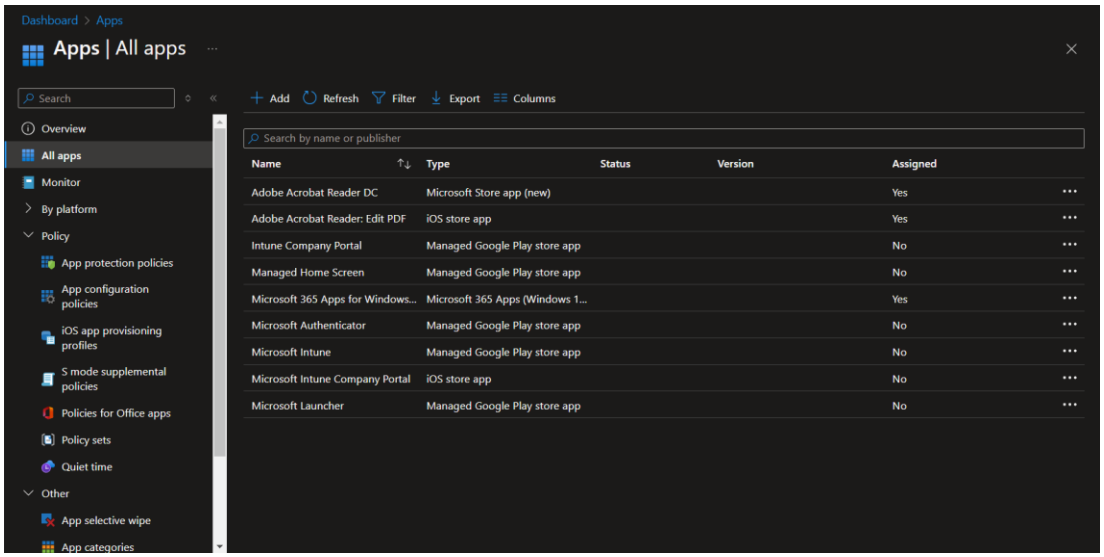


The Microsoft 365 App Settings GPO could then be dragged and dropped over the company domain (samrajan.com).



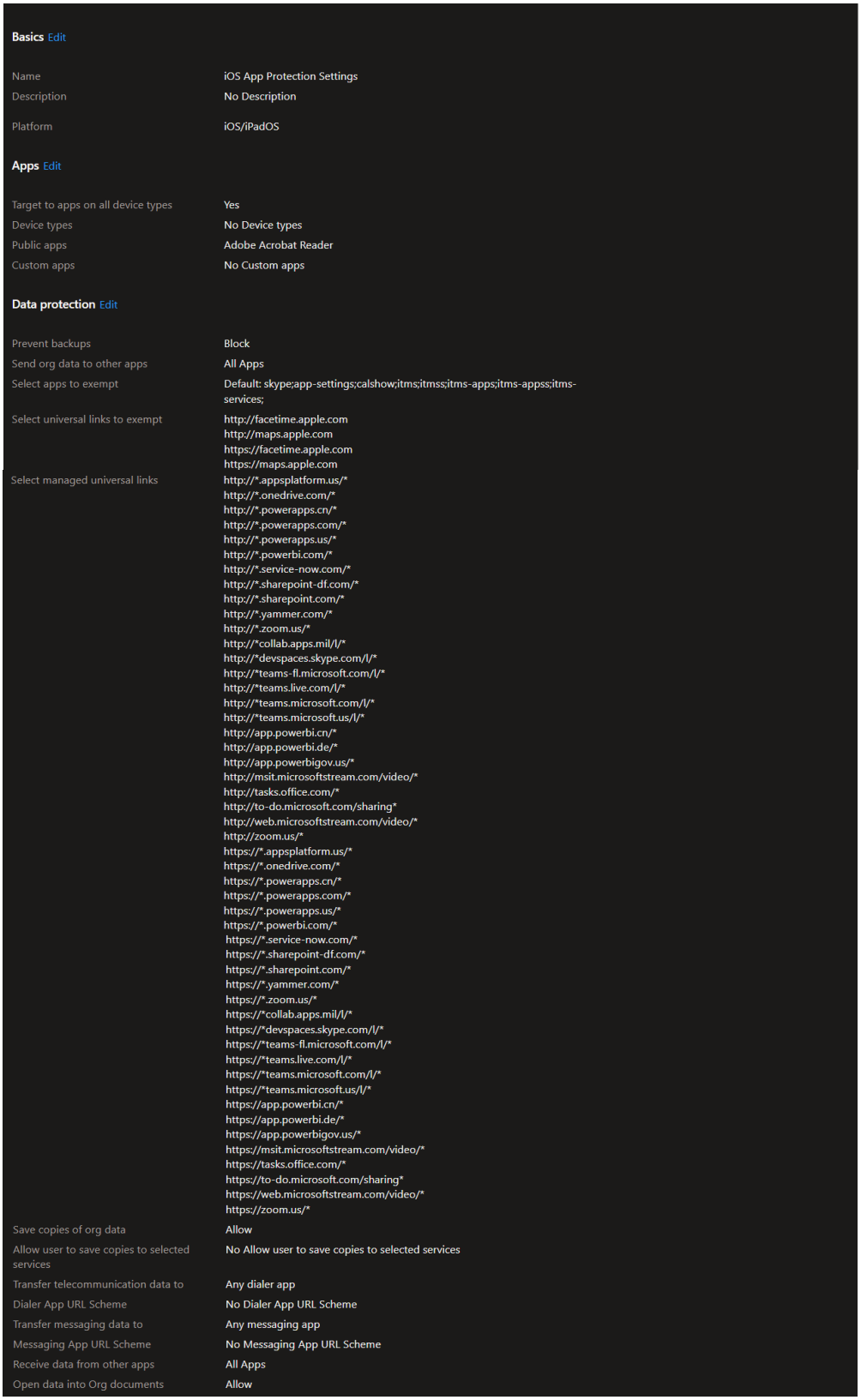
The dragged and dropped GPO was linked after clicking the OK button.

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.



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.



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	Default: skype;app-settings;calshow;itms;itmss;itms-apps;itms-appss;itms-services;
Select universal links to exempt	http://facetime.apple.com http://maps.apple.com https://facetime.apple.com https://maps.apple.com
Select managed universal links	http://*.appsplatform.us/* http://*.onedrive.com/* http://*.powerapps.cn/* http://*.powerapps.com/* 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://*.powerapps.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
Dialer App URL Scheme	No Dialer App URL Scheme
Transfer messaging data to	Any messaging app
Messaging App URL Scheme	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

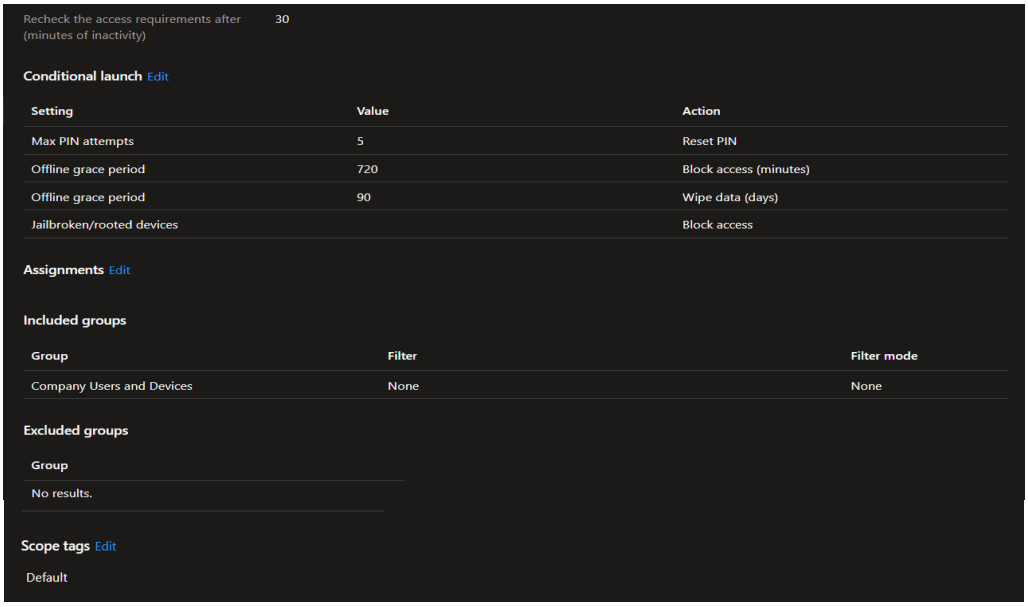
Target to apps on all device types	Yes
Device types	No Device types
Public apps	Adobe Acrobat Reader
Custom apps	No Custom apps

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

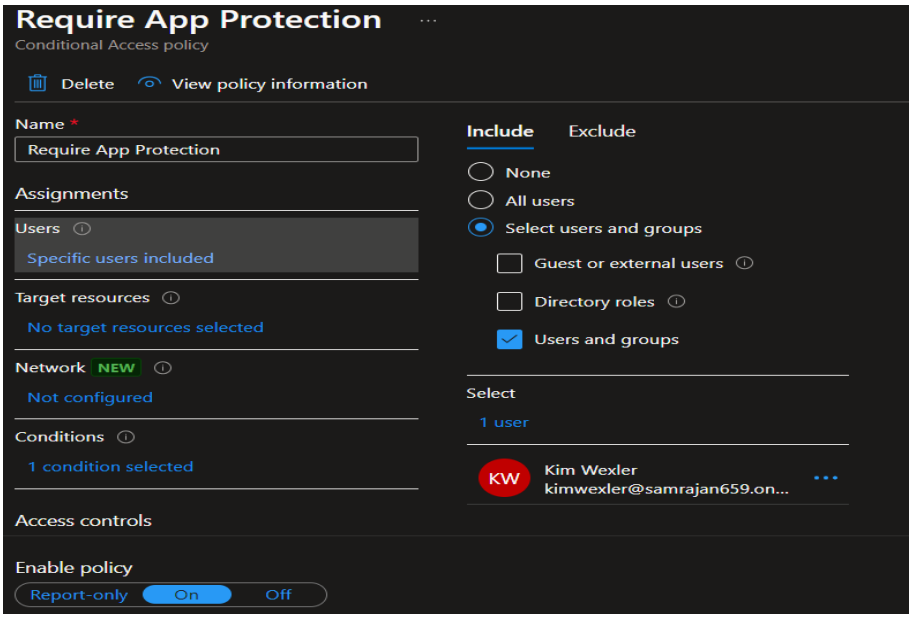
Access requirements Edit

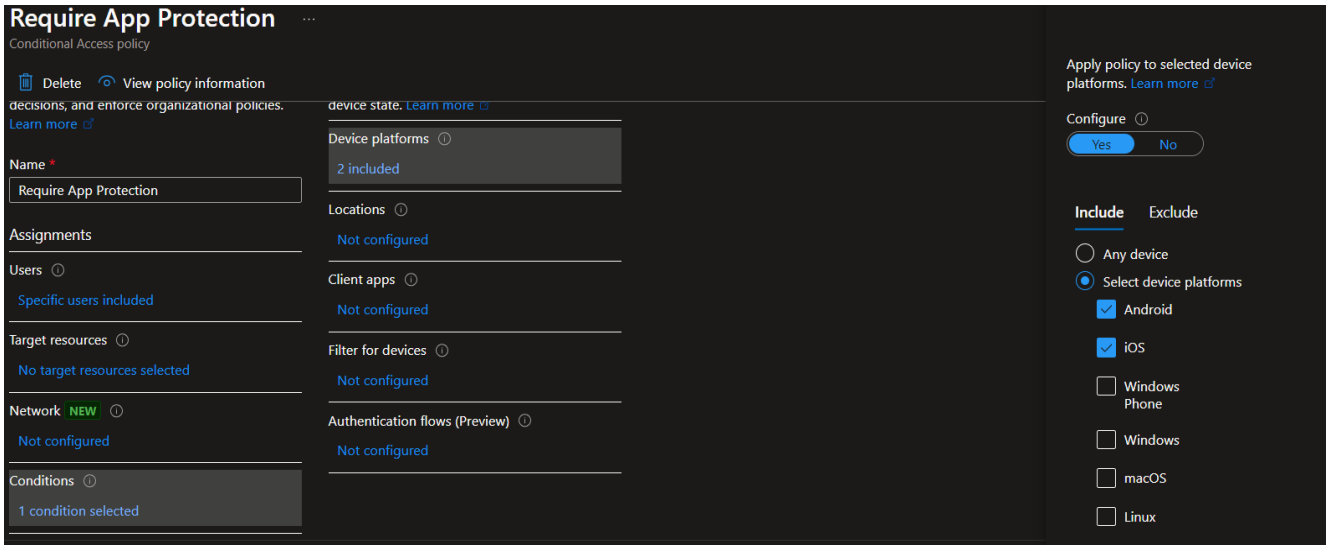
PIN for access	Require
PIN type	Numeric
Simple PIN	Allow
Select minimum PIN length	6
Biometrics instead of PIN for access	Allow
Override biometrics with PIN after timeout	Require
Timeout (minutes of inactivity)	30
Class 3 Biometrics (Android 9.0+)	Not required
Override Biometrics with PIN after biometric 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

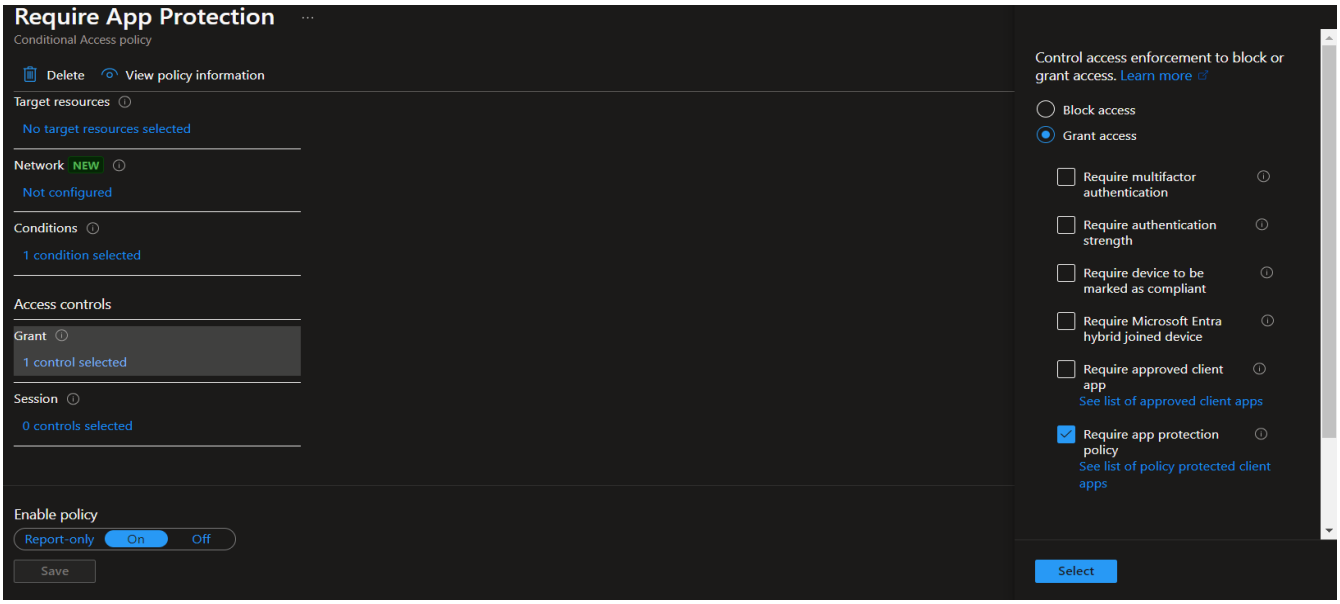


APP for Android devices. This APP specifically outlines app restrictions.

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.



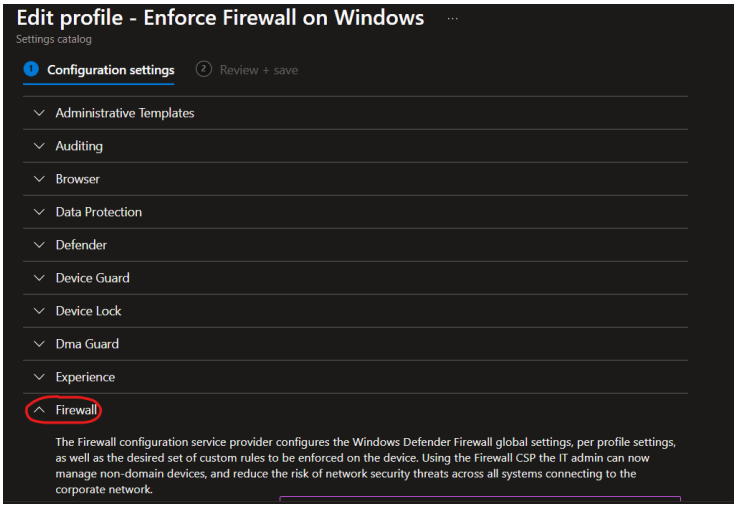




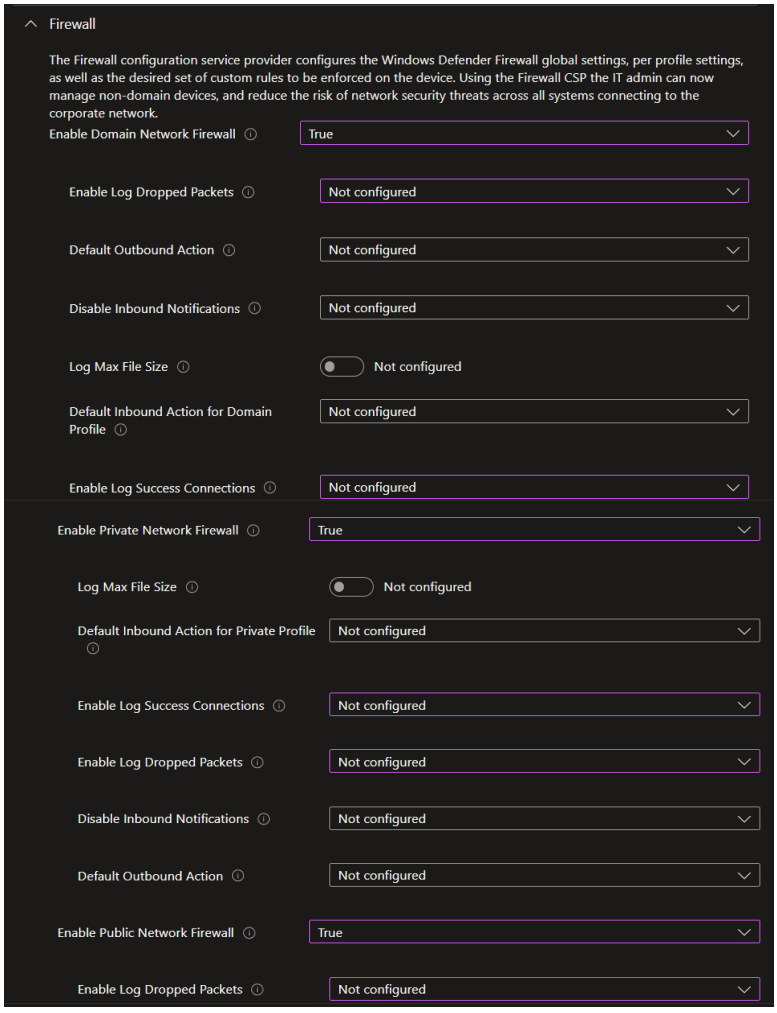
This conditional access policy was configured for both iOS and Android devices to require app protection.

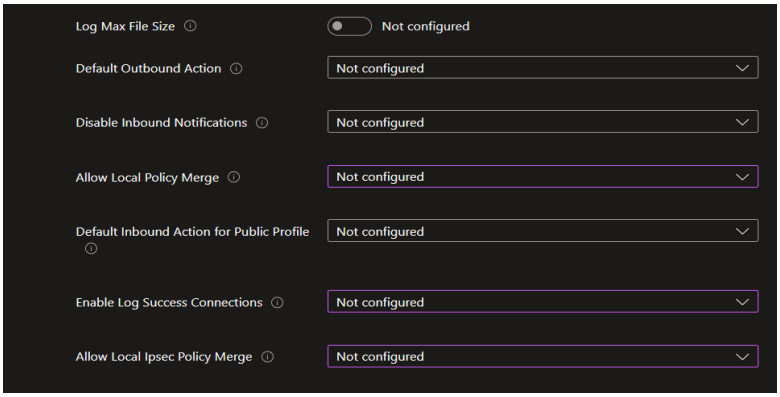
Configuring Endpoint Security

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.

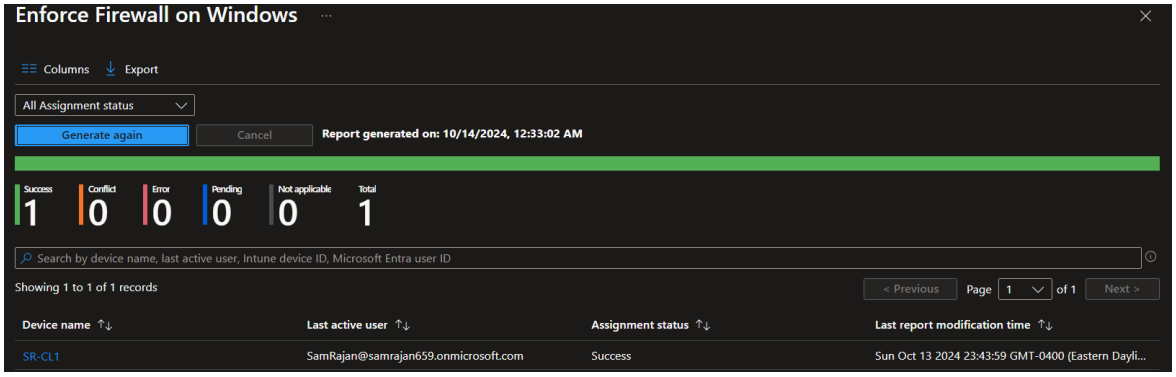


All settings except for the firewall settings were set to "Not configured". This was done to remove any default recommended settings and ensure only the firewall settings were configured.

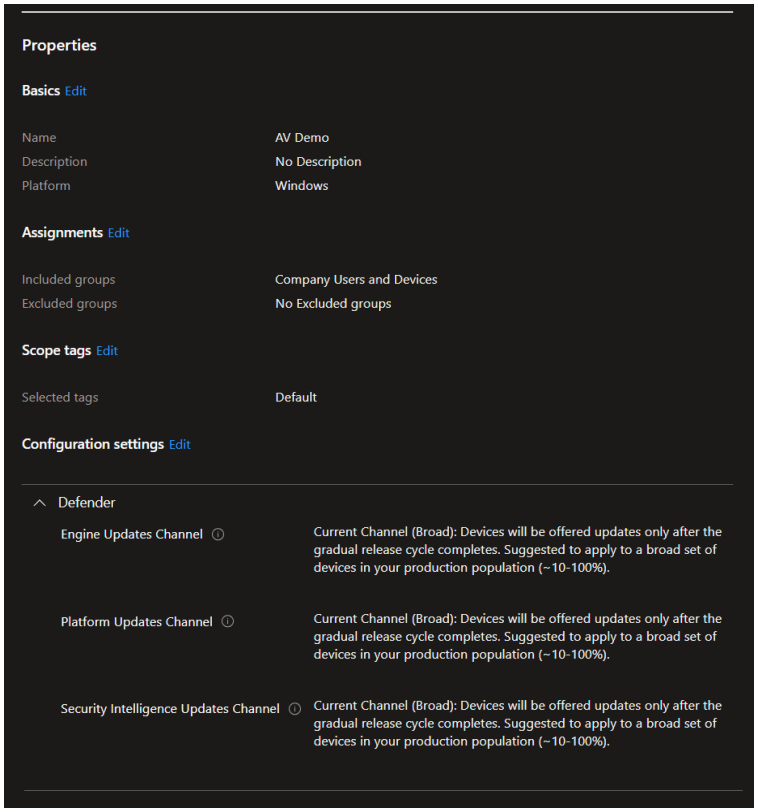




By navigating to Endpoint Security > Security baselines > Security Baseline for Windows 10 and later > Enforce Firewall on Windows > View report, it was confirmed that the baseline was successfully applied to the Windows 11 client (SR-CL1).

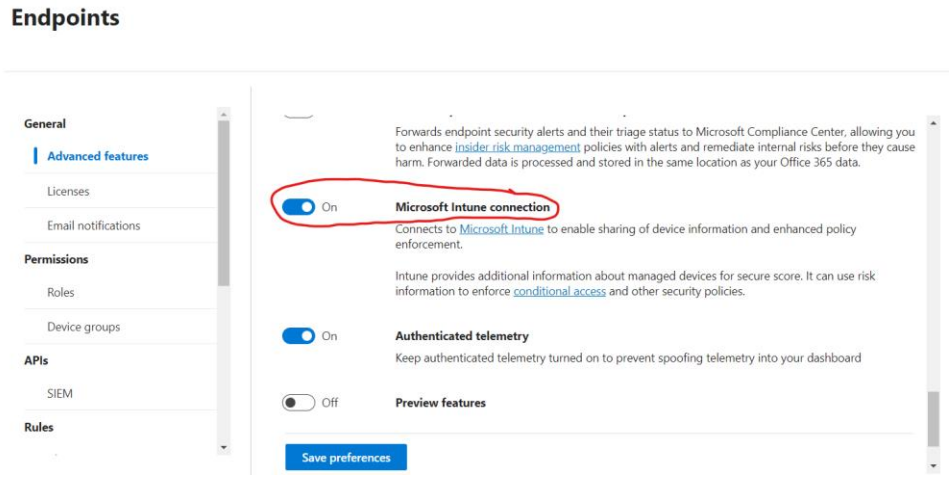


An antivirus policy was configured by navigating to Endpoint Security > Antivirus > Create Policy.

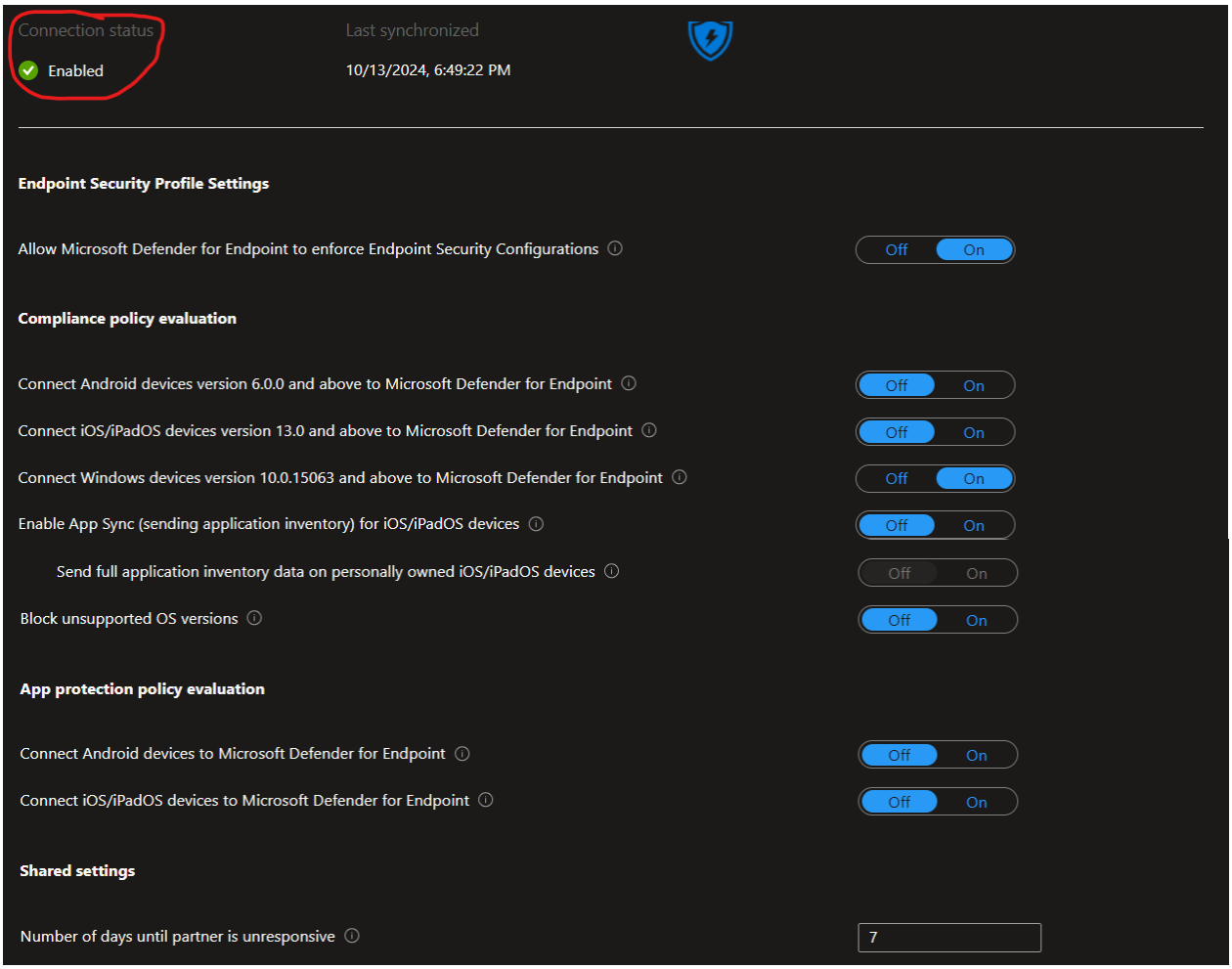


The policy covers settings for the Engine, Platform, and Security Intelligence update channels.

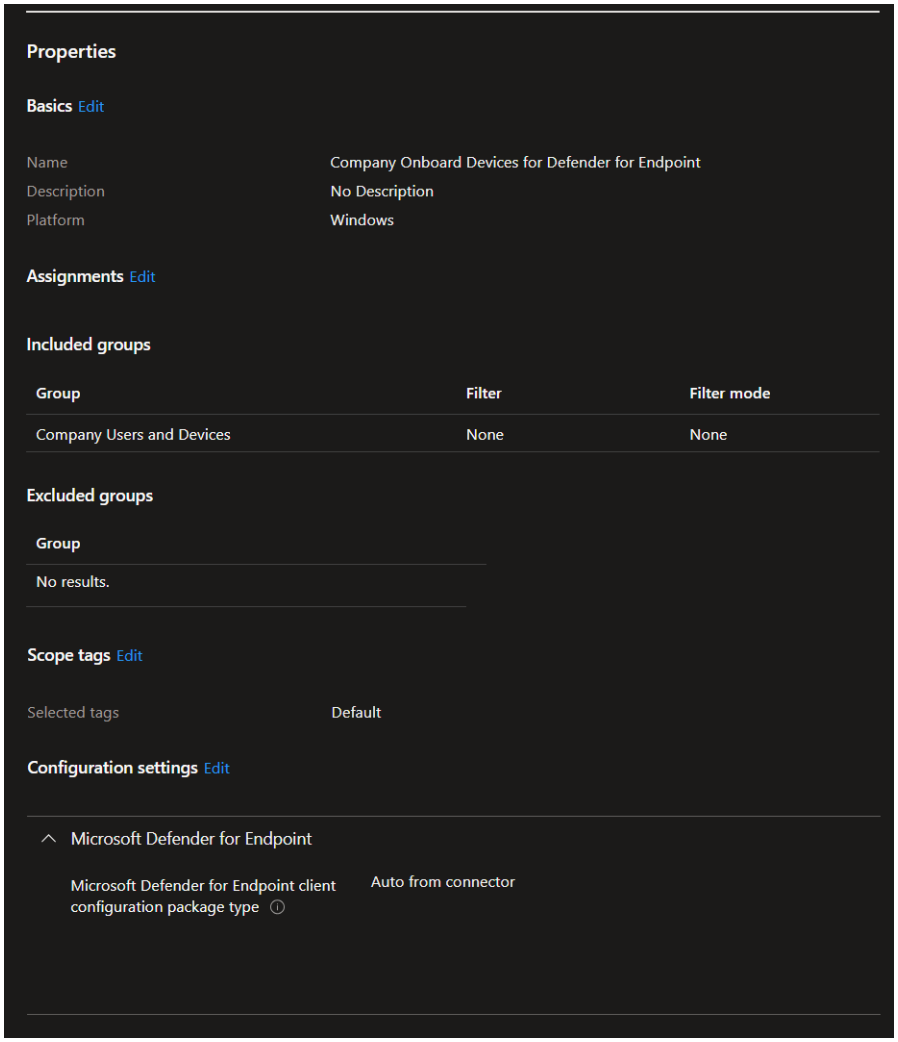
Devices can be onboarded to Microsoft Defender for Endpoint which is an endpoint security platform designed to help prevent, detect, investigate, and respond to advanced threats. The first step in doing this was to go to security.microsoft.com and navigate to System > Settings > Endpoints > Advanced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



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.

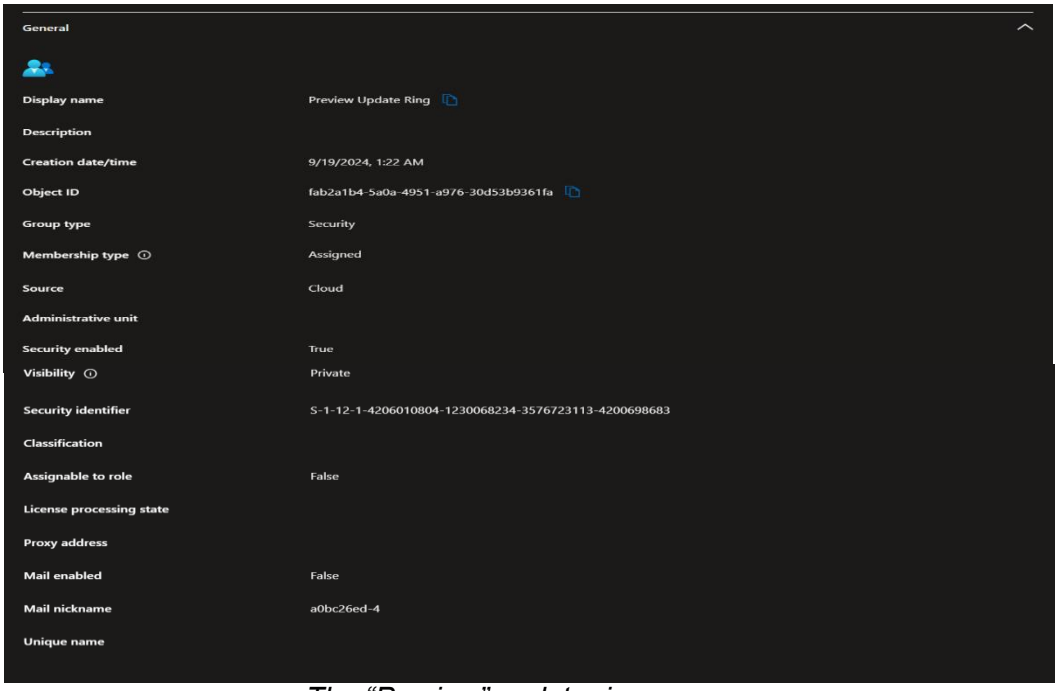


Then, a policy for endpoint detection and response which specified an automatic response was configured. This was accomplished by navigating to Endpoint Security > Endpoint detection and response > Create policy.

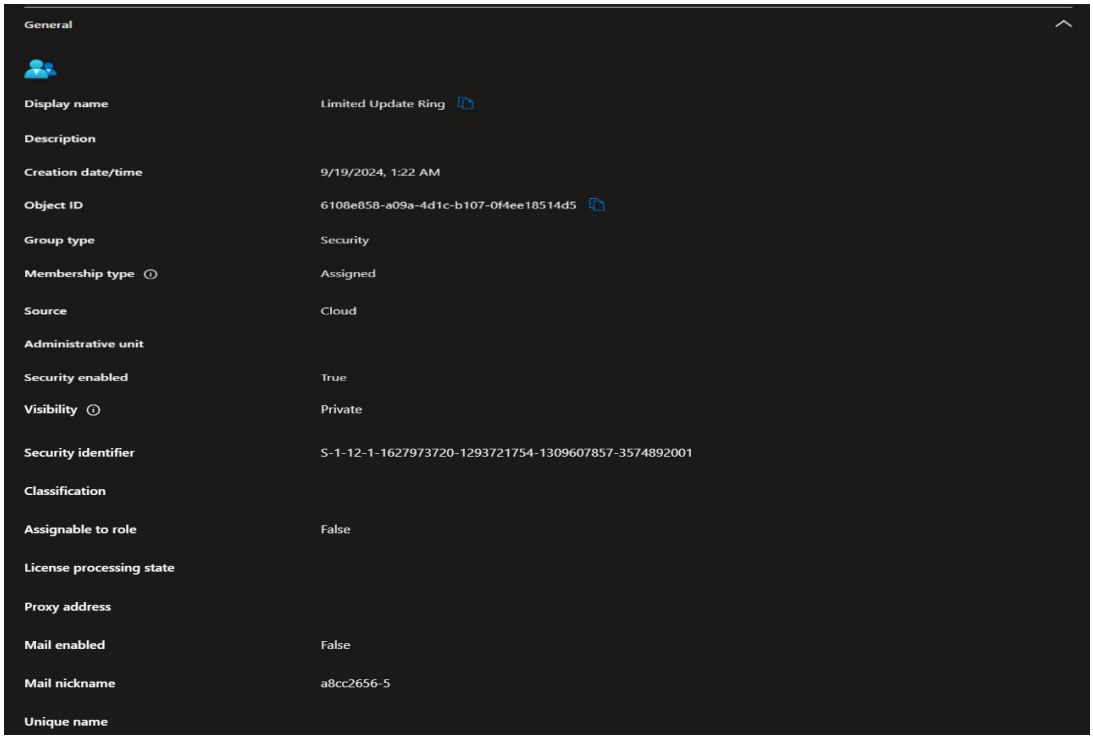


Managing Device Updates by Using Intune

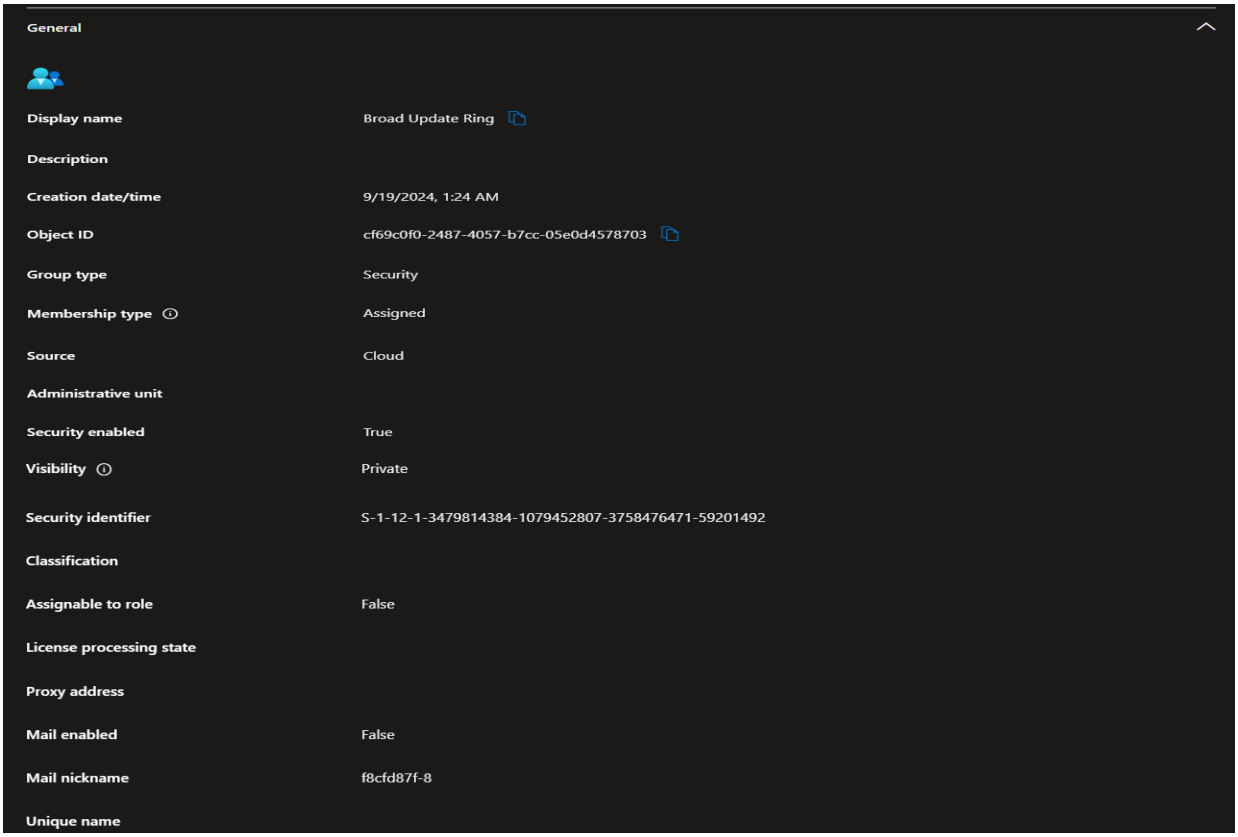
Update rings in Intune are used to specify how and when Windows as a Service updates Windows 10/11 devices with feature and quality updates. Firstly, three groups were created in Intune (Groups > New group) for different update ring types.



The “Preview” update ring group.

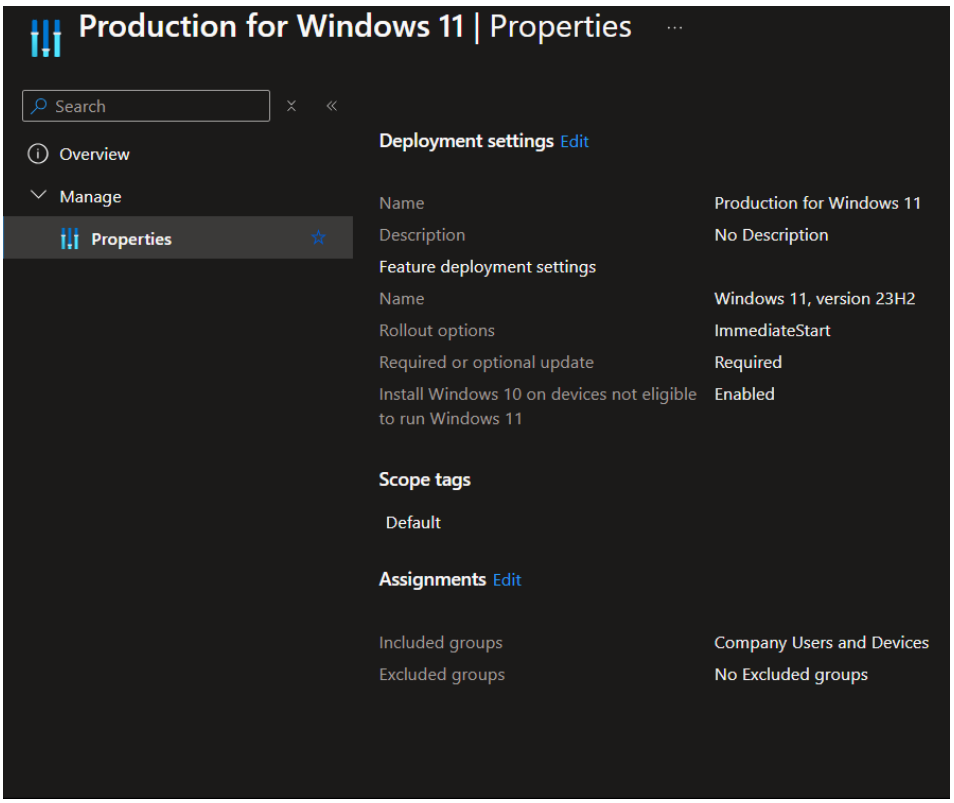


Limited” update ring group.



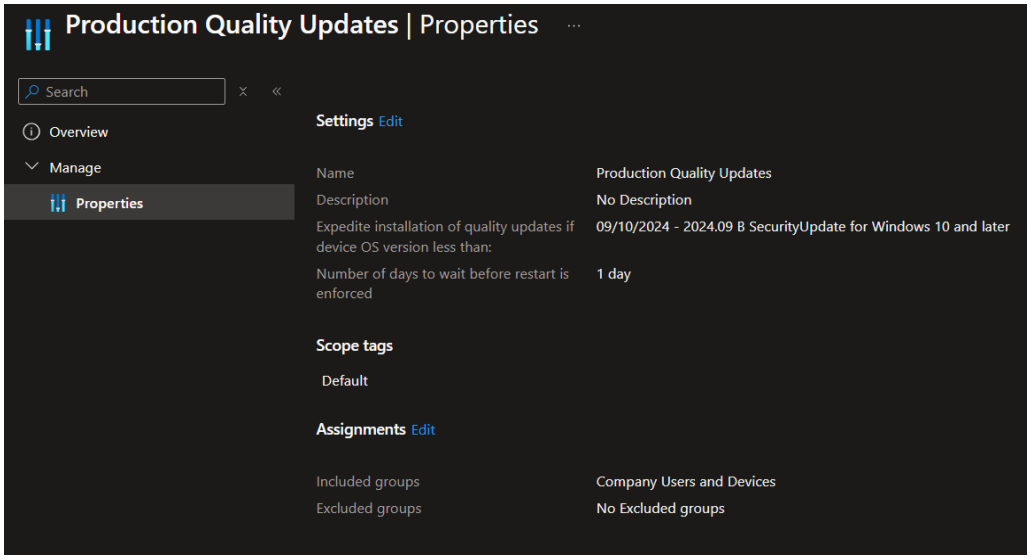
The “Broad” update ring group.

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



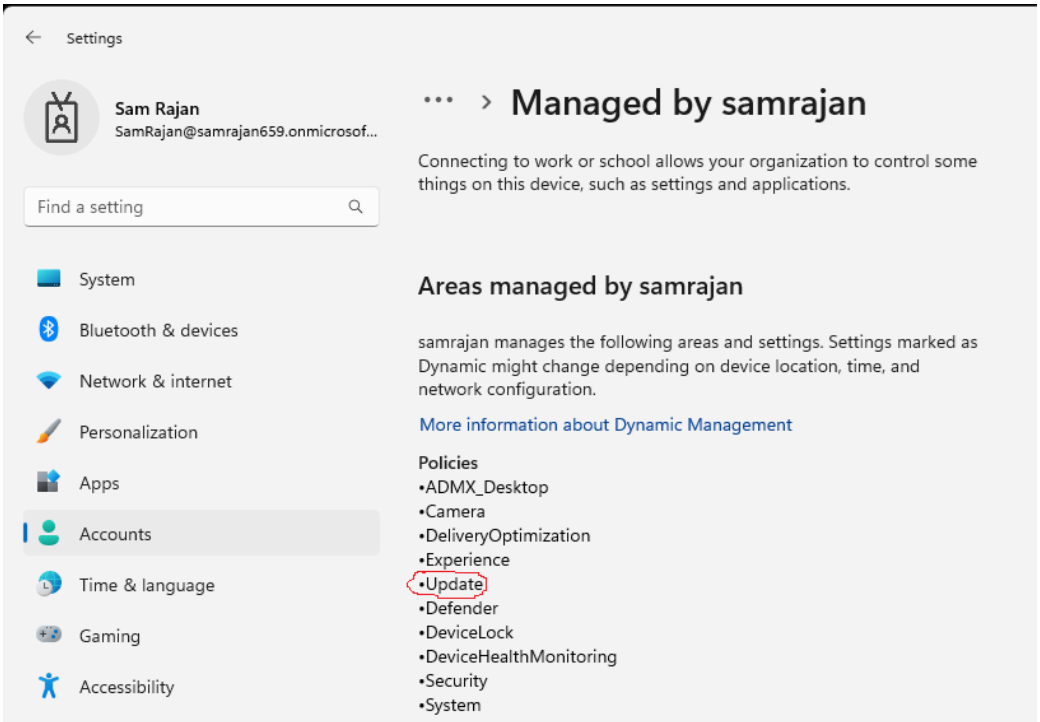
The feature update policy settings.

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

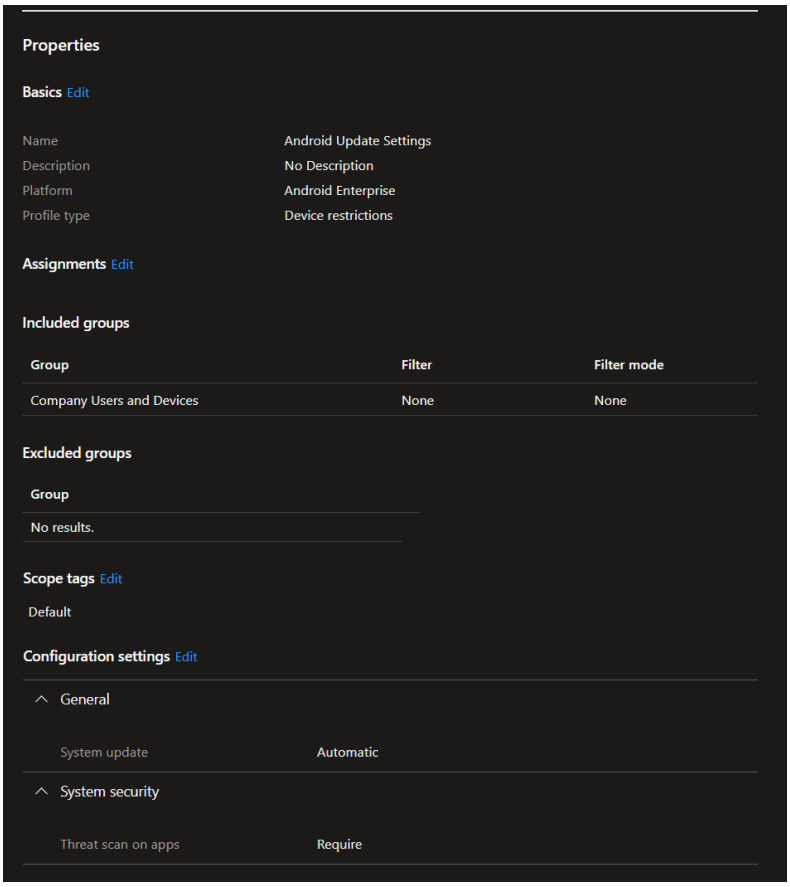


The quality update policy settings.

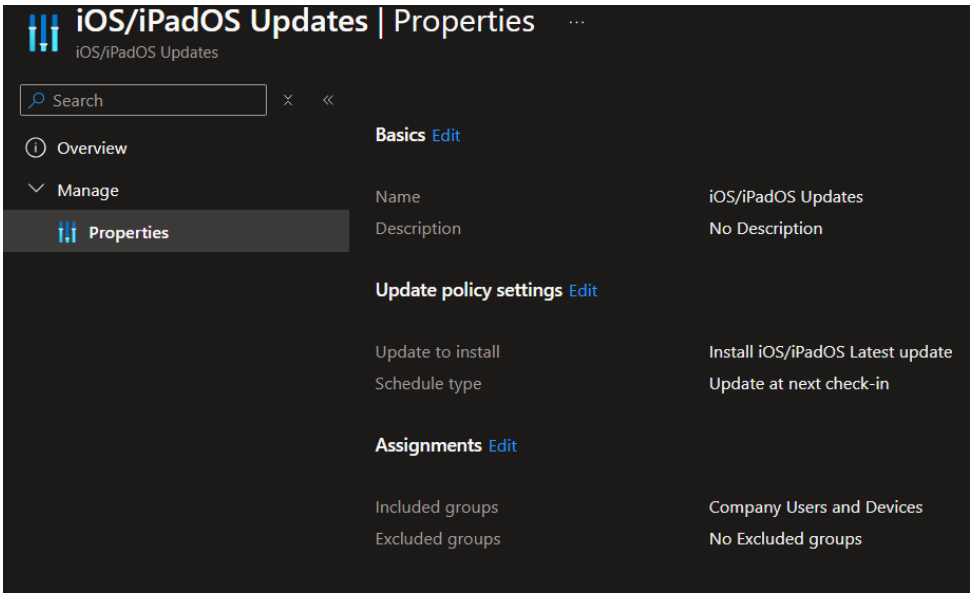
Upon opening the Settings app on the Windows 11 client machine and navigating to Accounts > Access Work or School > Managed by samrajan (under registered work/school account) > Info, updates were seen among the areas managed by samrajan (the domain). Thus, this confirmed that the policy settings were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



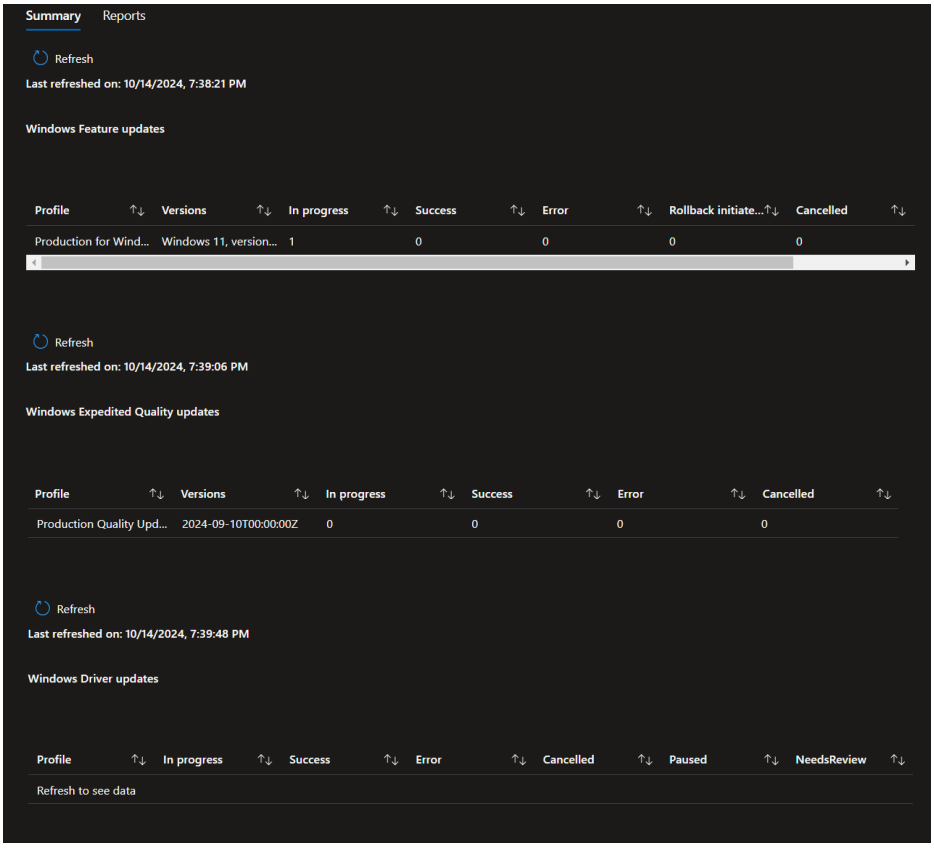
Update settings for Android devices were configured by navigating to Devices > Configuration > Policies > Create.



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

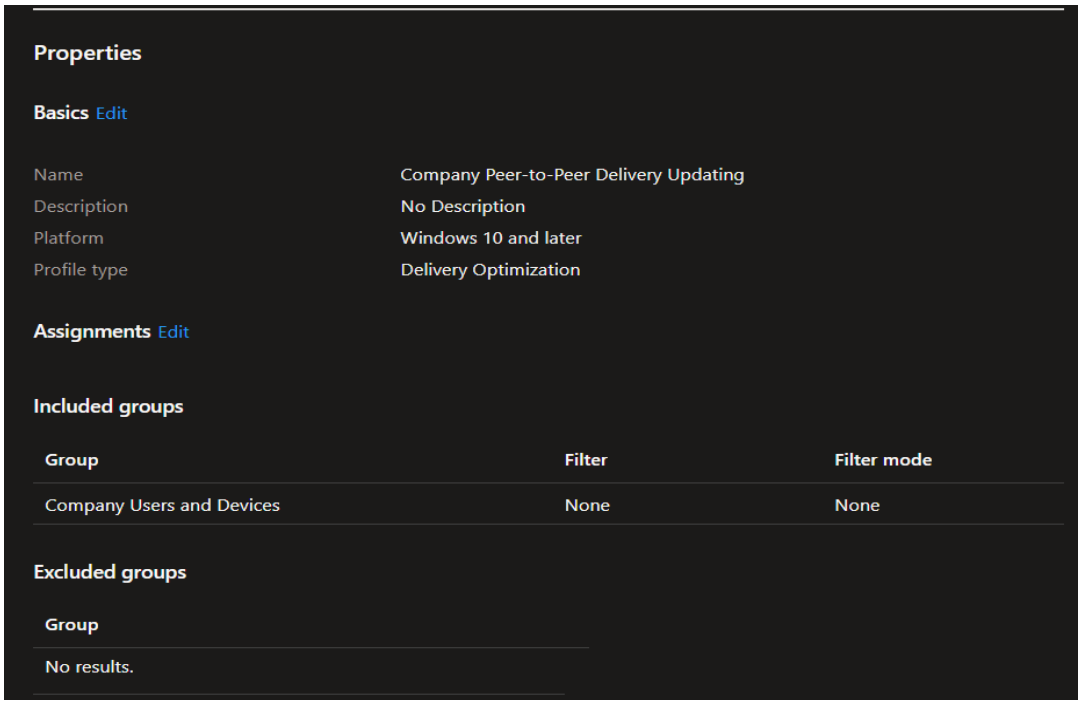


Updates could be managed by navigating to Reports > Windows Updates > Summary.



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.



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)