



# Intune MDM - Trusted Connection Customer Admin and End-user Setup Steps

June, 2025

<b>Summary</b>	<b>2</b>
Stepwise instructions for Customer Admins	2
Stepwise instructions for Customer End-Users	2
<b>Stepwise instructions for Customer Admins</b>	<b>3</b>
Getting Trusted Connection Client Licenses	3
Download Trusted Connection iOS Client Licenses in Apple Business Manager	4
Download Trusted Connection Android client from Google Play	6
Deploy Intune	7
Install Trusted Connection by platform	8
Wrap the MSI to the Intune app.	8
Edit Trusted Connection client properties	11
Install Trusted Connection Android app to Intune portal (from Google Play)	16
Creating Staging Profiles for Android devices	20
Android enterprise enrollment types	20
Create staging profile and assign apps	23
Review Token & generate QR code	25
Enroll an Android device via token (QR code)	27
Filters for Android Devices	36
Install the Certificate	39
Install Trusted Connection iOS app to Intune portal (from Apple Business Manager)	45
Further references: Microsoft Intune Documentation	54
<b>Stepwise instructions for Customer End-Users</b>	<b>56</b>
Android instructions	56
iOS instructions	59



## Summary

This document provides guidance for customer administrators to deploy Trusted Connection on Intune-managed Windows, Android, and iOS devices. Please note that the following guidelines are for a fully managed device management scenario.

Both Trusted Connection and Intune are supported on Windows, Android, macOS and iOS operating systems.

## Stepwise Instructions for Customer Admins

1. Getting Trusted Connection Client Licenses
2. Deploy Intune
3. Install Trusted Connection by platform
  - a. MSI to Intune portal
  - b. Android app to Intune portal (from Google Play)
  - c. iOS app to Intune portal (from Apple Business Manager)
4. Further references: Microsoft Intune Documentation

## Stepwise Instructions for Customer End-Users

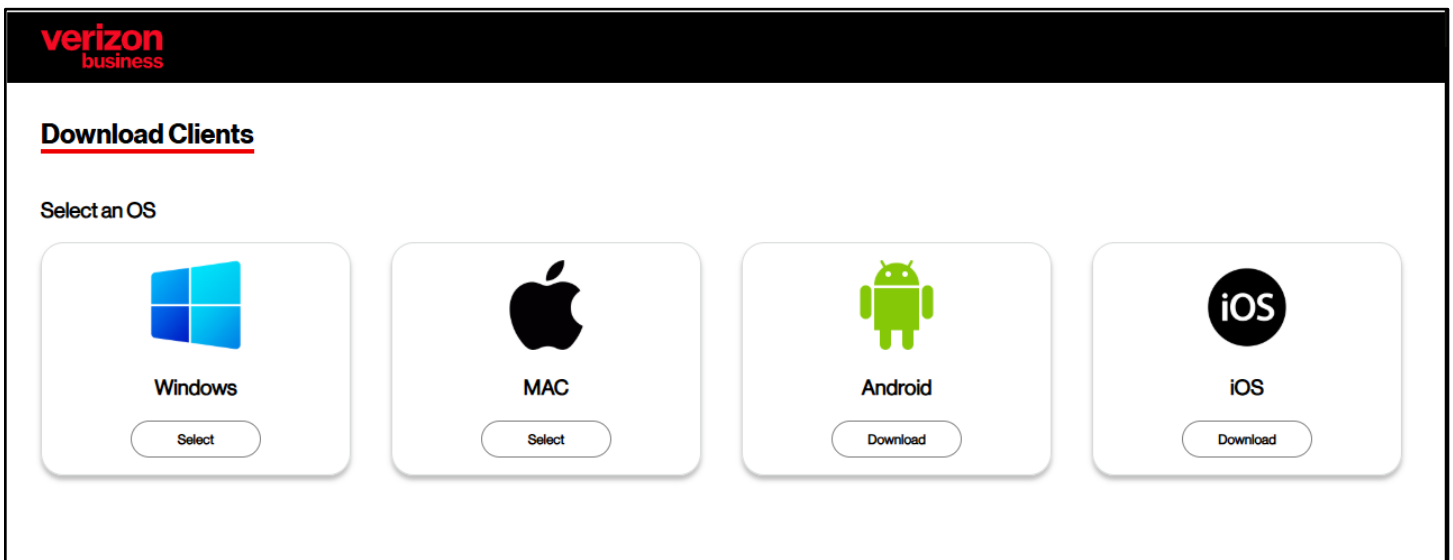
1. Android Instructions
2. iOS Instructions



## Stepwise Instructions for Customer Admins

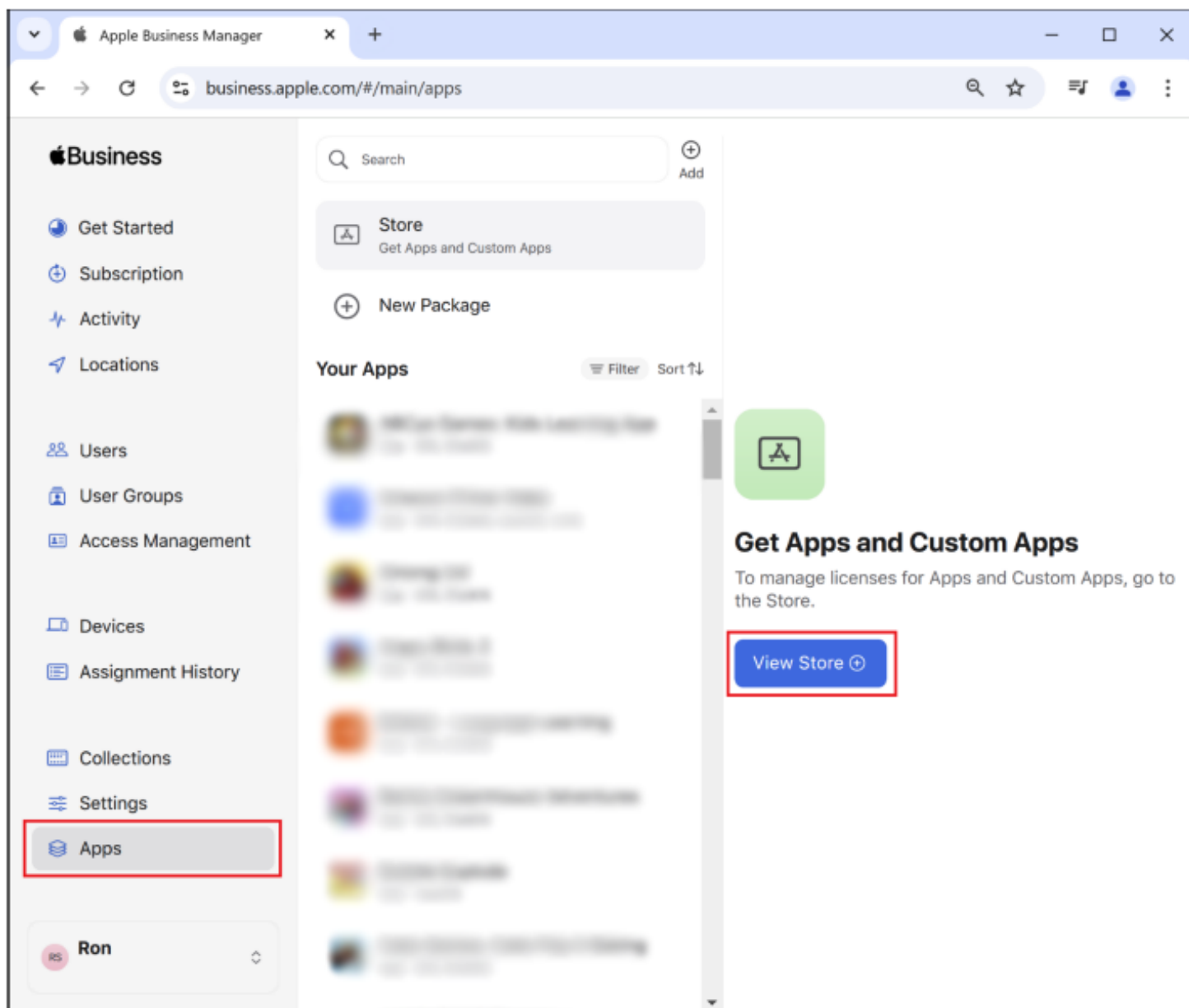
### Getting Trusted Connection Client Licenses

Download clients for Microsoft, Mac, Android & Apple OS  
<https://download.trustedconnection.verizon.com/index.html>



## Download Trusted Connection iOS Client Licenses in Apple Business Manager

- **Step 1:** Log on to your Apple Business Manager account.  
<https://business.apple.com>
- **Step 2:** Click on Apps, then click on View Store.







- **Step 3:** Enter “Trusted Connection” in the search field, then select the Trusted Connection application from the search results.
- **Step 4:** Enter the Quantity of licenses purchased in Verizon systems, then click Get to complete the purchase.

The screenshot displays the Apple Business Manager interface. On the left, a search bar contains the text "Trusted Connection". Below it, a list of search results is visible, with the top result being the "Trusted Connection" app by Verizon Wireless, priced at \$0.00. The main content area on the right shows the app details for "Trusted Connection" by Verizon Wireless. It includes a "Buy Licenses" section with a table:

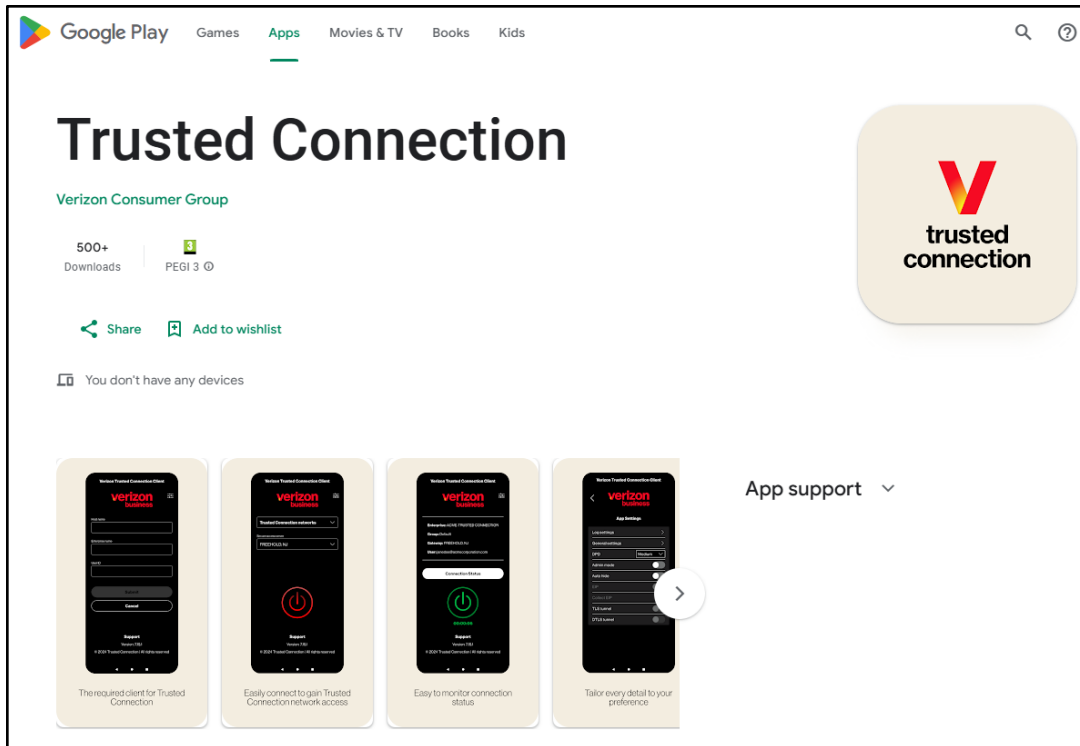
Price	Quantity	Payment Method
\$0.00	20	None

Below the table, the "Total Cost" is shown as \$0.00. A blue "Get" button is located at the bottom right of the "Buy Licenses" section.

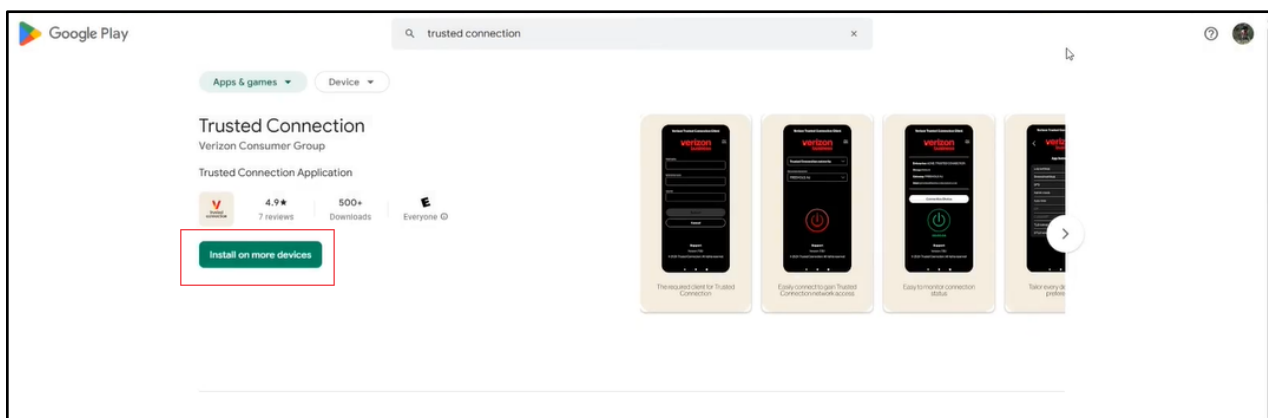


## Download Trusted Connection Android client from Google Play

- **Step 1:** Log on to your Google Enterprise account.  
<https://play.google.com/store/apps/details?id=com.verizon.trustedconnection>



Alternatively go to <https://play.google.com/store/> → Apps, → Search → Enter “Trusted Connection” in the search field.



- **Step 2:** Install Trusted Connection app, on the device.



## Deploy Intune

To begin using Trusted Connection, the customer has to ensure the Intune MDM platform is already set up - all the end user devices need to be added, configured, and enrolled in the MDM platform. It is advised to complete the Intune MDM platform deployment steps before proceeding with Trusted Connection setup.

1. **Set up Intune** - The first step when deploying Microsoft Intune is to set up your Intune environment. This will give you access to the Microsoft Intune admin center, which is a web-based console for managing your devices, apps, and users.
2. **Add and protect apps** - Use this step to add Trusted Connection app and licenses (Important: you'll need to make sure this is set up with Win32).
3. **Check for compliance and turn on Conditional Access** - Plan for and configure device compliance settings and policies to help protect organizational data by requiring devices to meet your organizational requirements.
4. **Configure device features** - Configure a minimum or baseline set of security and device features that all devices must have.
5. **Enroll your devices** - During Microsoft Intune enrollment, a mobile device management (MDM) certificate is installed on the device. This certificate allows Intune to enforce enrollment profiles and restrictions, as well as company-defined policies and profiles.

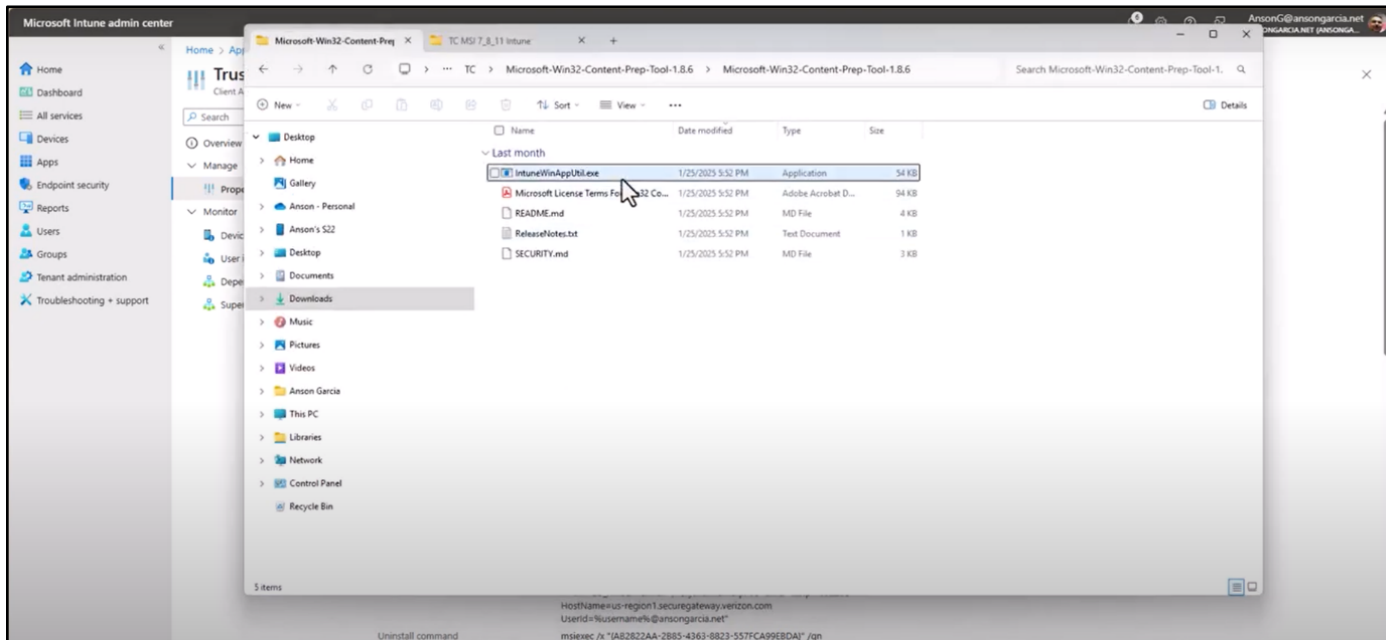
Depending on the device platforms you manage, additional requirements may apply. For instance, managing iOS/iPadOS and macOS devices necessitates an Apple MDM push certificate and potentially an Apple token. Managing Android devices may require a managed Google Play account. If you utilize certificate authentication, a SCEP or PKCS certificate might be necessary.

- a. Android enrollment guide
- b. iOS/iPadOS enrollment guide
- c. macOS enrollment guide
- d. Windows enrollment guide

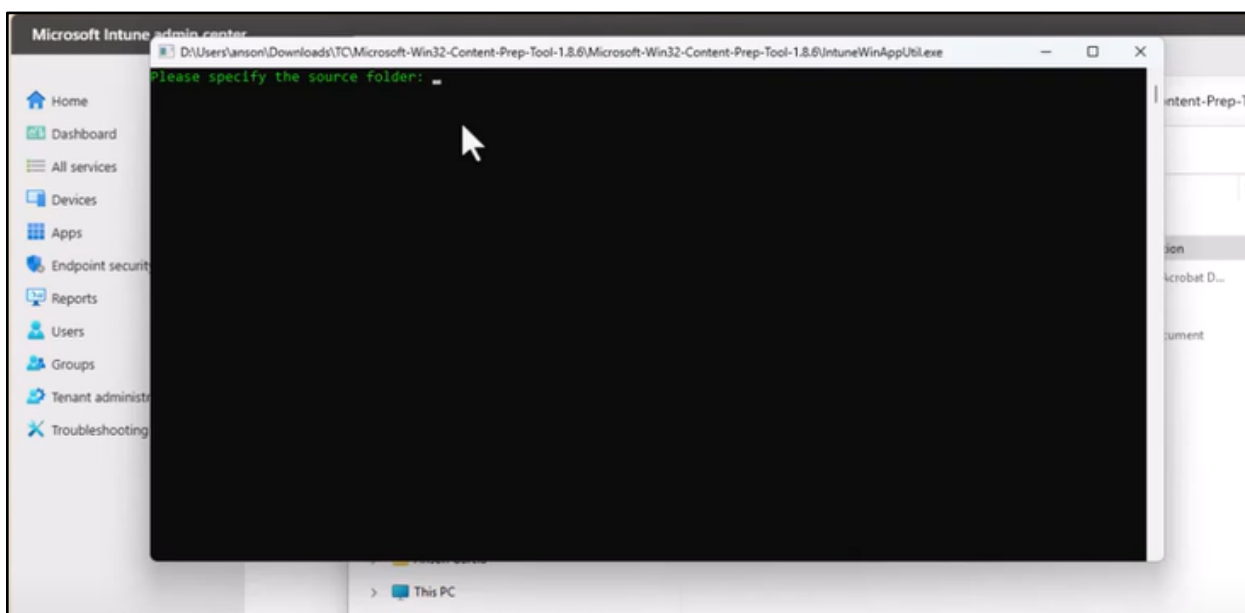
## Install Trusted Connection by platform

### Wrap the MSI to the Intune app.

- **Step 1:** Log on to your Microsoft Intune admin center account. <https://intune.microsoft.com/>
- **Step 2:** Before adding the Trusted Connection app, you have to wrap the MSI to the Intune app. The way to do it is by using a downloadable Intune win app utility. Download: [intunewinapputil.exe](#) [here](#)

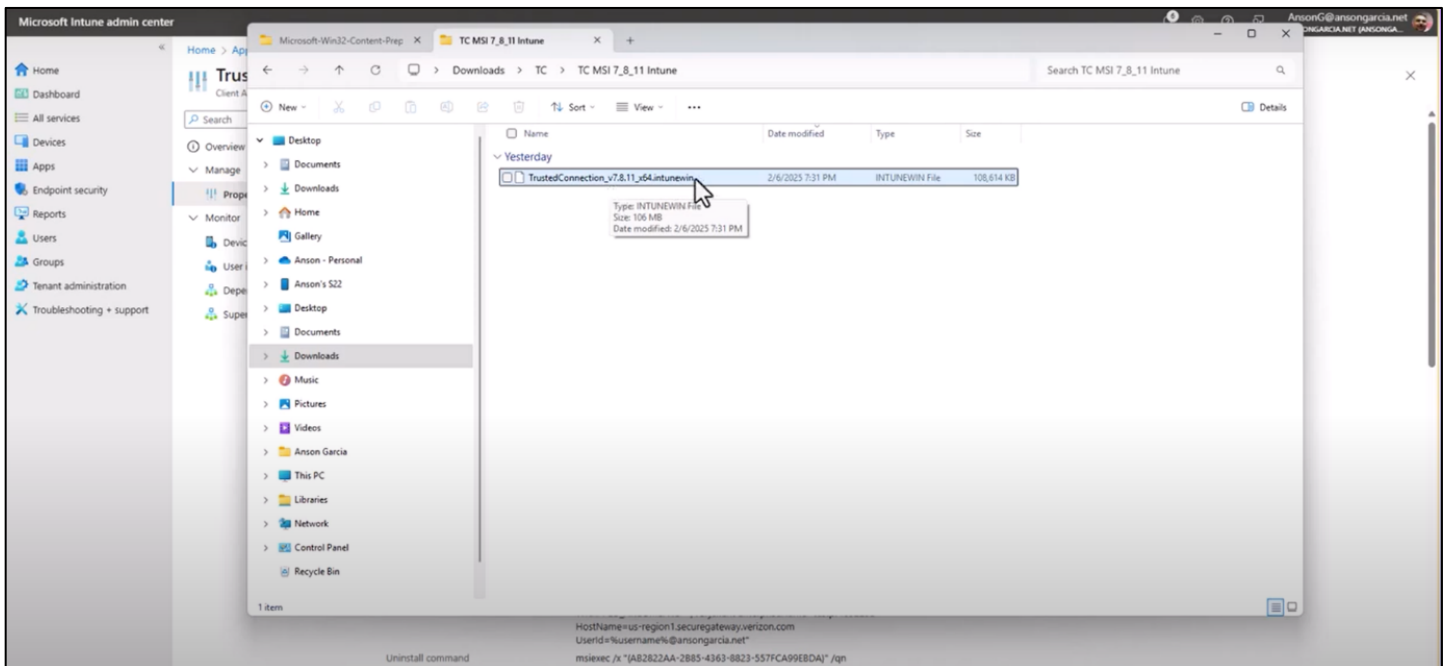


- **Step 3:** Running the utility will prompt you for the destination folder, the file to be packaged, and the MSI file. It will also ask where you want the resulting package to be saved.

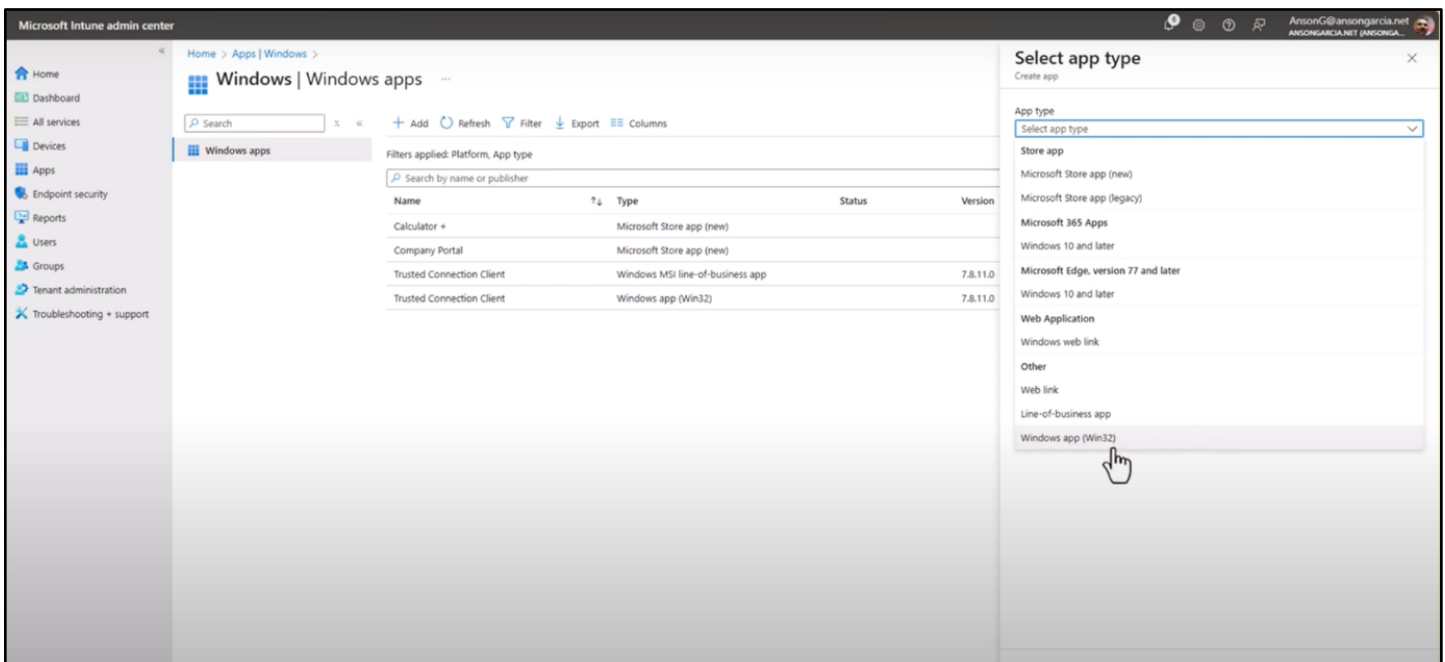




- **Step 4:** All the MSI information will be packed into an Intune win extension file. With that extension file, you can create/add a new app.



- **Step 5:** Go back to Microsoft Intune admin center, select Apps → Windows apps → +Add and select the app type Windows app (Win32) as indicated below



Once it is created, you will have a Win32 app that will provide more flexibility and data.



**Step 6:** Then select the Trusted Connection client with Win32.

Microsoft Intune admin center

Home

Dashboard

All services

Devices

Apps

Endpoint security

Reports

Users

Groups

Tenant administration

Troubleshooting + support

Home > Apps > Windows >

Windows | Windows apps

Search

+ Add Refresh Filter Export Columns

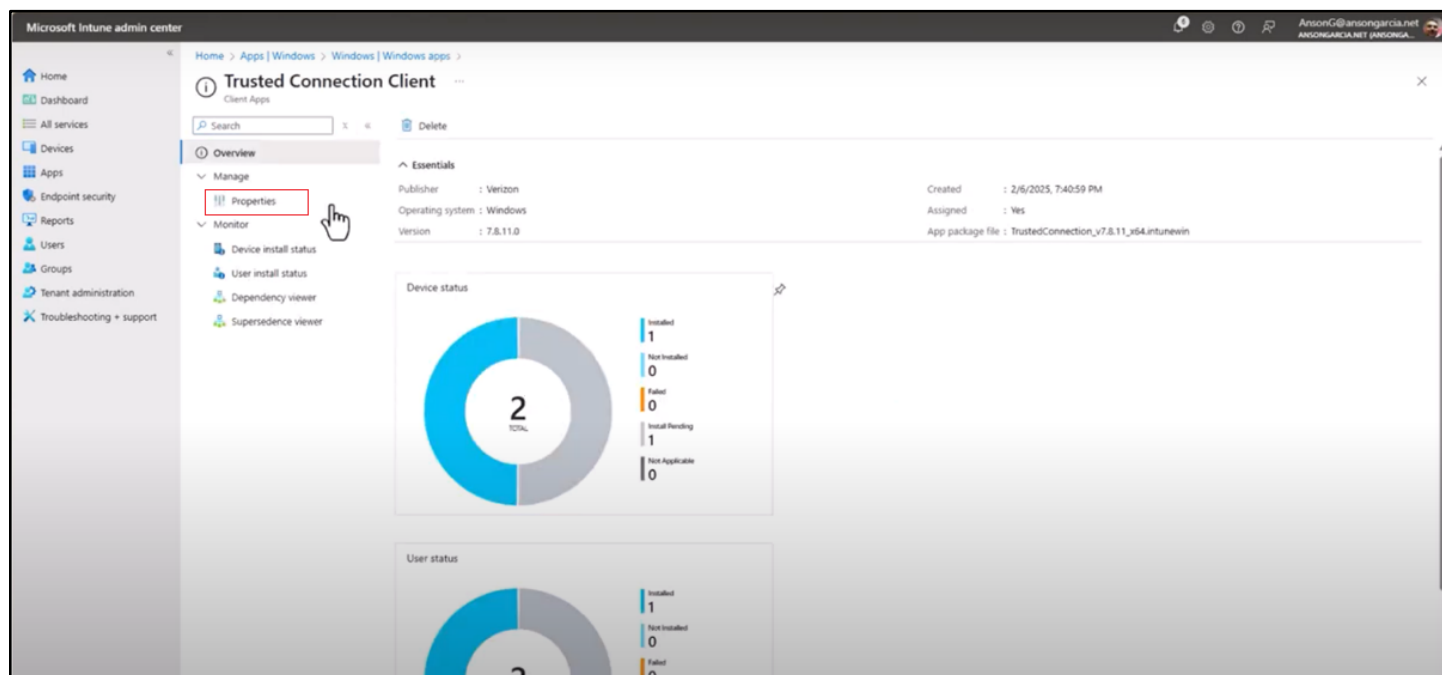
Filters applied: Platform, App type

Search by name or publisher

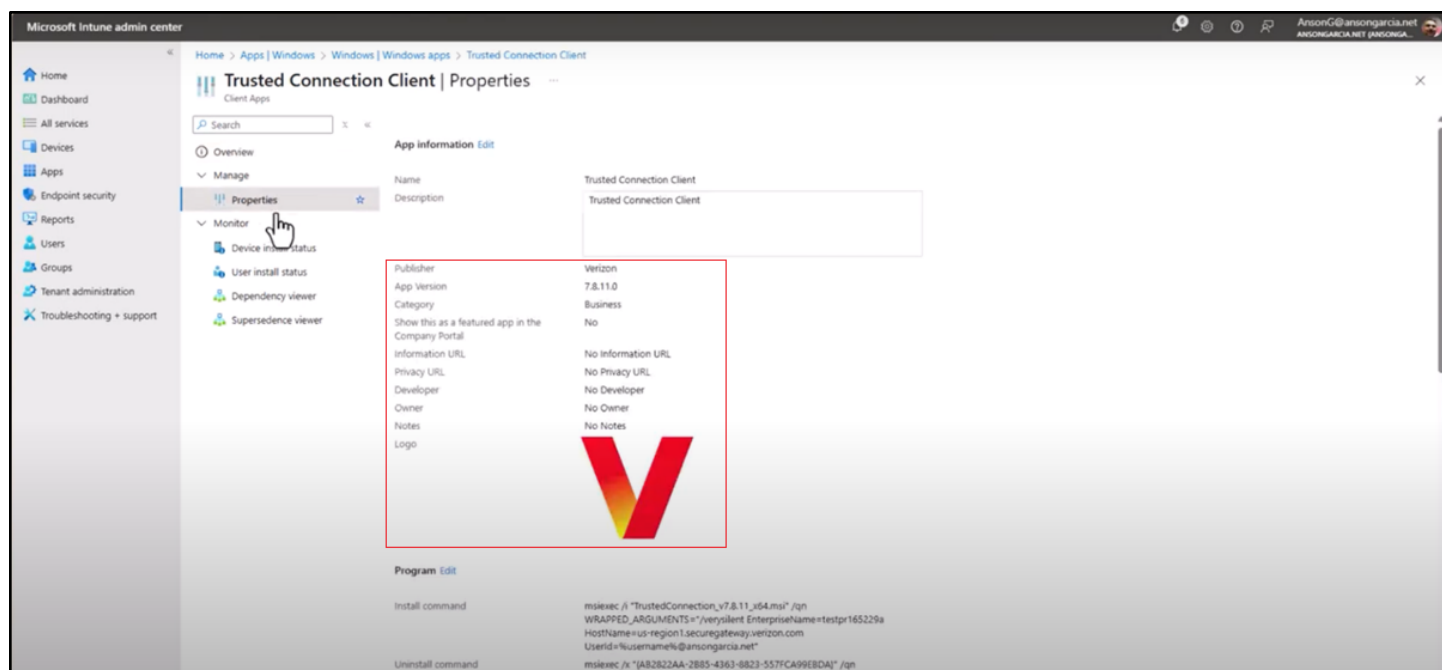
Name	Type	Status	Version	Assigned
Calculator +	Microsoft Store app (new)			Yes
Company Portal	Microsoft Store app (new)			Yes
Trusted Connection Client	Windows MSI line-of-business app		7.8.11.0	No
Trusted Connection Client	Windows app (Win32)		7.8.11.0	Yes

## Edit Trusted Connection client properties

- **Step 1:** Once the Trusted Connection Client is selected in Apps, click on Properties.



- **Step 2:** Within the Properties section, the screen will have plenty of information that you can input (e.g., URL's).





It also provides the whole Install command in one argument, it also creates an Uninstall command which will be needed for upgrades or mass uninstalls. Install behaviour, success codes.

Microsoft Intune admin center

Home > Apps > Windows > Windows apps > Trusted Connection Client

### Trusted Connection Client | Properties

Client Apps

Search

Notes

Logo

No Notes

Program Edit

Install command

```
msiexec /i "TrustedConnection.v7.11.x64.msi" /qn  
MBAAPPID_ARGUMENTS="/veryclient EnterpriseName=testpr165229a  
HostName=us-region1.securegateway.verizon.com  
UserId=\\user\\user@ansongarcia.net"
```

Uninstall command

```
msiexec /x "{A82822AA-2885-4363-8823-557FCA99EBDA}" /qn
```

Installation time required (mins)

60

Allow available uninstall

Yes

Install behavior

User

Device restart behavior

App install may force a device restart

Return codes

0 Success  
1707 Success  
3010 Soft reboot  
1641 Hard reboot  
1618 Retry

Requirements Edit

Operating system architecture

x64,x64

Minimum operating system

Windows 10 1607

Disk space required (MB)

20

Physical memory required (MB)

4

Minimum number of logical processors required

1

- **Step 3:** By modifying the Requirements, you can view the necessary operating systems (including minimum versions), disk space, and configure supplementary prerequisites before installation.

Microsoft Intune admin center

Home > Apps > Windows > Windows apps > Trusted Connection Client

### Trusted Connection Client | Properties

Client Apps

Search

Notes

Logo

No Notes

Program Edit

Install command

```
msiexec /i "TrustedConnection.v7.11.x64.msi" /qn  
MBAAPPID_ARGUMENTS="/veryclient EnterpriseName=testpr165229a  
HostName=us-region1.securegateway.verizon.com  
UserId=\\user\\user@ansongarcia.net"
```

Uninstall command

```
msiexec /x "{A82822AA-2885-4363-8823-557FCA99EBDA}" /qn
```

Installation time required (mins)

60

Allow available uninstall

Yes

Install behavior

User

Device restart behavior

App install may force a device restart

Return codes

0 Success  
1707 Success  
3010 Soft reboot  
1641 Hard reboot  
1618 Retry

Requirements Edit

Operating system architecture

x64,x64

Minimum operating system

Windows 10 1607

Disk space required (MB)

20

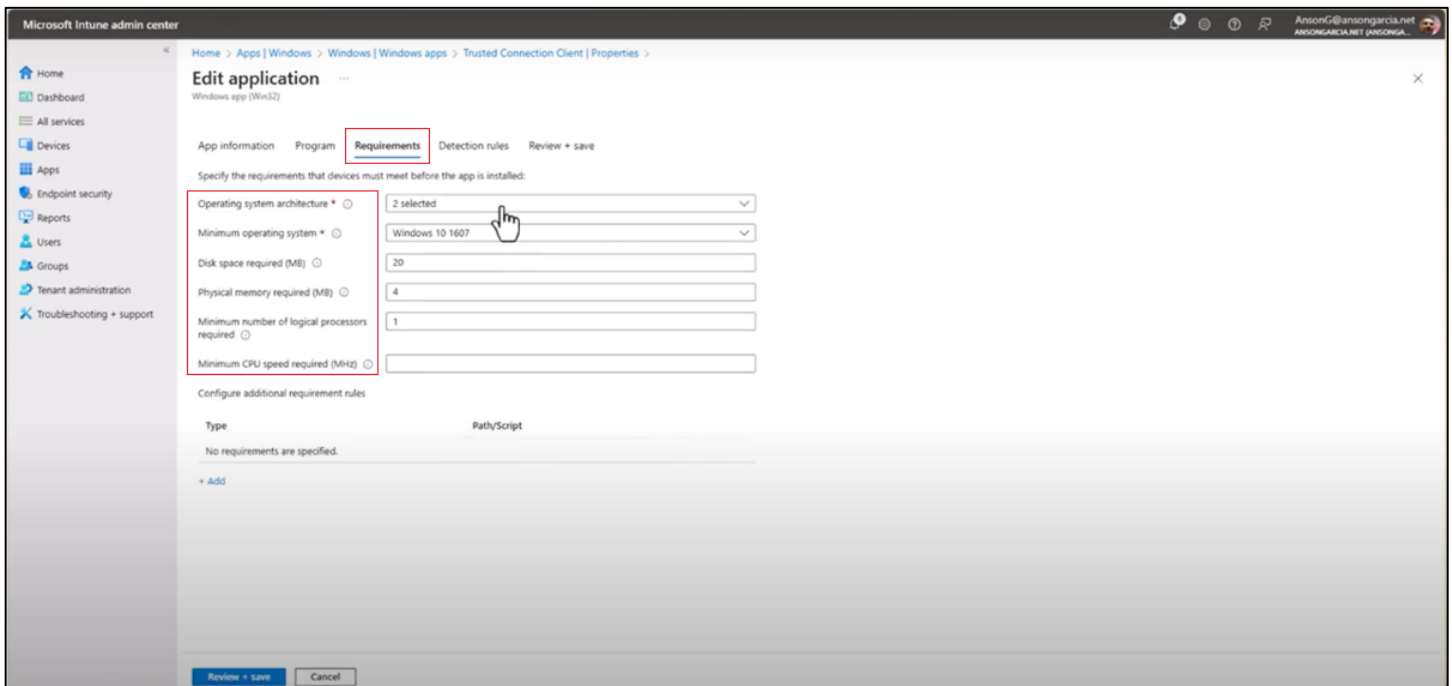
Physical memory required (MB)

4

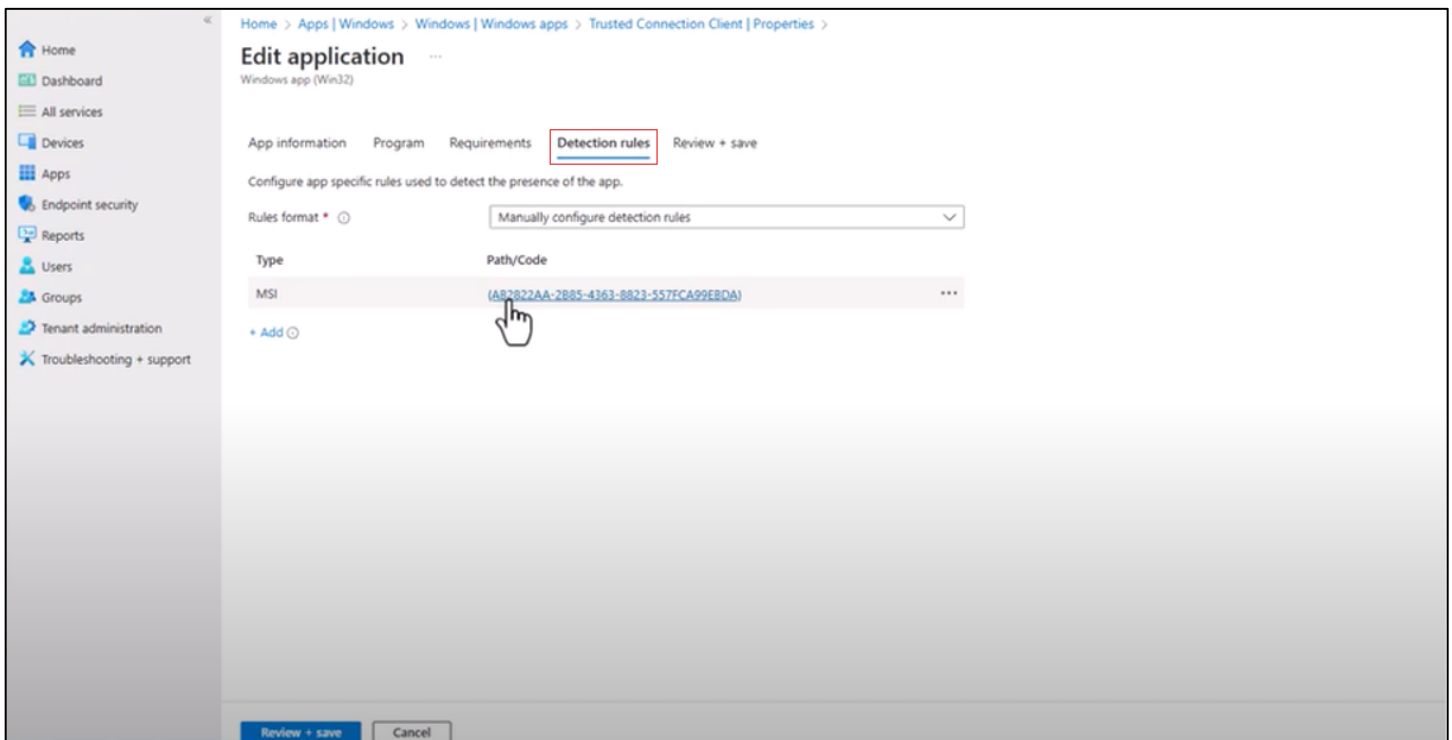
Minimum number of logical processors required

1



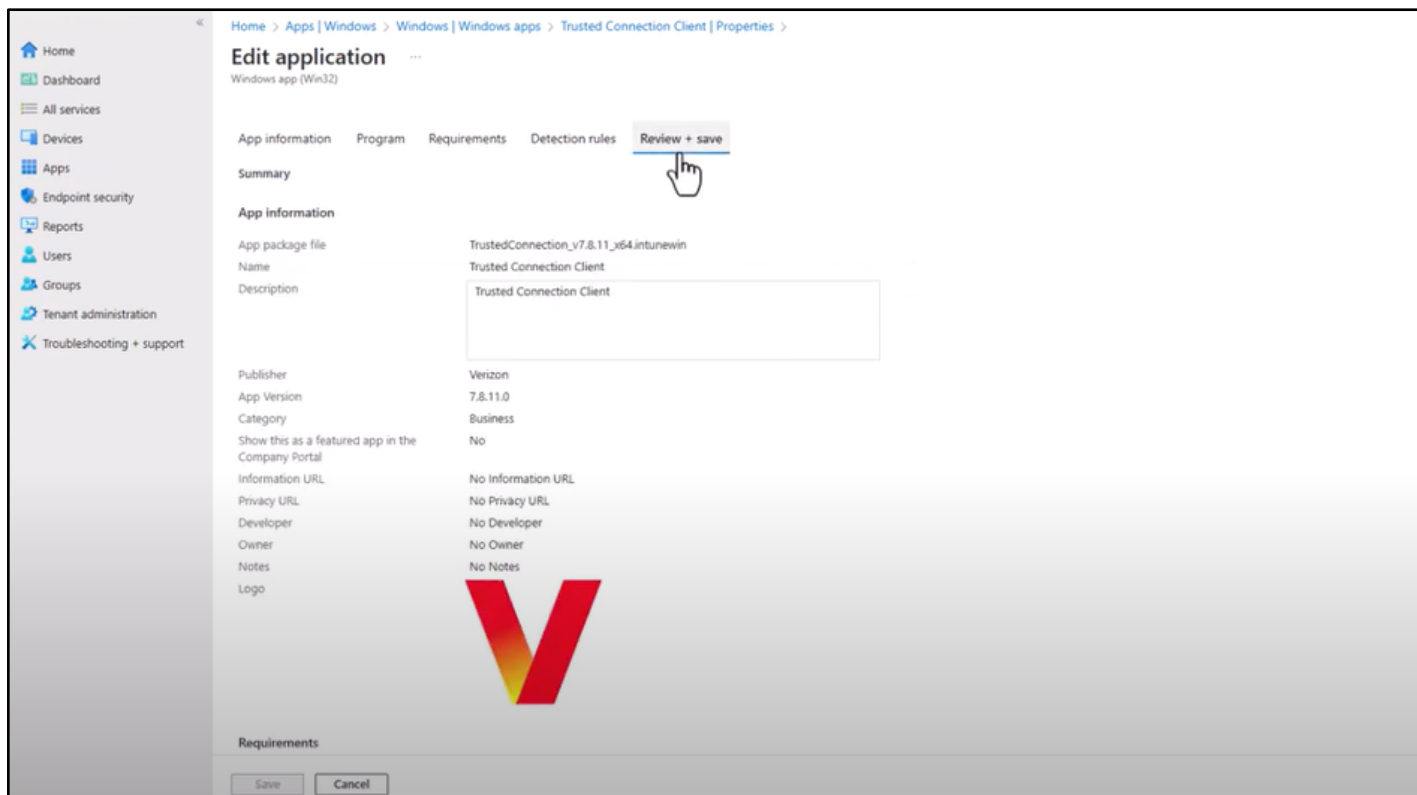


- **Step 4:** By going to Detection rules, application ID provides check if this application ID exists in the registry. If it does, then no install needs to be done. This ID can also be used for uninstalling the previous IDs before installing the upgrade packages.

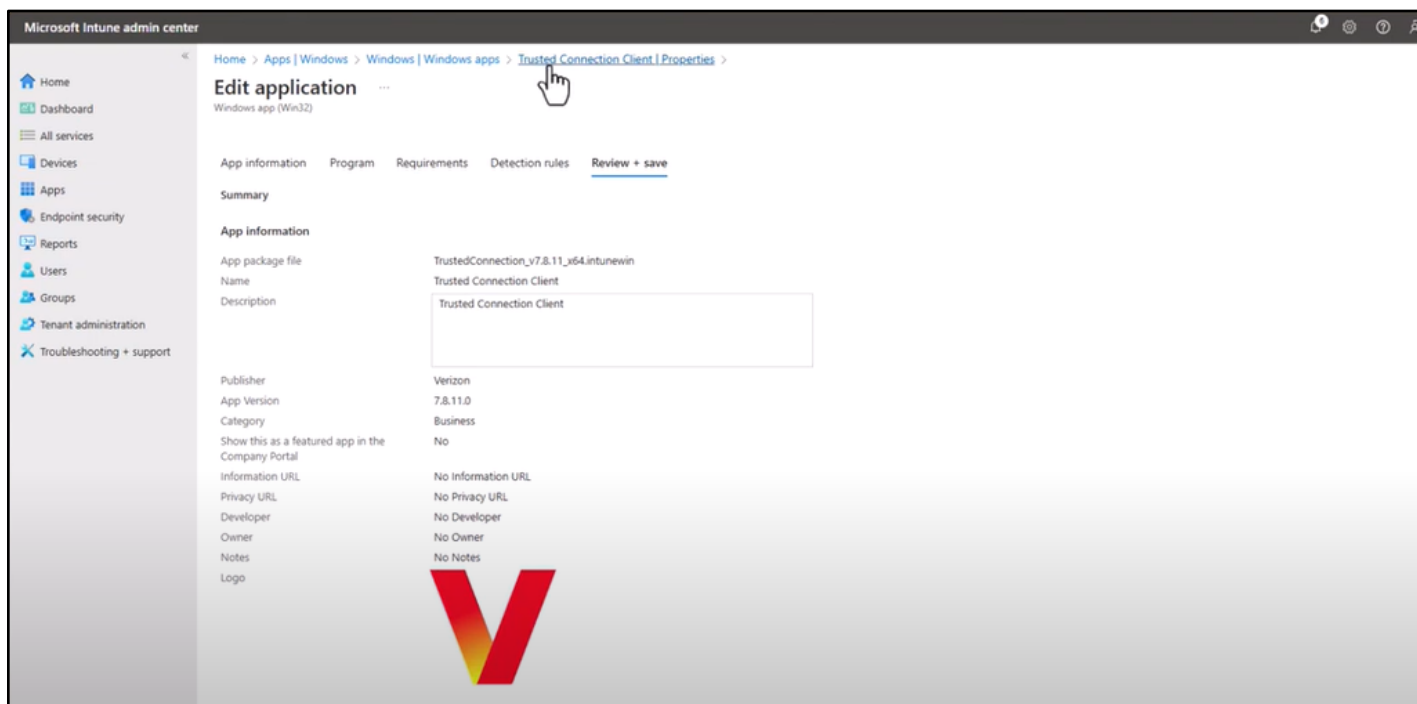




- **Step 5:** Once ready, just Review + save and you'll be back to the Edit application function.



- **Step 6:** Once it is deployed, go back to Trusted Connection Client | Properties





- **Step 7:** Win32 applications offer significant flexibility for Intune management, including setting up dependencies, supersedence for upgrades (like uninstalling previous versions), assigning installation groups, and managing device enrollment.

Microsoft Intune admin center

Home

Dashboard

All services

Devices

Apps

Endpoint security

Reports

Users

Groups

Tenant administration

Troubleshooting + support

Home > Apps > Windows > Windows apps > Trusted Connection Client

Trusted Connection Client | Properties

Client Apps

Search

Overview

Manage

Properties

Monitor

Device install status

User install status

Dependency viewer

Supersedence viewer

Operating system architecture

Minimum operating system

Disk space required (MB)

Physical memory required (MB)

Minimum number of logical processors required

Minimum CPU speed required (MHz)

Additional requirement rules

Detection rules

Rules format

Detection rules

Dependencies

Supersedence

Assignments

Group mode

Group

Filter mode

Filter

End user notifications

Availability

Installation deadline

Restart grace period

Delivery optimization...

Required

Included

Available for enrolled devices

Included

Uninstall

x86,x64

Windows 10 1607

20

4

1

No Minimum CPU speed required (MHz)

No Additional requirement rules

Manually configure detection rules

MSI (AB2822AA-2885-4363-8823-557FCA99E8DA)

No Dependencies

No Supersedence

TC-App\_Install-ACG

None

None

Show all toast notificat...

As soon as possible

As soon as possible

Disabled

Content download in ...

All users

None

None

Show all toast notificat...

As soon as possible

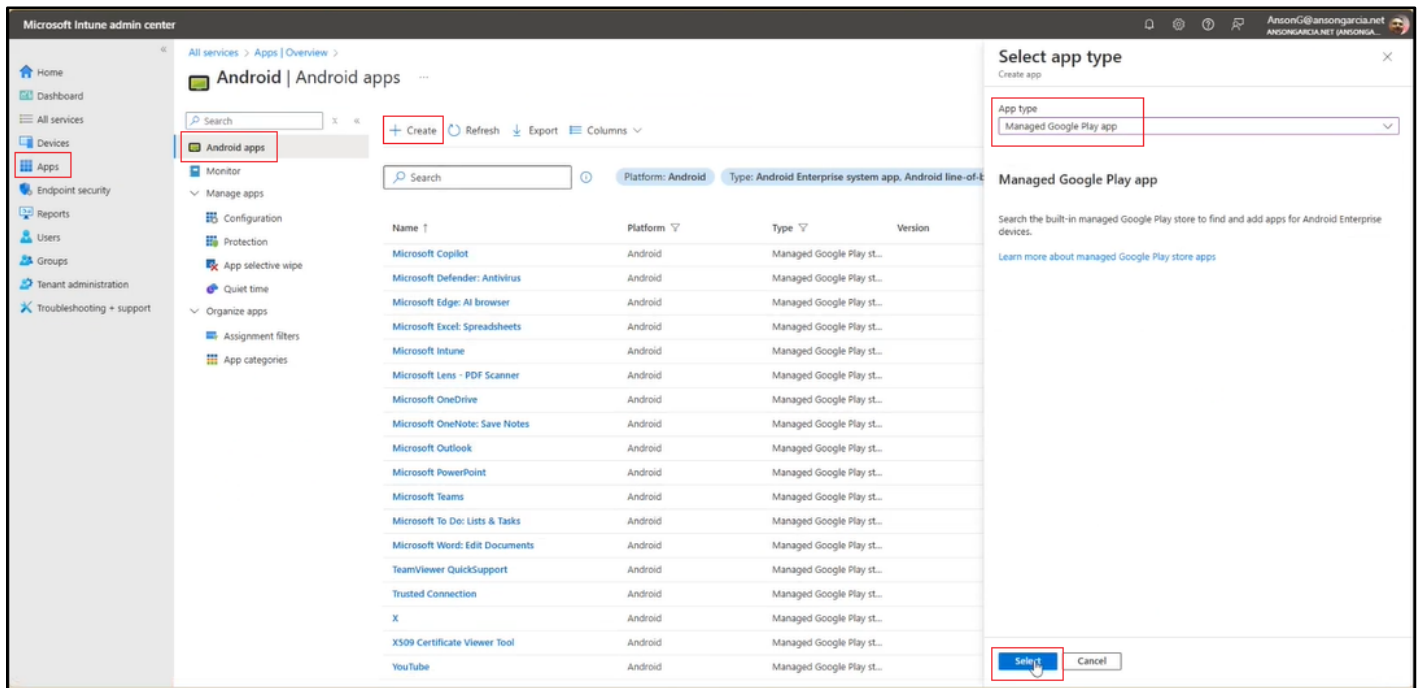
Disabled

Content download in f...

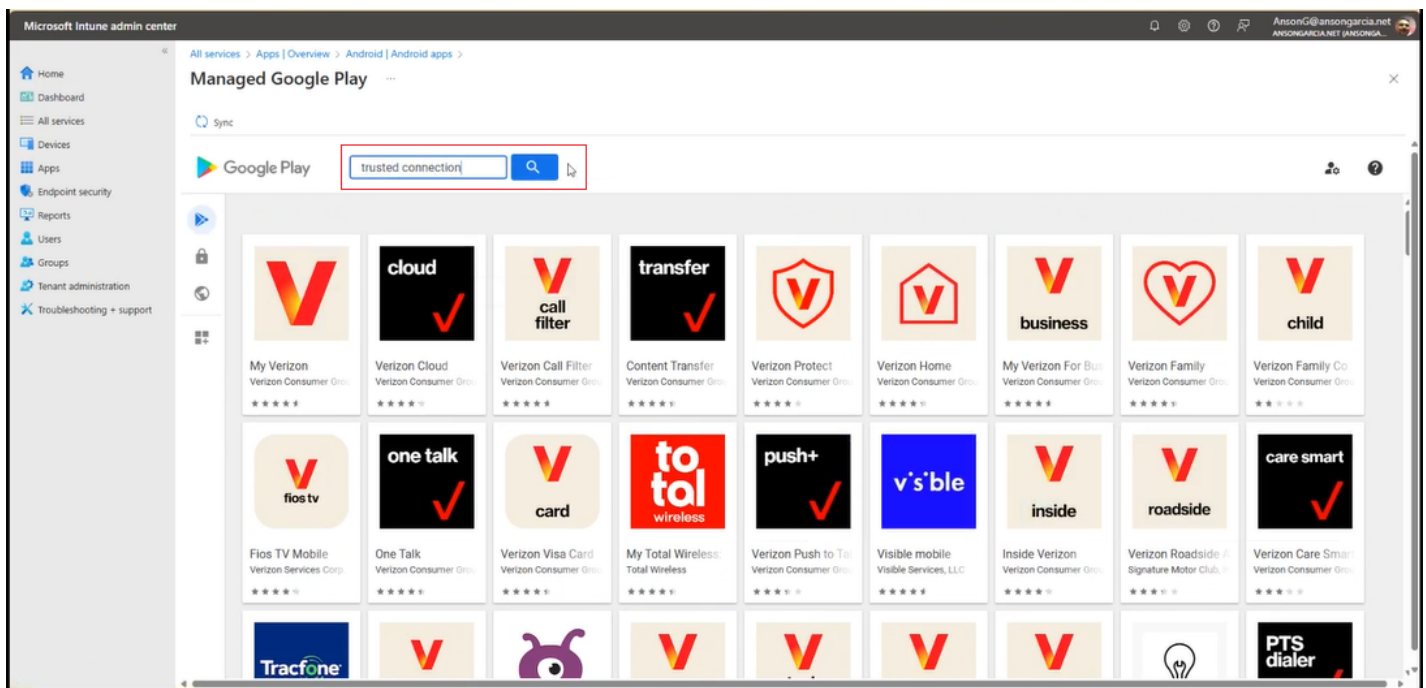


## Install Trusted Connection Android app to Intune portal (from Google Play)

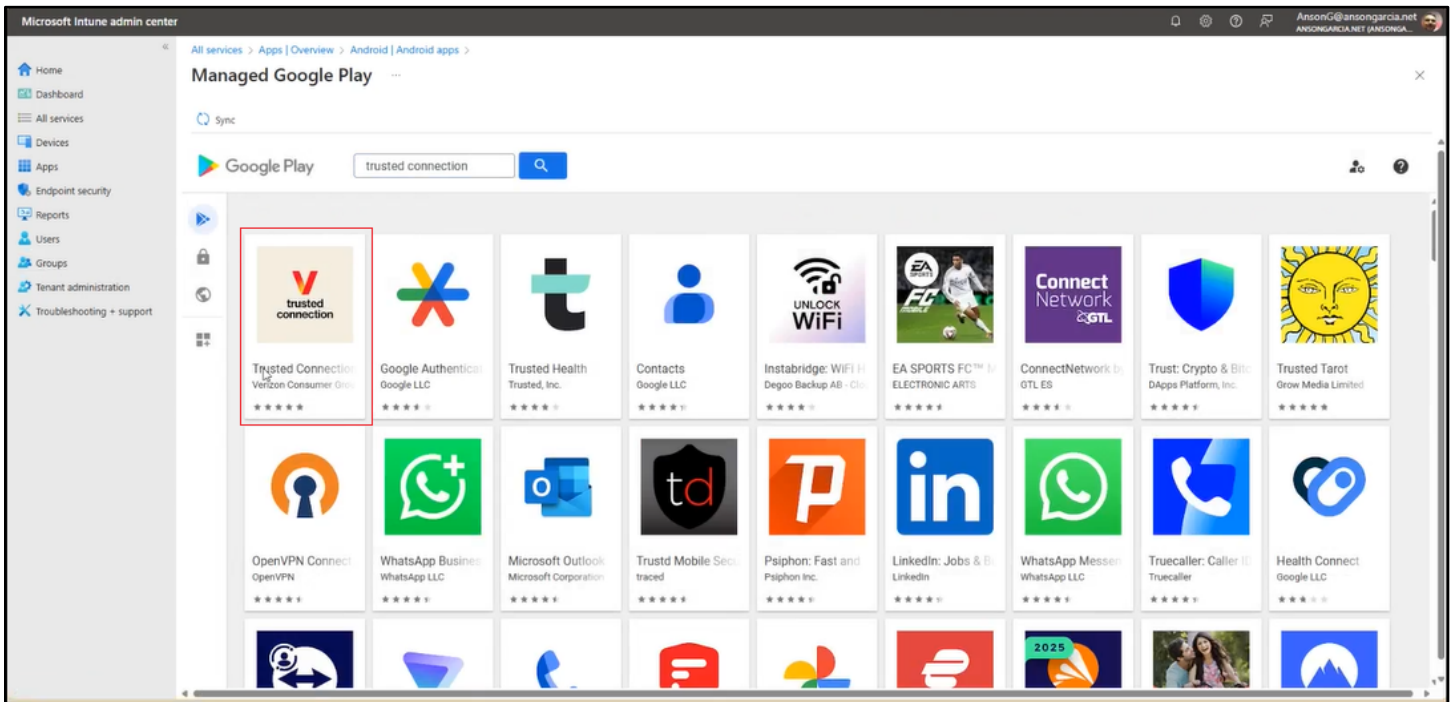
- **Step 1:** Add the Trusted Connection app from the Intune admin center by going to Apps → Android Apps → + Create → Select app type “Managed Google Play app” → Save



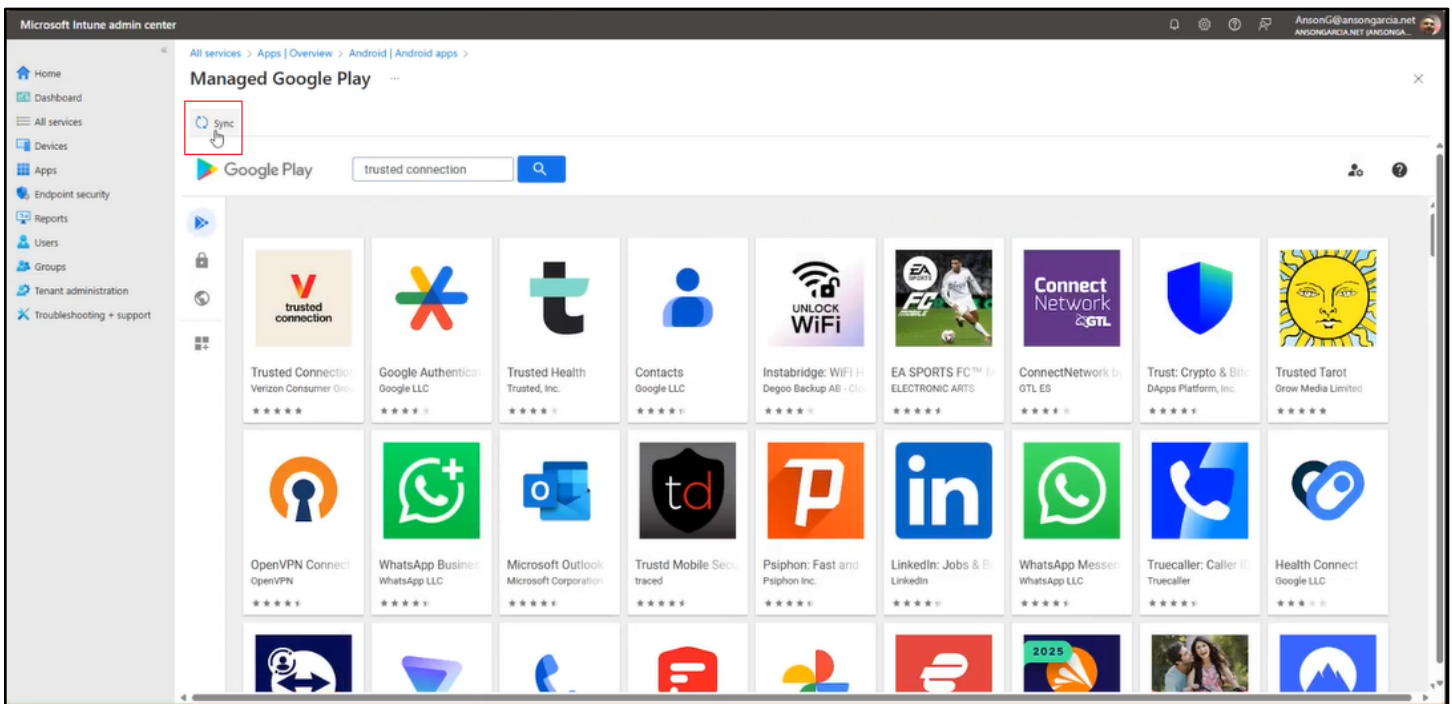
- **Step 2:** Once in the Google Play Store, look for Trusted Connection in the Search area.



- **Step 2a:** Select Trusted Connection.



- **Step 2b:** Synch and go back to Android | Android apps



- **Step 3:** Look for the newly installed Trusted Connection in the list of apps and click on it.

The screenshot shows the Microsoft Intune admin center interface. On the left is a navigation pane with options like Home, Dashboard, All services, Devices, Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main area is titled 'Android | Android apps'. It features a search bar, a '+ Create' button, and a 'Columns' dropdown. Below these is a table of installed apps. The 'Trusted Connection' app is highlighted with a red box.

Name	Platform	Type	Version	VPP token name	Assigned	Developer
Microsoft Copilot	Android	Managed Google Play st...			Yes	...
Microsoft Defender: Antivirus	Android	Managed Google Play st...			No	...
Microsoft Edge: AI browser	Android	Managed Google Play st...			Yes	...
Microsoft Excel: Spreadsheets	Android	Managed Google Play st...			Yes	...
Microsoft Intune	Android	Managed Google Play st...			Yes	...
Microsoft Lens - PDF Scanner	Android	Managed Google Play st...			Yes	...
Microsoft OneDrive	Android	Managed Google Play st...			Yes	...
Microsoft OneNote: Save Notes	Android	Managed Google Play st...			Yes	...
Microsoft Outlook	Android	Managed Google Play st...			Yes	...
Microsoft PowerPoint	Android	Managed Google Play st...			Yes	...
Microsoft Teams	Android	Managed Google Play st...			Yes	...
Microsoft To Do: Lists & Tasks	Android	Managed Google Play st...			Yes	...
Microsoft Word: Edit Documents	Android	Managed Google Play st...			Yes	...
Trusted Connection	Android	Managed Google Play st...			Yes	...
Trusted Connection	Android	Managed Google Play st...			Yes	...
X509 Certificate Viewer Tool	Android	Managed Google Play st...			Yes	...
YouTube	Android	Managed Google Play st...			Yes	...

- **Step 4:** Go to properties

The screenshot shows the 'Trusted Connection' app page in the Microsoft Intune admin center. The 'Overview' tab is selected, and the 'Properties' sub-tab is highlighted with a red box. The page displays essential information about the app, including its publisher, operating system, and license status. Below this, there are two donut charts showing device and user status.

**Essentials**

- Publisher: Verizon Consumer Group
- Operating system: Android
- Total licenses: 0
- Created: 1/25/2025, 10:28:47 AM
- Assigned: Yes
- Available licenses: 0

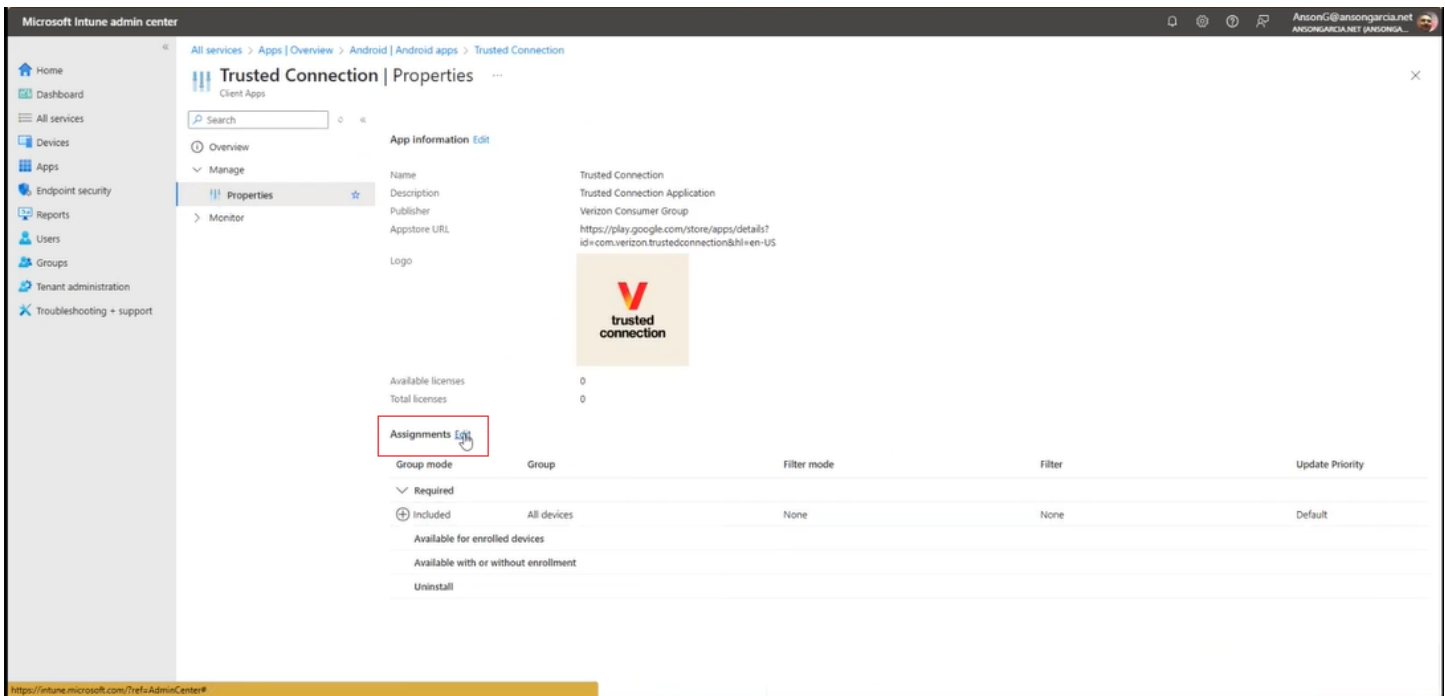
**Device status**

Installed	Not installed	Failed	Install Pending	Not Applicable
2	0	0	0	0

**User status**

Installed	Not installed	Failed	Install Pending
2	0	0	0

- **Step 5:** You can Edit the Assignments to deploy the configuration to a specific device, device groups or all devices.



Microsoft Intune admin center

All services > Apps > Overview > Android > Android apps > Trusted Connection

### Trusted Connection | Properties

Client Apps

Search

Overview

Manage

Properties

Monitor

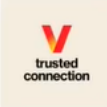
App information [Edit](#)

Name: Trusted Connection

Description: Trusted Connection Application

Publisher: Verizon Consumer Group

Appstore URL: <https://play.google.com/store/apps/details?id=com.verizon.trustedconnection&hl=en-US>

Logo: 

Available licenses: 0

Total licenses: 0

**Assignments [Edit](#)**

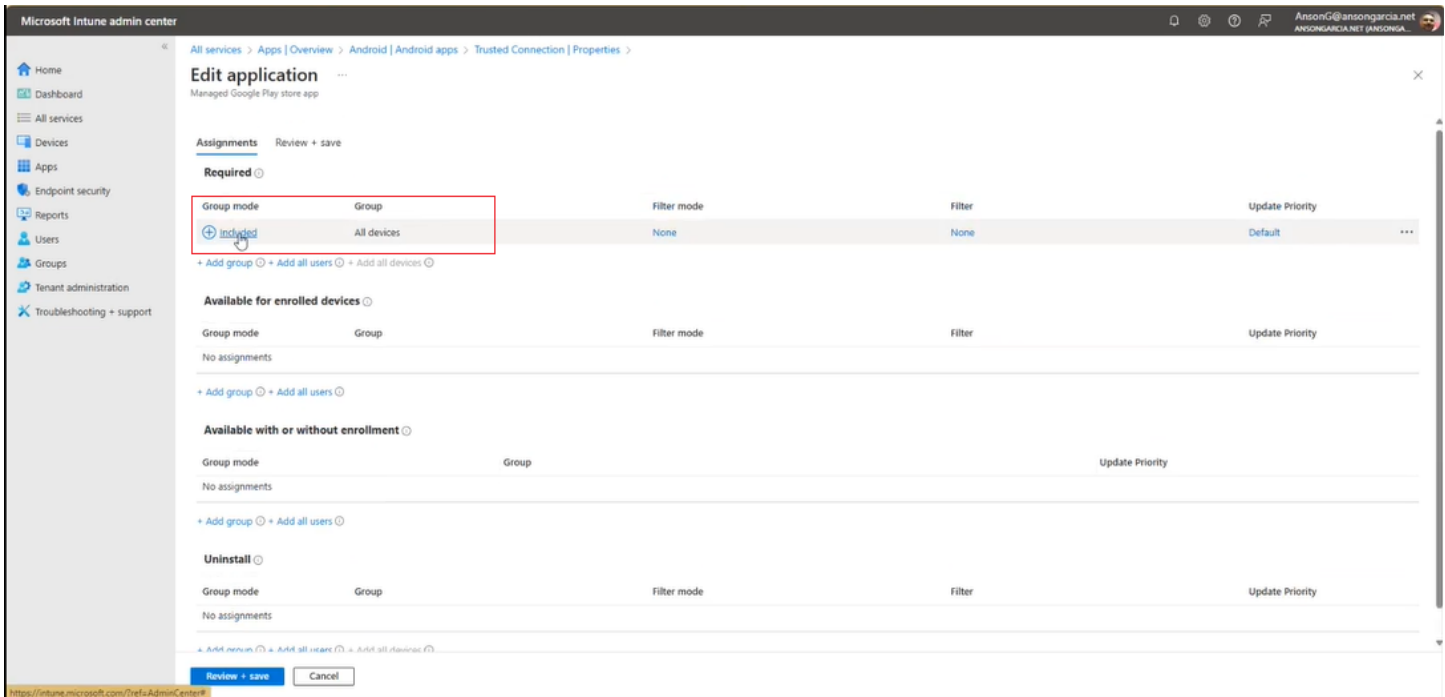
Group mode	Group	Filter mode	Filter	Update Priority
Required				
Included	All devices	None	None	Default

Available for enrolled devices

Available with or without enrollment

Uninstall

<https://intune.microsoft.com/trefa/AdminCenter#>



Microsoft Intune admin center

All services > Apps > Overview > Android > Android apps > Trusted Connection | Properties

### Edit application

Managed Google Play store app

Assignments [Review + save](#)

Required

Group mode	Group	Filter mode	Filter	Update Priority
Included	All devices	None	None	Default

+ Add group + Add all users + Add all devices

Available for enrolled devices

Group mode	Group	Filter mode	Filter	Update Priority
No assignments				

+ Add group + Add all users

Available with or without enrollment

Group mode	Group	Filter mode	Filter	Update Priority
No assignments				

+ Add group + Add all users

Uninstall

Group mode	Group	Filter mode	Filter	Update Priority
No assignments				

+ Add group + Add all users

[Review + save](#) [Cancel](#)

<https://intune.microsoft.com/trefa/AdminCenter#>



# Creating Staging Profiles for Android devices

A staging profile enables a staged enrollment process for Android Enterprise devices, where the initial provisioning steps are completed beforehand. With it, you can complete both the admin and end user stages of pre-provisioning, so minimal interaction is required of the end-user when they receive their device.

- Android enterprise enrollment types
- Create staging profile and assign apps
- Review Token & generate QR code
- Enroll an Android device via token (QR code)

## Android enterprise enrollment types

The following table shows the different profiles that can be used during enrollment. We have identified that “Android Enterprise corporate owned work profile” best suits most enterprise needs as it is the option that has the least user error plus involving a large volume of new and existing corporate devices which are associated with single users.

Enroll Android devices in Microsoft Intune

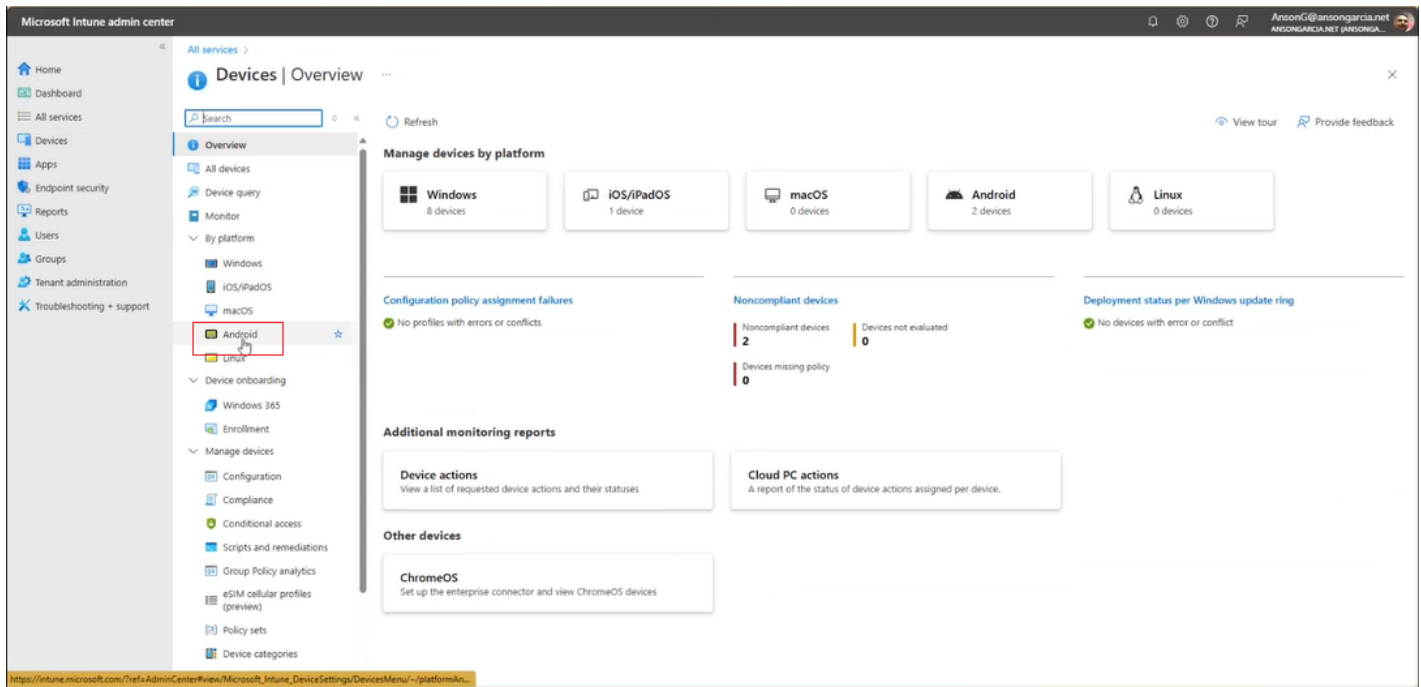
<https://aka.ms/AndroidEnrollmentGuide>

This topic is 2 of 5  
Page 2

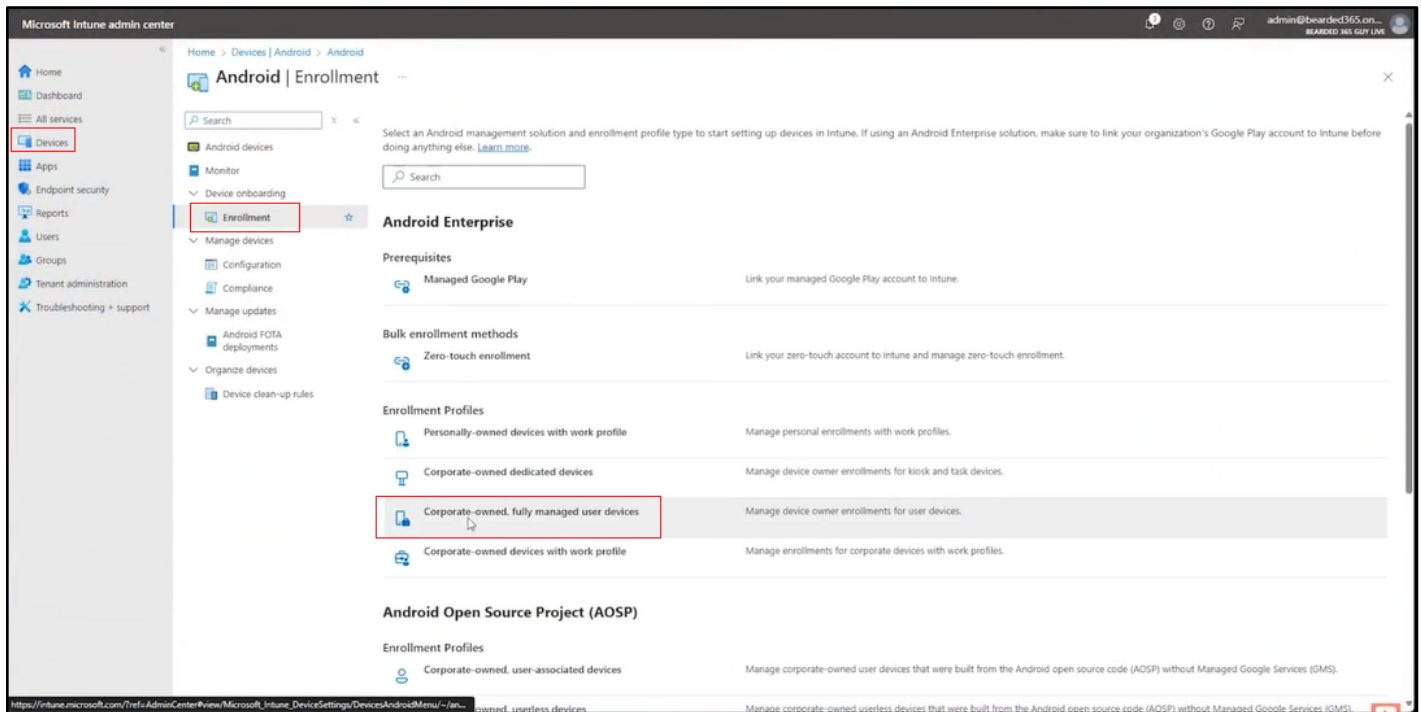
Feature	BYOD: Android Enterprise personally owned devices with a work profile	Android Enterprise dedicated devices	Android Enterprise fully managed	Android Enterprise corporate owned work profile	Android Open Source Project
Use Google Mobile Services (GMS).	✔	✔	✔	✔	✘ Device doesn't support GMS. Some countries don't support GMS.
Devices are personal or BYOD.	✔ You can mark these devices as corporate or personal.	✘ These devices should be enrolled using Android Enterprise personally owned devices with a work profile.	✘ These devices should be enrolled using Android Enterprise personally owned devices with a work profile.	✘ These devices should be enrolled using Android Enterprise personally owned devices with a work profile.	✘ Android Enterprise personally owned devices with a work profile support GMS.
You have new or existing devices.	✔	✔	✔	✔	✔
Need to enroll a few devices, or a large number of devices (bulk enrollment).	✔	✔	✔	✔	✘ Can only enroll one device at a time.
Devices are associated with a single user.	✔	✘ Not recommended. These devices should be enrolled using Android Enterprise fully managed.	✔	✔	✔
You use the optional device enrollment manager (DEM) account.	✔	✘ The DEM account isn't supported.	✘ The DEM account isn't supported.	✘ The DEM account isn't supported.	✘ The DEM account isn't supported.
Devices are managed by another MDM provider.	✘ When a device enrolls, MDM providers install certificates and other files. These files must be removed.	✘ To be fully managed by Intune, users need to unenroll from the current MDM provider, and then enroll in Intune.	✘ To be fully managed by Intune, users need to unenroll from the current MDM provider, and then enroll in Intune.	✘ To be fully managed by Intune, users need to unenroll from the current MDM provider, and then enroll in Intune.	✘ To be fully managed by Intune, users need to unenroll from the current MDM provider, and then enroll in Intune.
Devices are owned by the organization or school.	✘ Not recommended for organization-owned devices.	✔	✔	✔	✔



- **Step 1:** First go to Devices and select the Android platform. This will take you to the Android Enrollment section.



- **Step 2:** Next under Enrollment Profiles, select the Corporate-owned fully managed user devices option. This will prompt you to +Create policy to assign enrollment policies and tokens for your staging profile.





Microsoft Intune admin center

Home

Dashboard

All services

Devices

Apps

Endpoint security

Reports

Users

Groups

Tenant administration

Troubleshooting + support

All services > Android | Enrollment >

Corporate-owned, fully managed user devices

Android enrollment

Create and assign enrollment policies and tokens for corporate-owned, fully managed user devices. [Learn more.](#)

+ Create policy

Refresh

Export

Columns

0 items

Search

Policy state: Active

Add filters

Name ↑

No data found

## Create staging profile and assign apps

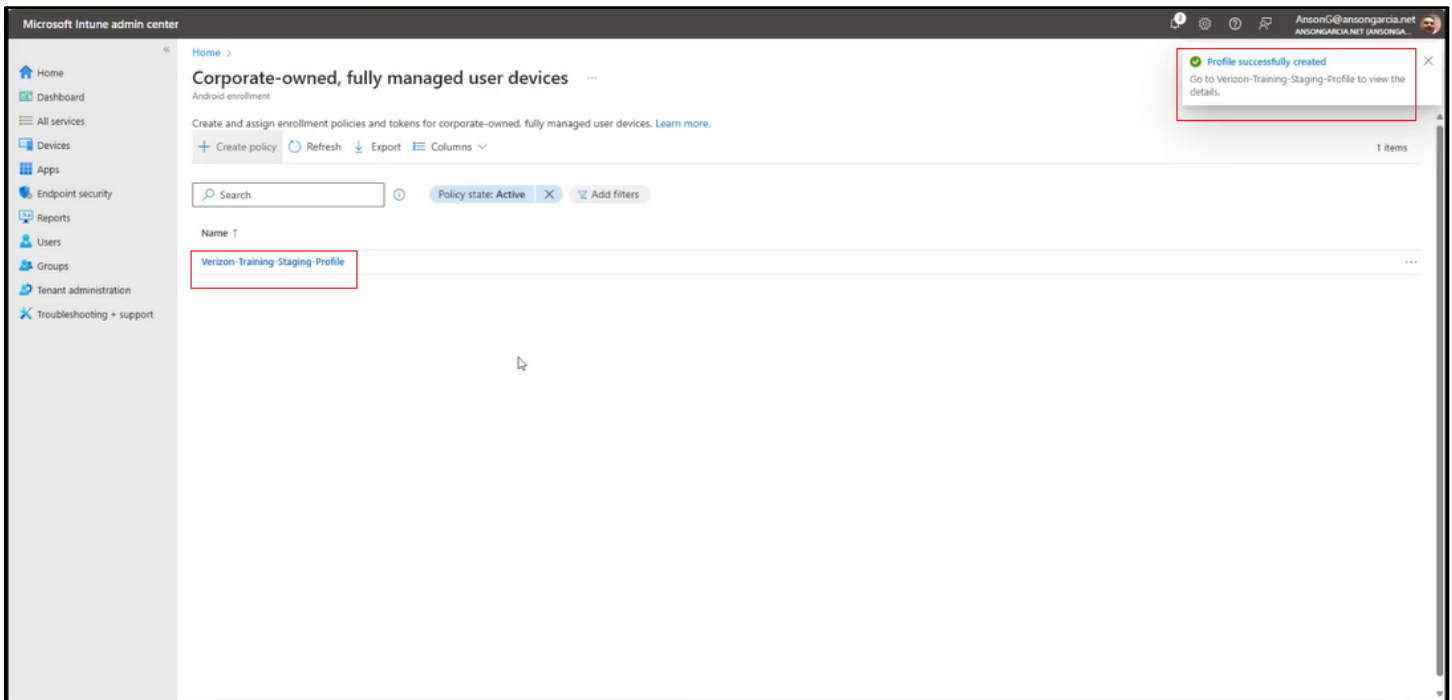
- **Step 1:** By Creating a profile, you will also be creating a Token which will be used to auto-generate a QR code. These tokens will have a validity and will expire thus helping you to control the time the End Users take to use it. Then click Next and Create.

The screenshot shows the 'Create profile' page in the Microsoft Intune admin center. The page is titled 'Create profile' and has a breadcrumb trail: 'Home > Corporate-owned, fully managed user devices >'. The left sidebar contains navigation links: Home, Dashboard, All services, Devices, Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main content area has two tabs: 'Basics' (selected) and 'Review + create'. Under the 'Basics' tab, there are four fields: 'Name' (with a dropdown menu showing 'Verizon-Training-Staging-Profile'), 'Description' (with a text box containing 'test'), 'Token type' (with a dropdown menu showing 'Corporate-owned, fully managed, via staging'), and 'Token expiration date' (with a calendar picker showing 'April 2025'). At the bottom of the page, there are two buttons: 'Previous' and 'Next' (highlighted with a red box).

The screenshot shows the 'Create profile' page in the Microsoft Intune admin center, now at the 'Review + create' step. The page title is 'Create profile' and the breadcrumb trail is 'Home > Corporate-owned, fully managed user devices >'. The left sidebar is the same as in the previous screenshot. The main content area has two tabs: 'Basics' and 'Review + create' (selected). Under the 'Review + create' tab, there is a 'Summary' section and a 'Basics' section. The 'Summary' section lists the profile details: Name (Verizon-Training-Staging-Profile), Description (test), Token type (Corporate-owned, fully managed, via staging), and Token expiration date (07/31/25). The 'Basics' section is empty. At the bottom of the page, there are two buttons: 'Previous' and 'Create' (highlighted with a red box).



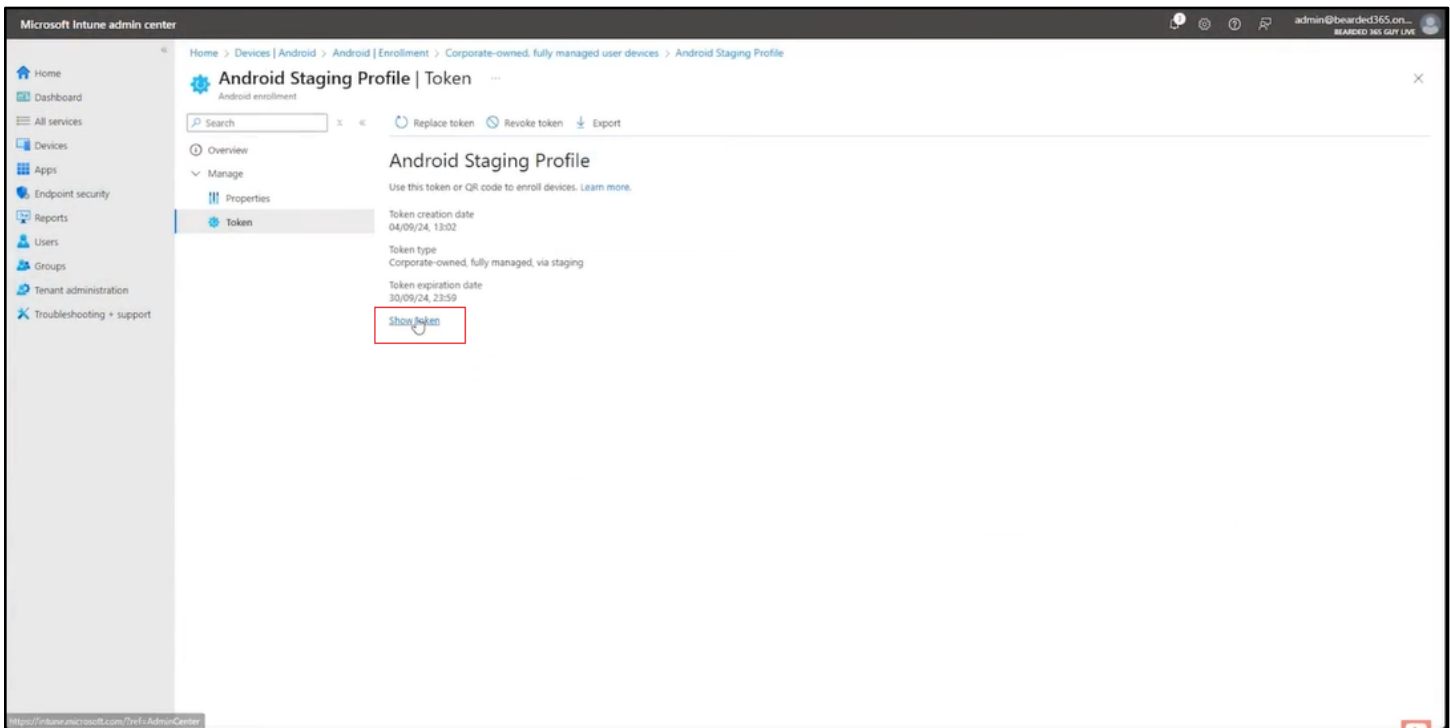
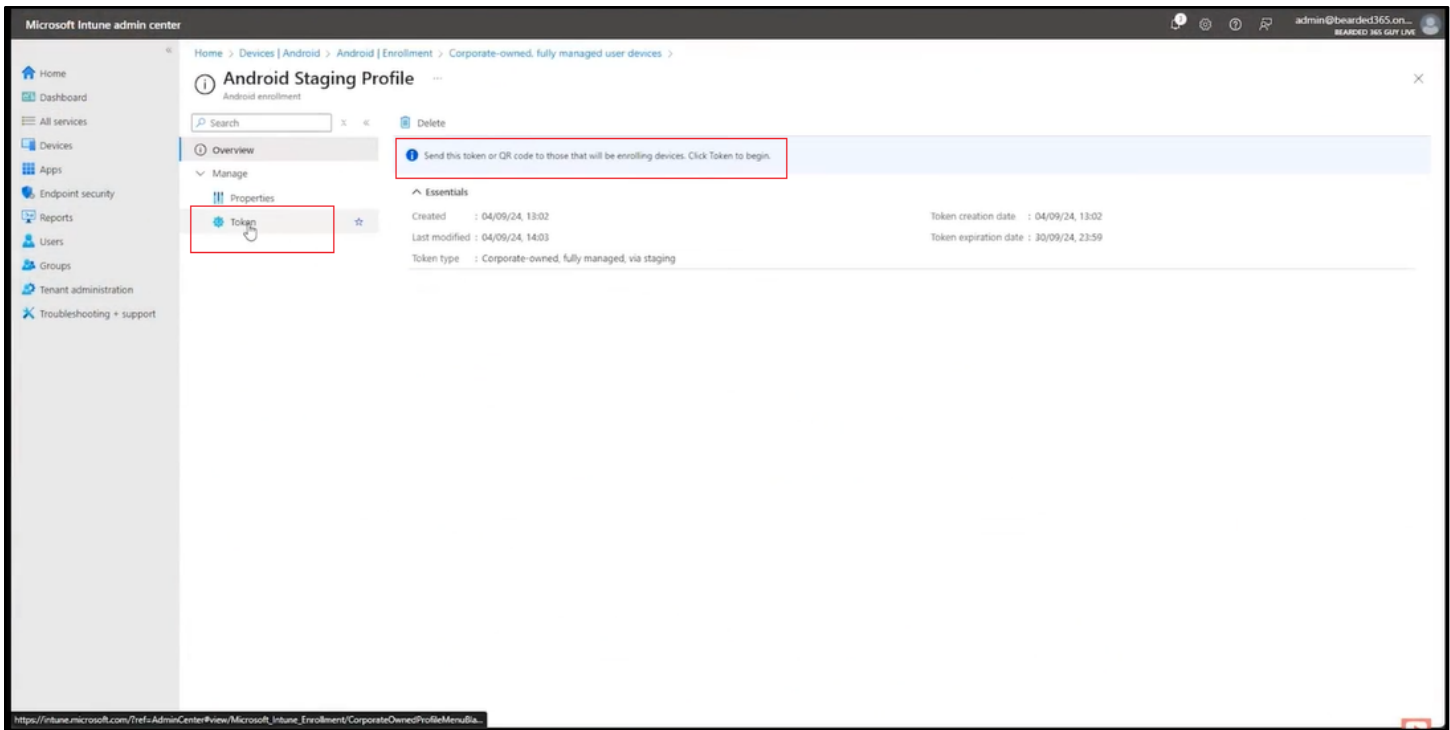
- **Step 2:** Back to the Corporate-owned fully managed user devices section, you'll see that the Profile has been successfully created.



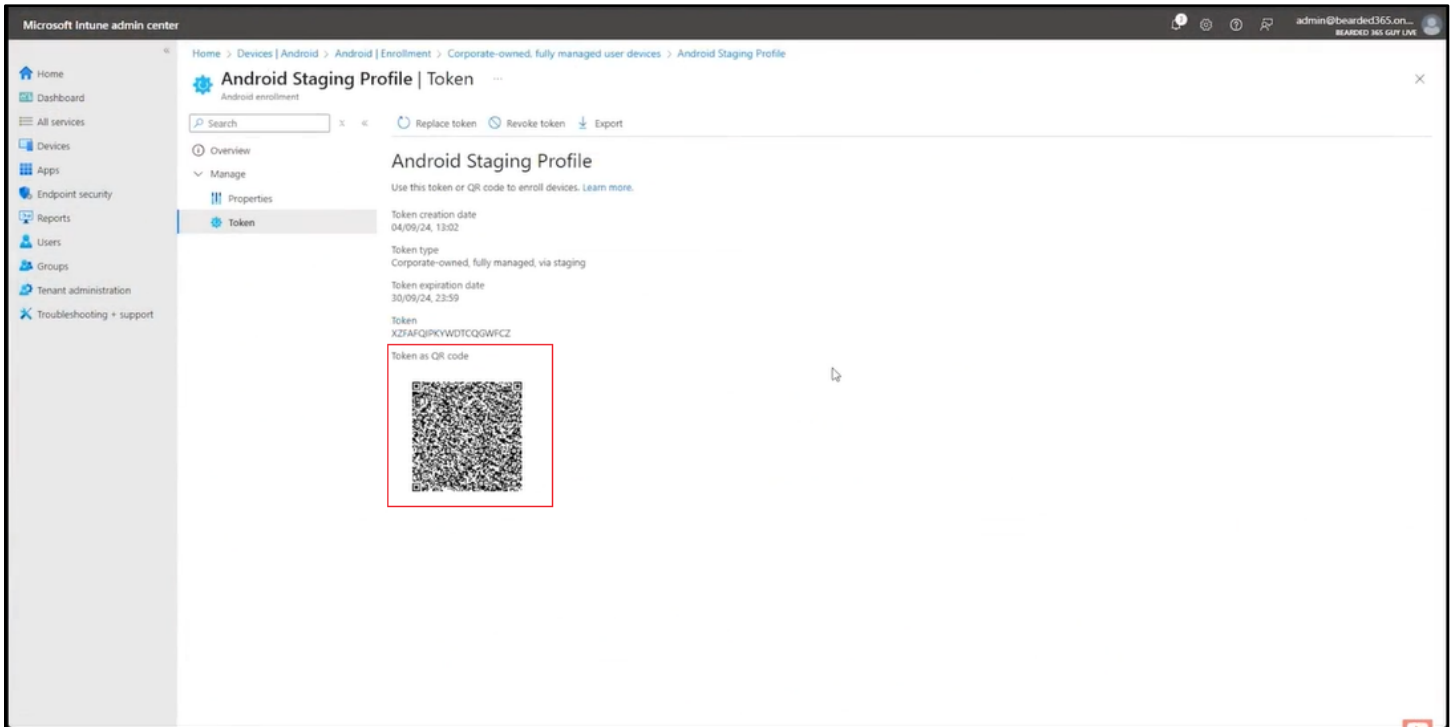


## Review Token & generate QR code

- **Step 1:** By accessing your newly created staging profile, you will be able to see the Token as QR code



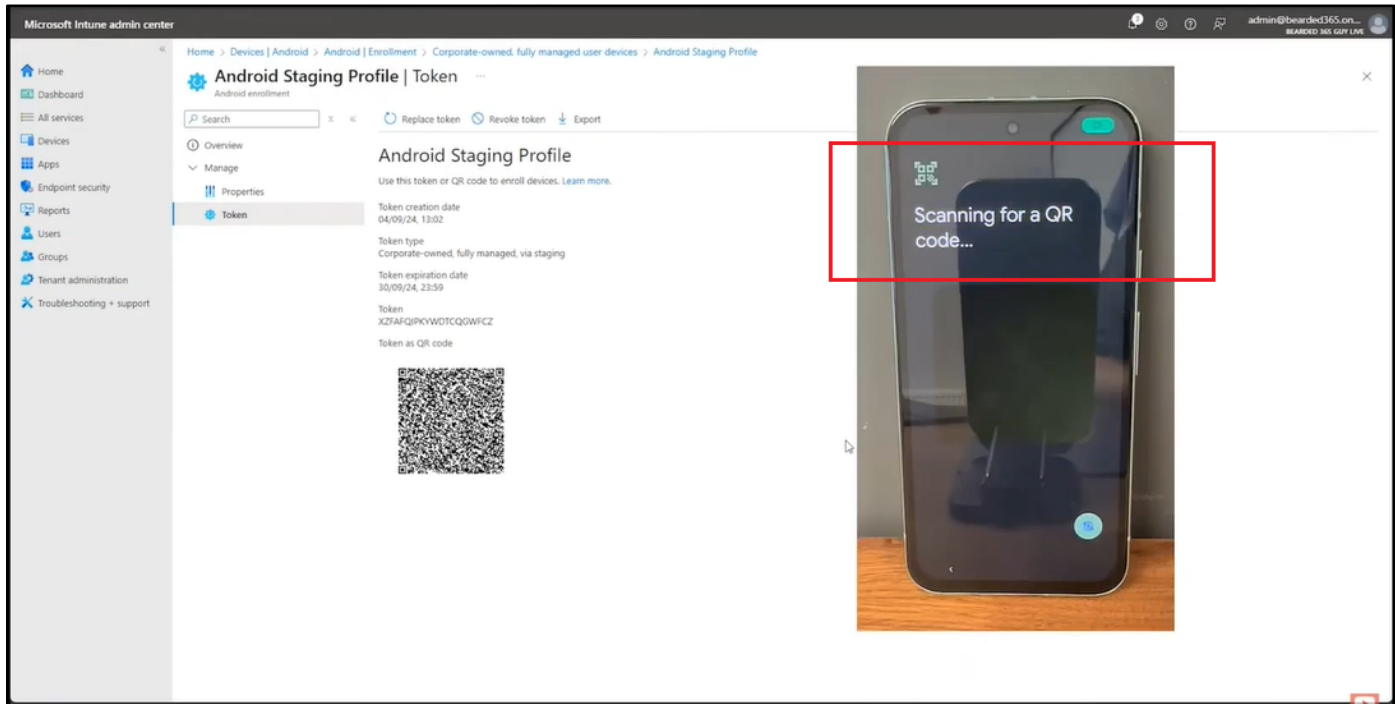
- **Step 2:** You can now use or send the QR code to enroll corporate Android devices



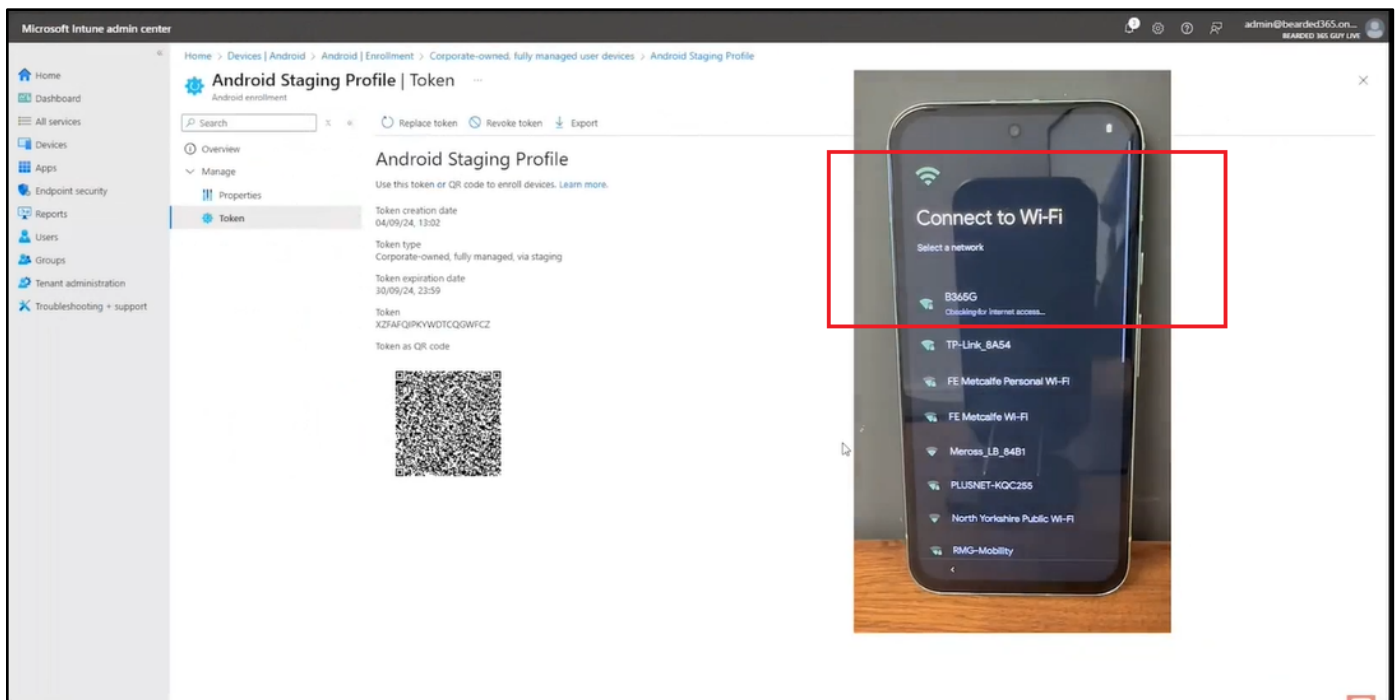


## Enroll an Android device via token (QR code)

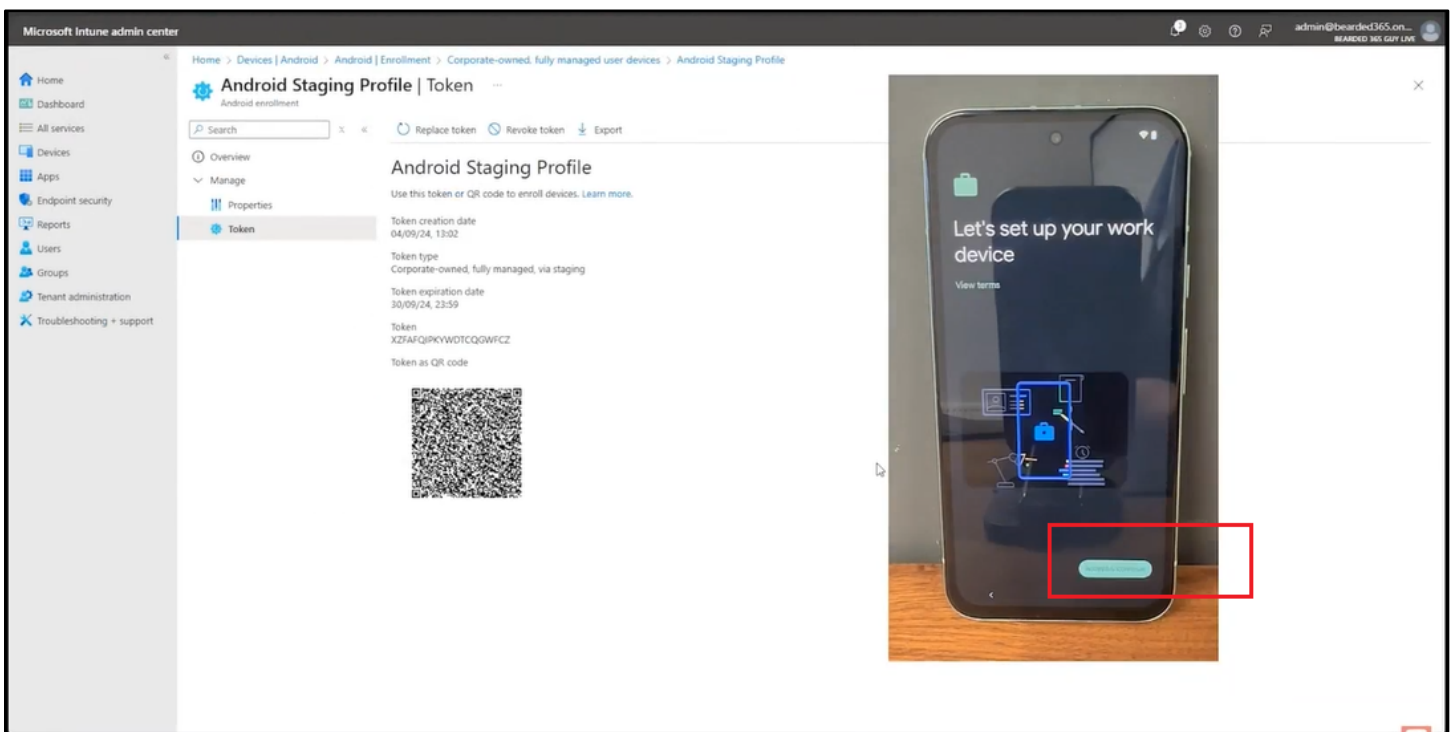
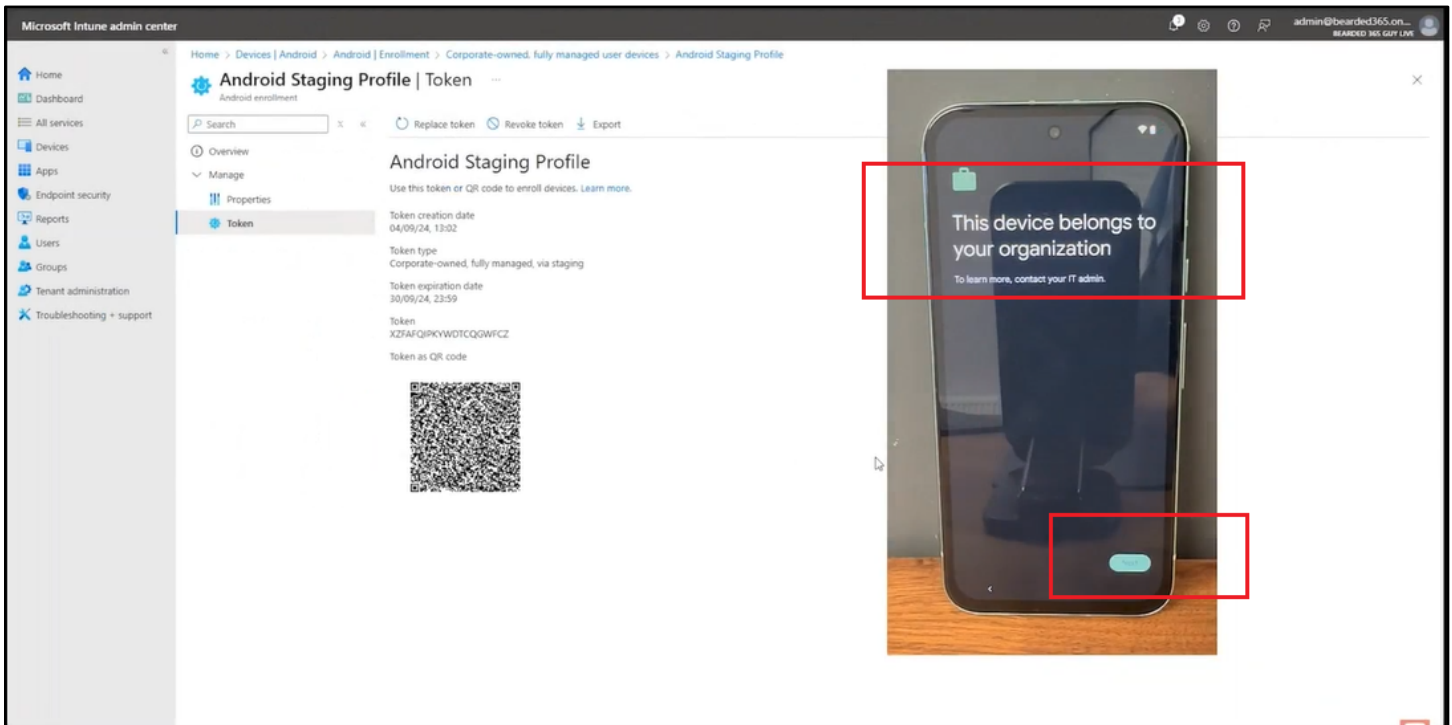
- **Step 1:** Reset (backup suggested for existing devices) and scan the QR code



- **Step 2:** Connect to Wi-Fi

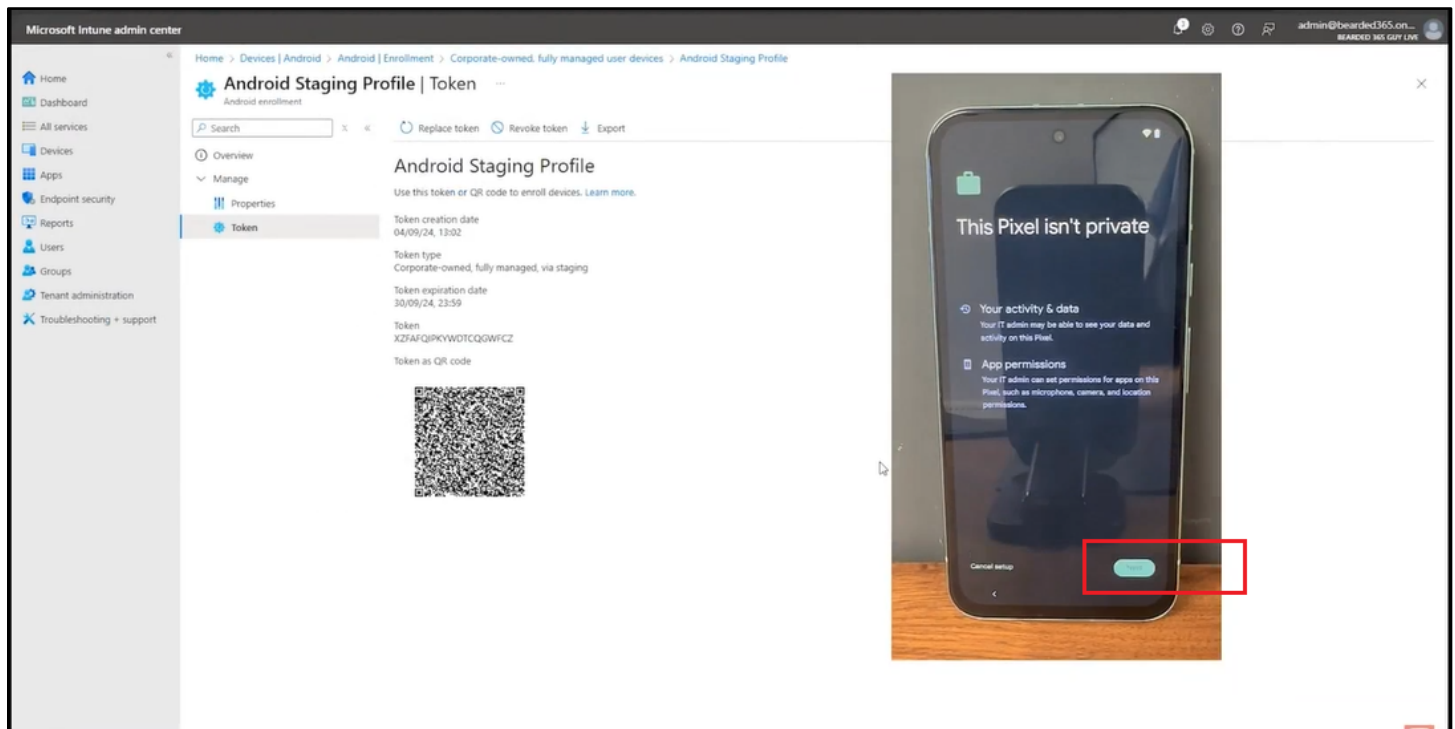
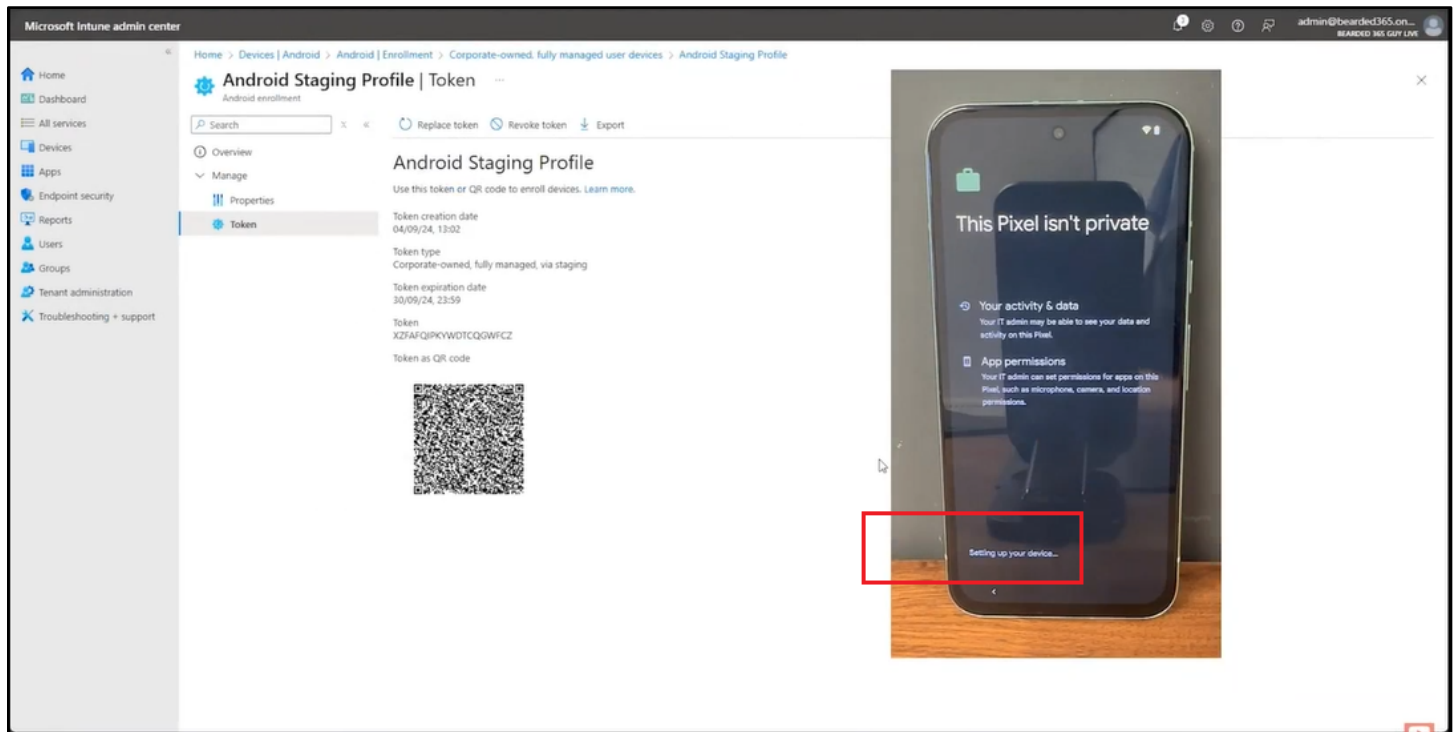


- **Step 3:** The device will show it belongs to your organisation, click Next and Setup Device

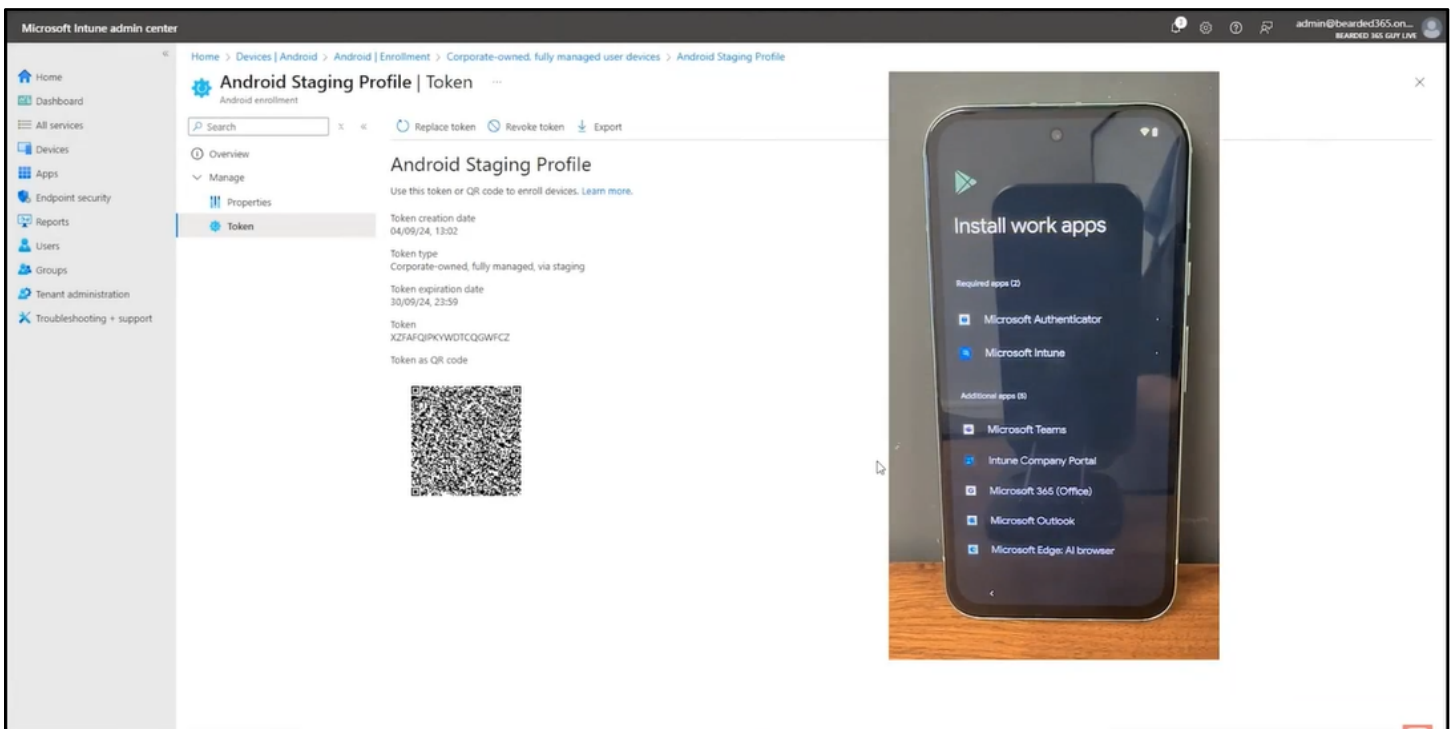
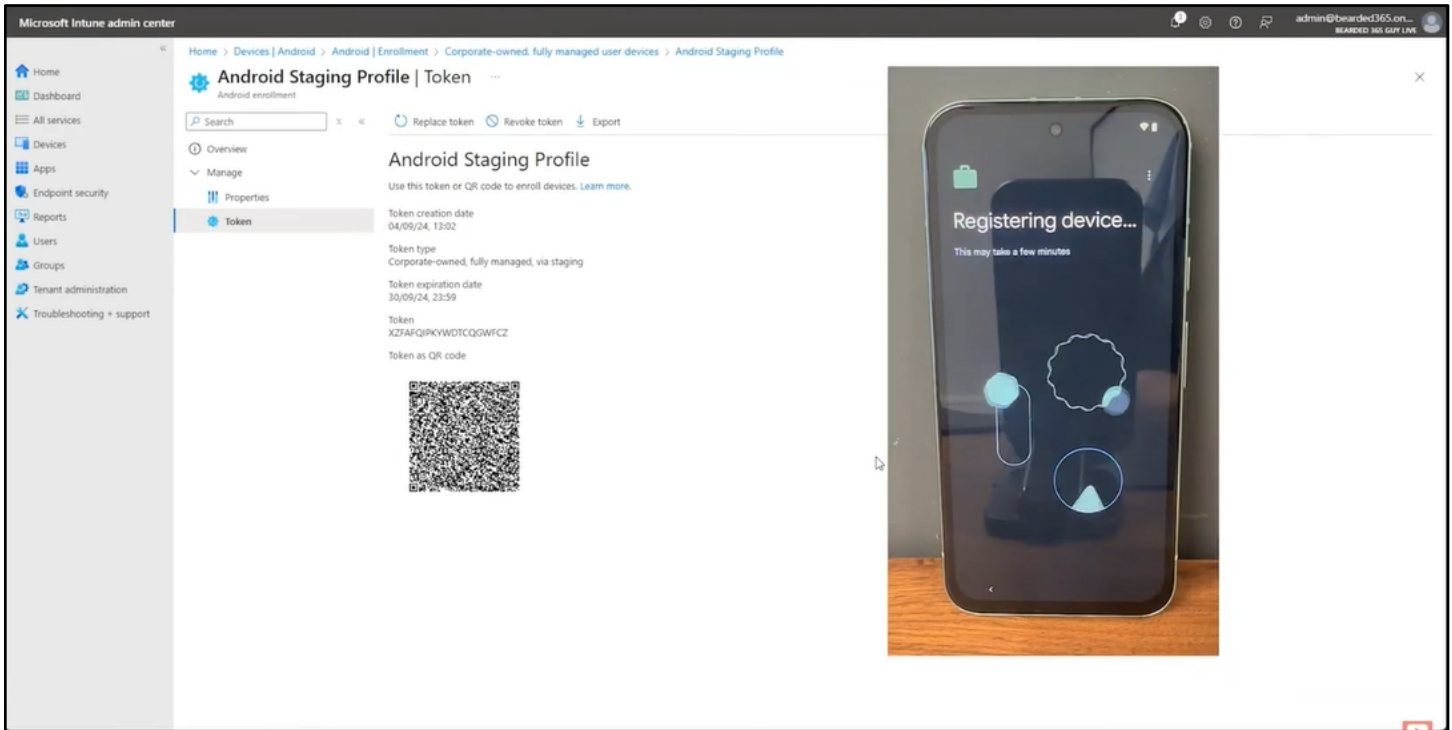




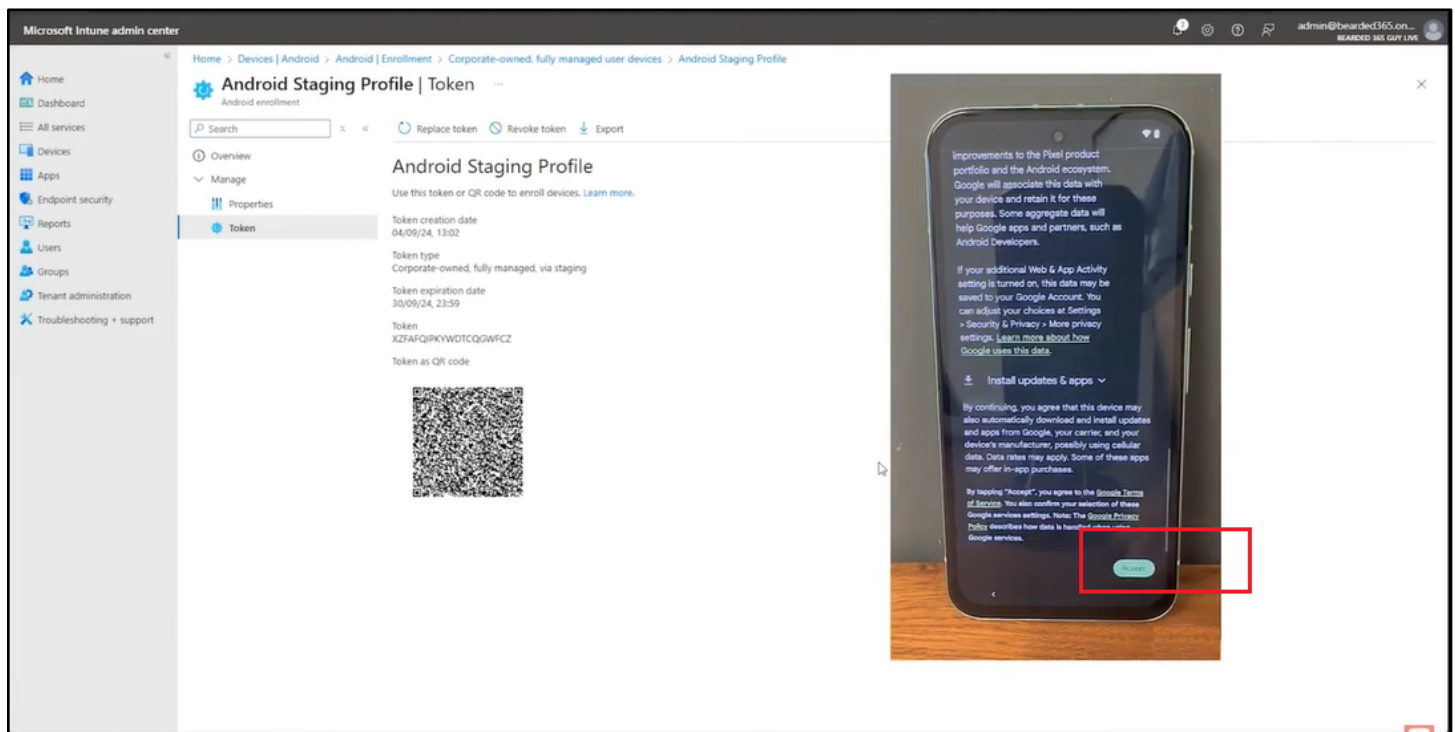
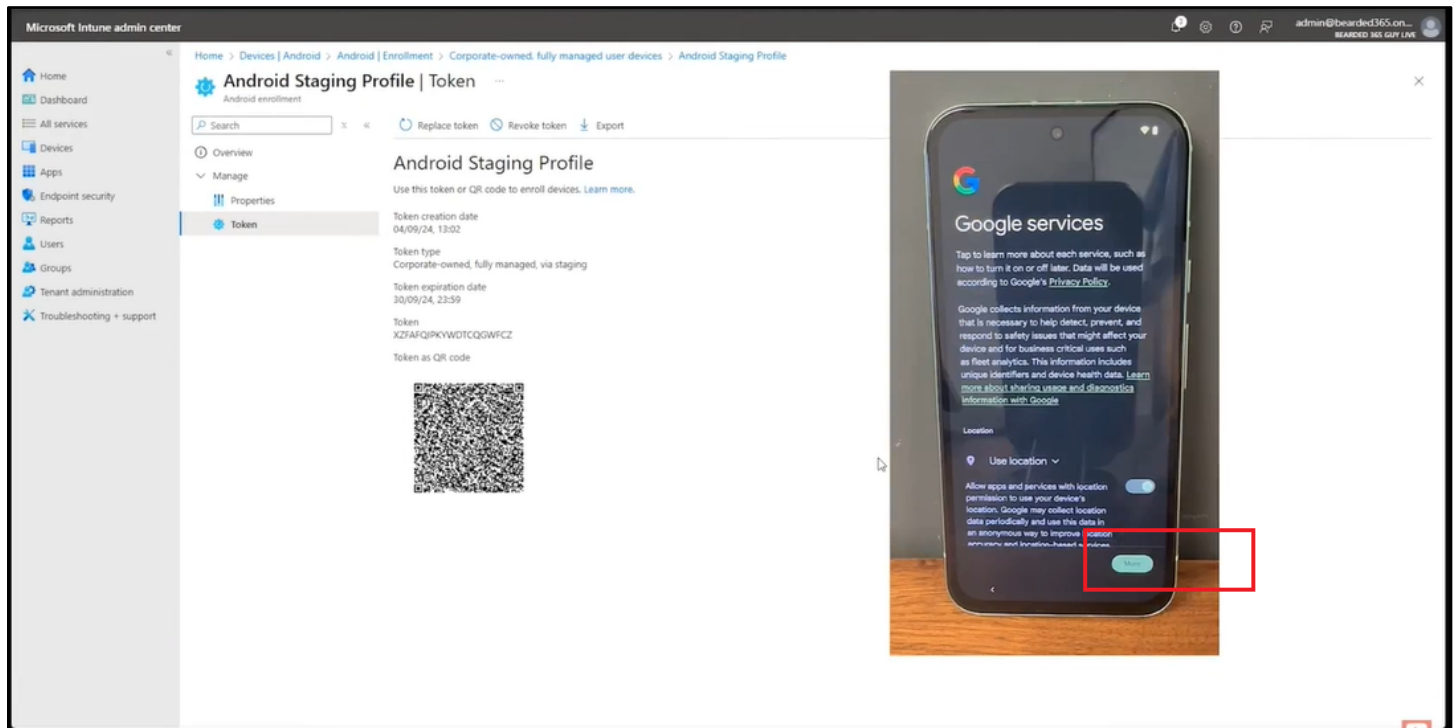
- **Step 4:** The device will start setting up and ask if you wish to proceed.



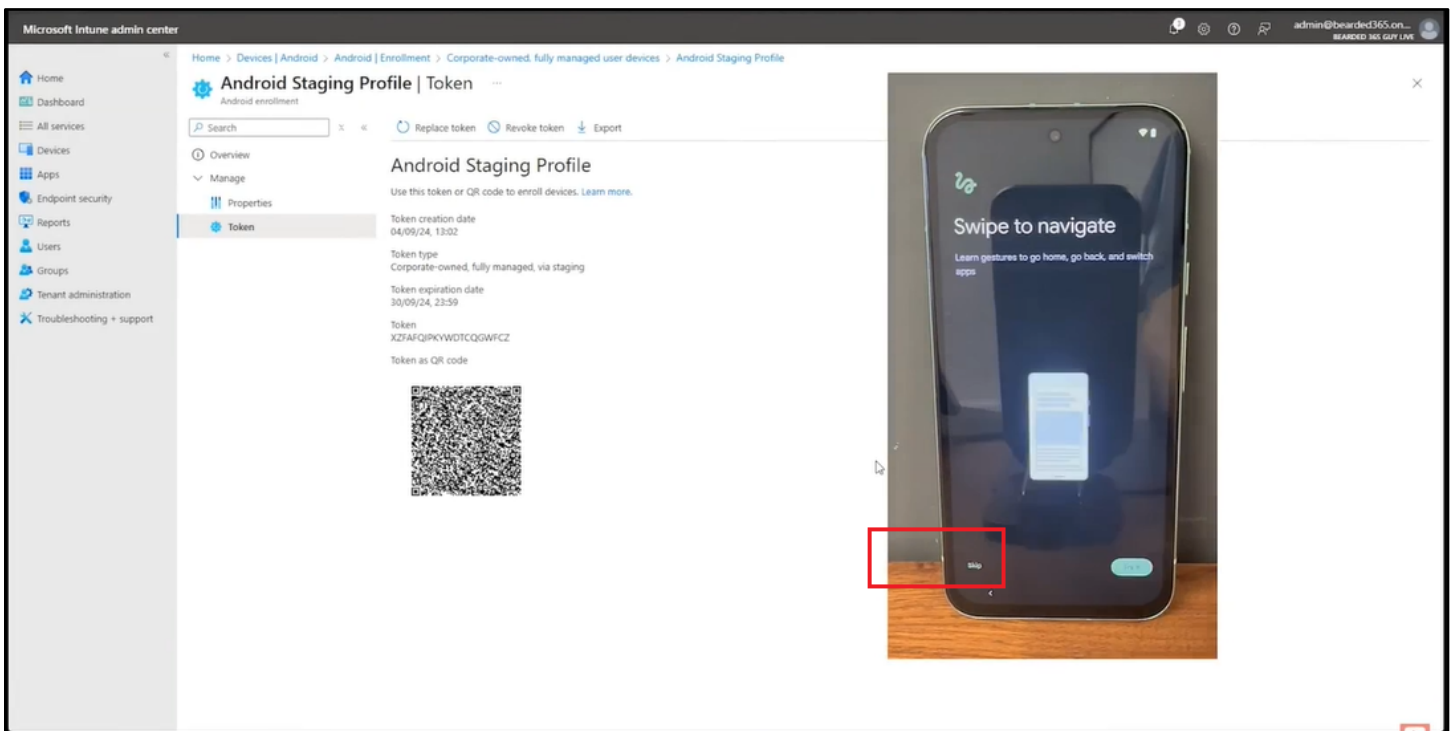
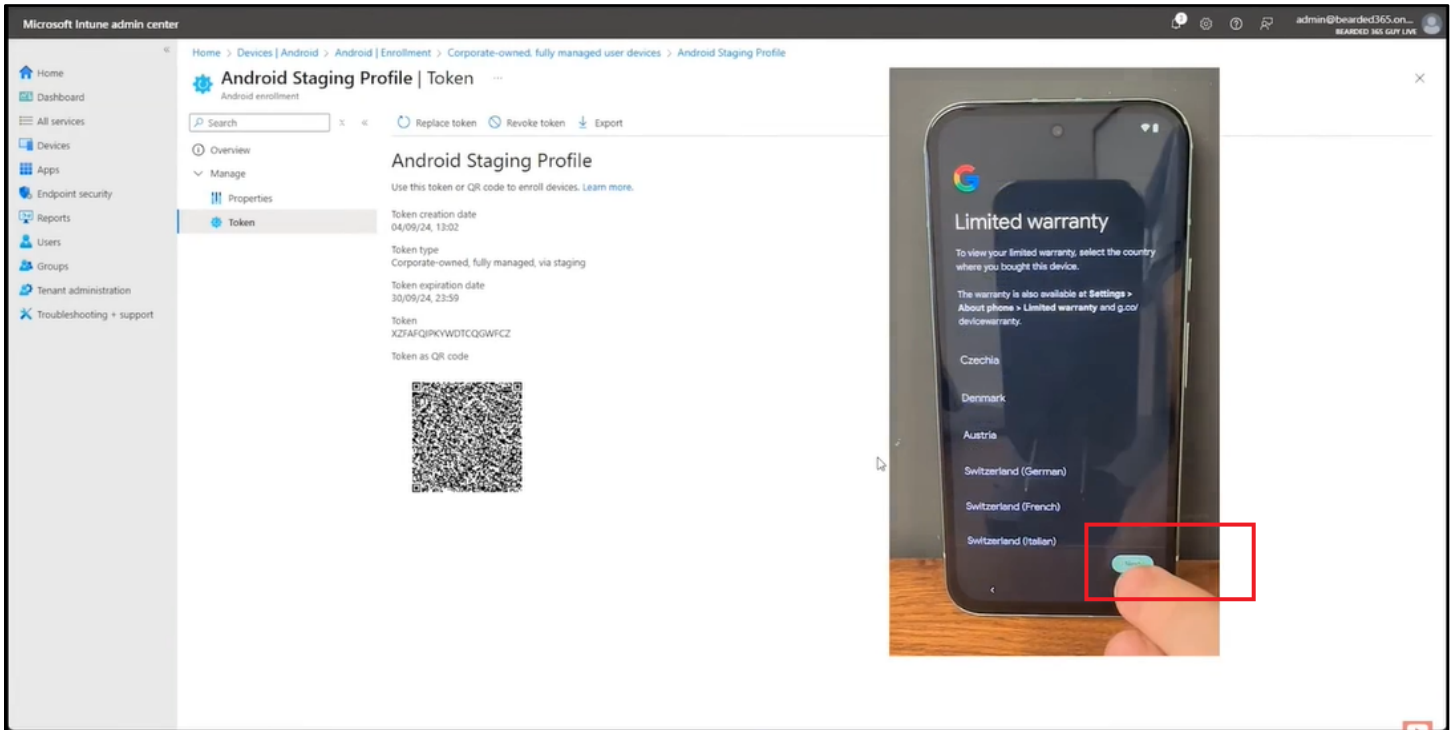
- **Step 5:** The device will be registered & will start installing the apps as defined in the staging profile



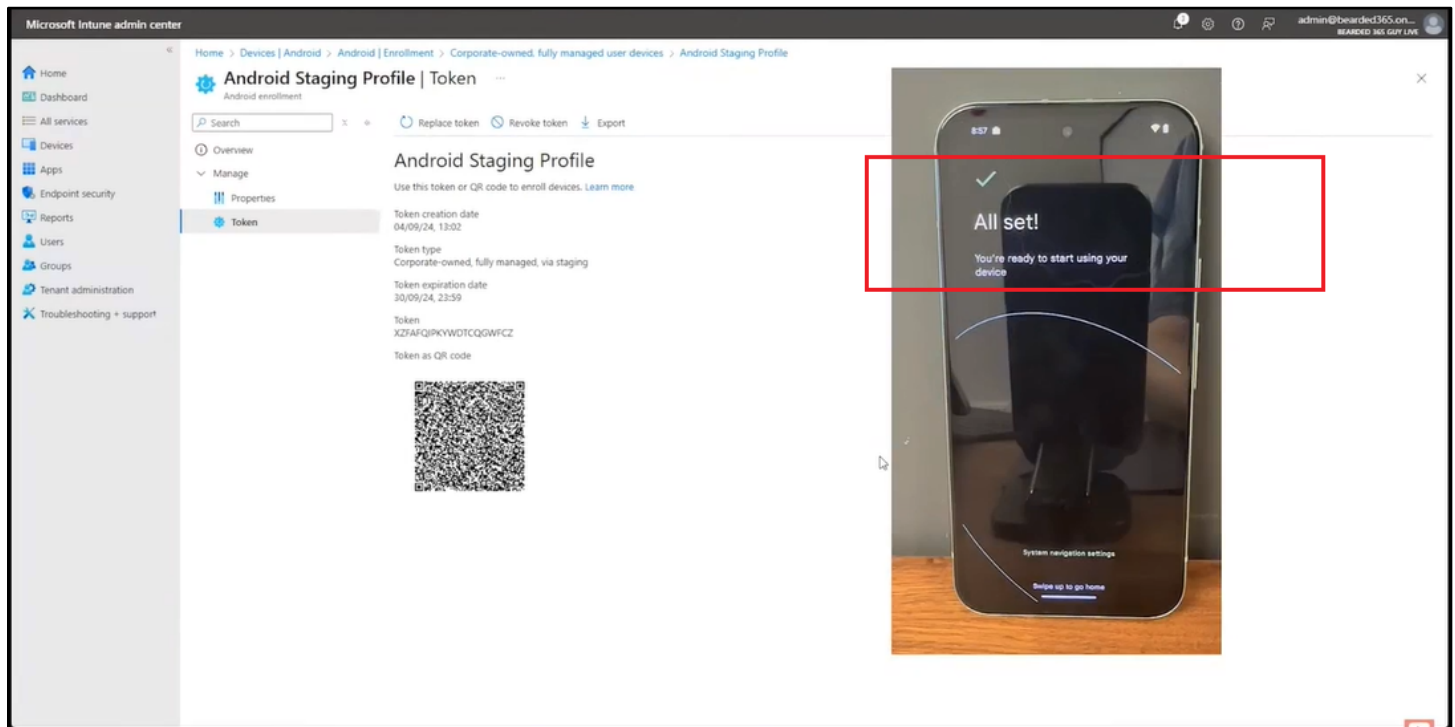
- **Step 6:** Read the Google services click more and Accept at the end



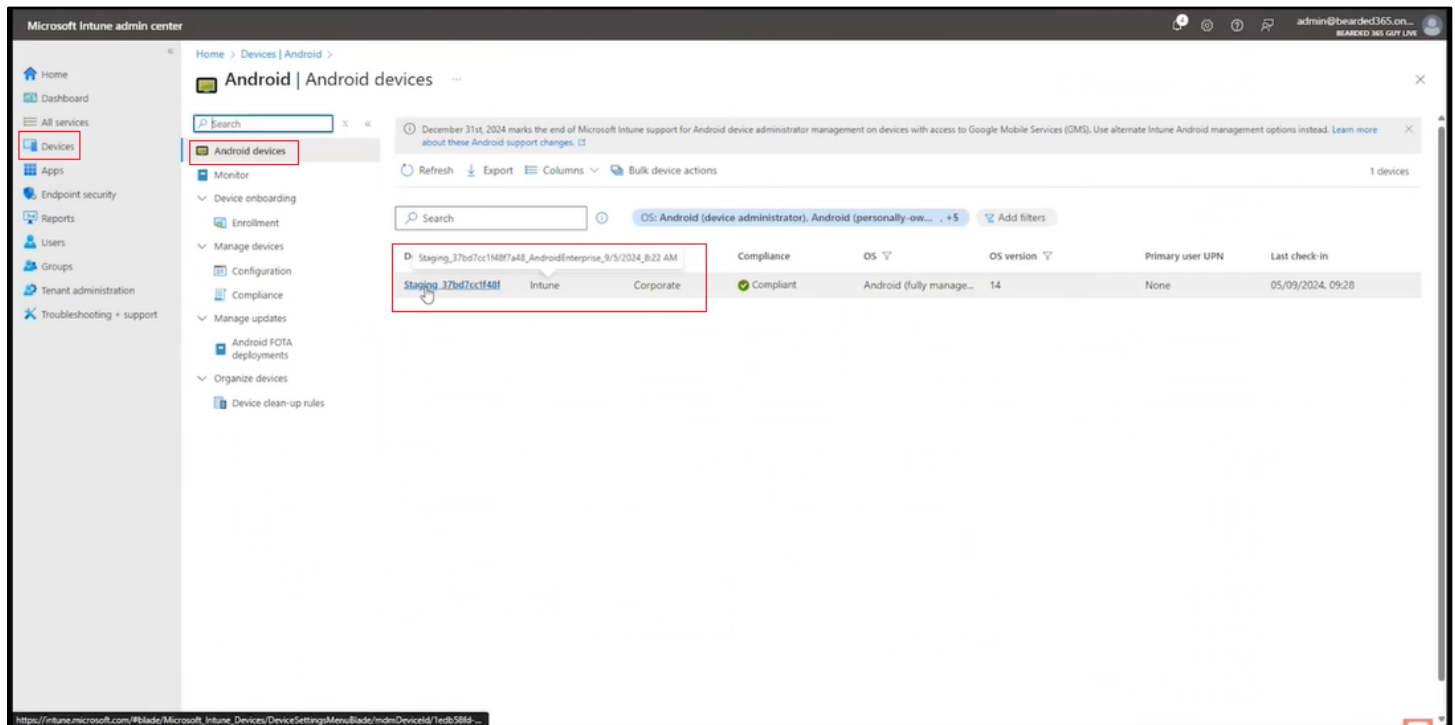
- **Step 7:** Proceed with the Limited warranty and Skip the navigation gestures



- **Step 8:** All set, the device has been set-up



- **Step 9:** Go back to Android devices to confirm the device has been added. Click on the device name to see Overview.



- **Step 10:** The Primary User is not set yet (this will appear after the End User's first log in to Intune).

Microsoft Intune admin center

Home > Devices > Android > Android devices > Staging\_37bd7cc1f48f7a48\_AndroidEnterprise\_9/5/2024\_8:22 AM

Overview

Essentials

Device name : Staging\_37bd7cc1f48f7a48\_AndroidEnterprise\_9/5/2024\_8:22 AM

Management name : Staging\_37bd7cc1f48f7a48\_AndroidEnterprise\_9/5/2024\_8:22 AM

Ownership : Corporate

Serial number : 45291JKB05184

Phone number : ---

Device manufacturer : Google

Primary user : None

Enrolled by : ---

Compliance : Compliant

Operating system : Android

Device model : Pixel 8a

Last check-in time : 05/09/2024 9:28:28

Remote assistance : ---

Device actions status

Action	Status	Date/Time	Error
No data			

- **Step 11:** In Managed Apps you will find all the apps installed on the device

Microsoft Intune admin center

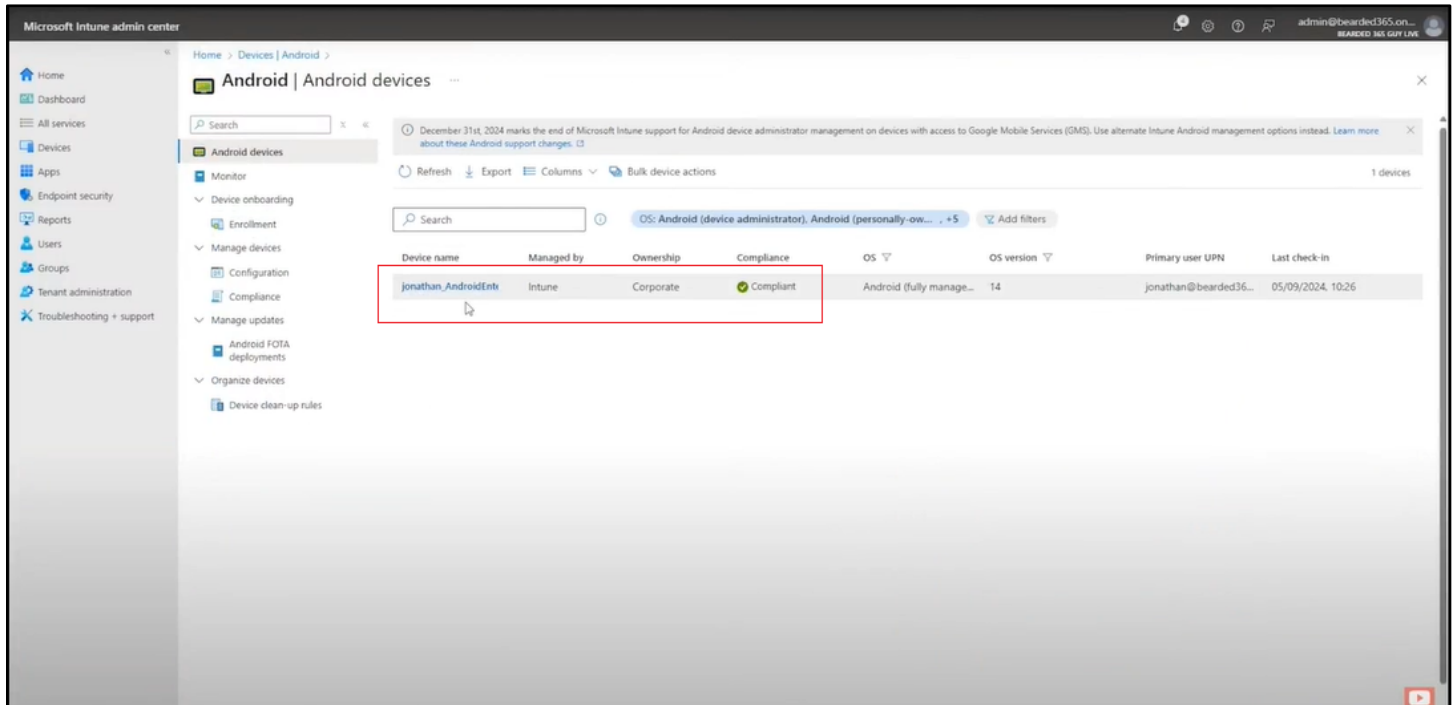
Home > Devices > Android > Android devices > Staging\_37bd7cc1f48f7a48\_AndroidEnterprise\_9/5/2024\_8:22 AM

Managed Apps

Application	Version	Resolved intent	Installation status
Microsoft 365 (Office)	16.0.17928.20046 (44188619)	Required install	Installed
Microsoft Teams	1416/1.0.0.2024162202 (2024162225)	Required install	Installed
Microsoft Intune	2024.08.01 (240801260)	Required install	Installed
Microsoft Authenticator	6.2407.5.108 (202451083)	Required install	Installed
Intune Company Portal	5.0.6327.0 (5685284)	Required install	Installed
Microsoft Outlook	4.2432.0 (42432808)	Required install	Installed
Microsoft Edge: AI browser	128.0.2739.64 (273906405)	Required install	Installed



- **Step 12:** The device can now be shipped to the user for first Log in to Intune.
- **Step 13:** Once the user logs in to Intune for the first time, the device will display the assigned user

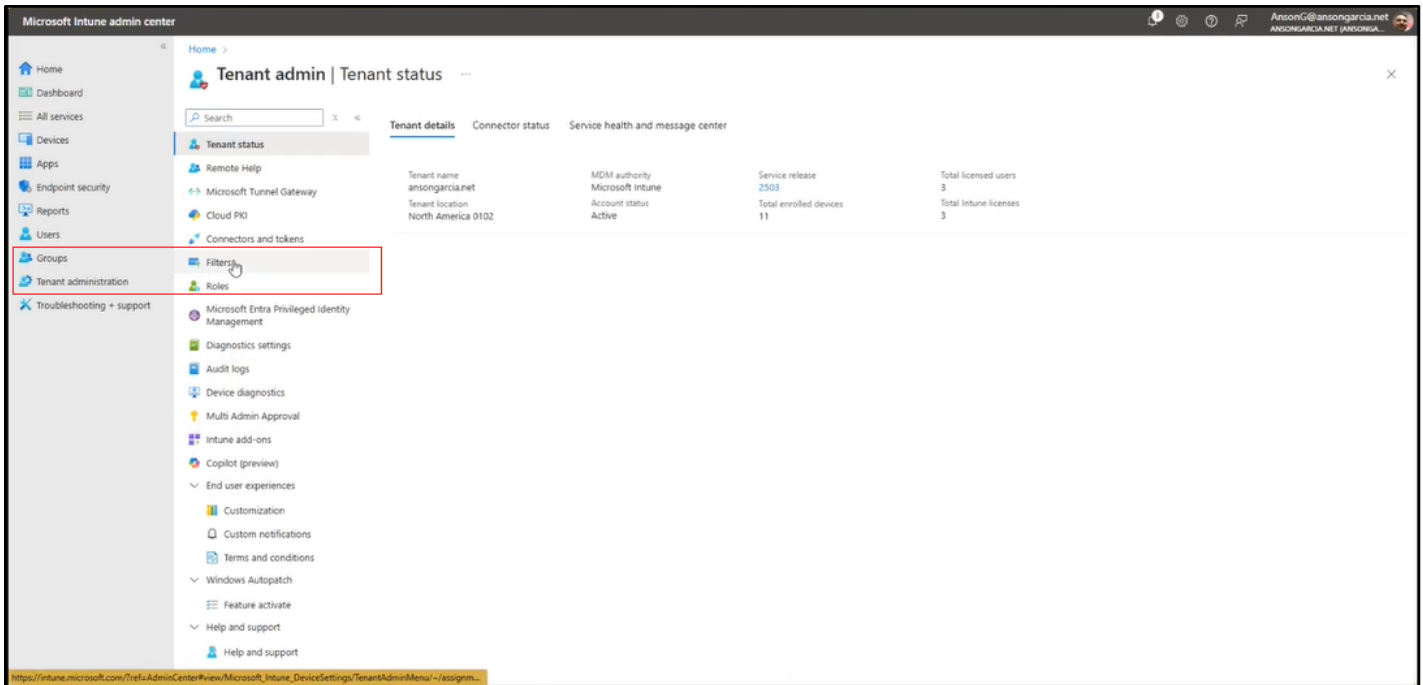


The screenshot shows the Microsoft Intune admin center interface. The left sidebar contains navigation links for Home, Dashboard, All services, Devices, Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main content area is titled 'Android | Android devices' and includes a search bar, a refresh button, an export button, and a columns dropdown. A table lists the devices, with one device, 'Jonathan\_AndroidEnt', highlighted by a red box. The table columns are Device name, Managed by, Ownership, Compliance, OS, OS version, Primary user UPN, and Last check-in.

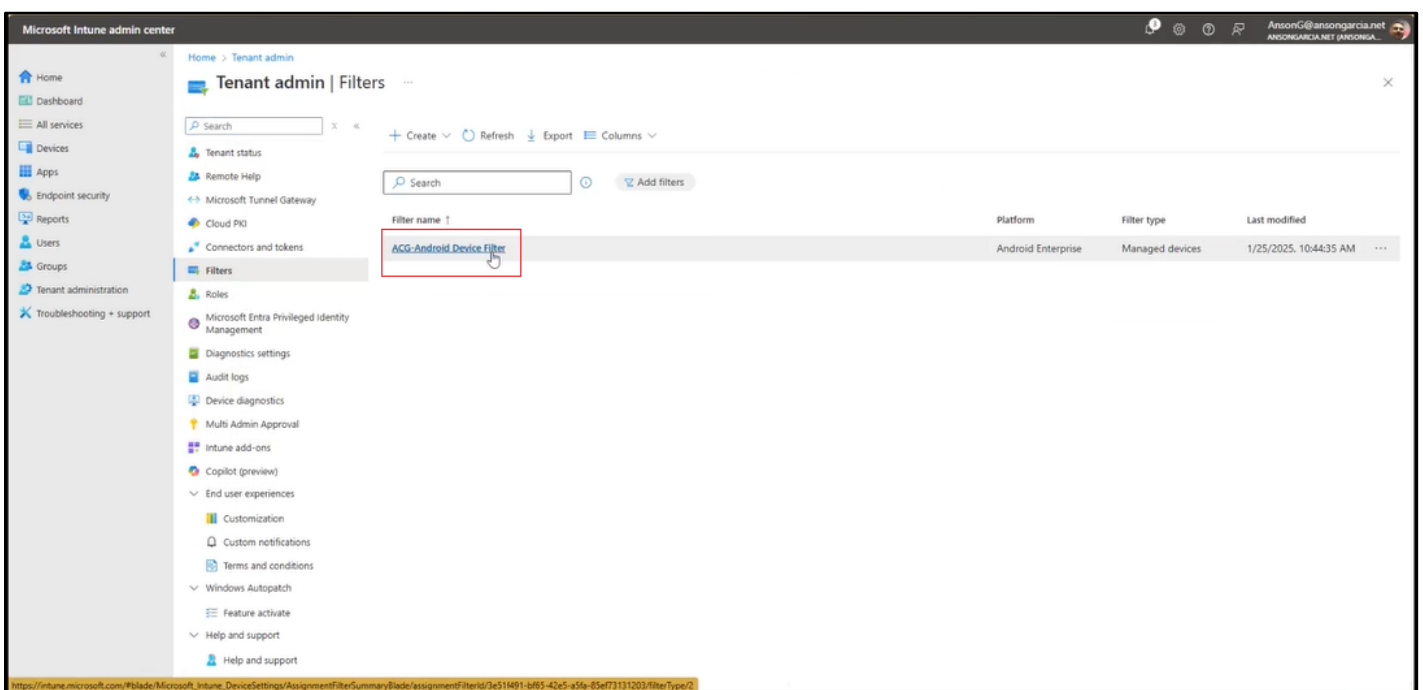
Device name	Managed by	Ownership	Compliance	OS	OS version	Primary user UPN	Last check-in
Jonathan_AndroidEnt	Intune	Corporate	Compliant	Android (fully manage...	14	jonathan@bearded36...	05/09/2024, 10:26

## Filters for Android Devices

- **Step 1:** Filters are a useful way to administrate users and devices. They allow you to establish rules which under a staging profile will be managed.



- **Step 2:** You can create new and edit existing filters to review and modify the rules that will determine the behaviour of the tenants attached to those filters.





Microsoft Intune admin center

Home > Tenant admin > Filters > ACG-Android Device Filter

Properties Associated assignments

Summary

Basics **Rules** Edit

Filter name ACG-Android Device Filter

Description No Description

Platform Android Enterprise

Rules Edit

Rule syntax

```
(device.enrollmentProfileName -eq 'ACG-Android Staging Profile')
```

Microsoft Intune admin center

Home > Tenant admin > Filters > ACG-Android Device Filter > Edit ACG-Android Device Filter

Rules Review + save

You can use the rule builder or rule syntax text box to create or edit the filter rule. [Learn more about creating filters](#)

And/Or Property Operator Value

enrollmentProf... Equals -Training-Staging-Profi... The value is in between 1 and 3072 characters long.

+ Add expression

Rule syntax Edit

```
(device.enrollmentProfileName -eq 'ACG-Android Staging Profile')
```

Filter preview

You can see the devices that match the filter rules.

Preview

Review + save Cancel



Microsoft Intune admin center

Home

Dashboard

All services

Devices

Apps

Endpoint security

Reports

Users

Groups

Tenant administration

Troubleshooting + support

Home > Tenant admin > Filters >

ACG-Android Device Filter

Properties

Associated assignments

Summary

Basics [Edit](#)

Filter name

ACG-Android Device Filter

Description

No Description

Platform

Android Enterprise

Rules [Edit](#)

Rule syntax

{device.enrollmentProfileName -eq "Verizon-Training-Staging-Profile"}

ACG-Android Device Filter filter updated

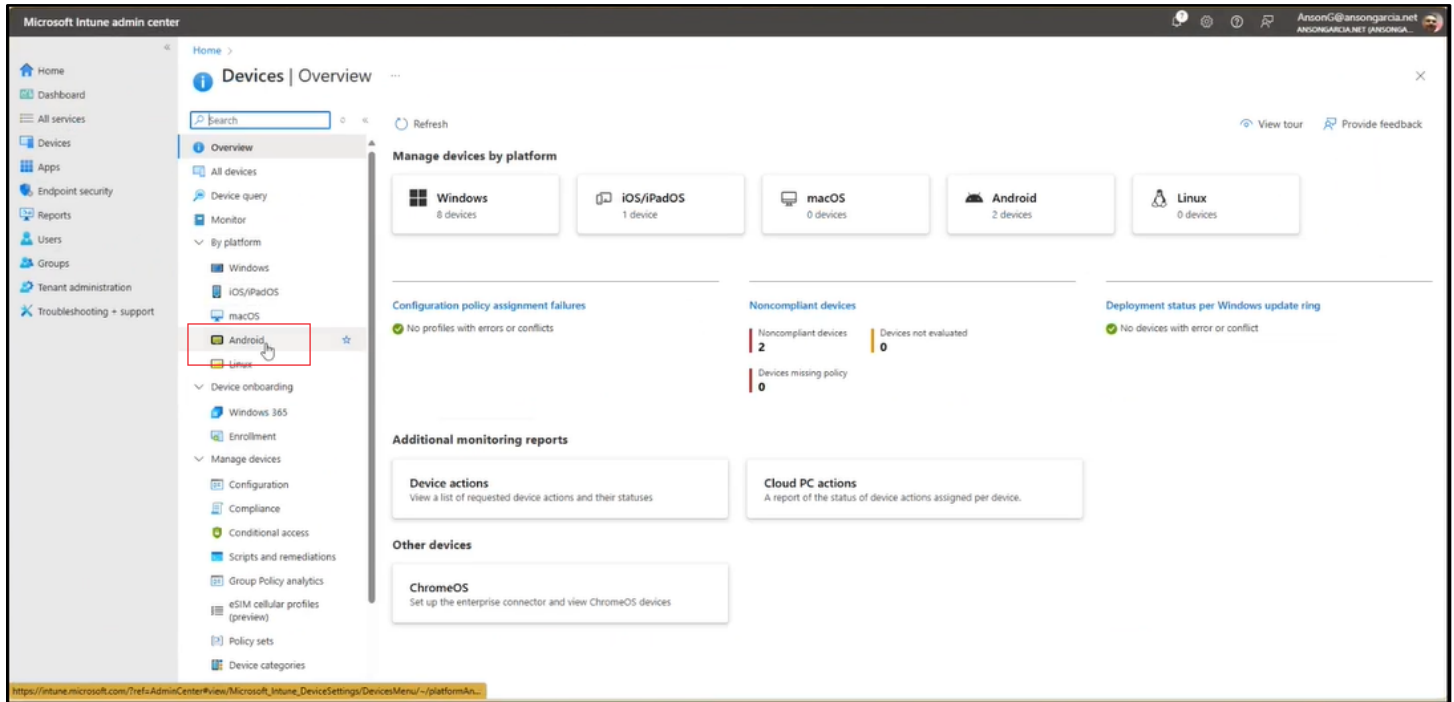
ACG-Android Device Filter filter has been updated

https://intune.microsoft.com/TrefaAdminCenter#

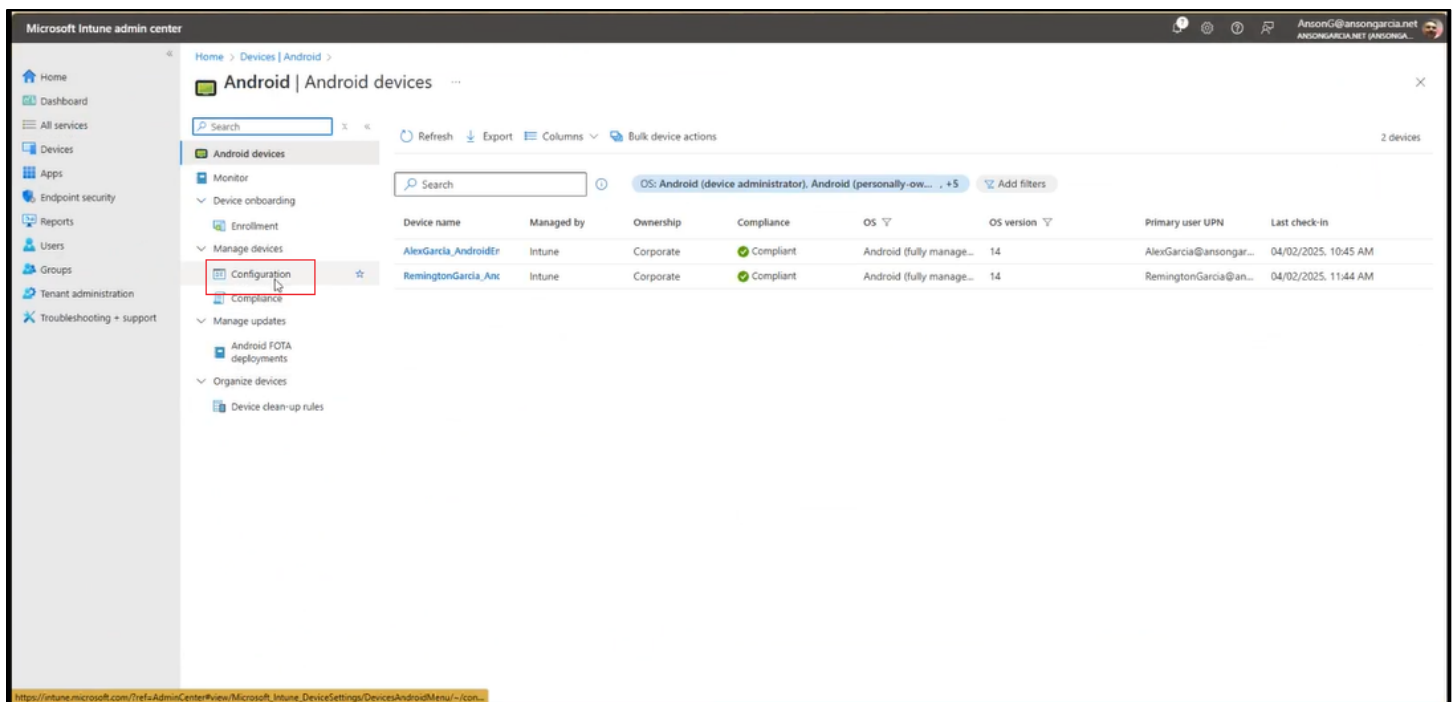


## Install the certificate

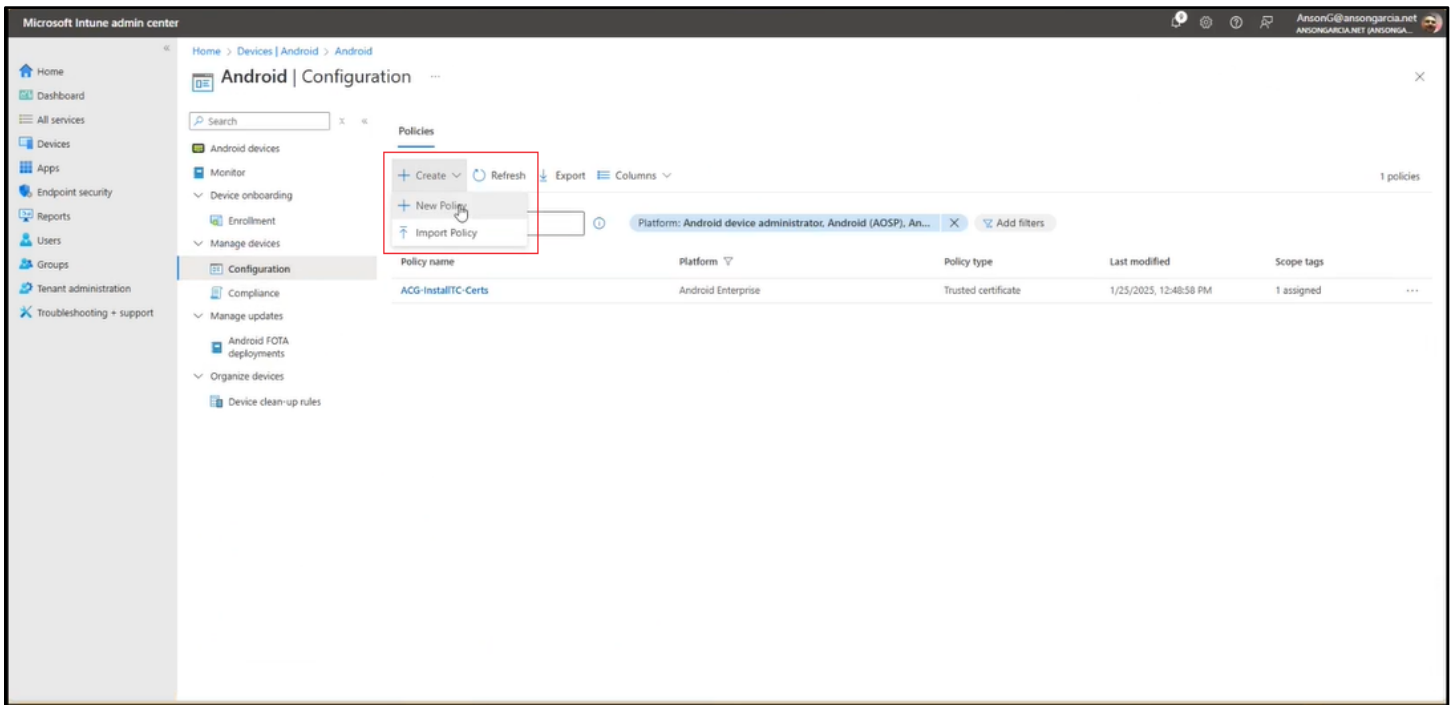
- **Step 1:** To install the certificate, go to Devices → Android



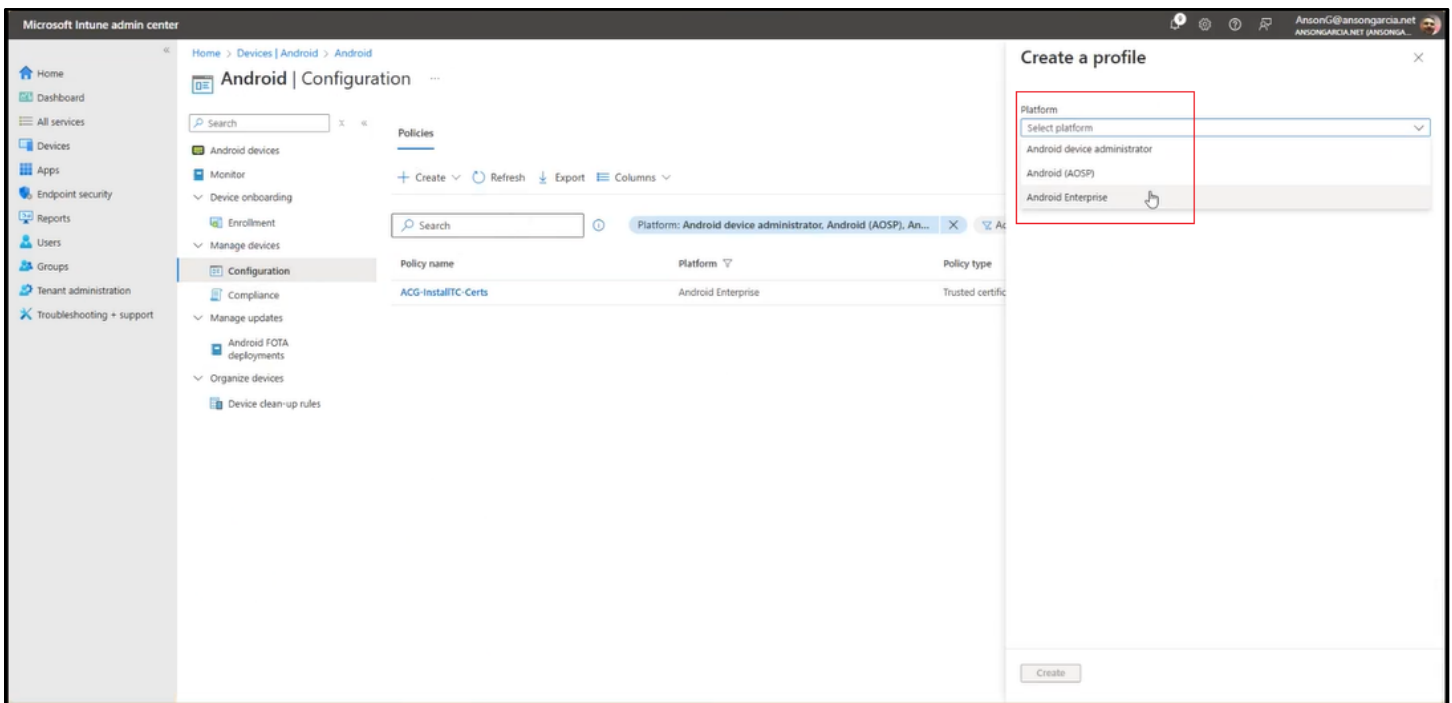
- **Step 2:** A list of enrolled devices will show. Go to Configuration under Manage devices



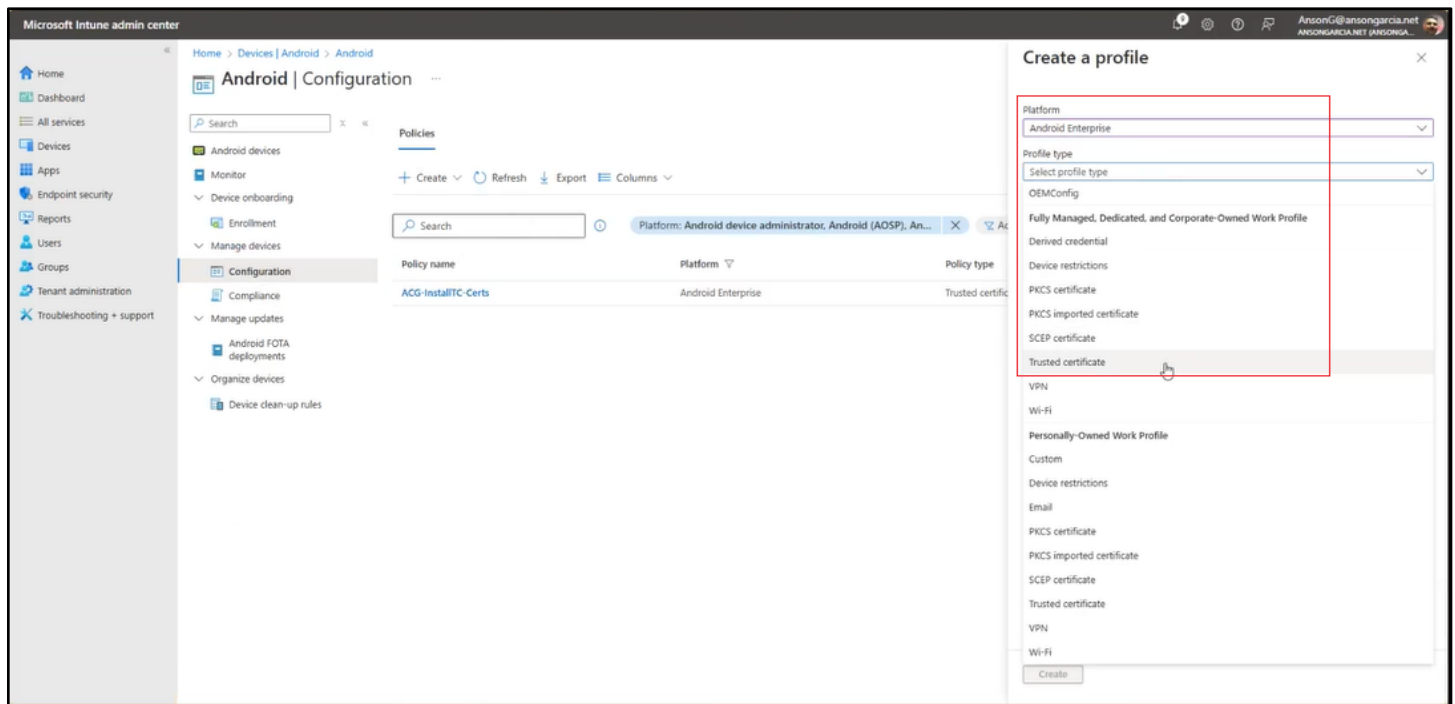
- **Step 3:** In Configuration, click on + Create to display the drop down options and select + New Policy



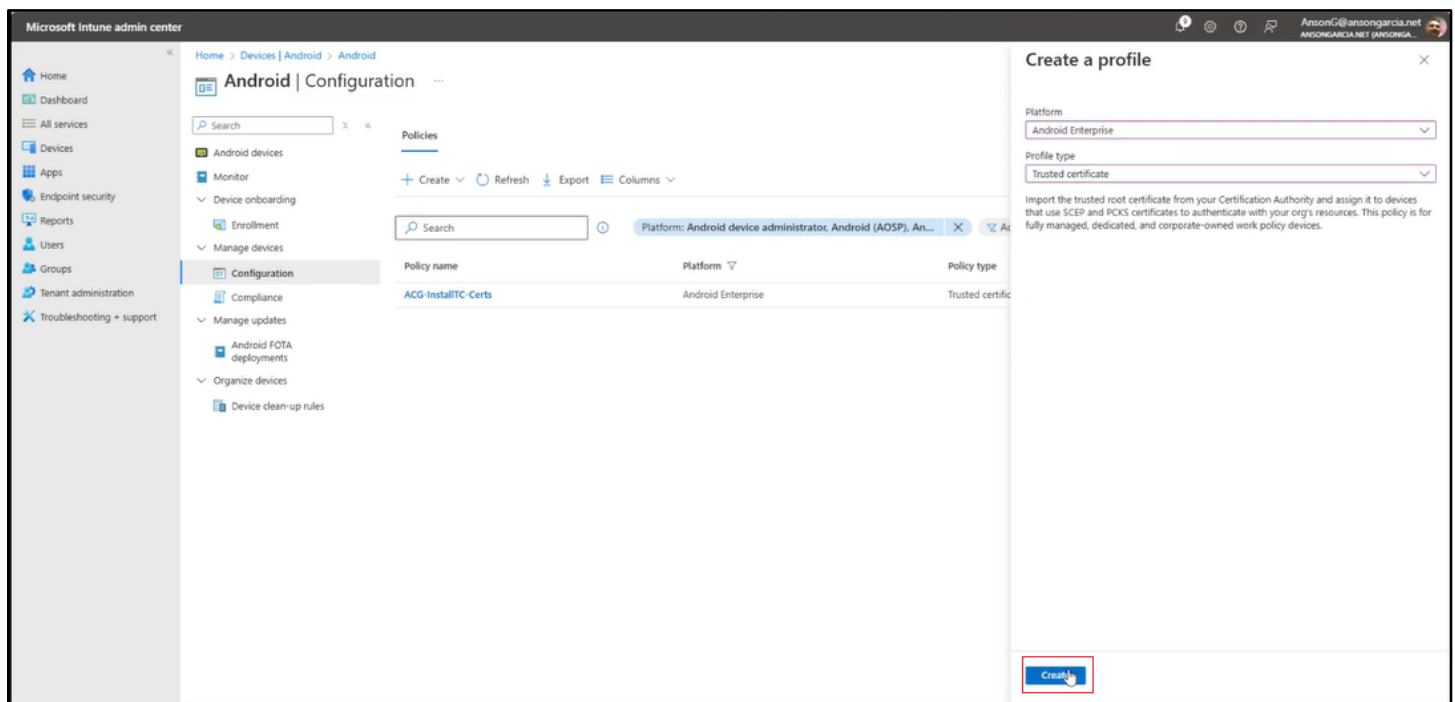
- **Step 4:** To create a New Policy, select the Android Enterprise platform option under Create a profile



- **Step 5:** Once Android Enterprise is selected, a new drop down list of options will be displayed to select the Profile type, then select Trusted certificate



- **Step 6:** Click Create





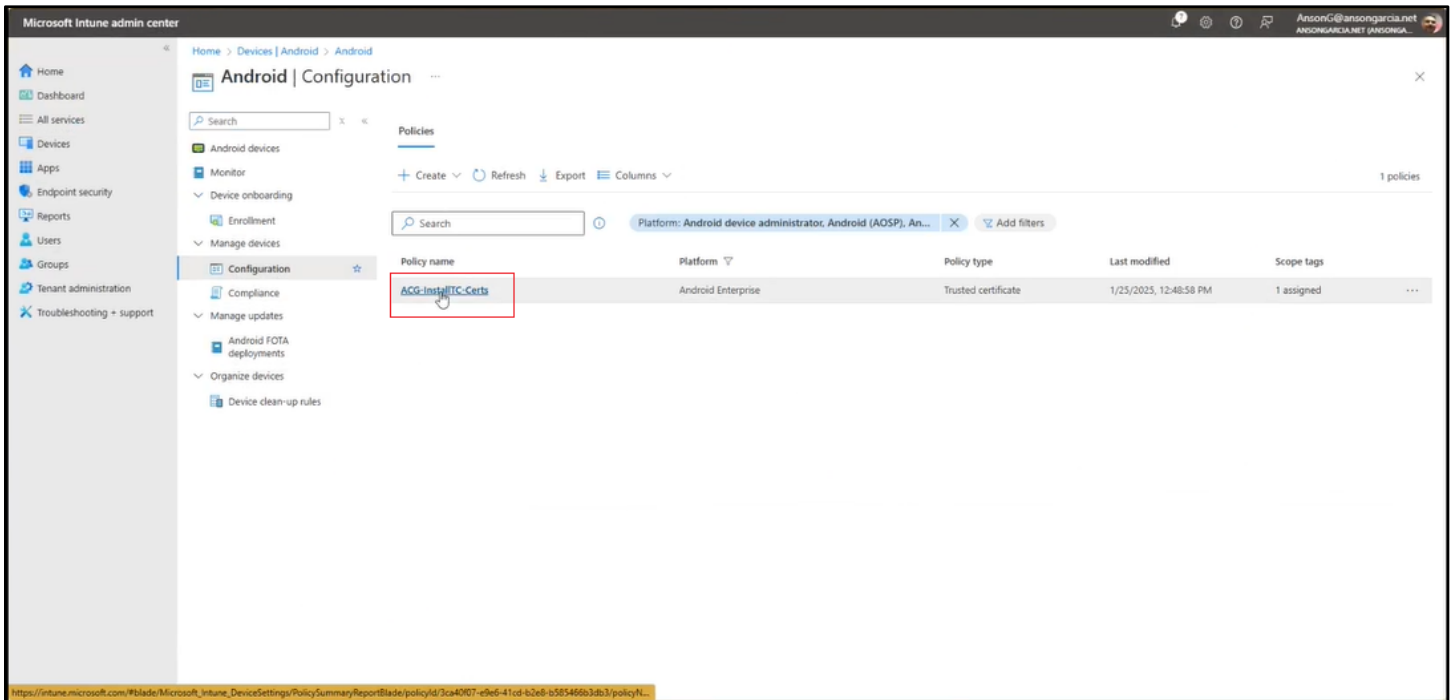
- **Step 7:** This will display the new Trusted certificate where the Name and Description can be added. Click Next

The screenshot shows the 'Trusted certificate' configuration page in the Microsoft Intune admin center. The page is titled 'Trusted certificate' and is part of the 'Android Enterprise' configuration. The 'Basics' tab is selected, showing fields for 'Name' (dASDa), 'Description' (ASDAS), 'Platform' (Android Enterprise), and 'Profile type' (Trusted certificate). The 'Next' button is highlighted with a red box.

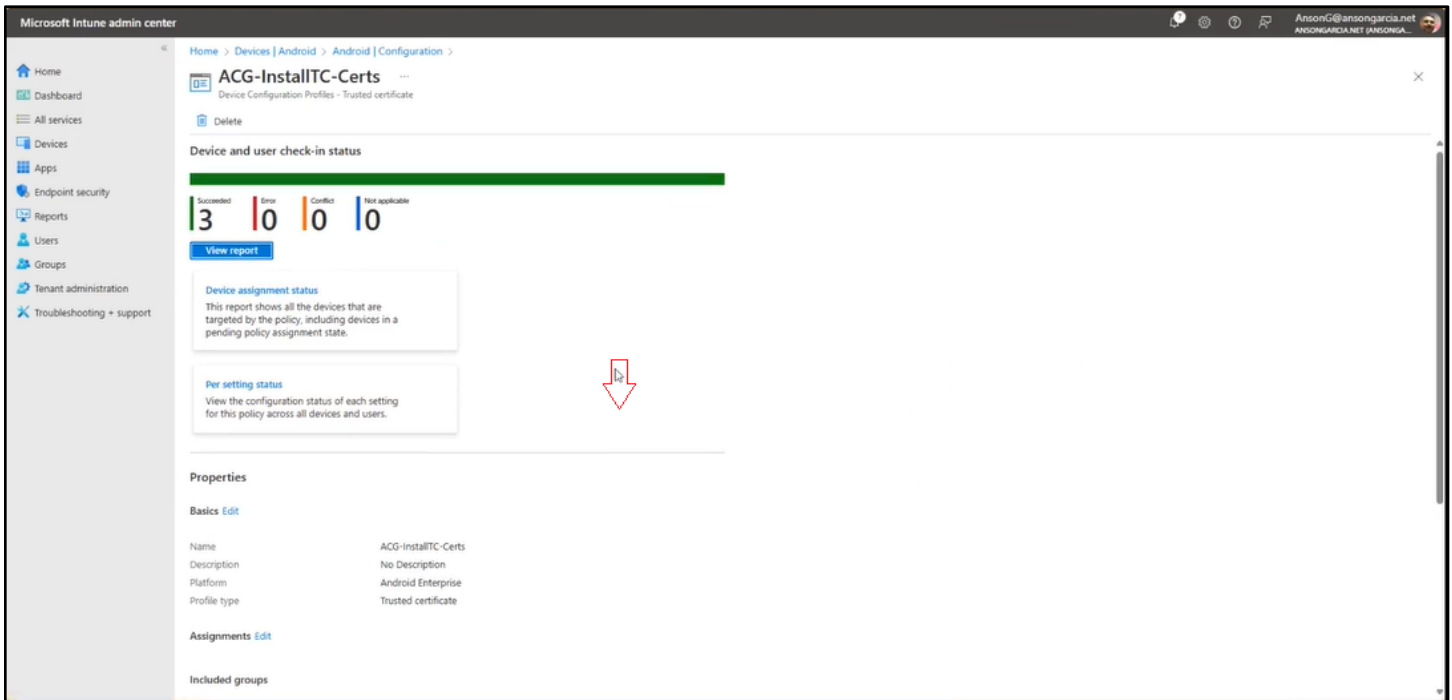
- **Step 8:** This is the stage where the Certificate file can be uploaded, Assigned and Created

The screenshot shows the 'Trusted certificate' configuration page in the Microsoft Intune admin center, now at the 'Configuration settings' tab. The 'Certificate file' field is highlighted with a red box, indicating where to upload the certificate file. The 'Next' button is also highlighted with a red box.

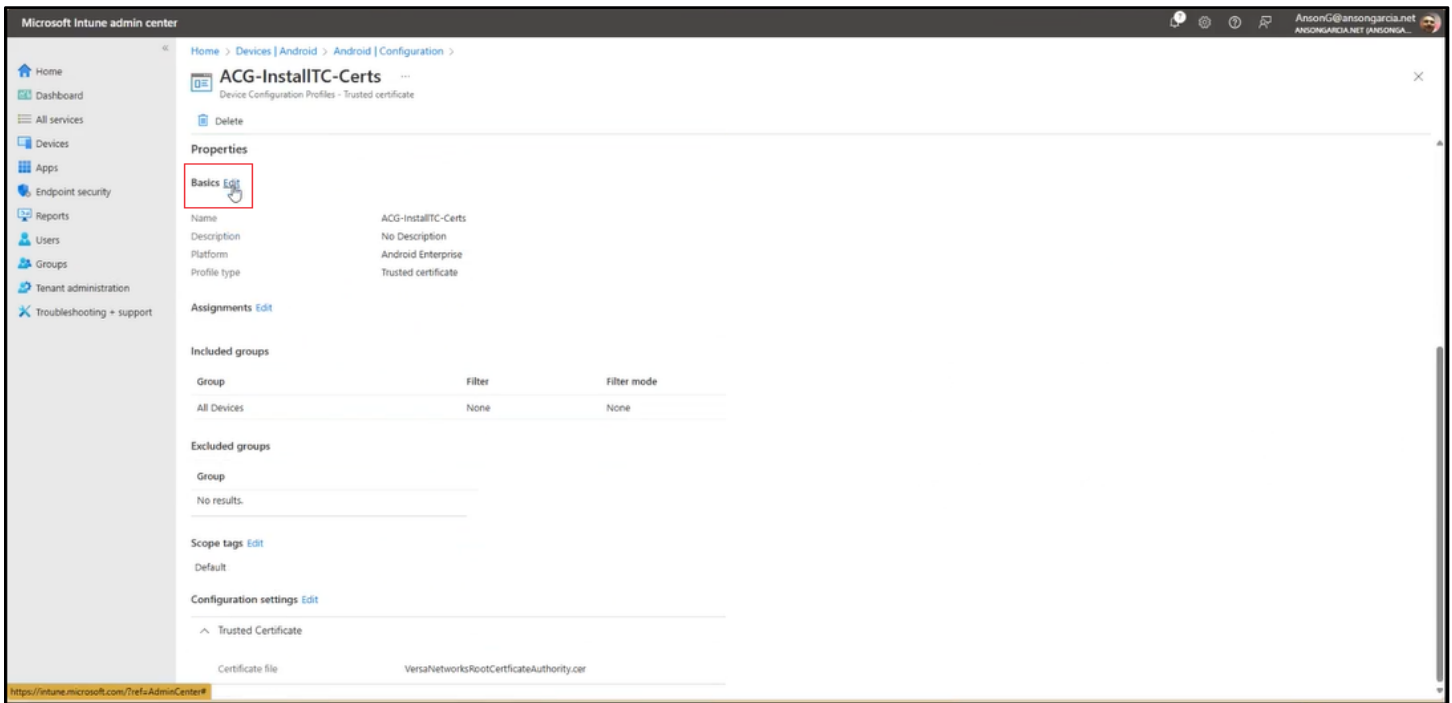
- **Step 9:** Once the Certificate is fully created and assigned, you can click on it to review the configuration



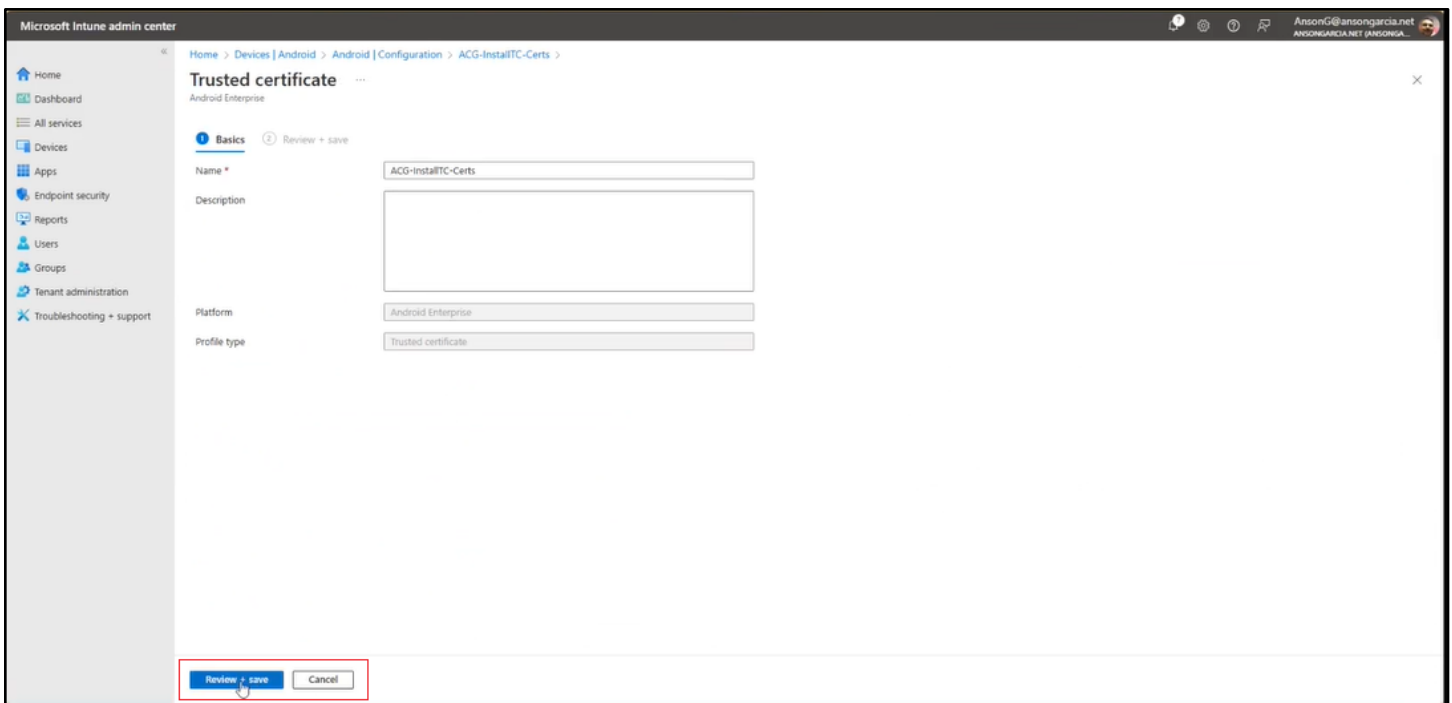
- **Step 10:** It will display the current status and by scrolling down, you'll be able to find all the configuration settings that can be edited.



- **Step 11: Edit Basics**



- **Step 12: Review the certificate Basics are correct & Save**

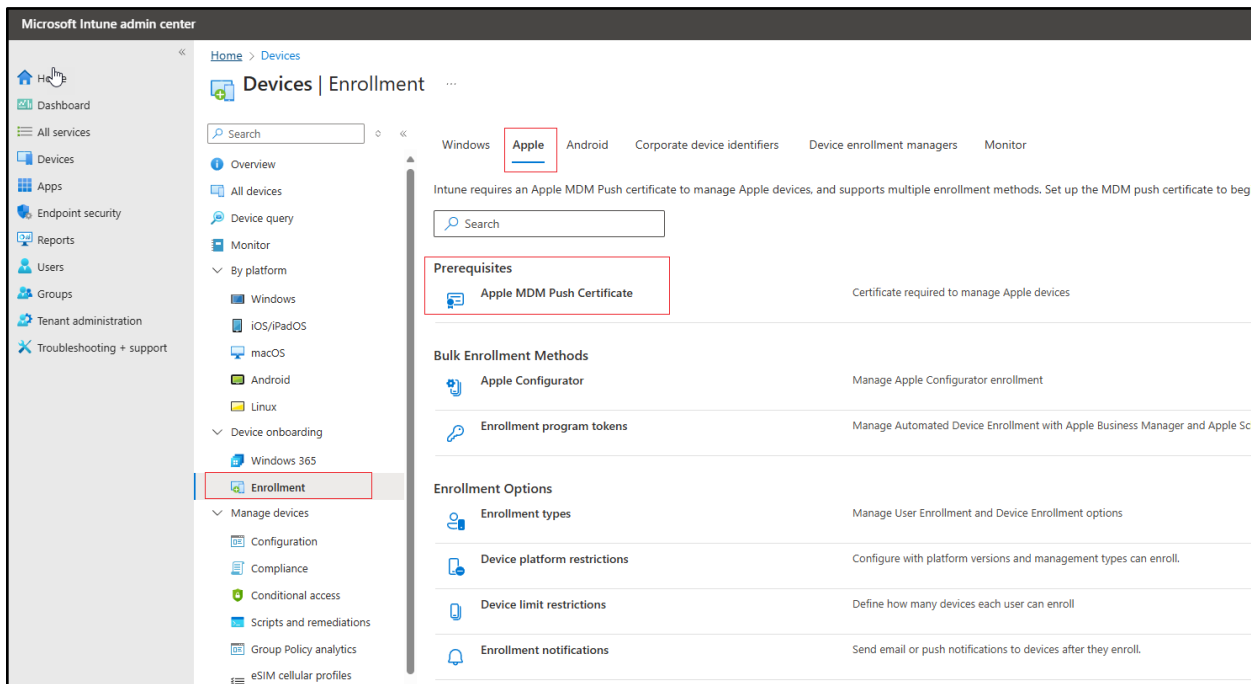


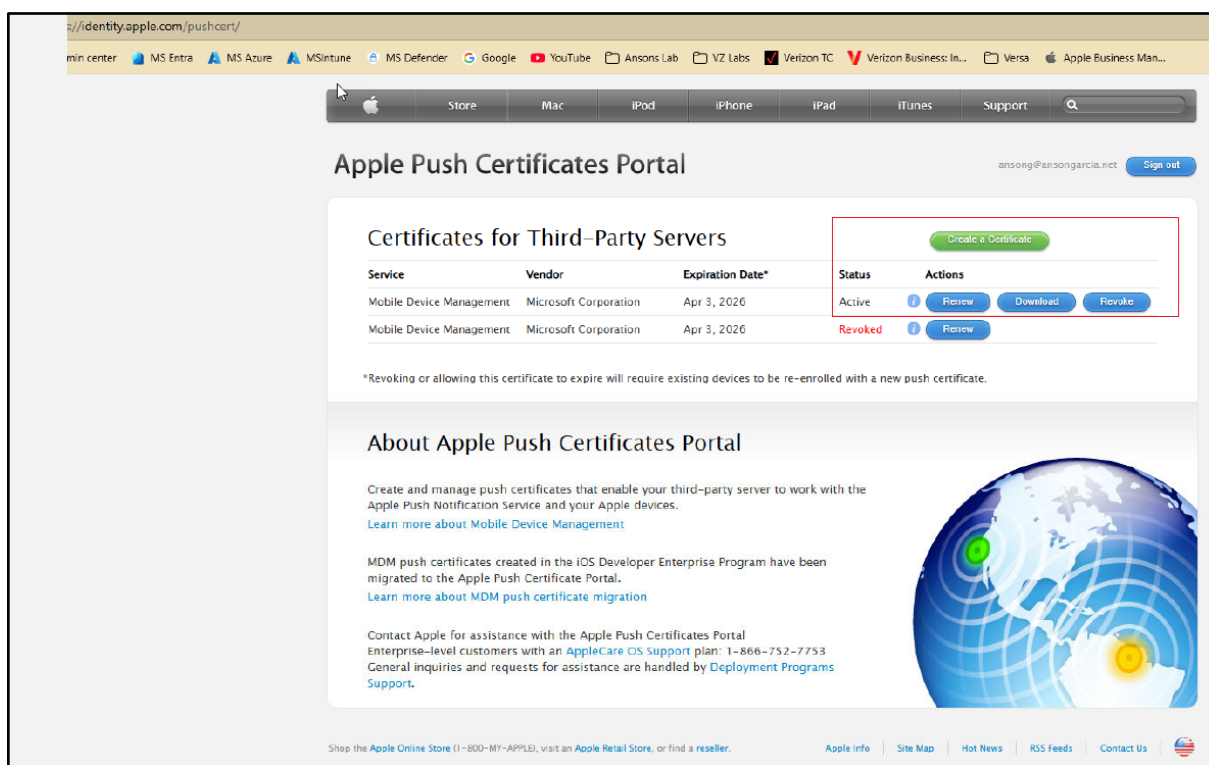


## Install Trusted Connection iOS app to Intune portal (from Apple Business Manager)

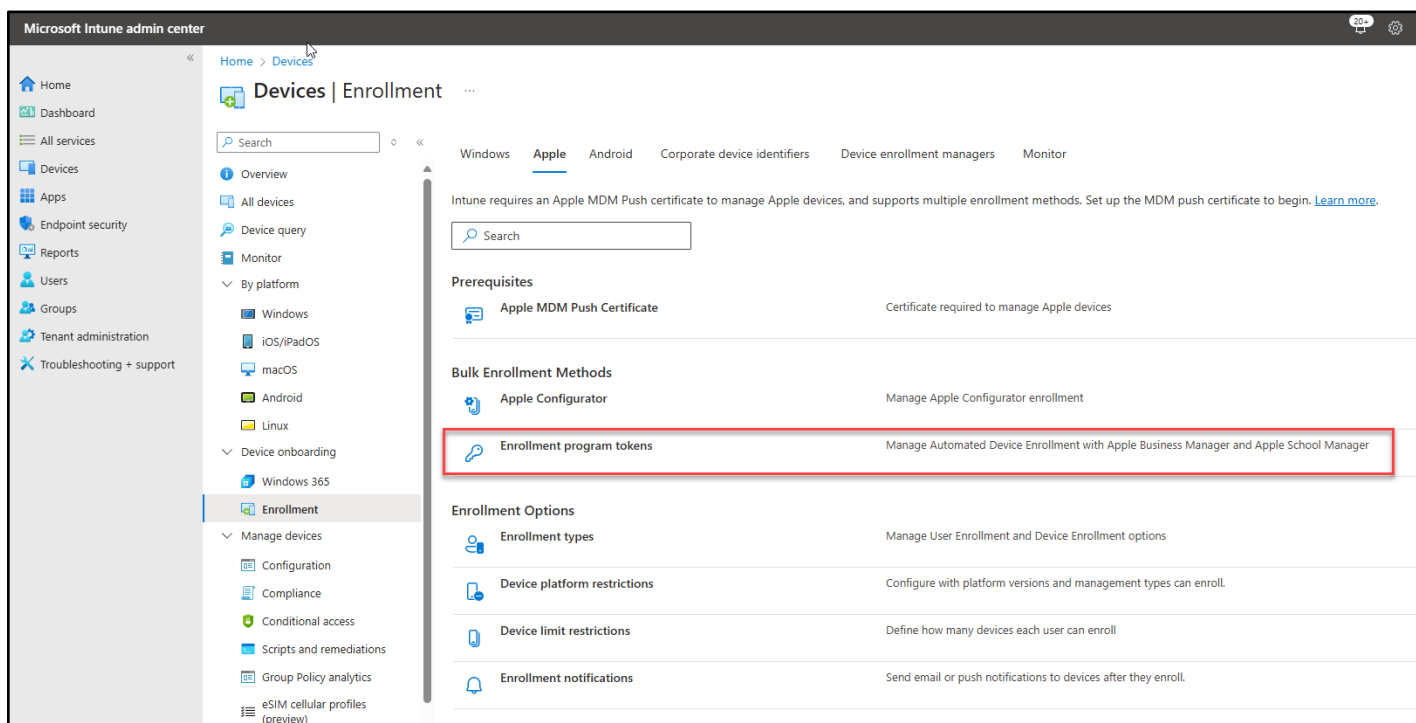
This process starts on Intune, but requires access to the Apple Business Manager for certificate creation & download.

- **Step 1:** Go to Devices → Enrollment → create Apple MDM Push Certificate

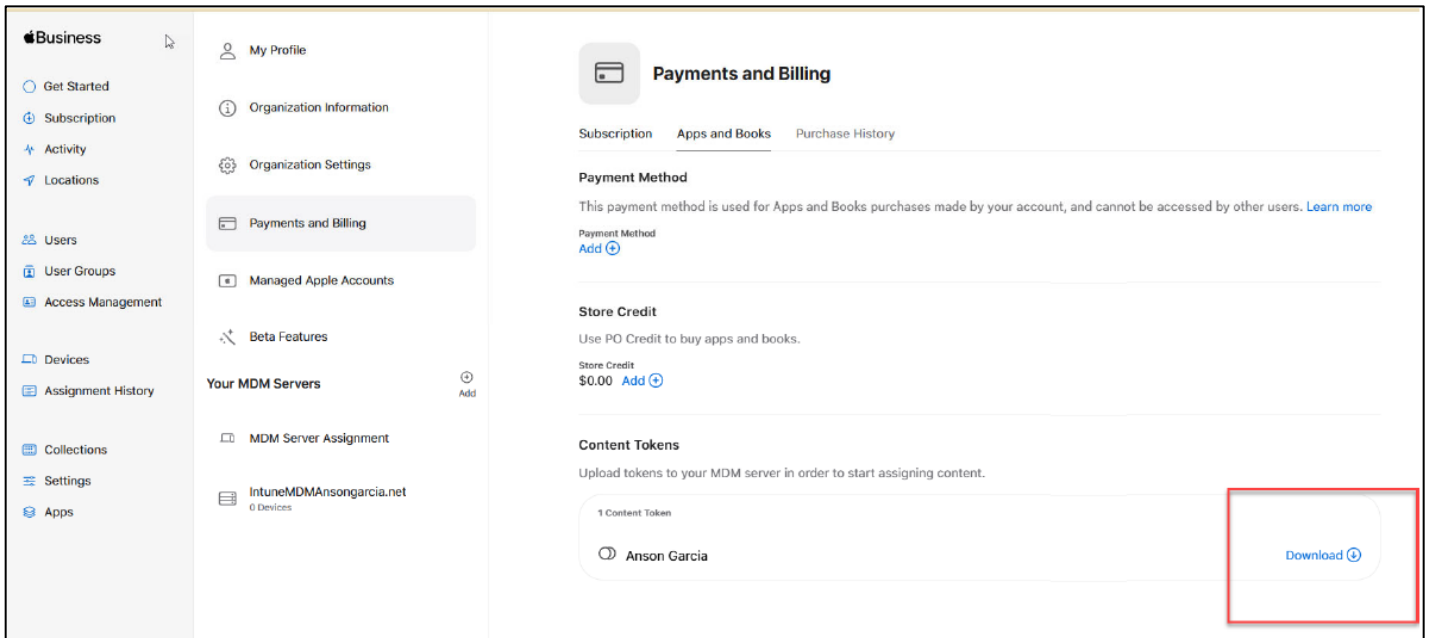




## • Step 2: Connect MS Intune to Apple Business Manager

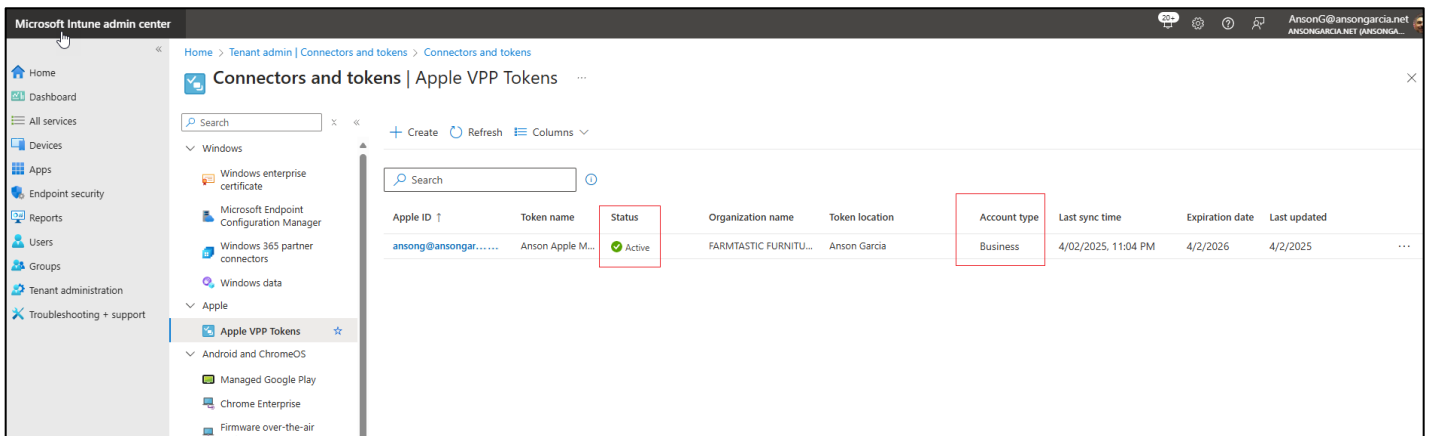


- **2a: Download public key**



- **2b: Create token via Apple Business Manager**
  - This will pop out to ABM
  - Go to Name and then Preference
  - Add MDM Server
  - Download MDM Server Token

This will sync with Intune as shown below





Microsoft Intune admin center

Home > Tenant admin | Connectors and tokens > Connectors and tokens | Apple VPP Tokens >

## Anson Apple MDM | Properties

Search

Manage

Properties

Essentials

State: valid

Expiration date: 4/2/2026

Last successful sync: 4/2/2025

Basics [Edit](#)

Token Name: Anson Apple MDM

Apple ID: ansong@ansongarcia.net

Token Location: Anson Garcia

Settings [Edit](#)

Take control of token from another MDM: No

Country/Region: United States

Type of VPP account: Business

Automatic app updates: Yes

Scope tags [Edit](#)

Default

- **Step 3: Add Application to ABM**

Apple Business

Subscription

Activity

Locations

Users

User Groups

Access Management

Devices

Assignment History

Apps and Books

Search content by Name, Keyword, ISBN, or URL

Sort By

8 Total

**Pandora: Music & Podcasts**  
Pandora Media, LLC · iOS and tvOS  
★★★★★ \$0.00

**YouTube**  
Google · iOS and tvOS  
★★★★★ \$0.00

**Intune Company Portal**  
Microsoft Corporation · iOS App  
★★★★★ \$0.00

**Microsoft Outlook**  
Microsoft Corporation · iOS App  
★★★★★ \$0.00

**Microsoft Authenticator**  
Microsoft Corporation · iOS and visionOS  
★★★★★ \$0.00

**Microsoft Teams**  
Microsoft Corporation · iOS and visionOS  
★★★★★ \$0.00

**Apple Business Essentials**  
Apple · iOS and macOS  
★★★★★ \$0.00

**Trusted Connection**  
Verizon Wireless · iOS App  
★★★★★ \$0.00

8 Apps · 0 Books

FARMTASTIC FURNITURE



• **3a:** Create a VPP Connector

Microsoft Intune admin center

Home > Tenant admin | Connectors and tokens > Connectors and tokens

### Connectors and tokens | Apple VPP Tokens

Search

+ Create Refresh Columns

Windows

- Windows enterprise certificate
- Microsoft Endpoint Configuration Manager
- Windows 365 partner connectors
- Windows data

Apple

- Apple VPP Tokens**

Android and ChromeOS

- Managed Google Play
- Chrome Enterprise
- Firmware over-the-air update

Cross platform

- Microsoft Defender for endpoint

Apple ID	Token name	Status	Organization name	Token location	Account type	Last sync time	Expiration date	Last updated	
ansong@ansongarcia.net	Anson Apple M...	Active	FARMTASTIC FURNITU...	Anson Garcia	Business	4/02/2025, 11:04 PM	4/2/2025	4/3/2025	...

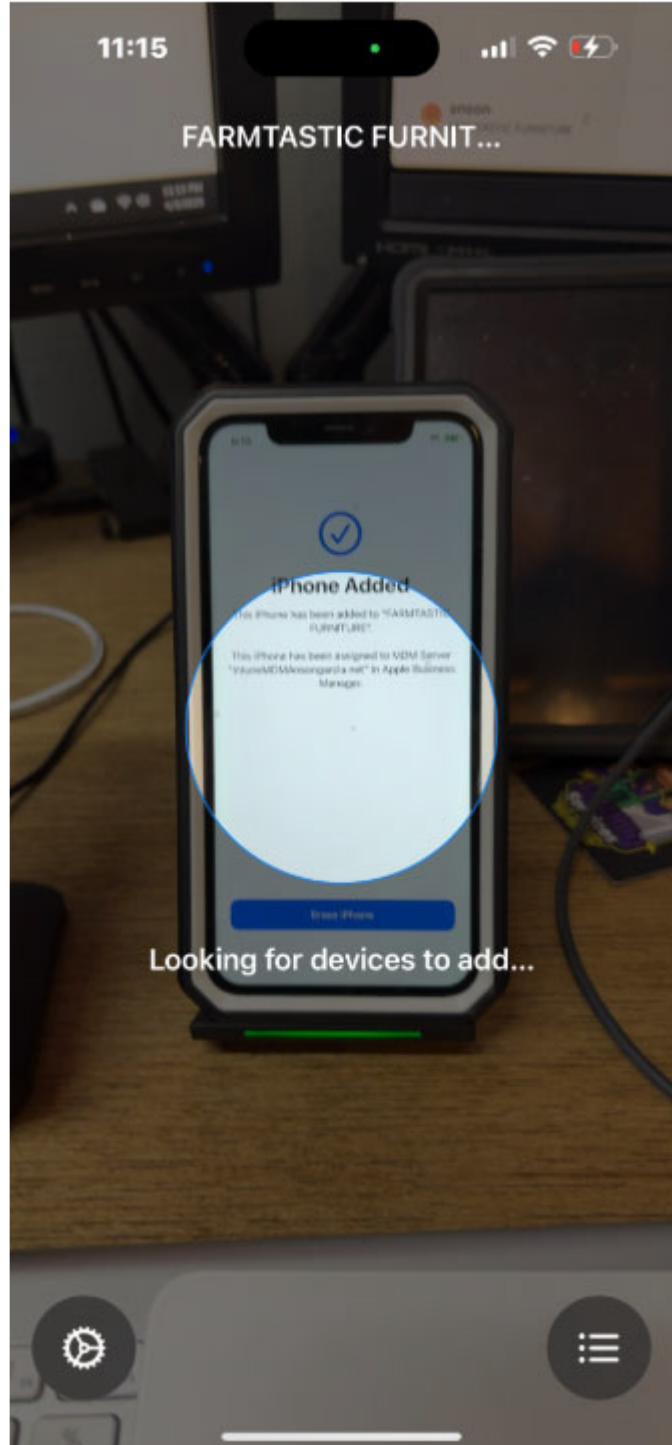
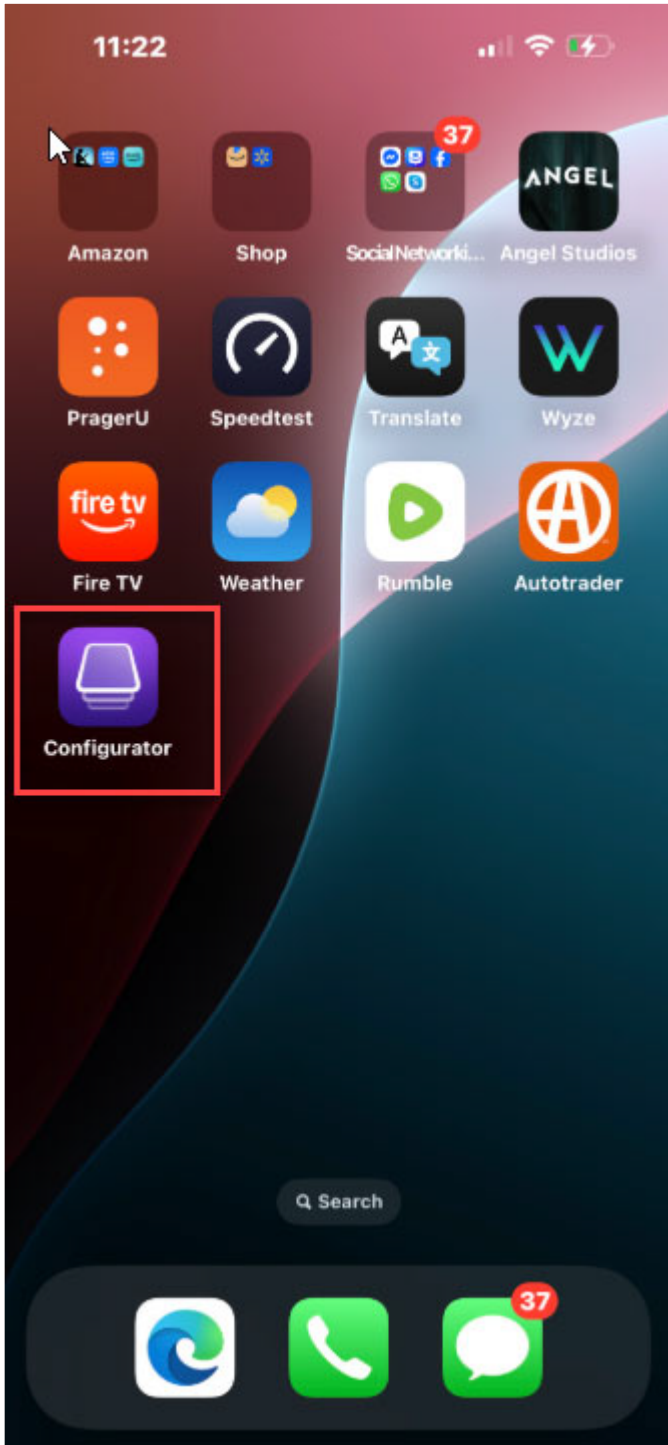
Sync

Revoke licenses

Delete

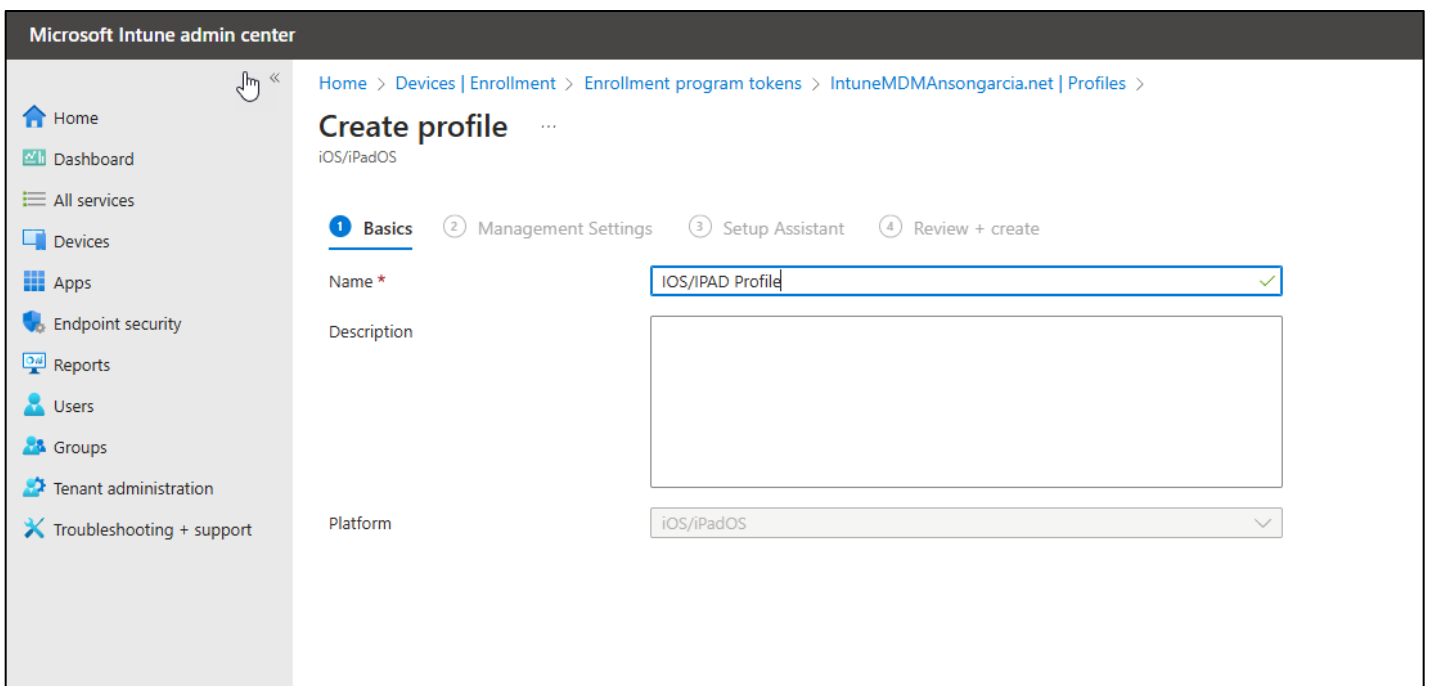
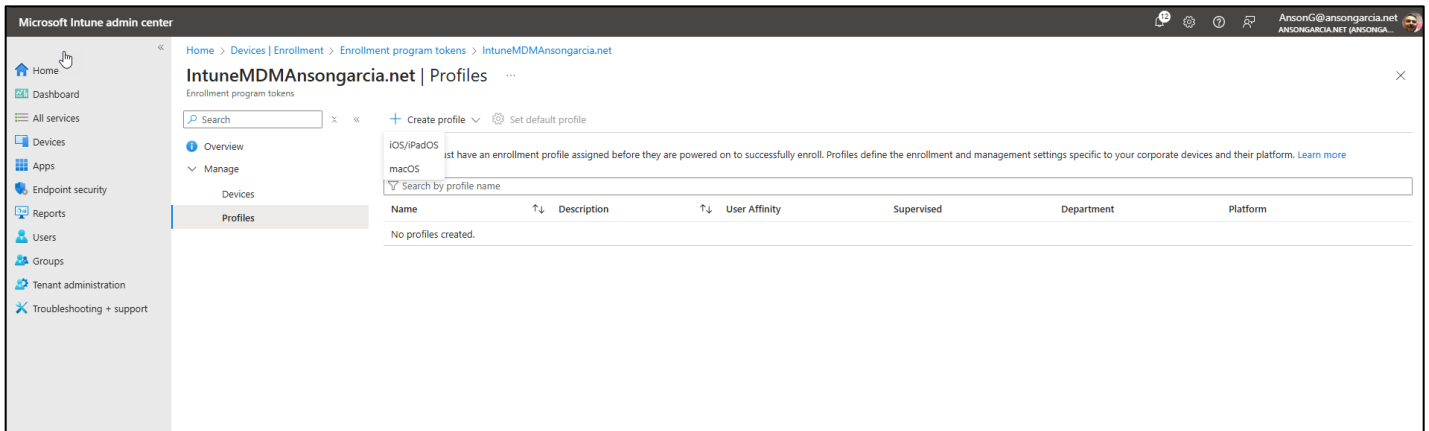
Assign scope tags

- **Step 4:** Install Apple Configurator on a Stand-Alone Phone
  - **4a:** Login to Apple Configurator with ABM Credentials
  - **4b:** Go to settings on Apple Configurator and choose MDM





- **Step 5: Create an Enrollment Profile**



Microsoft Intune admin center

Home > Devices | Enrollment > Enrollment program tokens > IntuneMDMAnsongarcia.net | Profiles >

## Create profile

iOS/iPadOS

✓ Basics

2 Management Settings

3 Setup Assistant

4 Review + create

Define enrollment and management settings for your iOS/iPadOS devices. [Learn more](#)

**User Affinity & Authentication Method**

User affinity \* ⓘ

Enroll with User Affinity

Authentication Method ⓘ

Company Portal

Install Company Portal with VPP ⓘ

Use Token: ansong@ansongarcia.net

Run Company Portal in Single App Mode until authentication ⓘ

Yes No

**Management Options**

Supervised ⓘ

Yes

ⓘ Supervision is required for devices using Company Portal as their authorization method.

Locked enrollment \* ⓘ

Yes

Sync with computers: \* ⓘ

Allow All

Apple Configurator certificates: ⓘ

Select certificate file to upload

**Uploaded Certificates**

No certificates, select a certificate file to import.

**Device Name**

Apply device name template (supervised only) ⓘ

Yes No

Previous

Next





Microsoft Intune admin center

Home > Devices > Enrollment > Enrollment program tokens > IntuneMDMAnsongarcia.net

### IntuneMDMAnsongarcia.net | Devices

Enrollment program tokens

Search [ ] Sync Assign profile Delete Refresh Filter Columns Export

Overview  
Manage

Last requested sync: 04/03/23, 11:10 PM  
Last successful sync: 04/03/23, 3:04 PM

Intune syncs enrollment program devices from Apple. After syncing but before powering on the device, you must assign the devices to an enrollment profile to enable enrollment. You cannot learn more

Search by Serial Number

Serial Number	Platform	Details	Removed From ABM/ASM	Profile Assigned
D13D08WN72J	iOS/iPadOS	IPHONE 11 BLACK 64GB VER-USA	No	N/A

Assign Profile

Enrollment Profile  
iOS/iPad Profile

Assign

- Step 6: Assign VPP applications to users  
Select each application

Microsoft Intune admin center

Home > Apps > iOS/iPadOS

### iOS/iPadOS | iOS/iPadOS apps

Search [ ] Create Refresh Export Columns

Monitor  
Manage apps  
Configuration  
Protection  
iOS app provisioning profiles  
App selective wipe  
Organize apps  
Assignment filters  
App categories  
eBooks

Platform: iOS Type: Built-in iOS app, iOS line-of-business app, iOS store app, +5 Add filters

Name	Platform	Type	Version	VPP token name	Assigned	Developer
Intune Company Portal	iOS	iOS volume purchase pr...		Anson Apple VPP Token	No	...
Microsoft Outlook	iOS	iOS volume purchase pr...		Anson Apple VPP Token	No	...
Microsoft Teams	iOS	iOS volume purchase pr...		Anson Apple VPP Token	No	...
Trusted Connection	iOS	iOS volume purchase pr...		Anson Apple VPP Token	No	...
YouTube	iOS	iOS volume purchase pr...		Anson Apple VPP Token	No	...



Deploy applications to all users or specific groups as needed.

Microsoft Intune admin center

Home

Dashboard

All services

Devices

Apps

Endpoint security

Reports

Users

Groups

Tenant administration

Troubleshooting + support

Home > Apps > iOS/iPadOS > iOS/iPadOS apps > Intune Company Portal

Intune Company Portal | Properties

Overview

Manage

Properties

Monitor

Search

Overview

Manage

Properties

Monitor

Publisher

Appstore URL

Applicable device type

Category

Show this as a featured app in the Company Portal

Information URL

Privacy URL

Developer

Owner

Notes

Logo

Company Portal helps simplify the tasks you need to do...

Microsoft Corporation

No Appstore URL

iPad

iPhone and iPod

Other apps

No

https://apps.apple.com/us/app/intune-company-portal/id719171358

No Privacy URL

No Developer

No Owner

No Notes

App type

Supports device context assignment

Available licenses

Total licenses

iOS Volume-Purchased Program

true

10

10

Assignments

Edit

Group mode

Group

Filter mode

Filter

VPN

License type

Prevent automatic a...

Uninstall on device ...

Required

Available for enrolled devices

Uninstall

Microsoft Intune admin center

Home

Dashboard

All services

Devices

Apps

Endpoint security

Reports

Users

Groups

Tenant administration

Troubleshooting + support

Home > Apps > iOS/iPadOS > iOS/iPadOS apps > Intune Company Portal | Properties >

Edit application

iOS volume purchase program app

Assignments

Review + save

Required

Available for enrolled devices

Uninstall

Group mode

Group

Filter mode

Filter

VPN

License type

Prevent automatic a...

Uninstall on device ...

Install as removable

+ Add group

+ Add all users

+ Add all devices

Available for enrolled devices

Group mode

Group

Filter mode

Filter

VPN

License type

Prevent automatic a...

Uninstall on device removal

No assignments

+ Add group

+ Add all users

+ Add all devices

Uninstall

Group mode

Group

Filter mode

Filter

License type

No assignments

+ Add group

+ Add all users

+ Add all devices

Review + save

Cancel



To enable Trusted Connection on specific users or devices, ensure the application assignment is properly configured.

The screenshot shows the Microsoft Intune admin center interface. The left sidebar contains navigation options: Home, Dashboard, All services, Devices, Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main content area is titled 'iOS/iPadOS | iOS/iPadOS apps'. It includes a search bar, a '+ Create' button, and a 'Refresh' button. Below these are filters for 'Platform: iOS' and 'Type: Built-in iOS app, iOS line-of-business app, iOS store app, +5'. A table lists several apps, including 'Intune Company Portal', 'Microsoft Outlook', 'Microsoft Teams', 'Trusted Connection', and 'YouTube'. The 'Assigned' column for these apps is highlighted with a red box, showing 'Yes' for all except 'YouTube', which shows 'No'.

Name	Platform	Type	Version	VPP token name	Assigned	Developer
Intune Company Portal	iOS	iOS volume purchase pr...		Anson Apple VPP Token	Yes	
Microsoft Outlook	iOS	iOS volume purchase pr...		Anson Apple VPP Token	Yes	
Microsoft Teams	iOS	iOS volume purchase pr...		Anson Apple VPP Token	Yes	
Trusted Connection	iOS	iOS volume purchase pr...		Anson Apple VPP Token	Yes	
YouTube	iOS	iOS volume purchase pr...		Anson Apple VPP Token	No	

## Further references: Microsoft Intune Documentation

The following link leads to the official product documentation for Microsoft Intune including:

6. Getting started with Microsoft Intune
7. How-to guides
8. Troubleshooting
9. Platform and industry guides

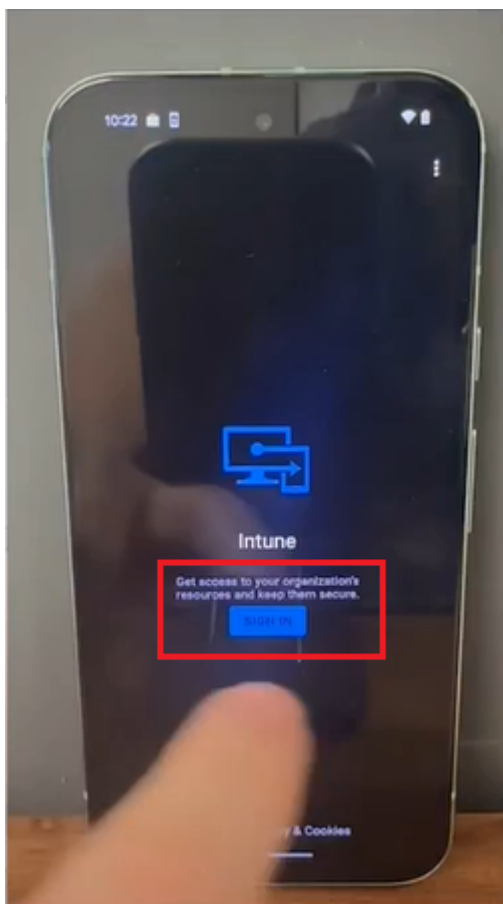
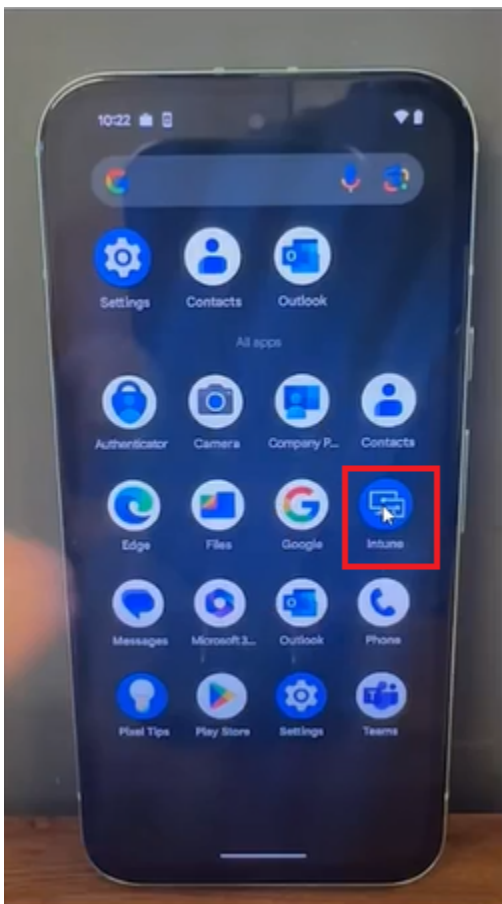
<https://learn.microsoft.com/en-us/intune/intune-service/>

## Stepwise Instructions for Customer End-Users

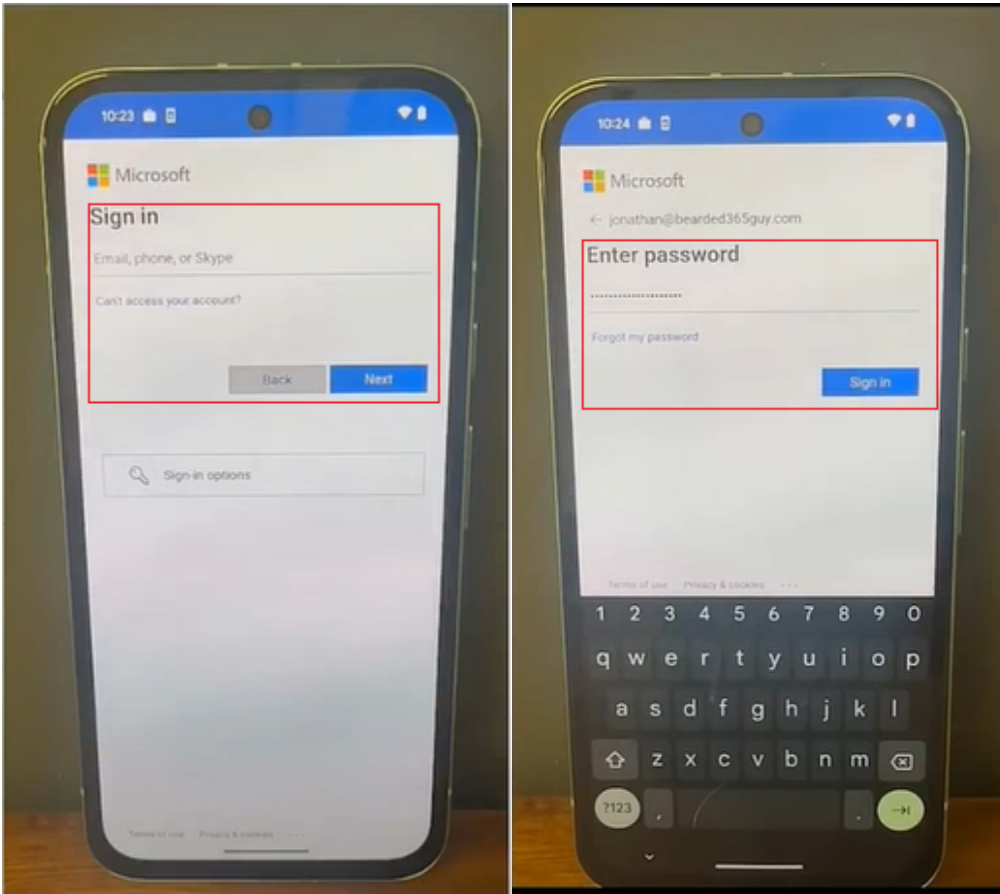
### Android Instructions

The following is only applicable if a staging Profile for Android devices has previously been created and installed on the device. These steps are for end-users to complete the final sign-in to Intune and user-specific settings.

- **Step 1:** End User Log in to Intune



- **Step 2:** Log in to Microsoft 365 credentials:



**Important note:** If after login to Intune, the device hasn't got Trusted Connection activated an Administrator should provide the QR code(with the appropriate staging profile) to be scanned by the device and follow the installation process as described in [Add an Android into Intune](#) procedure (this includes a device reset, so a full backup is recommended for existing devices).

**Disclaimer:** These guidelines are specific to a fully managed Android device scenario for Microsoft Intune. For different MDM management models, the end user might have to manually "trust" the Trusted Connection certificates to complete the process. Android treats user-installed certificates (those not pre-installed in the system trust store) as untrusted by default for SSL/TLS connections. This is a deliberate security measure to prevent potential man-in-the-middle (MITM) attacks, as user-installed certificates could be malicious or compromised. Since Android 7.0 (Nougat), apps no longer automatically trust user-installed certificates unless explicitly configured to do so via the app's Network Security Configuration. When a certificate is pushed to an Android device (e.g., via email, download, or MDM), the user must manually install it (Settings > Security > Encryption & Credentials > Install a Certificate). Even after installation, apps won't trust it for secure connections unless the app's configuration allows it or the certificate is added to the system trust store (which typically requires root access or MDM-level control).



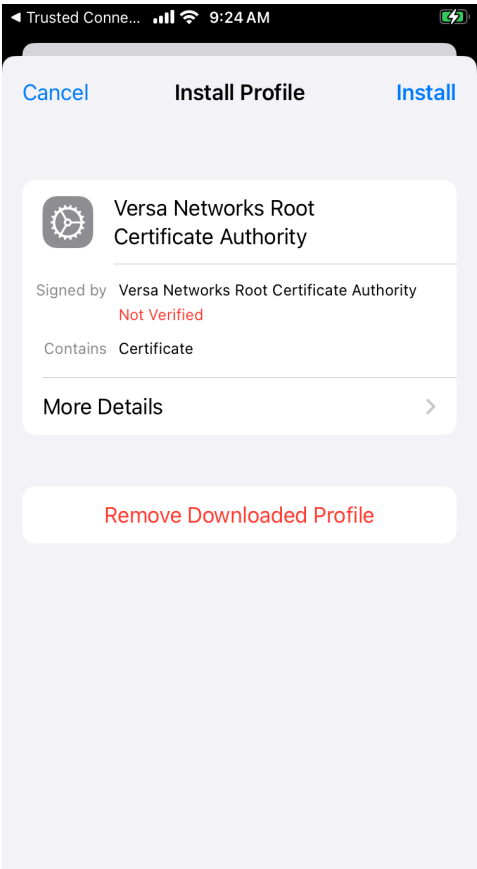
For a fully managed Android device under Microsoft Intune, the customers should be able to automate the certificate installation process by using MDM. If the customer is facing any issue or required to manually trust certificates, the customer needs to work directly with the Microsoft Intune support team for guidance and next steps.



## iOS Instructions

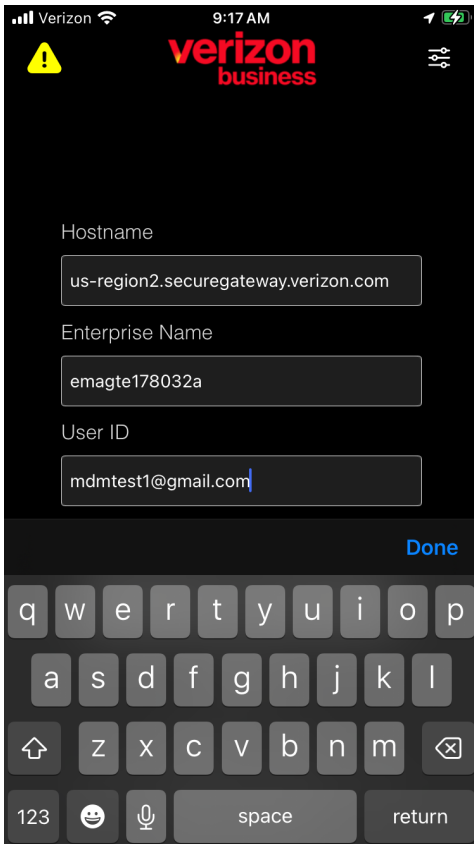
Intune can push out the Trusted Connection Clients to devices, but it doesn't support a managed configuration. This means that end-users will need to complete the configuration of the Client to work with the Trusted Connection service. Here are the instructions for an end-user on iOS device:

- **Step 1:** Open the Trusted Connection Client on your device. You will be presented with a “Privacy Policy” screen. Please select “Agree”.
- **Step 2:** You will then be presented with “Trusted Connection would like to find and connect to devices on your local network”. Please select “Allow”.
- **Step 3:** You will now be presented with the following notice “This website is trying to download a configuration profile. Do you want to allow this?” Please select “Allow”. Once downloaded, you will see a screen saying “Kindly install the certificates to continue.” You will then be automatically taken to settings, where you will see the “Profile Downloaded.”
- **Step 4:** Please click on “Profile Downloaded” and click install the “Versa Network Root Certificate Authority”. Please click on “Install” and once completed “Done”.





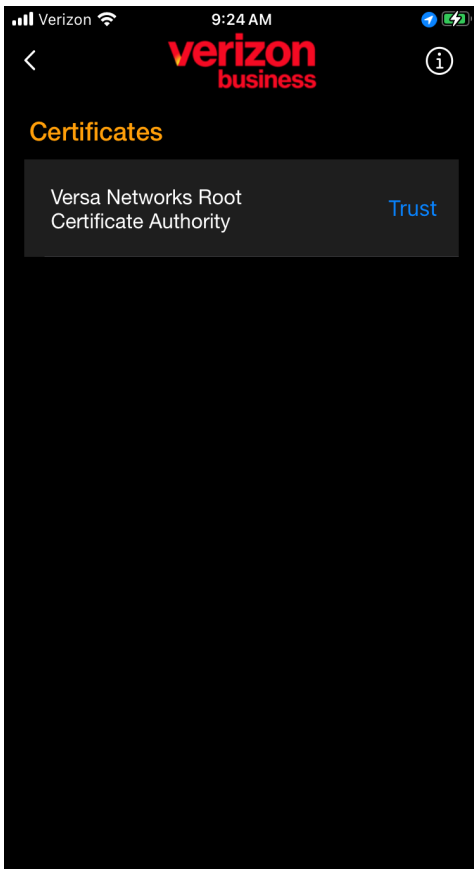
- **Step 5:** Please go back to the Trusted Connection Client and click on the yellow warning triangle in the top left-hand corner.







- **Step 6:** Please select “Trust” for the “Versa Network Root Certificate Authority” and hit the back button.



- **Step 7:** Set the Hostname, Enterprise Name and input your User ID and click “Done” followed by “Submit”. The Hostname and Enterprise name will be provided to you by your company Admin e.g.:

**Hostname:** us-region2.securegateway.verizon.com (please do not use, this is an example only).

**Enterprise Name:** emagte178032a (please do not use, this is an example only).

You will now be taken to your companies Identify Platform (IdP) where you’ll be asked for your Username and Password.

- **Step 8:** Once you’ve successfully logged into your company's IdP platform, please click “Allow” to enable Trusted Connection to send you notifications and select “Allow” to permit Trusted Connection to “Add a VPN Configuration”. Finally, turn on “Location Services” using the “Settings” link.
- **Step 9:** Please go back to the Trusted Connection Client and finally click the “big red power button” and you will now be connected to Verizon’s Trusted Connection service.