NHSmail Intune Service

Operations Guide for Intune Local Administrators and Onboarding Managers

Document Control

Document Information

File Name:	NHSmail Intune Service Operations Guide for Intune Local Administrators and Onboarding Managers
Author(s):	Callum Campbell, Courtney Whyne, Phillip Evans, Stephanie Hall, Hanifa Miah, Carolina Cadenas, Nike Arthur, Stephen Hockley, Erwin Zengerink, Kapil Kulkarni, Andrew Simpson, Andrew Heron, Jasmine Smith, Paul Hill
Version:	12.10

Document Revision History

Version	Date	Changed By	Change
V.01	01/06/21	Callum Campbell / Stephanie Hall	Draft Mobile Early Adopters content added
V1.0	01/07/21	Stephen Hockley / Phil Evans / Stephanie Hall	Draft Windows 10 and HoloLens 2 Early Adopters content added
V2.0	26/07/21	Courtney Whyne / Callum Campbell / Stephanie Hall	Mobile Devices Live Service content added
V3.0	16/08/21	Stephen Hockley / Carolina Cadenas	Win10 and HoloLens2 Live Service content added
V3.1	01/09/21	Stephanie Hall	Group Management app content added
V4.0	10/09/21	Stephen Hockley / Phil Evans	Co-management and certificates sections added
V5.0	21/09/21	Erwin Zengerink / Stephanie Hall	Data visibility content added
V6.0	27/09/21	Kapil Kulkarni / Callum Campbell	ABM link steps added
V6.1	04/10/21	Callum Campbell / Courtney Whyne	Renewing ABM / VPP token content added
V7.0	20/10/21	Callum Campbell	Android Custom apps content added
V8.0	10/11/21	Stephanie Hall	NHSmail Intune SharePoint detail added
V8.1	18/11/21	Carolina Cadenas / Erwin Zengerink	MAM content added
V9.0	22/11/21	Nike Arthur / Courtney Whyne	Samsung Knox and Win 10 mobile applications management content added
V9.1	06/12/21	Callum Campbell / Courtney Whyne	Android minimum OS, enrolment restrictions and AAD groups list updated
V10.0	07/01/22	Courtney Whyne / Callum Campbell Gaurav Malhari	Updates/ Review of Android and iOS section. Updates to section 10 – MAM
V10.1	15/03/2022	Callum Campbell Nike Arthur Stephanie Hall	Section 5.2 Multi-org descriptions Section 11.9 Upgrading to Win 11 using Intune Removal of Section 4.1.2 lice
V10.2	10/06/2022	Phil Evans, Courtney Whyne, Carolina Cadenas	Updates to provide guidance on the ‘Centralised’ Model with new postures and administrative routines

V10.3	04/07/2022	Phil Evans, Courtney Whyne, Carolina Cadenas	Updates from NHSD to include Intune Local Admins instead of Local Admins and Windows10/11
V10.4	01/09/2022	Courtney Whyne, Carolina Cadenas	Updated security baselines
V10.5	10/10/2022	Callum Campbell, Nike Arthur, Carolina Cadenas	Updated content for Group Policy Analytics, Global-Defender for Endpoint Baselines, Global-Edge-Baseline, and minor formatting changes.
V10.6	31/01/2023	Phil Evans, Andrew Heron, Nike Arthur	Updated content for – Microsoft Store Repository Autopilot Manufacturer Provisioning Read-Only RBAC role Zebra Mobility Extensions
V10.7	16/03/2023	Philip Evans, Andrew Heron	Updated sections 6.5 – RBAC Read-Only process Updated section 6.9 to remove steps on how to identify RBAC role as this is no longer visible. Updated section 9.10 – Zebra MX extensions
V10.8	17/03/2023	Andrew Heron	Updated section 9.11– Android Teams Rooms Devices, Updated section 9.10 – Zebra MX extension, Updated section 9.3 – Android Shared Enrollment Updated section 12.7.5 – Windows feature update readiness reports Updated section 12.7.6 – Windows Feature Update Compatibility Risks Updated Notes section 9.7 – Android Application Management. Updated entire document to replace references of MEM and Microsoft Endpoint Manager with Microsoft Intune
V10.9	01/05/2023	Andrew Heron	Updated wording in section 9.2 9.2 Single User Android Device Enrolment 9.12 – Google Zero Touch enrollment
V10.10	23/05/2023	Andrew Heron	Updates to section 6.26 – GPO analytics
V11	14/06/2023	Andrew Heron	Added 5.5 and 5.6 Apple VPP Apps and iStore Apps Updated section 4.1 wording and RBAC settings Updated Table contents and heading formatting for entire document. Updated section 7.3 Monitoring App Protection Policies Updated Figure 1 in section 3. Updated descriptions in Glossary Reviewed all screenshots

V11.1	19/07/2023	Andrew Heron	Updated section 6.4 Android Application Management Created section 8.8 Driver updates for Windows 10 Created section 13.1 Microsoft Tunnel
V11.2	31/07/2023	Andrew Heron	Moved reporting from Section 15 into Intune features and practises 4.10. Updated diagram in section 3.
V.11.3	01/08/2023	Andrew Heron	Added section 6.4.2 Android Private or paid for apps Updated all references of group management naming standard with new format - <ODS>.sg.Intune-xx-xx
V.11.4	01/09/2023	Andrew Heron	Added section 16 – Windows Autopatch
V.11.5	01/10/2023	Andrew Heron	Added section 8.5.6 Policies for Office Apps Added section 6.10 Naming of Android Devices
V.11.6	01/11/2023	Andrew Heron	Added section 8.11 – Windows Hello for Business Added MacOS deployment guide to section 5. Reconfigured numbering and layout of section 5 iOS and Mac
V.11.7	01/01/2024	Andrew Heron Paris Horan	Added section 4.11 – Items created when onboarding Updated licencing information throughout the doc
V.11.8	01/02/2024	Andrew Heron	Added section 6.9.4 New Managed Home screen settings Added section 5.4.5 Setup assistant with modern auth
V12.2	01/02/2025	Andrew Heron	Updated EMS powerapp screenshots Windows 365 info added – Section 8.12 Updated Android renaming script
V.12.3	01/03/2025	Paul Hill	Added Section 5.6 iOS Defender For Endpoint Added Section 6.10 Android Defender for Endpoint
v.12.4	03/04/2025	Paul Hill	6.10 Android Personal Device Enrolment 5.6 iOS Personal Device Enrolment

v.12.5	16/04/2025	Paul Hill	5.6.1 iOS Personal Device Enrolment Restriction 6.10.1 Android Personal Device Enrolment Restriction
V. 12.6	04/09/2025	Paul Hill	8.12.1 W365 Frontline Cloud PCs
V 12.7	11/09/2025	Andrew Heron	8.12.2 Windows 365 Link devices
V 12.8	16/10/2025	Andrew Heron	3.5.3.x – EMS PowerApp updates
V 12.9	16/01/2026	Paul Hill	8.12.1 W365 Frontline Cloud PC – addition of cloud apps
V 12.10	18/03/2026	Andrew Heron	Updated iOS enrolment recommendations.

Contents

1. Document Overview

This Operations Guide will support Intune Local Administrators (Intune LAs) and Onboarding Managers to implement NHSmail Intune as an MDM solution within their organisation for corporate fully managed iOS/iPadOS, Android, Windows 10/11 and HoloLens 2 devices.

The document will explain how Intune Local Administrators can enrol iOS/iPadOS, Android, Windows 10/11 and HoloLens 2 devices onto Intune and manage devices, Groups, users and applications successfully.

The document will also provide important guidance for Onboarding Managers to support the completion of all prerequisite activities as outlined in the NHSmail Intune Service Terms of Reference (ToR) document.

At a high-level, this document covers the following key areas of Intune device enrolment and management: Intune features, Intune policy assignment best practices, RBAC and scope tags, naming standards, application management, device configurations, security group management, wiping devices, reporting, and offboarding.

Please note:

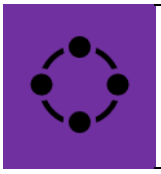
1. This document is not an exhaustive guide to Intune but is intended to support Intune LAs and Onboarding Managers to begin using the service and support with upskilling. Due to the individual nature of each organisation, you may encounter issues which are not referenced in this guide. If this is the case, all onboarded organisations can request additional technical support by raising an incident or service request via Helpdesk Self-Service.
2. Any recommendations suggested in this guide are offered as **guidance only**. Intune LAs should consider these recommendations but should only follow the recommendations if they deem these to be the best course of action for their organisation. As outlined in the NHSmail Intune Terms of Reference (ToR) document; 'Once an organisation has completed Intune provisioning, that organisation becomes wholly responsible for their assigned Device Applications, device configuration, compliance assignments and any adopted or amended policy.'
3. This document will be updated regularly to reflect any technical changes, updates and/or necessary guidance pertaining to new features.

1.1 Highlighted Notes

!	**Important Note** This highlighted note indicates important information for the readers' awareness.

Critical Notes that will require action

This highlighted note indicates a required action to be completed.



Managed Centrally

This highlighted note indicates a setting which is centrally managed and is therefore not configurable by an Intune Local Admin.

Recommendation / Recommended Use

This highlighted note indicates a general recommendation or the recommended use of a process or action.

1.2 Document Purpose

This document is intended to be a comprehensive guidance and reference document used by Intune Local Administrators and Onboarding Managers working at organisations who have successfully onboarded onto the NHSmail Intune Service.

By providing a detailed overview of all enrolment and management processes, requirements and technical considerations, this document is intended to support Intune Local Administrators to independently manage iOS/iPadOS, Android, Windows 10/11 and HoloLens 2 devices in Intune and to support Onboarding Managers to complete all necessary pre-requisite activities.

The document should facilitate the quick and seamless enrolment of iOS/iPadOS, Android, Windows 10/11 and HoloLens 2 devices onto the platform and support effective technical troubleshooting including Intune LA management of Level 1 and Level 2 end user issues.

Intune Local Admins and Onboarding Managers should work towards the end goal of onboarding onto the NHSmail Intune platform, and enrolling and configuring devices ready for deployment, is to ensure that **end users can use Intune-enrolled devices as normal to complete all their usual work responsibilities**.

1.3 Document Audience

This Operations Guide is intended for use by **Intune Local Administrators and Onboarding Managers from NHSmail Intune organisations only**.

The document is **not** intended for use by end users.

For end user guidance materials designed to support end users to start using their devices and perform some simple technical troubleshooting, please follow the below links:

Quick Start End User Guides

- iOS/iPadOS Quick Start End User Guide:
    - https://support.nhs.net/knowledge-base/nhsmail-intune-service-ios-ipados-quick-start-end-user-guide/
- Android Quick Start End User Guide:
    - https://support.nhs.net/knowledge-base/nhsmail-intune-service-android-quick-start-end-user-guide/
- Windows 10 Quick Start End User Guide:
    - https://support.nhs.net/knowledge-base/nhsmail-intune-service-windows-10-quick-start-end-user-guide/
- HoloLens 2 Quick Start End User Guide:
    - https://support.nhs.net/knowledge-base/nhsmail-intune-service-hololens-2-quick-start-end-user-guide-2/

FAQs

- iOS/iPadOS FAQs:
    - https://support.nhs.net/knowledge-base/ios-ipados-frequently-asked-questions-faqs/
- Android FAQs:
    - https://support.nhs.net/knowledge-base/nhsmail-intune-service-android-faqs/
- Windows 10 FAQs:
    - https://support.nhs.net/knowledge-base/nhsmail-intune-service-windows-10-faqs/
- HoloLens 2 FAQs:
    - https://support.nhs.net/knowledge-base/nhsmail-intune-service-hololens-2-faqs/

Editable

- Editable versions of all Quick End User Guides and FAQs:
    - https://support.nhs.net/knowledge-base/editable-resources/

!	**Important Note** 'Trust' and 'Organisation' are used interchangeably within this document. Both refer to NHSmail organisations generally.

2. Glossary

Acronym	Full Term	Description
AD	Active Directory	Active Directory (AD) is a Microsoft technology used to manage computers and other devices on a network. It is a primary feature of Windows Server, an operating system that runs both local and Internet-based servers. Active Directory allows network administrators to create and manage domains, users, and objects within a network.
AAD	Azure Active Directory	Azure Active Directory (Azure AD) is Microsoft's enterprise cloud-based identity and access management (IAM) solution. Azure AD is the basis of the Office 365 system.
ADE	Automated Device Enrolment	Automated Device Enrolment allows you to enrol large numbers of devices remotely.
ABM	Apple Business Manager	Apple Business Manager (ABM) is an online portal for IT Administrators, who deploy iOS devices in an enterprise setting. The portal is used in connection with a third-party mobile device management (MDM) software for managing and distributing these Apple devices and applications.
API	Application Programming Interface	An Application Programming Interface (API) is a set of functions that allows applications to access data and interact with external software components, operating systems, or microservices. To simplify, an API delivers a user response to a system and sends the system's response back to a user.
AV	Anti-Virus	An antivirus program is a software utility designed to protect your computer or network against computer viruses.
COSU	Corporate-Owned, Single Use	A device management scenario where an organization owns and controls a dedicated device that is configured for a specific purpose or application.
CSR	Certificate Signing Request	A Certificate Signing Request is a small, encoded text file containing information about the organisation and the domain you wish to secure.

		It is required for the activation of a digital SSL certificate.
DBT	Design, Build, Test	The 'design-build-test' (DBT) cycle is a software paradigm that is widely practiced for the design of experiments and the rational optimization of technology.
EDR	Endpoint Detection and Response	Endpoint Detection and Response (EDR), is an endpoint security tool integrated into your cyber system to give you a real-time continuous monitor for malicious activity.
GA	General Availability	General Availability is the production release phase of the software lifecycle.
HSS	Helpdesk Self-Service	Helpdesk Self-Service is an online portal supporting the registering and resolution of tickets submitted by Intune LAs.
LST	Intune Live Service Team	The Intune Live Service Team is responsible for reviewing and actioning all submitted Helpdesk Self Service incidents and service requests tickets and communicating the progress and outcome of these tickets to the requesting Intune LA.
LAPS	Local Admin Password Solution	The Local Administrator Password Solution (LAPS) provides a solution to this issue of using a common local account with an identical password on every computer in a domain. LAPS resolves this issue by setting a different, random password for the common local administrator account on every computer in the domain.
LoB Apps	Line of Business Applications	Line of Business Applications is software used by business users to perform a business function.
LTSC	Long Term Servicing Channel	Windows Enterprise LTSC is a separate Long-Term Servicing Channel version. Long-term Servicing channel is not intended for deployment on most or all the PCs in an organisation; it should be used only for special-purpose devices.
Microsoft Intune	Microsoft Intune	Microsoft Intune helps deliver the modern workplace and modern management to keep data secure, in the cloud and on-premises. Microsoft Intune includes the services and tools you use to manage and monitor mobile devices, desktop computers, virtual machines, embedded devices, and servers.
MAM	Mobile Application Management	Mobile application management (MAM) describes the software and services responsible for provisioning and controlling access to internally developed and commercially available mobile apps used in business settings, on both company-provided and 'bring your own' mobile operating systems as used on smartphones and tablet computers.

MDM	Mobile Device Management	Mobile Device Management (MDM) is the process of enhancing corporate data security by monitoring, managing and securing the mobile devices such as laptops, smartphones and tablets used in enterprises. Mobile device management solutions allow IT admins to control and distribute security policies to the mobile devices in their organisations, ensuring the corporate network is secure.
ODS	Organisation Data Service	Unique code created by the Organisation Data Service within NHS Digital and used to identify organisations across health and social care.
OEM	Original Equipment Manufacturer	An original equipment manufacturer (OEM) is a company that produces parts and equipment that may be marketed by another manufacturer.
OOBE	Out of Box Experience	Out-of-box experience is the experience an end-user has when taking a product out of the box and preparing to first use it. The product settings have not yet been set up for the user.
OS	Operating System	The Operating System is software that controls the operation of a computer and directs the processing of programs.
RBAC	Role Based Access Controls	Role-based access control (RBAC) restricts network access based on a person's role within an organisation and has become one of the main methods for advanced access control. The roles in RBAC refer to the levels of access that people have to the network.
GA	General Availability channel	Microsoft Windows 10, version 21H2, feature updates for Windows 10 released annually, in the second half of the calendar year. The General Availability Channel replaces the previous "Semi-Annual Channel" as the primary and recommended channel for Windows 10 servicing.
SOE	Standard Operating Environment	A standard operating environment (SOE) is the basic operating system and software application installation load that is generally deployed throughout an organisation's user base.
T&Cs	Terms and conditions	The terms and conditions that detail the rules that apply to fulfilling a particular contract.
TDA	Technical Design Authority	A Technical Design Authority is the group or person responsible for ensuring a solution meets goals, needs and specifications.
ToR	Terms of Reference	Provides a full list of pre-requisites, terms of services, key responsibilities and requirements needed to onboard onto the NHSmail Intune. Also includes details of the support available to organisations onboarded to NHSmail Intune.

TPM	Trusted Platform Module	A Trusted Platform Module (TPM) is a specialized chip on an endpoint device that stores RSA encryption keys specific to the host system for hardware authentication.
Trust	Also known as a local org., organisation.	An organisational unit within the NHS, generally serving either a geographical area or a specialised function.
UPN	User Principal Name	A User Principal Name is the name of a system user in an e-mail address format.
VPP	Volume Purchase Programme	The Apple Volume Purchase Program (VPP) is a service that allows organisations that have registered for the Apple VPP to purchase iOS apps in bulk.
WaaS	Windows as a Service	Windows as a service is the approach Microsoft introduced with Windows 10 to deploy, update and service the operating system

3. High-Level Overview of the NHSmail Intune Solution

NHSmail Intune is a recently introduced device management capability leveraging Intune for Windows and mobile devices. The NHSmail Intune solution provides a means of enrolling, configuring, and securing devices from a central NHSmail 'tenant' using policies and restrictions.

The administration of NHSmail Intune has been designed to provide individual organisations with flexible deployment options, allowing Intune LAs to localise and contextualise some configurations to their specific requirements.

The NHSmail Intune service is provided through the National Microsoft 365 E3 License and supports the following key features/benefits:

- Intune for Mobile Device Management (MDM)
- Windows 10/11, iOS/iPadOS, Android enrolment
- Windows 10/11, iOS/iPadOS, Android Apps/Config Policies
- Windows 10/11, iOS/iPadOS, Android Groups

An NHSmail standardised set of apps, settings and policies for each platform has been configured and deployed, creating 'Postures' (standards of common policies). This will be configured globally across the NHSmail tenant, applying to the following platforms:

- Windows 10/11
- Apple iOS/iPadOS

- HoloLens 2
- Androids

Per-organisation ‘scoping’ of Intune configuration items is provided by Role-Based Administration Configuration (RBAC), which limits administration to only the organisation’s users and devices.

Intune LAs will have the option to make configurations and their own policy changes to devices, via the RBAC model. However, to ensure that devices are maintaining a minimum level of security, Intune LAs **will not** be able to change or remove the core Centralised Compliance Policies, Centralised Configuration Profiles, Global Autopilot Deployments, Centralised App Protection Profiles (MAM) and Intune Security baselines (that are set globally and therefore not available as part of the RBAC model).

Conditional Access (CA) configuration is provided to bring user or device ‘signals’ together, to grant access and enforce organisational policies. CA policies at their simplest are ‘if-then’ statements; if an end user wants to access a resource, then they must complete an action. For example: A doctor wants to access a clinical application and is therefore required to perform multi-factor authentication to access it.

The following diagram illustrates the high-level NHSmail Intune solution architecture, incorporating Intune and related components that will manage organisations’ devices:

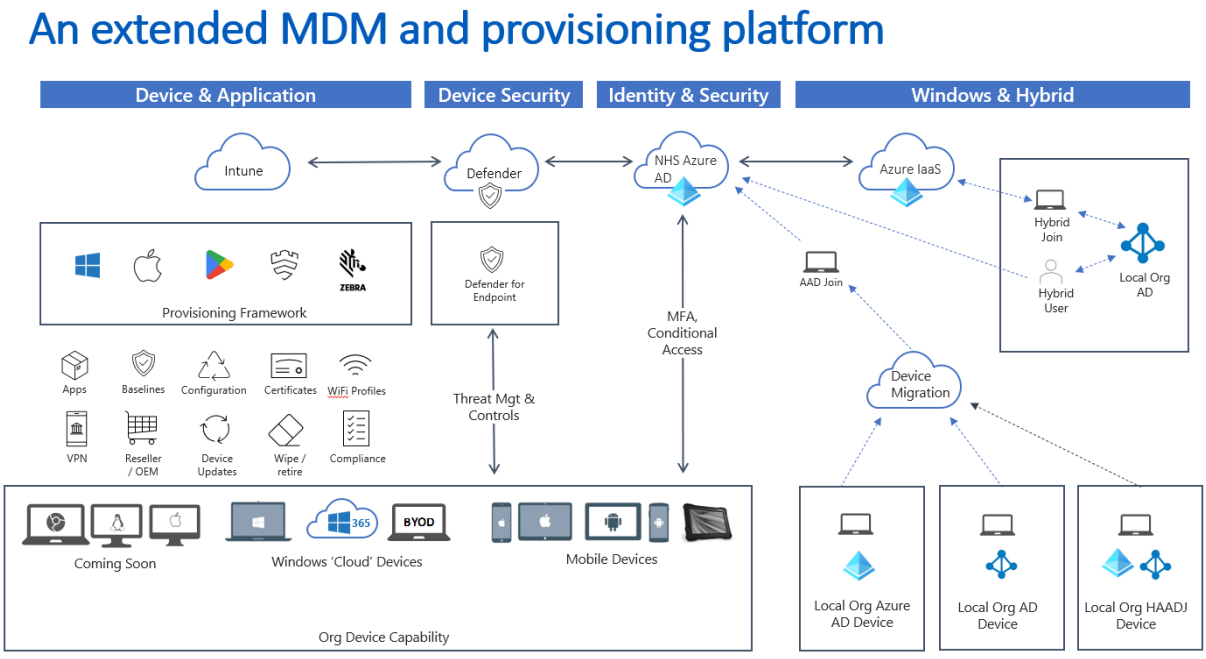


Figure 1: Intune High-level architecture

3.1 Data Visibility within NHSmail Intune

Organisations who onboard the NHSmail Intune tenant are joining a single tenant containing multiple organisations. Management of an organisation's devices and changes to an organisation's data are limited to an organisation as far as possible through custom permissions, however some areas cannot be controlled by such custom permissions and limited data pertaining to other organisations may be visible. In particular, some monitoring and reporting views data pertaining to other organisations are visible and can in some cases be exported, such as device names and UPNs of assigned users. Please see Certificate Services for Intune for more details on this.

!	**Important Note** Organisations **must treat any such data as confidential**.

!	**Important Note** **Organisations are responsible** for protecting their sensitive data and ensuring that they follow their local data security policies - particularly regarding naming standards and free text fields.

In addition, organisations can make changes in some areas (for example Android applications that can affect other organisations so care should be exercised when accessing and managing these areas. Please see the section on Android Application Management in this document for more details on this.

This has been outlined in the NHSmail Intune Terms of Reference (ToR) document which all organisations are required to read and agree to prior to onboarding onto NHSmail Intune.

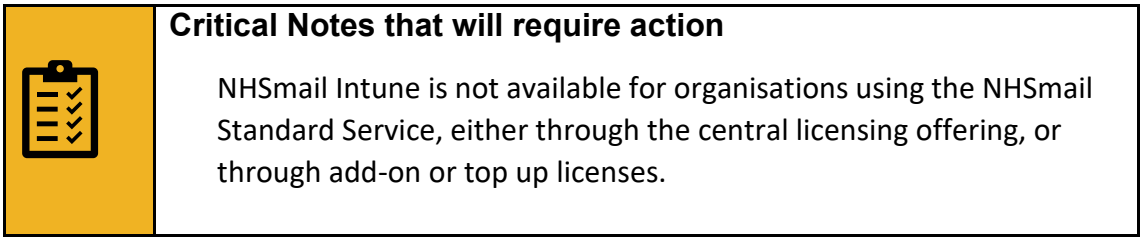
3.2 Enrolment Prerequisites

!	**Important Note** The onboarding and enrolment pre-requisites are relevant to both Intune Local Administrators and Onboarding Managers.

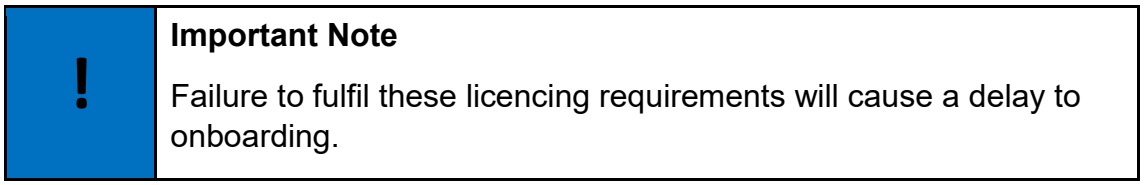
	**Critical Notes that will require action** Both Intune Local Administrators and Onboarding Managers are required to complete actions to ensure the below prerequisites are fulfilled.

3.2.1 Licensing for NHSmail Intune

As part of the new licensing agreement with Microsoft, **Enhanced organisations** now have access to NHSmail Intune as a standard offering. This means you can access the service by assigning the M365 E3 Restricted License to all users via the National License in the portal and toggling on Intune. Click here for information on how to assign the national license.



3.2.2 NHSmail Intune Licensing Terms and Requirements



- M365 E3 Restricted licences should be assigned following the guidance here.
- M365 E3 Restricted licences licences are required for all end users and Intune LAs who will be using the Intune service on Single User Devices.
- For Shared Devices, M365 E3 Restricted licences licence is required for the Win10 Autopilot Shared Device Mode but are not required for the following Shared Device Modes:
    - iPadOS Non-User Affinity / Guest Mode
    - iOS Managed Apple ID
    - Android Shared Device Mode (Dedicated)

3.3. Support available to Onboarded Organisations

The below terms detail the service support which will be available to all organisations onboarded onto the NHSmail Intune Service.

Details of the service support, service responsibilities and supporting documentation for onboarded organisations is detailed in full in the NHSmail Intune Terms of Reference (ToR) document which should have been read and agreed to by all organisations prior to onboarding.

For the reference of all Intune LAs at onboarded organisations, details of the service support available, service responsibilities of both Intune LAs and the Intune Live Service Team and support model processes are provided below. Please refer to these sections and the NHSmail Intune Platform RACI chart if you are an Intune LA who is unsure of their service responsibilities or would like to know more about the options available for raising an incident or service request via Helpdesk Self-Service.

3.3.1 Service Support

- All onboarding requests , service requests, and Level 3 incidents will need to be raised as tickets via Helpdesk Self-Service (HSS) on the NHSmail Portal.
- Helpdesk Self-Service should be used in the first instance for all incidents requiring the support of the Intune Live Service team and should be limited to Level 3 incidents or service requests.
- All completed and submitted Incidents and Service Requests will be sent to the Intune Live Service Team for review and the Intune Local Admin who submitted the form/s will be updated on the progress and outcome of any request via the standard incident process.

3.3.2 Service Requests

The following Service Requests will appear as drop-down options on the Helpdesk Self-Service form available. Intune LAs can submit any of the below for review by the Intune Live Service Team. If your service request falls outside of the areas stated below, Intune LAs are required to select ‘Other’ and fill in the description box with their service request. The Intune Live Service Team will update the requestor with the resolution and close the ticket.

- Windows 10/11 BitLocker recovery key
- Request an Android enrolment profile (Shared Device)
- Request to offboard an organisation from the NHSmail Intune Service
- Request to onboard your organisation’s Apple Business Manager (ABM) for Apple Devices
- Request to add a certificate connector
- Request to add a multi-organisation
- Query related to security posture
- Request for Cloud+SSO track, and hybrid join track
- Request for an Intune policy configuration query
- Bring your own device security controls (BYOD)
- Other

!	**Important Note** Requests from Intune LAs to update Windows 10/11 baselines (centrally managed) can be requested. Please complete a Service Request Form via Helpdesk Self-Service, and the request will be considered by the NHSmail Technical Design Authority (TDA). There is no requirement for NHSmail to approve requests for changes to these set policies and RBAC Settings, however the outcome of the request will be communicated to the ticket requestor.

3.3.3 Incidents

The following Incident can be submitted for review by the Intune Live Service Team. Intune LAs can submit any of the below for review by the Intune Live Service Team. If your incident falls outside of the areas stated below, Intune LAs are required to select 'Other' and fill in the description box with their incident, attaching screenshots where relevant. The Intune Live Service Team will update the requestor with the resolution and close the ticket.

- Organisation onboarding
- Device enrolment
- Intune Role Based Access Control (RBAC) Permissions
- Device configuration and policies (Intune LA Delegated)
- Intune Group Management Tool
- Resetting Devices
- Applications
- Bring your own device security controls (BYOD)
- Conditional Access
- Centrally managed configuration (Security Posture)
- Cloud + SSO Track and Hybrid Track: VPN Connectivity Issue
- Cloud + SSO Track and Hybrid Track: Device Failure
- Cloud + SSO Track and Hybrid Track: Sync Issue
- Cloud + SSO Track and Hybrid Track: Device not removed from Sync
- Cloud + SSO Track and Hybrid Track: Pre-Req Support
- Other

- It is highly recommended Intune LAs contact Helpdesk Self-Service at the earliest opportunity to ensure the raised ticket is directed to the correct team/s and can be reviewed and actioned promptly.

- The national NHSmail Helpdesk (Helpdesk@nhs.net) should only be contacted regarding incidents, service requests or onboarding requests if:
    - Intune LAs are unable to complete or understand the form
    - Form/s are not working
    - Out of Hours Support is required
    - There is an urgent escalation
- NHSmail Helpdesk can be contacted in any of the above scenarios via phone on 03332001133 or by emailing helpdesk@nhs.net, 24 hours a day, 365 days a year.
- If the Helpdesk is contacted in relation to an incident request, they provide links to relevant information on the NHSmail Support Site or will direct the Intune LA to the Incident Form accessible via Helpdesk Self-Service.
- If the Helpdesk is contacted in relation to a service request, they will log the query and direct the Intune LA to the Service Request Form accessible via Helpdesk Self-Service. If the Intune LA contacting the Helpdesk is unable to complete either the Incident Form or the Service Request Form, the Helpdesk will be able to complete either Form on behalf of the Intune LA and will submit the ticket for review to the Intune Live Service Team.
- Any tenant-wide technical updates, change in terms or general notices to all organisations onboarded onto the NHSmail Intune Service will be communicated to the Intune LAs and it is expected that the Intune LAs will communicate the update as appropriate within their organisation to ensure continuity of service.
- As a last resort, Intune LAs can wipe, reset, or remove devices from Intune. Wiping devices and removing them from Intune is the responsibility of organisations.
- Organisations have the option to offboard entirely from the Intune service. This process will take at least a day to complete and offboarding times may vary depending on how many devices have been enrolled in the tenant. Intune LAs will need to raise a service request via Helpdesk Self-Service if they want to offboard from the Intune service. The process for offboarding will require secondary sign-off from someone within the organisation.

3.4 Custom Configuration Requests (Exception Process)

All onboarded organisations are able to request for custom configuration which sits outside of the three postures of the centralised model to be allowed within their environments.

To request this, organisations will need to raise a service request via Helpdesk Self-Service (option: Query related to security posture) and will need to provide a business justification for requiring this custom configuration.

Any request will be reviewed by the Intune Live Service Team and NHS Digital, and we may wish to follow-up with you to discuss your requirements in more detail to ensure we are able to support you properly, and to explore options to facilitate your use of the platform outside of the three postures if this is needed.

3.5 Multi-Organisation Structure

!	**Important Note** The following is intended for those organisations for whom it has been deemed to onboard via the multi-Organisational approach.

!	**Important Note** The default onboarding approach onto the NHSmail Intune platform is Model 1 – Central Management. Model 2 (Multi-Organisational Parent / Child) onboarding will be assessed on a case-by-case basis and require business justification from the Organisation.

The multi-organisation model is designed for organisations who manage other NHS organisations' MDM solutions. There are two onboarding options available for organisations who may manage the devices of others, or alternatively have their devices managed by a different organisation. Outlined below is the conceptual explanation for each model.

3.5.1 Parent Organisations and Child Organisations

RBAC Role Naming Standards refers to "Parent" organisation and "Child" organisation - these terms are used to reference the different type of organisations. A Parent is the organisation that is referred to as the main organisation and is usually the organisation which has the Intune LA management. A Child is the sub-organisation, managed by the Parent.

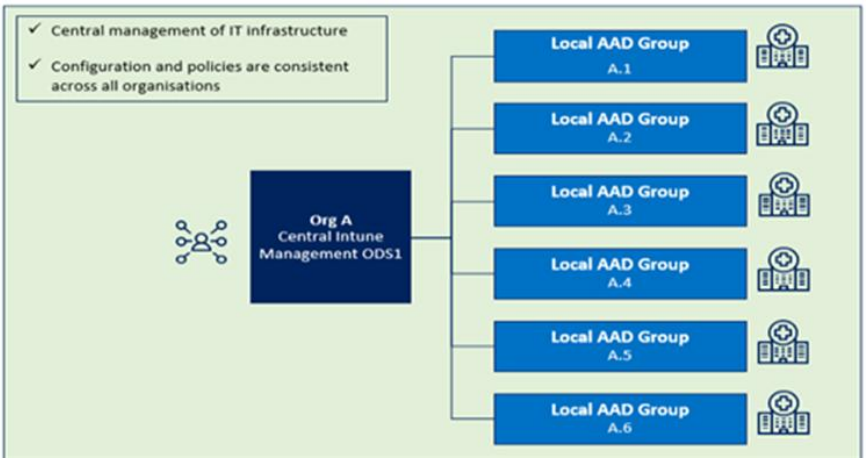
3.5.1.1 Model 1

Model 1 uses a centralised managed approach. Onboarding to the Intune platform will be similar to a standard organisation having its own baselines groups and standard policies, and the parent organisation's ODS Code becoming their centralised ODS code.

Under the Model 1 Approach the Child Organisation will be a part of their own AAD Groups – it is important to note these groups will share the same scope tag as the parent organisation. When implementing policies, these will belong to the Parent organisation however Intune LAs will have the ability to assign a Child

organisations' AAD group to the parent organisations' polices. These AAD groups will need to be created by the Intune LA; should any assistance be to create a large number of groups, please raise a Service Request via Helpdesk Self-Service.

The diagram below highlights the structure of Model 1.

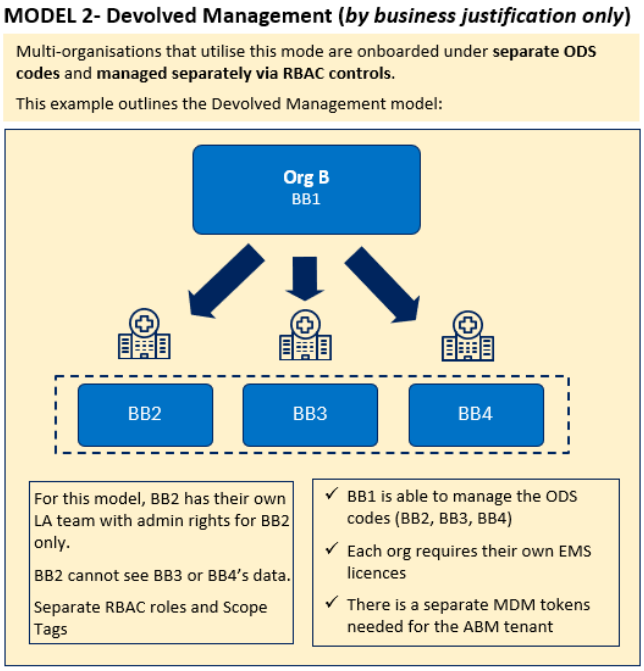


3.5.1.2 Model 2

The structure for Model 2 uses a similar approach to Model 1 in using the parent and child organisations and is **not** the default option. To allow for a smooth onboarding process and successful adoption onto the Intune platform, the Live Services Team must know in advance how your organisation is set-up and if this is the preferred option; this will not stop or hinder the onboarding process

In Model 2, each child organisation will have its own scope tag, AAD groups, Centralised policies and will be enrolled via on the onboarding script. The parent organisation will have the ability to view the child organisations in their structure, however other child organisations will not be able to view each other. Parent organisations will have access to other scope tags and visibility of all the child organisations in their group, unlike the child organisations.

The below diagram highlights the structure of the Model 2 approach:



Important Note

Due to current limitations with the Group Management, Intune LAs will only be able to manage organisations which are associated to their Primary ODS code. To manage a particular AAD group, it is necessary to be logged into an account belonging to that child organisation.

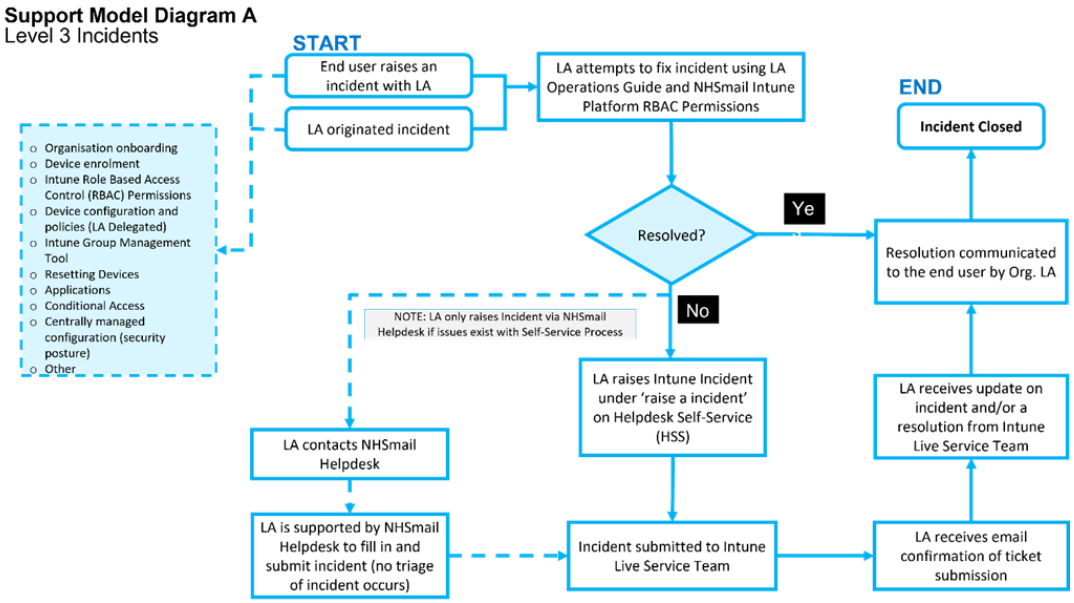
Should you require further assistance please raise a Service Request via Helpdesk Self-Service.

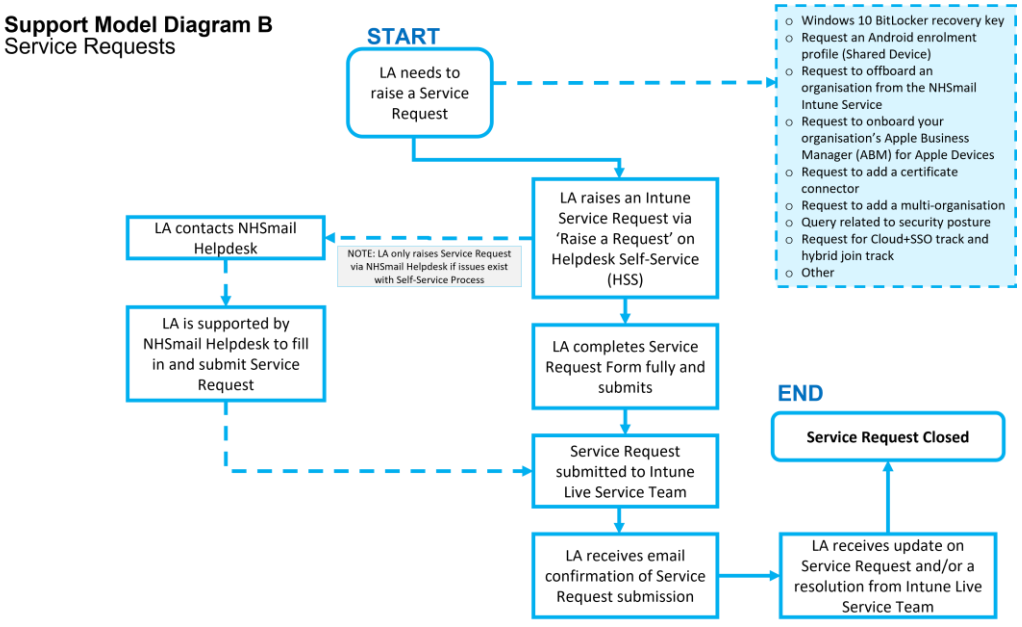
3.6 Service Responsibilities of Onboarded Organisations

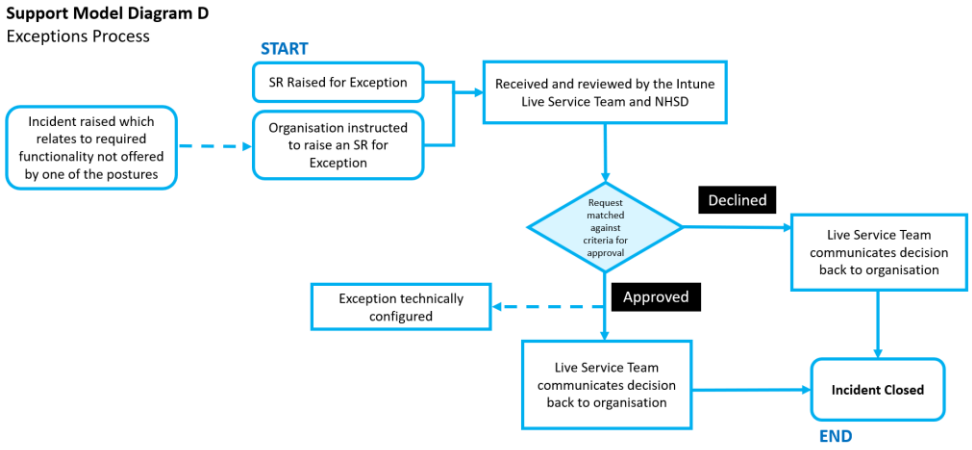
- Before raising an incident request, Intune LAs should ensure that they have referred to this guide to try to troubleshoot any issues.
- Organisations should ensure that all Intune LAs who have RBAC controls or are supporting end users using Intune-enrolled devices have access to Helpdesk Self-Service on the NHS Portal. Intune LAs will need to use their nhs.net credentials to log in and submit tickets.
- Organisations must ensure resources with suitable experience are available to provide Level 1 support (service desk and deskside support) and Level 2 triage and fix support (via delegated RBAC permissions) to end users
- Intune LAs are responsible for the enrolment and unenrolment of devices.
- Intune LAs are responsible for the management of all their devices.

- Following onboarding and creation of their organisation's bespoke environment in NHSmail Intune platform using scope tags, Intune LAs will be responsible for management of that environment.
- Intune LAs are responsible for managing local device configuration policies and profiles (apart from Windows 10/11 baselines)
- Once an organisation has completed Intune provisioning, that organisation becomes wholly responsible to assigned any of the Postures for Compliance Policies, Configuration profiles, APP and any other Device Application or adopted policy.
- Intune LAs are responsible for using scope tags (their ODS code) when creating items and objects in Intune, any objects or items created without a scope tag may be deleted by the Intune Live Service team without notice.

3.7 Support Model Diagrams







3.7.1 NHSmail Intune Platform RACI Chart

R **Responsible**: The individual(s) that complete the task.	**A** **Accountable**: The individual(s) that is ultimately answerable for the activity or decision.	**C** **Consulted**: The individual(s) to be consulted prior to a final decision or action.	**I** **Informed**: The individual(s) that need to be informed after a decision or action is taken.

Please note: All instances where the Intune Live Service Team need to be consulted (C) or informed (I) will happen automatically via the submission of Helpdesk Self-Service forms. Organisations are not required to do anything.

	ACTIVITY / SERVICE ITEM	ONBOARDED ORGANISATION / LAs				INTUNE LIVE SERVICES TEAM			
ONBOARDING ORG.	Read and agree to the Terms of Reference	R	A	C	I	R	A	C	I
	Provide requested information to assist with org. onboarding (technical and business readiness information)	R	A	C	I	R	A	C	I
	Complete all technical and business readiness activities to ensure org. is ready to onboard devices onto NHSmail Intune	R	A	C	I	R	A	C	I
GUIDANCE DOCUMENTATION	Own and manage key guidance documentation provided on NHSmail Support Site	R	A	C	I	R	A	C	I
	Send / distribute links to key guidance documentation to LAs once organisation has been onboarded	R	A	C	I	R	A	C	I
	Update key guidance documentation with any technical changes and/or service changes	R	A	C	I	R	A	C	I
SUPPORT	Provide Level 1 support to end users (e.g., Service Desk)	R	A	C	I	R	A	C	I
	Provide Level 2 support to end users	R	A	C	I	R	A	C	I
	Provide Level 3 support to organisation's LAs (via submitted incidents)	R	A	C	I	R	A	C	I
	Review and action Service Requests	R	A	C	I	R	A	C	I
	Upskilling LAs in Intune and NHSmail Intune Platform	R	A	C	I	R	A	C	I
INTUNE MANAGEMENT	Enrolment and unenrolment of devices	R	A	C	I	R	A	C	I
	Management of enrolled devices and organisation's device estate on NHSmail Intune	R	A	C	I	R	A	C	I
	Manage delegated device configuration policies and profiles (apart from Windows 10 baselines)	R	A	C	I	R	A	C	I
	Manage centrally-controlled Windows 10 Baselines	R	A	C	I	R	A	C	I

3.8 NHSmail Intune SharePoint Site

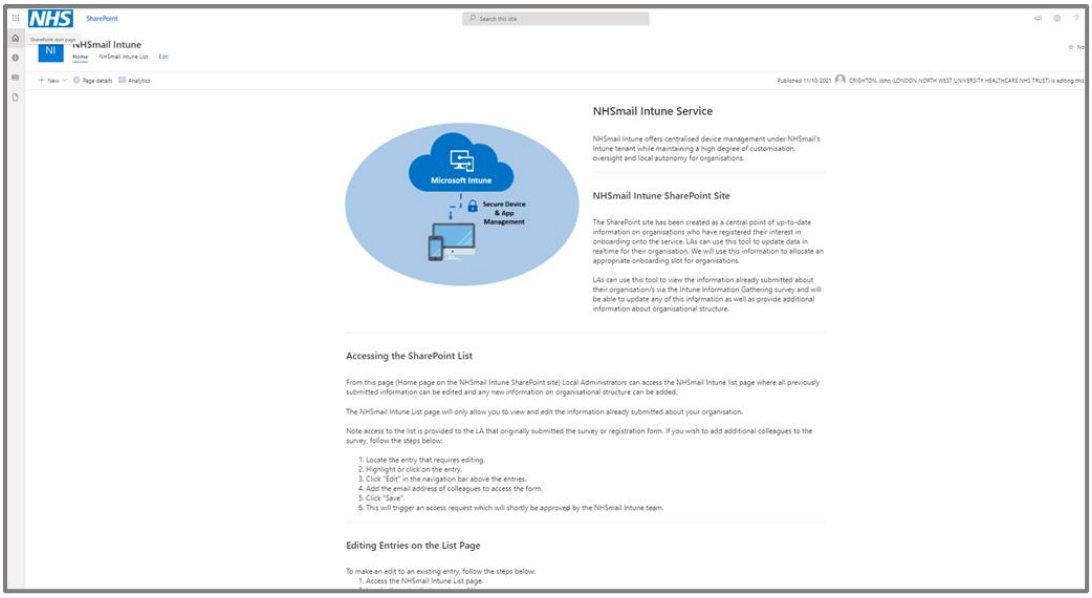
The NHSmail Intune SharePoint site has been created as a central point of up-to-date information for organisations who have registered their interest in onboarding onto the service and/or have been onboarded to NHSmail Intune. Intune LAs can use this tool to update data in real-time for their organisation.

All organisations who submitted a Registration of Interest (either via the Intune Information Gathering Survey or the Intune Registration Form) in Intune will have an entry on the NHSmail Intune SharePoint and will be able to view and update this information.

For onboarded organisations, updating the NHSmail Intune SharePoint if/when there is a change to your multi-organisation status (i.e., if your organisation will soon be managing another organisation's devices or your organisation's devices will soon be being managed by another organisation) or hybrid-join requirements,

will allow the NHSmail Intune Team to provide continued support to your organisation after onboarding.

Instructions on how to navigate the SharePoint and edit information can be found on the Home Page of the NHSmail Intune SharePoint (see below):



Please follow the below link to access the NHSmail Intune SharePoint:

- https://nhs.sharepoint.com/sites/LSP01_NHSmailIntuneComms

If you are experiencing access issues or are struggling to edit your organisation's information on the NHSmail Intune SharePoint, please raise a ticket via Helpdesk Self-Service.

4. Microsoft Intune Features and Practises

This section provides an overview of the key features of Microsoft Intune. Intune LAs will need to be aware of, and be able to make use of, all these features in order to be able to manage devices successfully using NHSmail Intune.

4.1.1 Intune Role Based Access Controls (RBAC) and Scope Tags

Intune allows the segregation of overarching configuration settings into two distinct categories: settings that are 'tenant-wide' and owned by Intune Global Administrators (some of which are typically set-once, effecting all users and devices); and settings that can be delegated to Intune LAs (via Roles).

The settings delegated to Intune LAs are limited in scope to ensure they only effect the devices and settings an Intune LA is responsible for. To facilitate this requirement, Intune has a robust RBAC model in place to provide general-purpose roles for every day administrative tasks, as well as custom roles for a more fine-grained approach to permission management, providing various levels of functionality within Intune.

Important Note

Throughout this document tenant-wide settings will be highlighted. Tenant-wide settings are centrally managed – these permissions are not delegated to Intune LAs.

Managed Centrally

Intune RBAC roles and scope tags are centrally managed by the Intune Live Service Team. Please raise an incident ticket via Helpdesk Self-Service if you have an issue with your RBAC roles.

There are 4 set of RBAC roles for the NHSmail Intune:

- EMS (Intune) Global RBAC Role
- EMS (Intune) Trust Admin Role
- EMS (Intune) 1st Line Support Role
- EMS (Intune) Read Only Role

4.1.2 EMS (Intune) Global RBAC Role

The Global RBAC role allows Intune LAs to view Managed Google Play apps that have a default scope tag, Centralised Compliance policies, Centralised App Protection Policies, Centralised App Configuration Profiles, Global Autopilot Profiles and Security Baselines. EMS-Global-RBAC-Role is the name of this custom role and is assigned to each ODS-Admin group, that includes the scoped groups for each organisation e.g., RD2-Admin includes RD2-Intune-Admins, RD2-Intune-Users and so on.

The permission for the EMS Global RBAC Role is the following:

Custom Role Delegation Area	Permissions
Device compliance policies	Read; Assign;View reports
Device configurations	Read
Enrolment programs	Assign profile;Read profile
Filters	Read
Managed apps	Read;Assign
Mobile apps	Read;View reports;Assign
Security baselines	Read

4.1.3 EMS (Intune) Trust Admin Role

A core principle of the design of the Intune environment is providing Intune LAs with the ability to administer their configuration items in isolation from other organisations. This includes administering their own devices, non-centralized policies, and apps via Intune. It is important that any changes made by an Intune LA only affects the devices and users within their organisation.

EMS-Trust-Admin-Role is the name of this custom role and is assigned to each ODS-Admin group, that includes the scoped groups for each organisation e.g., RD2-Admin includes RD2-Intune-Admins, RD2-Intune-Users and so on.

The below role permissions table details the capabilities Intune LAs have within Intune:

Custom Role Delegation Area	Permissions
Android for work	Read; Update app sync
Audit data	Read
Corporate device identifiers	Create; Delete; Read; Update
Device compliance policies	Assign; Delete; Read; Update; View reports
Device configurations	Assign; Create; Delete; Read; Update; View reports
Endpoint protection reports	Read
Enrolment programs	Create device; Delete device; Read device; Sync device; Assign profile; Create profile; Delete profile; Read profile; Update profile; Create token; Delete token; Read token; Update token
Managed apps	Assign; Read; Wipe; Create; Delete; Update
Managed devices	Delete; Read; Set primary user; Update; View reports
Mobile apps	Assign; Create; Delete; Read; Update; View reports; Relate
Organisation	Read
Policy Sets	Assign; Update; Delete
Remote tasks	Bypass activation lock; Clean PC; Initiate Configuration Manager action; Send custom notifications; Collect logs; Disable lost mode; Enable lost mode; Enable Windows Intune Agent; Get filevault key; Locate device; Manage shared device users; Play lost mode sound; Reboot now; Remote lock; Request remote assistance; Reset passcode; Retire;

Custom Role Delegation Area	Permissions
	Revoke App Licences; Rotate BitLockerKeys (preview); Rotate filevault key; Set device name; Shut down; Update device account; Windows defender; Wipe
Roles	Read
Security baselines	Read
Security tasks	Read
Terms and conditions	Assign; Read

Important Note

A custom Intune RBAC role will be created for all organisations onboarding onto the Intune environment based on the settings above. The RBAC role permissions are designed to provide an Intune Local Administrator with a standard set of permissions to perform administrative duties within Intune.

Important Note

Intune RBAC roles do not allow the delegation of Azure Active Directory access. Intune LAs will not be able to configure AAD Users and Groups through the native Intune portal.

4.1.4 EMS (Intune) 1st Line Support Role

First line support RBAC role is a restricted administrative role which provides read only permissions to an organisations Intune configuration (Apps, Config profiles etc.), whilst still enabling first line support workers to conduct remote tasks such as rebooting, wiping or syncing a device.

Organisations can create their own group that will contain users for this role e.g., ODS-1st Line Support. Intune LAs should use the Group Management App to create / manage Group. Please refer to Group Creation Management for more details. When creating a custom group for the 1st line RBAC role you will need to log a support request to the Intune Live Service team (refer to the Service Support in this document for guidance on raising a support request). This is required as the Intune Live Service Team will need add your custom 1st line group to your scope tag as well as add the custom RBAC role to that group.

The below role permissions table details the capabilities 1st Lines support admins will have within Intune:

Custom Role Delegation Area	Permissions
Android for work	Read
Audit data	Read
Corporate device identifiers	Read
Device compliance policies	Read
Device configurations	Read
Enrolment programs	Read device,Read token,Read profile
Filters	Read
Managed Google Play	Read
Managed apps	Read
Managed devices	Read
Microsoft Store For Business	Read
Microsoft Tunnel Gateway	Read
Mobile Threat Defence	Read
Mobile apps	Read
Remote tasks	Wipe;Set device name;Reset passcode;Windows defender;Send custom notifications;Remote lock;Shut down;Play sound to locate lost devices;Sync devices;Rotate filevault key;Locate device;Enable lost mode;Bypass activation lock;Disable lost mode;Update device account;Reboot now;Offer remote assistance;Enable Windows IntuneAgent
Roles	Read
Security baselines	Read
Security tasks	Read
Terms and conditions	Read

!	**Important Note** Members of the 1st Line Support Roles should have the correct licenses assigned to their accounts: M365 E3 licenses.

4.1.5 EMS (Intune) Read-Only RBAC role

The Read-Only RBAC role allows local Organisations to provide specific users with a 'Read-Only' type role for the Intune UI.

'Read-Only' Users who are provided this role will have broad visibility of configurations and devices for a local organisation, without the ability to add, create, modify, or delete items.

Use the following steps to Assign the Read-Only RBAC Role.

1. Raise a service request to the Helpdesk Self-Service to request a Read-Only RBAC Group

2. Once the group is created, access the Intune PowerApps Group Management application, and locate the ODS-Intune-Read-Only Group
3. Add the required ‘Read-Only’ users to the group.
4. The users now have Read-Only access to the Intune UI (Check that the user is Licensed to use Intune with an National License)

The below role permissions table details the capabilities Read Only admins will have within Intune:

Custom Role Delegation Area	Permissions
Android for work	Read
Audit data	Read
Corporate device identifiers	Read
Device compliance policies	Read, View reports
Device configurations	Read, View reports
Endpoint protection reports	Read
Enrolment programs	Read device, Read token, Read profile
Filters	Read
Managed apps	Read
Managed devices	Read, View reports
Mobile apps	Read, View reports
Organization	Read
Policy sets	Read
Roles	Read
Security baselines	Read
Security tasks	Read
Terms and conditions	Read

!	**Important Note** Members added to the Intune Read-Only RBAC role should not be concurrently included in the [ODScode]-Trust-Admin-Role membership.

4.1.5 RBAC Role Naming Standards

RBAC role naming standards have been set to facilitate the easy differentiation of each organisation’s administrative roles by the Intune Live Service Team.

!	**Important Note** The following naming standard is used for the creation of all new custom RBAC roles: [ODScode]-Trust-Admin-Role.

4.2 Scope Tags

Scope tags are used to provide a logical grouping of users, devices, policies and settings tied to a specific role. In this case, a custom role that will be created for “Trust IT Admins”. Scope tags provide a logical segregation of roles, settings and device management and as a result one organisation’s Intune Local Admin will not be able to access another organisation’s devices, policies or settings.

In addition to utilising custom scope tags, the solution will also utilise the “Default” built in Intune scope tag. This will be utilised to enable the visibility of centralised postures, policies, applications etc. The default scope tag is automatically added to all untagged objects that support scope tags within Intune.

!	**Important Note** The following naming standard is used for scope tags: [ODScode].

4.2.1 Delegation of Rights

NHSmail Intune allows segregation of overarching configuration settings into two distinct categories; settings that are ‘tenant-wide’ and settings that can be delegated to Intune LAs (via Roles). The table below details all settings which are ‘tenant-wide’ and all settings delegated to Intune LAs. Settings delegated to Intune LAs are limited in scope to ensure that they only affect the devices and settings to which an Intune LA is assigned.

Tenant-wide configurations Set by Central NHSmail IT Admins	Central NHSMail Configurations Set by Central NHSmail IT Admins	IntuneLocal Admin Configurations Delegated to Intune Local Admins
• MDM Authority • Apple MDM Push Certificate • Managed Google Play account • Windows Hello for Business & Automatic Enrolment • Microsoft Store for Business • Android Enterprise – Enrolment Profiles and Corporate owned fully managed enrolment • App Categories • Device Clean-up Rules • Conditional Access • Enrolment restrictions • Intune Company Portal – Branding and Customization • Microsoft Defender ATP • Security Baselines • Device Categories • Filters • Hybrid Infrastructure • Terms and Conditions • Central AP Profile and Windows Enrolment Status Page for Win10/11 & HoloLens 2 • RBAC and Scope Tags	• Custom notifications • Certificate connectors • BitLocker recovery keys • Policy sets • Android Enterprise – Corporate Owned Dedicated Devices • App Management • MAM – App Protection Policies • MAM – App Configuration Policies • Device Compliance Policies • Autopilot Profiles • Windows 10/11 update rings (central)	• Apple's Automated Device Enrolment • Apple VPP tokens • Apple Configurator profiles • Apple User enrolment • Device Management • Application Management • Custom Apps • AAD Group Management via Group Management App • iOS App Provisioning Profiles • Device Configuration Profiles (custom) • PowerShell Scripts • Update policies for iOS/iPadOS • Windows 10/11 update rings (custom)

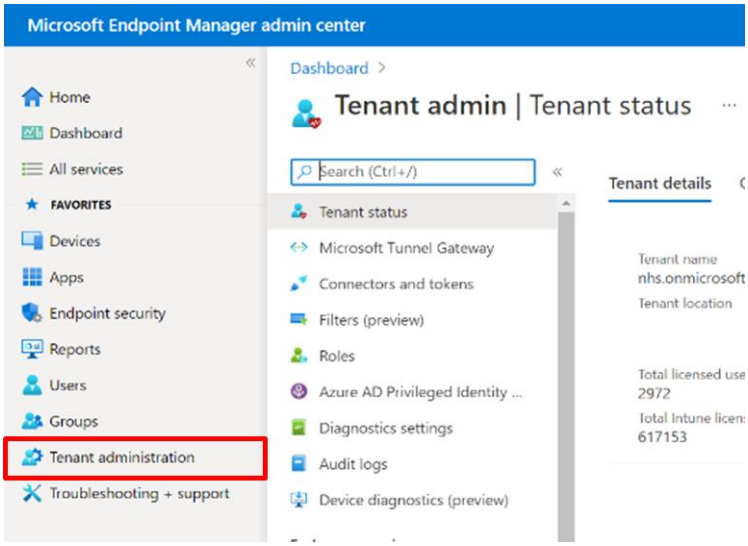
4.2.2 Identifying Scope Tags in Intune

Intune LAs managing devices via NHSmail Intune will need to be able to view scope tags to ensure that these are all configured correctly and are allowing the correct levels of access.

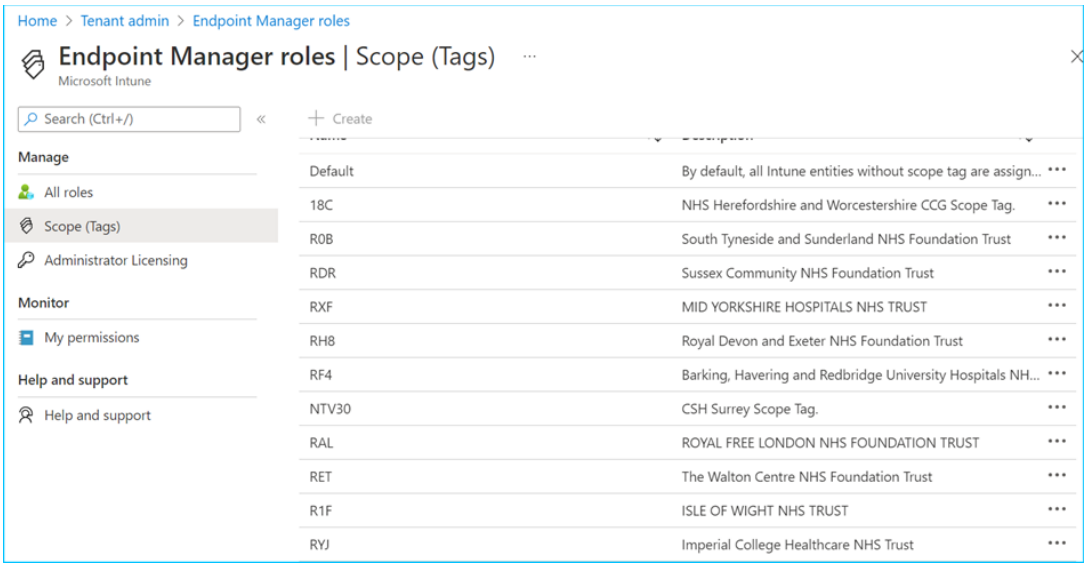
4.2.3 Steps to view Scope Tags

To view scope tags within Intune please follow the below steps:

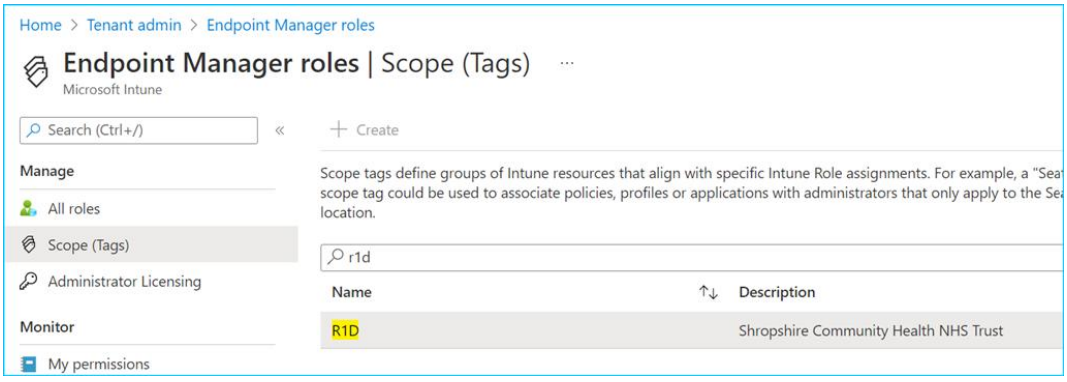
1. Navigate to the **Roles** section via the Tenant administration page.



2. Select **Scope (tags)**



3. Select your Unique Org Scope tags denoted by the ‘ODS’ prefix.



!	**Important Note** Any new device or users’ group **must** be added into the Scope tag to enable visibility of the devices within the Microsoft Intune portal.

4.3 Enrolment Restrictions

Important Note

Any changes made to the device type restrictions will affect all devices enrolled onto the NHSmail Intune tenant. No new device type restrictions should be created by Intune LAs for this reason.

There is a limit to the number of devices that can be linked to a user or administrator in Intune. These limits apply to all device types: Windows 10/11, iOS/iPadOS, Android and HoloLens 2 devices.

Role	Device enrolment Restriction
Administrators	15 Devices
Users	5 Devices

Important Note

There is also an enrolment restriction on Windows & macOS personal devices. Intune LAs and/or end users will be unable to enrol Windows & macOS personal devices onto the platform if they try. Any personal device will be removed without consultation.

Managed Centrally

Device type restrictions is a centralised feature. Please see below for the central enrolment settings which should **not** be changed.

Enrolment restrictions			
Setting	**Device Type**	**Platform**	**Personally Owned**
Device type restrictions	Android Enterprise (Work Profile	Allow	Allow
Device type restrictions	Android Device Admin	Allow	Block

Device type restrictions	iOS/iPadOS	Allow	Allow
Device type restrictions	macOS	Allow	Block
Device type restrictions	Windows (MDM)	Allow	Block

4.4 Naming Standards

The naming convention within the Intune environment will utilise each organisation's unique Organisation Data Service (ODS) code. This will be used as an identifier for groups, profiles, policies, settings and applications. This helps differentiate each organisation's scoped grouping of configuration items when viewed either by an Intune LA or the Intune Live Service Team.

For example, "Trust1" would use the ODS prefix: "SD001".

An example policy would be: "SD001-Windows 10-CompliancePolicy".

ODS codes are unique identifying codes allocated to most NHS providers.

If you are unsure of your organisation's ODS code, please use this link to find / confirm it: https://odsportal.digital.nhs.uk/Organisation/Search

!	**Important Note** Intune LAs will be required to use the below as a prefix to any group that is created. There will be a section for free text to enable an Intune LA to configure the group name. • <ODS>.sg.Intune-Users-[Free text for admin] • <ODS>.sg.Intune-Windows10-Devices-[Free text for admin] • <ODS>sg.Intune-Android-Devices-[Free text for admin]

4.4.1 Azure Active Directory Group Naming Standards

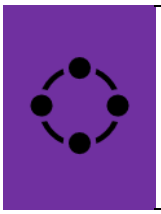
AAD group naming standards are in place to ensure that both Intune LAs and the Intune Live Service Team can easily identify an organisation's AAD group. AAD groups are very important as they are used for policy and app assignments within Intune. It is therefore crucial that Intune LAs can easily identify what is contained within a AAD group.

4.4.2 Central AAD Groups

The below groups have been configured by the NHSmail Intune Live Service Team and are **managed centrally**.

- EMS-Intune-Admins (Group for Intune Admins)
    - This is a nested group, each individual Trust-Admin AAD Group is added into this Central Group.
- EMS-MDM-User-Scope (Intune Requirement)
    - This is a nested group. Each individual Trust-User group is appended to this group. This group is used to enable automatic enrolment of devices for users, any new user group must be appended to this Central AAD group.

- EMS-MDM-Conditional-Access-Scope
    - This group nests each organisations <ODS>.sg.Intune-Users-Conditional-access group.



Managed Centrally

The above groups are managed centrally. Please raise an incident ticket via Helpdesk Self-Service if you have an issue relating to these groups.

4.4.3 Organisation-specific AAD Groups

The below groups are configured as part of the onboarding process for a new organisation.

An Intune LA from your organisation will have submitted the Onboarding Request Form – available to nominated Intune LAs via Helpdesk Self-Service – and as part of that will have submitted some technical information which allowed the Intune Live Service Team to be able to set up the below groups.

These groups are a central repository for the different device platforms and users and are intended to facilitate the management of a single organisation's users and devices. The AAD groups are then added to the Unique Trust RBAC role and scope tag to ensure that Intune LAs can manage their users and devices.

Critical Notes that will require action.

These groups are intended to be managed and updated by Intune LAs.

<ODS>sg.Intune-Admins Groups

- This group is used to store all Trust-Admins within a specific organisation. This AAD group is utilised as part of the custom RBAC role to provide administrative access to the Intune environment.

<ODS>sg.Intune-Users Groups

- This group is an all-user group which should include all users who are going to be enrolling devices into Intune. **Users will not be able to enrol their device if they are not included in this group.**

<ODS>sg.Intune-Users-MAM Groups

- This user group has any of the Centralised Posture of Application Protection Policies applied to it.

<ODS>dsg.Intune-Windows10-Devices

- This group is a dynamic device-based group which is used to store all Windows 10 devices within an organisation.

<ODS>dsg.Intune-iOS-Devices

- This group is a dynamic device-based group which is used to store all Apple devices within an organisation.

<ODS>sg.Intune-Android-Devices

- This group is a dynamic device-based group which is used to store all Android devices within an organisation.

<ODS>dsg.Intune-HoloLens2-Devices

- This group is a dynamic device-based group which is used to store all HoloLens 2 devices within an organisation.

<ODS>dsg.Intune-Android-Shared-Devices

- This group is a shared device-based group which is used to store all shared Android devices within an organisation.

<ODS>dsg.Intune-Apple-Shared-Devices

- This group is a shared device-based group which is used to store all shared Apple devices within an organisation.

<ODS>sg.Intune-Users-Conditional-Access

- This user group is scoped to Conditional Access Policies for device compliance, used to limit access to compliant devices and applications

!	**Important Note** All new AAD groups must follow the above-mentioned naming standards.

4.4.4 Intune Policy Naming Standards

The below naming standards should be utilised by Intune LAs when creating policies to ensure that policies are applied properly:

Configuration Policies

- <ODS>-Apple-Shared-[Policy Type/Free text]
- <ODS>-Apple-[Policy Type/Free text]
- <ODS>-Android-[Policy Type/Free text]
- <ODS>-Android-[Policy Type/Free text]
- <ODS>-Windows10-[Policy Type/Free text]
- <ODS>-Hololens2-[Policy Type/Free text]

Enrolment Profiles

- <ODS>-Shared Device-iOSEnrolment-Profile
- <ODS>-iOS-Enrolment-Profile
- <ODS>-Android-Shared Device
- <ODS>-Android-AAD-Shared Device

Apple Business Manager (ABM) Connectors

ABM Token

- <ODS>-ABM-Production

VPP token

- <ODS>-VPP-Token

4.4.5 Device Naming Standards

The below naming standards should be utilised by Intune LAs when naming devices:

!	**Important Note** Intune LAs should be aware that there are no device naming standards for Android devices. This is a limitation in the Intune portal however there has been a feature request that has been logged with Microsoft to implement this feature.

iOS/iPad Single User

- <ODS>-{{DEVICETYPE}}-{{SERIAL}}

iOS/iPad Shared Devices

- <ODS>-SharedDevice-{{DEVICETYPE}}-{{SERIAL}}

MacOS Single User

- <ODS>-MacOS-Firstname-Lastname-{{Serial}}

MacOS Shared Devices

- <ODS>EnrollmentProfileName-MacOS-{{Serial}}

!	**Important Note** Liver service provides an automation to allow the renaming of devices. Customized scripts can be run to establish a device naming convention

Windows 10/11

Device Type	Naming convention
Windows 10/11 Laptop	**<ODS>-L**[Free Chars]
Windows 10/11 Desktop	**<ODS>-D**[Free Chars]
Windows 10/11 Tablet	**<ODS>-T**[Free Chars]

Hololens 2

- <ODS>-HOLOLENS-XXXXXX

!	**Important Note** There is a **15 Character limit** for Windows 10/11 and HoloLens 2 Device Names. The available free characters available is determined by the length of ODS code. E.g., an organisation with a 5-digit ODS code will use a prefix of 7 characters. The ODS code plus the Hyphen (-), Hardware Identifier (L, D, or H) which leaves 8 characters free.

!	**Important Note** There is a need to differentiate between HoloLens 2 devices and regular Windows 10/11 due to different dynamic policies being applied.

4.5 Group Creation Management

!	**Important Note** LAs are now also able to manage their groups from the NHS portal. Please see the attached link for more information

Intune LAs at all onboarded organisations can create and manage Groups themselves without requiring write access to Azure AD.

The NHSmail Intune Security Group Management App allows Intune LAs granular control over the creation, editing and deletion of their organisation's groups within Intune and permits Intune LAs to closely and independently manage Groups scoped to their organisation, Group owners and Group members.

Intune LAs will be able to complete the following actions via the Security Group Management App:

- View and Search Groups: Intune LAs will be able to view and search all Groups assigned to the scope tagged ODS code in Intune.
- Create Groups: Intune LAs will be able to create Groups for users and Win 10 devices (excluding dynamic groups).
- Edit and Delete Existing Groups: Intune LAs will be able to edit and delete existing Groups and will be able to view Group owners and members.
- Add and Remove Group Members: Intune LAs will be able to add and remove Group members for user groups and Win 10 device groups including with a csv. File and add and remove members to the organisation's Intune Administration Group.

!	**Important Note** Intune LAs are not be able to do group creation or management through the native Intune portal.

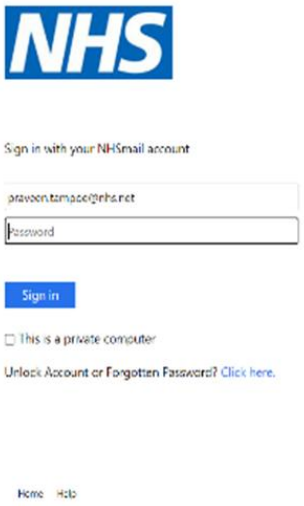
!	**Important Note** Intune LAs should be able to sign into the Security Group Management App with SSO if they are logged into their NHSmail account.

The following sections will provide a step-by-step guide to accessing and using the application for the first time, provide key information on what to expect when using the applications and detail how to give a new admin access to the application.

4.5.1 How to access the Security Group Management App (First Time)

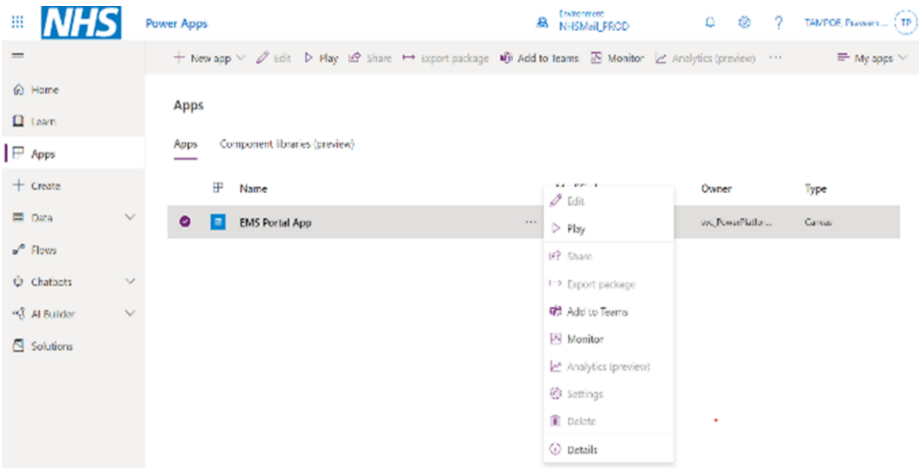
To begin using the application, please follow these steps the first time you try to access the app:

1. Ensure you are logged into NHSmail Portal using your nhs.net credentials.

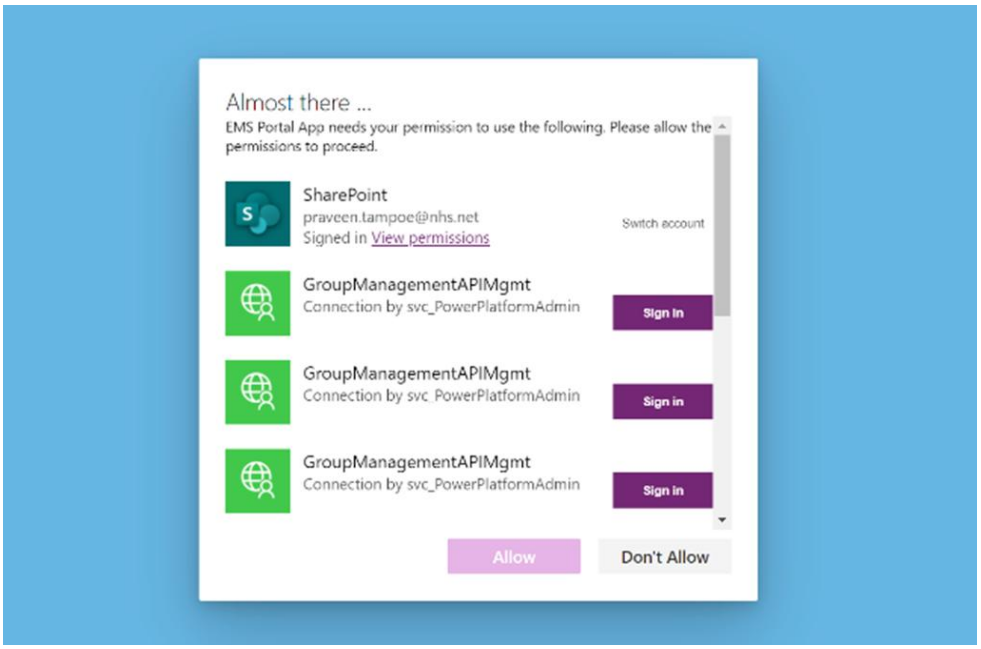


2. Go to the following link: https://make.powerapps.com/environments/762c3051-5c30-48ed-adde-537f357687dd/apps

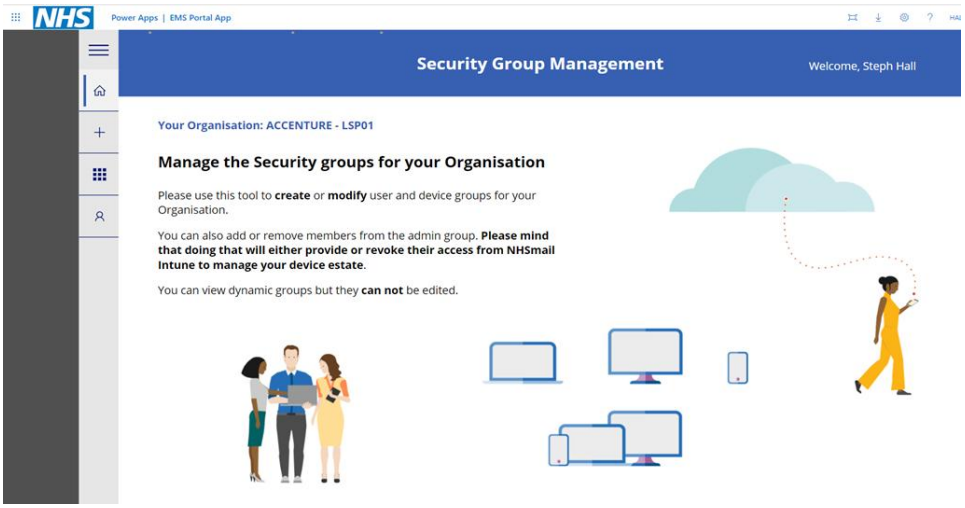
3. Select the three dots next to the EMS Portal app and select **Play**.



4. Select **Sign in** next to one of the GroupManagementAPIMgmt connections and then select **Allow**.



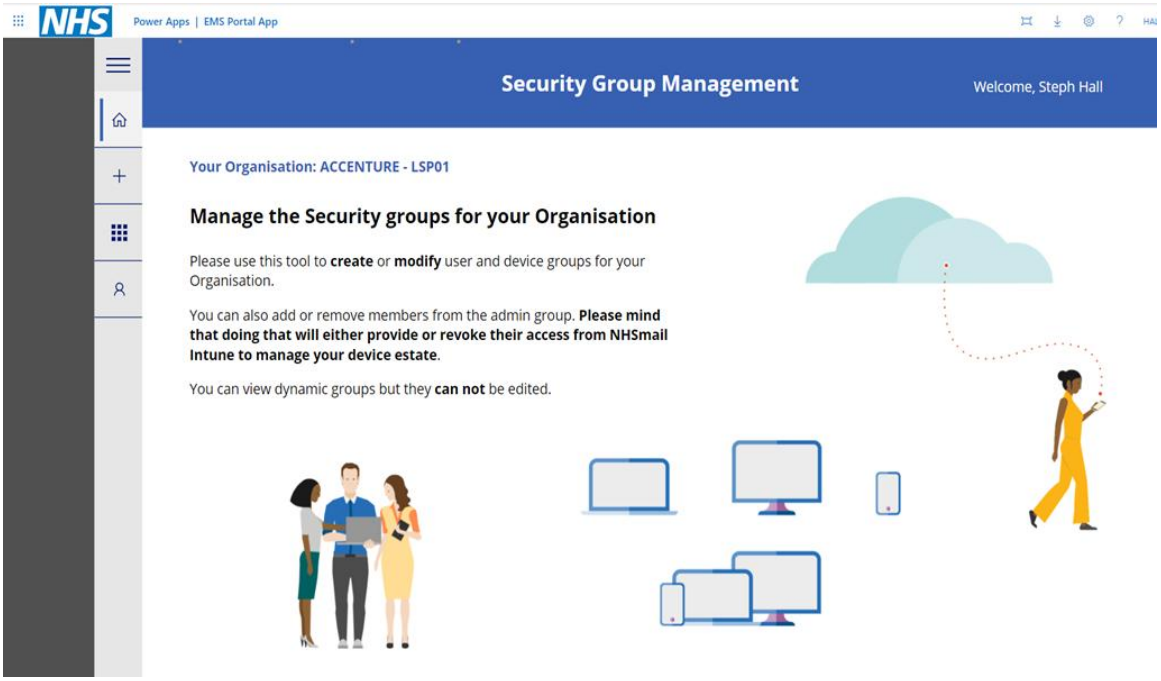
5. Once you have successfully accessed the application you will see the below screen. For all future use of the application, you will not be required to complete steps 1-4. If you are logged in via your nhs.net credentials, you will be able to access the app directly via the link: https://make.powerapps.com/environments/762c3051-5c30-48ed-adde-537f357687dd/apps



4.5.2 Providing Access to new admins

To provide a new admin with access to the Security Group Management app, please follow the below steps:

1. Navigate to the application using this link: EMS Portal App – Power Apps
2. Select the grid toggle to view all groups.



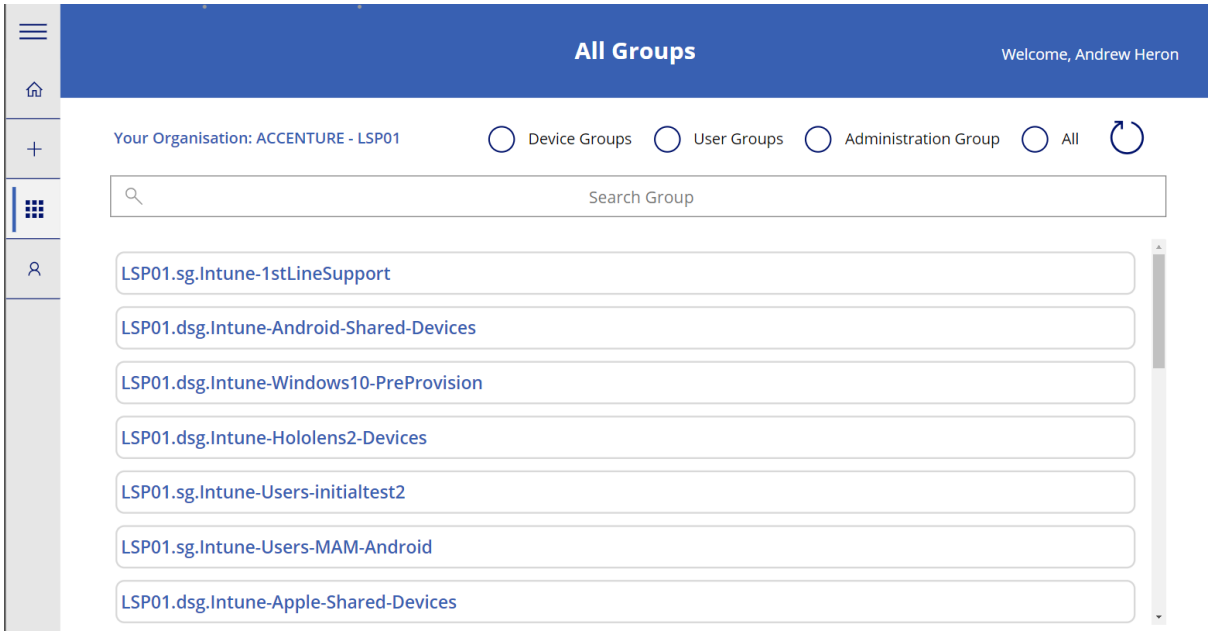
3. Filter for your Intune Admin Group by selecting the circle next to ‘Administration Group’.
4. Select the group.
5. Select **Add**.
6. Consent to proceeding.
7. Confirm that **Group Members** is selected.

8. Search for the admin using the find items box.
9. Select the admin.
10. Select **Add**.
11. Wait for approximately **30 minutes** for the new admin/s to get access to the application.
12. Ask all new admins to follow the instructions detailed in EMS (Intune) 1st Line Support Role.

4.5.3 Using the Security Group Management App

Please see below for important information which should be borne in mind by all users of this application:

- When using the application, Intune LAs at large organisations can expect to wait for approximately 60 seconds per 30,000 users retrieved by the app.
- When opening Groups with a high number of members, Intune LAs can expect to wait 60-120 seconds for the app to retrieve all members of the Group.
- When creating a new Group, the new Group can take around 60 seconds to appear. Intune LAs are advised to use the refresh button on the 'All Groups' page during this process:



- When uploading a large .csv file (30,000 users or more for example), Intune LAs can expect this to take 1-2 hours to finish processing.
- When uploading .csv files, please use the template provided within the application.

Important Note

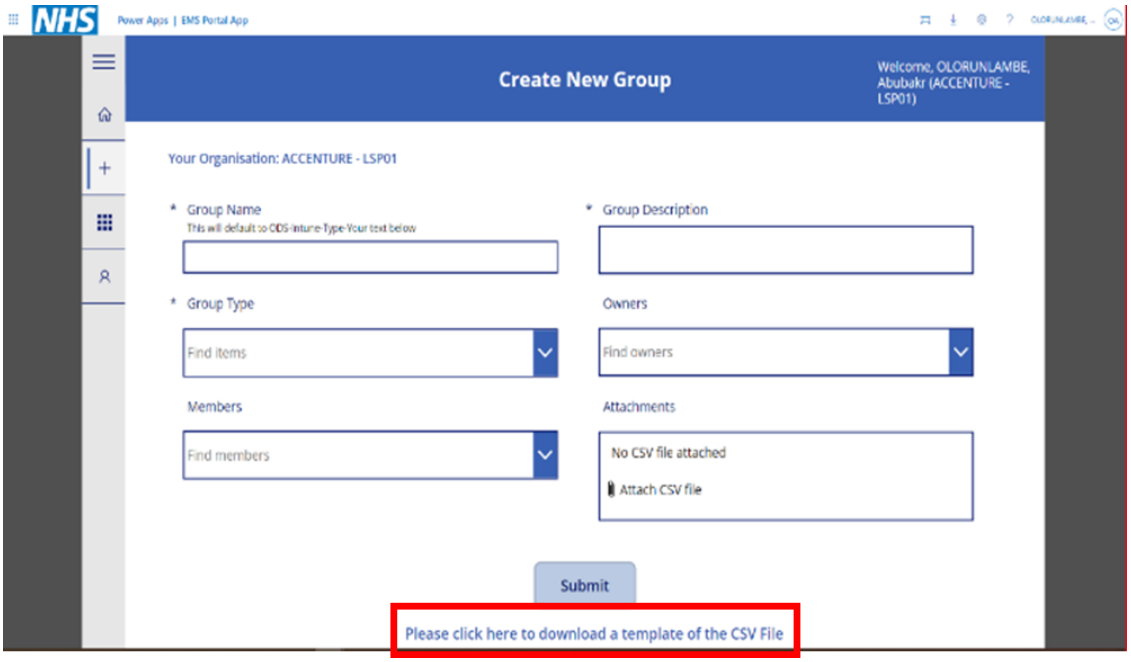
Intune LAs do **not** have the ability to create dynamic groups using the Security Group Management App.

If an Intune LA wishes to create a dynamic group for their organisation, they should raise a service request using Helpdesk Self-Service.

Important Note

When uploading a .csv file of user's email addresses, Intune LAs need to ensure that there are **no spaces in the cells containing each email address**. Each cell should contain only the characters of the email address.

Any spaces, either before the email address of after, will be counted as characters by the app. The app will fail to identify the information in the cell as an email address if there are too many characters and will not add the user's email to the group.



Important Note

If you've managing a multi org then you will need to log into that particular domain account to access the AAD that belong to the child org.

Important Note

The device groups created during onboarding **should not** be modified through the Security Group Management App.

Important Note

Any groups created should be assigned to the scope tag ODS code in NHSmail Intune.

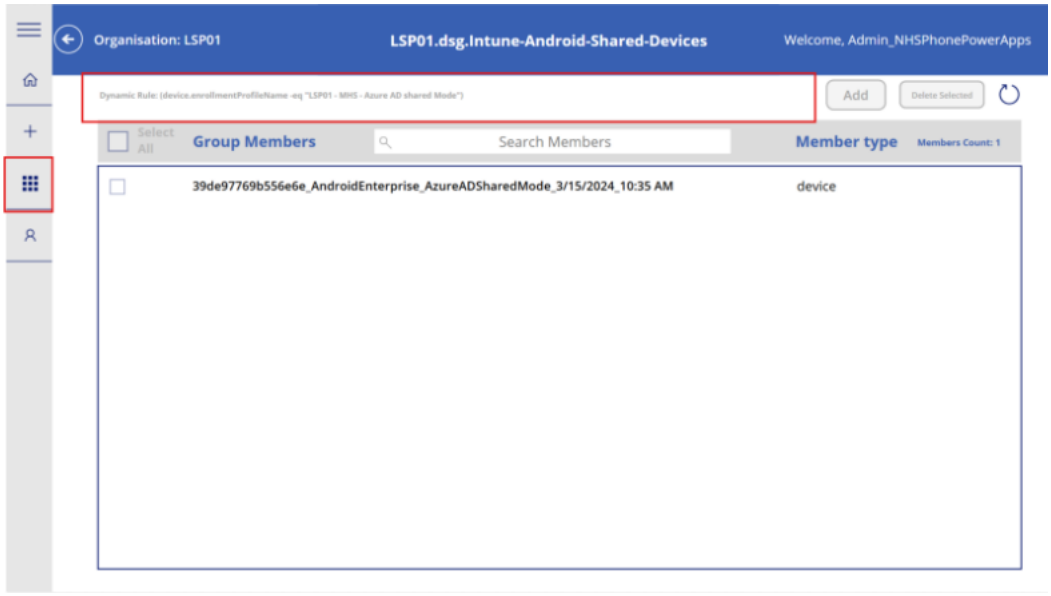
Managed Centrally

The NHSmail Intune Security Group Management App is managed centrally. Intune LAs who encounter any issues accessing and/or using the application should raise an Incident ticket via Helpdesk Self-Service (option: Intune Group Management Tool).

4.5.3.1 Viewing dynamic rules

LAs are unable to create dynamic rules from Intune or the PowerApp, but a view of the current dynamic rule in place can be seen from the Devic group Management Tool.#

Navigate to Groups and then select the group in which you wish to query. The dynamic rule will be displayed at the top of the screen in a syntax format.



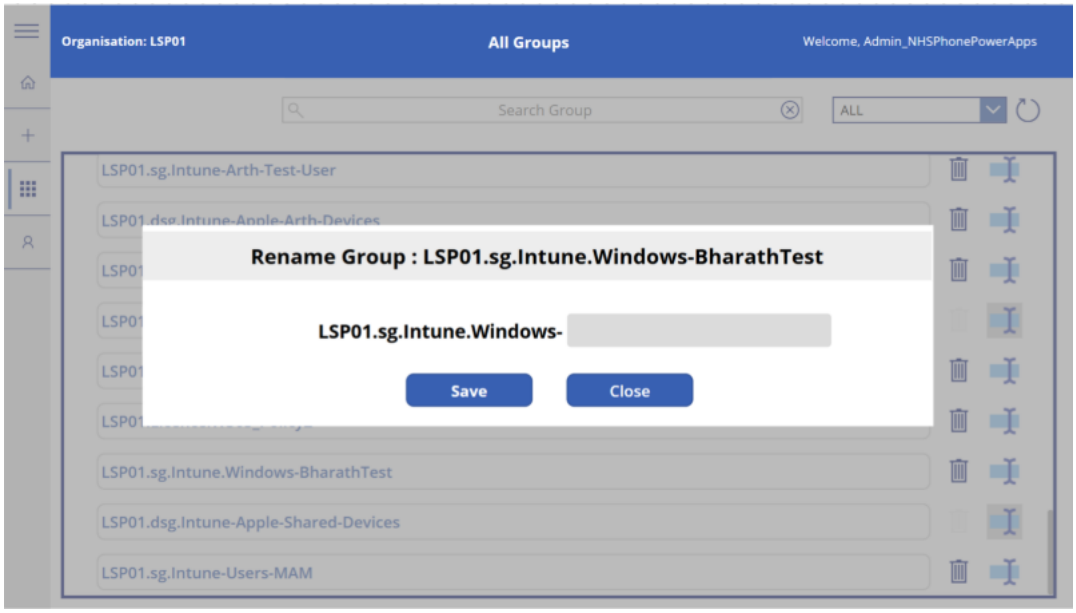
Important Note

All dynamic groups must be requested though a Service Request

4.5.3.2 Group renaming

There is a prefix enforcement to keep the naming standard in place (ODS.DSG.Intune-).

By selecting the cursor icon next to your group displayed in the app, LAs can rename the suffix

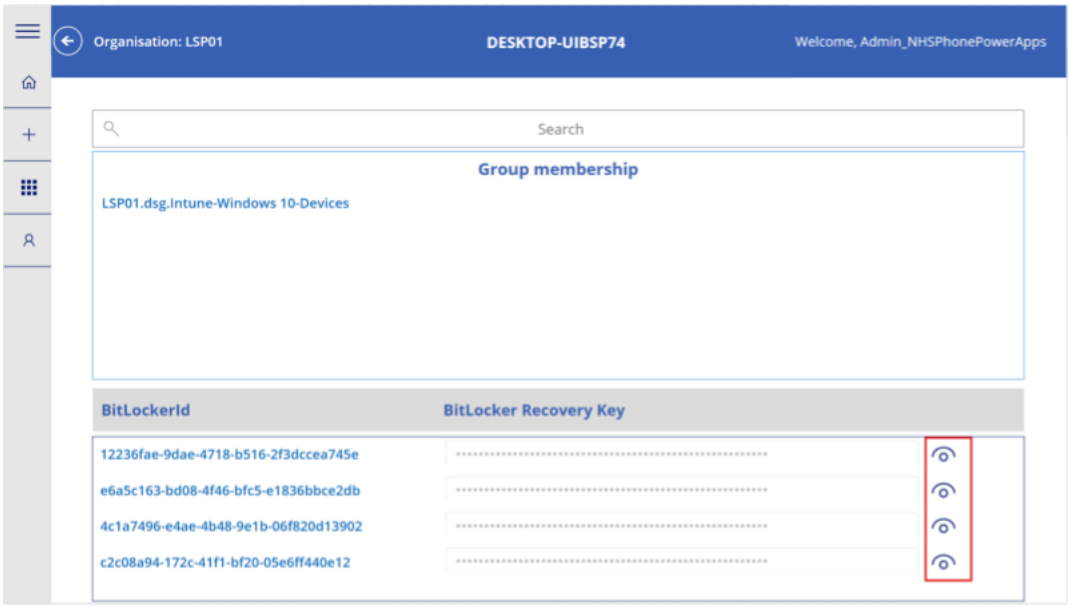


4.5.3.3 BitLocker keys

BitLocker keys do not have an available RBAC role and therefore we are unable to grant access to BitLocker keys in Intune.

As a work around you are able to gather BitLocker Keys for all windows devices from the PowerApp

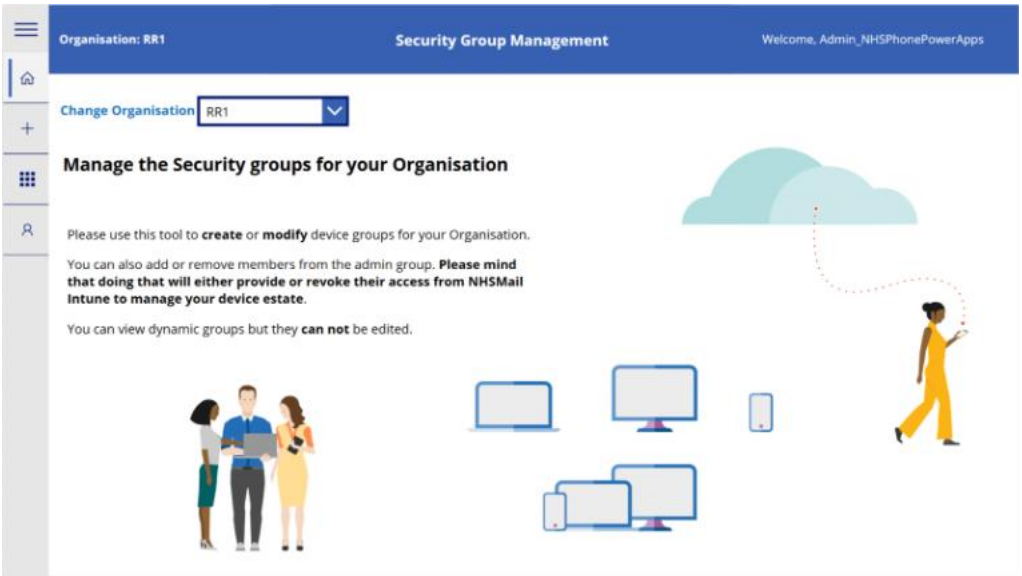
Navigate to All Devices, filter by Windows, select the device and displayed at the bottom of the screen you will see the available BitLocker keys.



4.5.3.4 Multi Org usage

The PowerApp can now support admins of multiple organisations.

Simply browse to the home screen of the PowerApp and from the drop down at the top left, chose the ODS code of the organisation you wish to make changes to.

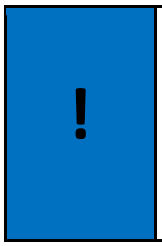


4.5.4 Automated All User Security Groups

Automated all user's security groups are available for organisations onboarded to the NHSmail Intune Service. The automated all user security group will not be available to manage in the Group Management app.

To request that your all user security group is added to your Intune user group, please submit an Intune Service Request via Helpdesk Self-Service (option: Other).

For more information on the automated all users security group, please refer to this link: https://support.nhs.net/knowledge-base/automated-all-users-security-groups/



Important Note

Prior to adding all users security group to your Intune user group, all users **must** be assigned National licence.

If users are not assigned an EMS licence, they will receive an error.

Recommendation / Recommended Use

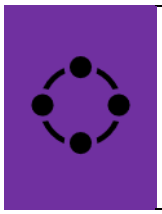
We recommend you utilise all users security groups for Intune if you have a common set of policies amongst users.

If you wish to have different policies for different members of the group, please continue to manage your groups via the Group Management App.

4.5.5 Nested Groups

Nested groups are groups within which are stored multiple subgroups (or child groups). Each nested group is therefore comprised of the parent group and its subgroups. The subgroup/s inherit the attributes and properties of the parent group, saving configuration time.

There are several centrally configured nested groups and some centrally configured policies such as the enablement for automatic enrolment for user devices which are applied to nested groups. Please refer to Central AAD Groups in this document.



Managed Centrally

Intune LAs are not required/or able to edit these groups. These groups are managed centrally and do not require any amendments from Intune LAs.

4.5.6 Intune Policy Assignment Best Practice

This section covers best practice recommendations for Intune LAs using Intune, when assigning policies, settings and using assignment filters.

4.5.6.1 Dynamic vs. Assigned AAD Groups

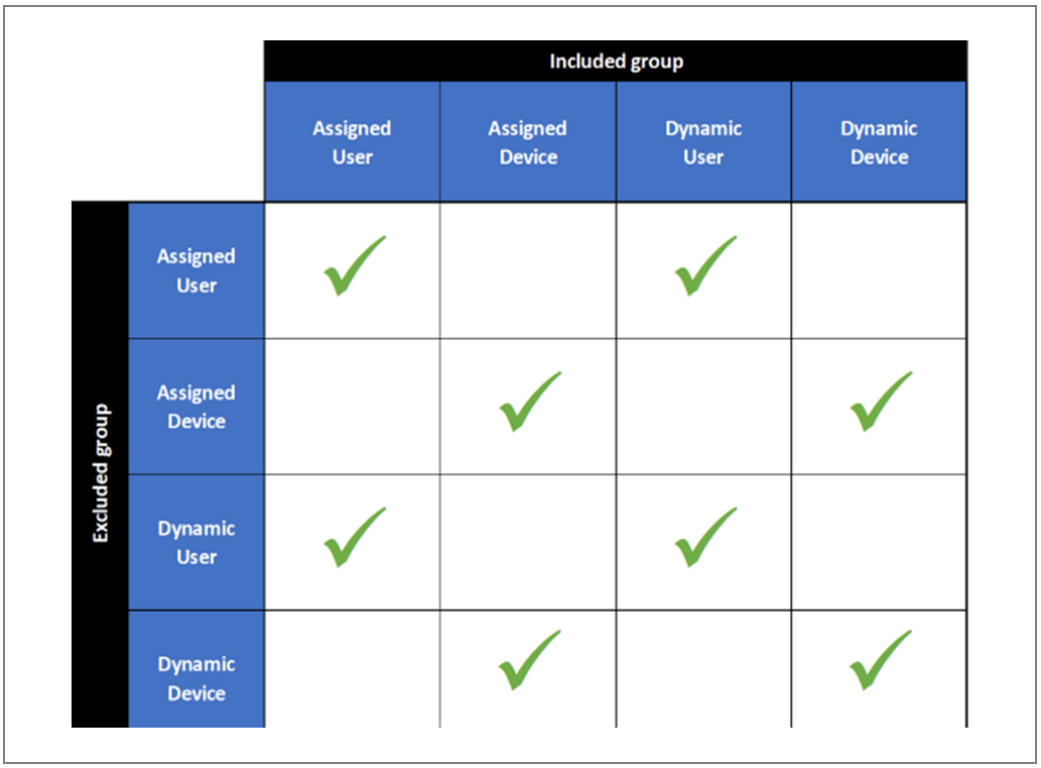
AAD has two primary group types “Dynamic” and “Assigned” (also known as “Static”) groups.

Both assigned and dynamic groups can be used for policy assignments; however, these groups are different (see below) and Intune LAs should become familiar with which type of group to use depending on the specific scenario requiring the assignment of these to policies.

- Assigned groups – Manually add users or devices into a static group.
- Dynamic groups – Automatically add users or devices to user groups or device groups based on an expression you create.

Recommendation / Recommended Use

Policies assigned to a dynamic group may take longer to apply. For time sensitive configurations, it is recommended to use an assigned group.



4.5.6.2 Device Groups

If you want to apply settings on a device, regardless of who is signed in, then assign your profiles to a devices group. Settings applied to device groups always go with the device, not the user.

Critical Notes that will require action

For shared devices, policies will need to be assigned to the device group.

4.5.6.3 User Groups

Profile settings applied to user groups always go with the user and stay with the user when signed into an associated device.

Recommended Use

It is recommended to use user groups for policy and app assignment. Policies and apps assigned to a user group apply immediately, providing a much smoother enrolment process for devices such as Android which may require users to setup a device password.

Critical Notes that will require action

Intune LAs should assign policies to user groups rather than device groups.

4.5.6.4 Exclusion Groups

Exclusions takes precedence over inclusion for policies and apps in the following same group type scenarios:

- Including user groups and excluding user groups.
- Including device groups and excluding device group.

For example, you can assign a device profile to an <ODS>.sg-Intune-Users-Dentistry user group but exclude members in the <ODS>.sg-Intune-Users-Dentistry-Senior Management Staff user group. Since both groups are user groups, All Dentistry users except the Senior Management staff get the profile.

Important Note

Use caution when excluding dynamic device groups from any policy assignment. Consider the latency associated with an Azure AD dynamic device group calculation.

It is not recommended to use dynamic groups for exclusion. It is possible for a device to be assigned a policy even if it has been added to a dynamic AAD exclusion group since dynamic groups do not sync as quickly as an assigned group

Important Note

Intune doesn't evaluate user-to-device group relationships. If you assign profiles to mixed groups, the results may not be what you want or expect.

For example, you assign a device profile to the 'All Users' user group but exclude an All-Android-Devices device group. In this mixed group profile assignment, All users get the profile. The exclusion does not apply.

For more information and support on policy assignment please refer to the below article:

Assign policies in Microsoft Intune

4.5.7 Assignment Filters

Filters allow an admin to narrow the assignment scope of a policy within Intune. As an example, using filters allows you to target devices with a specific OS version or a specific manufacture.

Filters provide the ideal solutions for scenarios such as:

- Deploying a device restriction policy to only iOS devices that are only a part of e.g., the dentistry department.
- Deploying an Android app to only android tablets e.g., in the audiology department users' group.

Filters also provide the following benefits:

- Filters improve flexibility as well as granularity when it comes to assigning Intune policies and apps.
- They are used when assigning app, profiles, and policies, in addition they dynamically target devices that are based on the device properties you entered.
- Can be used and reused on multiple scenarios in 'Include' or 'Exclude' mode.
- Ability to create queries based on the platforms e.g., iOS/iPadOS, Android, Windows 10/11 (in subsequent releases).

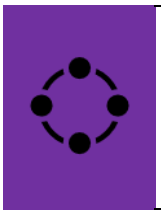
Managed Centrally

Intune filters are controlled and managed centrally. Intune LAs should raise a service request ticket via Helpdesk Self-Service (option: Other) if they require a filter to be created.

4.6 Conditional Access (CA)

Azure Conditional Access provides a means of securing access to Azure services, apps or data based on pre-qualified ‘conditions’ that are prescribed through policies. These Conditional Access Policies are configured by Central Tenant Administrators and applied to all users.

The baseline NHSmail Conditional Access policies apply to Cloud apps and resources, requiring that service access is being performed on a secure & managed device (via Device Compliance).



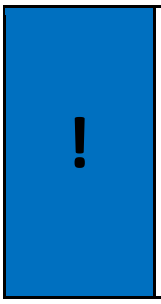
Managed Centrally

Conditional Access policies are managed centrally, so there are no CA policy items to configure for Intune LAs. All Conditional Access policies are created and managed by Central Intune Admins.

Conditional Access is Managed centrally by the EMS team; however, it can be applied by adding users to the following group to enforce conditions such as device compliance:

<ODS>.sg-Intune-Users-Conditional-Access

(This group is nested within a centrally managed parent group that applies the conditional access policy itself)



Important Note

Conditional Access will ultimately block users whose devices do not meet the requirements for a device compliance policy. Before adding users en-masse to Conditional Access (for device compliance), consider introducing and testing user experience with test or pilot users.

The NHSmail Device Compliance policies include periods of ‘grace’ before marking the device ‘non-compliant’, discussed further in following sections.

The following policy is currently provided to support scenarios where organisations are seeking to enforce device compliance, applied across users and their devices in the organisation:

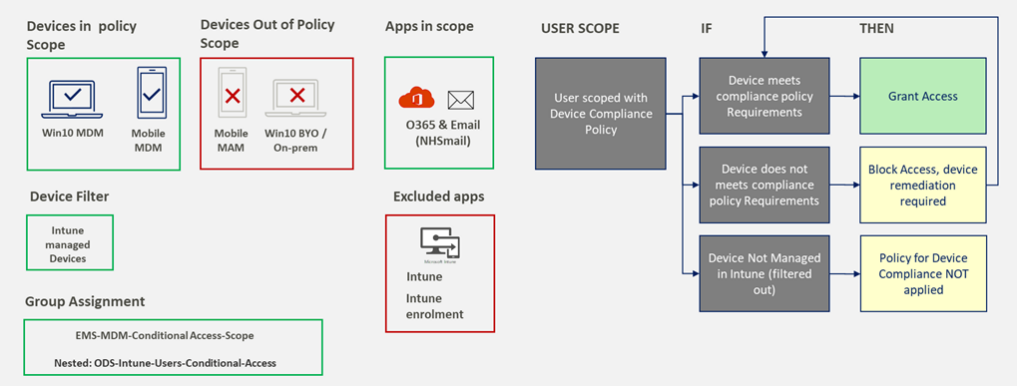


Figure 2: Conditional Access - Device Compliance

The above diagram emphasises that the conditional access policy applies only to devices that are managed via Intune. On-premises (AD) Devices and some Personal Devices may not be enrolled and will be ignored by a policy filter.

The Policy items applied are:

CA Policy	Sub-category	Settings
Assignments	Users and Groups	Include: EMS-MDM-Conditional-Access-Scope
Cloud app or actions	Cloud apps	Include: All cloud apps Exclude: Intune Enrolment

Conditions	Client apps	3 included:
		• Modern authentication clients
		  ○ Mobile apps and desktop clients
		• Legacy authentication clients
		  ○ Exchange ActiveSync clients
		  ○ Other clients

Device Platforms	Include Exclude	Any Device Devices not managed by Intune (e.g. pleBYO)
Grant	Grant Access	**Require device to be marked as compliant**

Conditional Access policies (including the above) are assigned to **user groups only** and not devices, ensuring that access is secured across all devices the user signs in with.

Managed Centrally

Intune LAs who encounter an issue with a Conditional Access policy and/or would like to request an amendment to a policy, should raise a service request via Helpdesk Self-Service (option: Conditional Access).

Important Note

Please note that the device based Conditional Access policy only applies to manged devices and not BYOD/personal devices.

4.7 Device Compliance Policies

Intune compliance policies define the rules and settings which users and devices must meet to be compliant. Intune compliance policies can:

- Include actions that apply to devices that are noncompliant. Actions for noncompliance can alert users to the conditions of non-compliance and safeguard data on noncompliant devices.
- Be combined with Conditional Access, which can then block users and devices that don't meet the rules.

There are two parts to compliance policies in Intune:

Compliance policy settings: Tenant-wide settings that are like a built-in compliance policy which every device receives. Compliance policy settings set a baseline for how compliance policy works in your Intune environment, including whether devices that haven't received any device compliance policies are compliant or noncompliant. These settings are not editable by individual organisations.

Important Note

Compliance policy settings are not editable by individual organisations.

Centralised device compliance policies: Centralised platform-specific rules configure by the NHSMail Central Admin to get deploy to groups of users or devices. These rules define requirements for devices, like minimum operating systems or the use of disk encryption. Devices must meet these rules to be considered compliant.

To see device compliance policy settings:

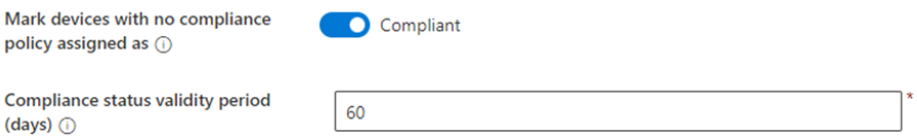
1. Sign into **Microsoft Intune admin Centre**.

2. Navigate to **Endpoint Security > Device Compliance > Policies**.

4.7.2 Central Intune Device Compliance Policy

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

The settings are set as follows:



4.7.3 Centralised Device Compliance Policies

There are 12 default Centralised compliance policies. The below platforms have 3 different Postures with a different level of complexity.

- Windows10 and later
- iOS/iPadOS
- Androids

Shared Apple devices, Shared Android devices and HoloLens 2 devices have one Centralised Compliance policy each.

The available postures for Compliance Policies are:

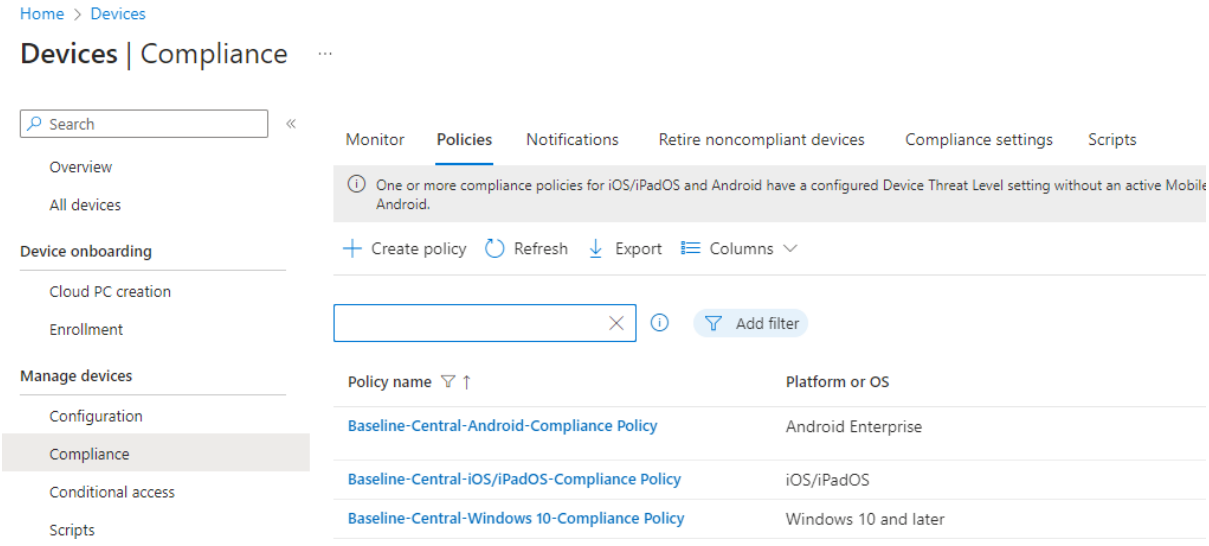
- **Baseline**: provides default compliance settings for simple use cases / test devices.
- **Enhanced**: A more restrictive, but still mainstream posture. Aligns closely to the old model ‘pencilled-in’ configurations.
- **Restrictive**: Provides the most advanced compliance settings for high security/sensitivity use cases.

!	**Important Note** Centralised Device Compliance policies are not editable by the Intune Local admins however they are able to assign /unassign their Organisation Users/Devices groups.

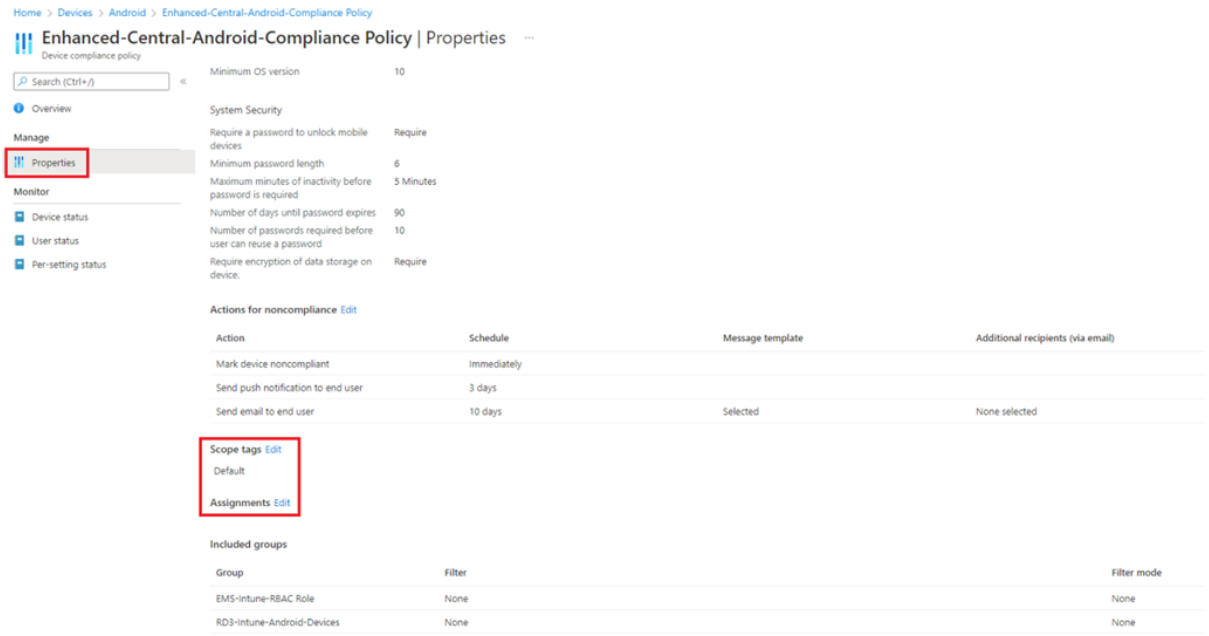
To see the list of the Centralised compliance policies, follow the steps below:

1. Open Microsoft Intune Admin Center
2. Select Devices > Compliance
3. Select the Policies tab

4. The lists of the Centralised policies will be displayed as per below:



4. Intune LA can examine and assign a Device or User AAD group to any of these policies by selecting the policy > **Properties** > **Assignments**



5. Centralised policies use the Default as scope tag and can't be modified by Intune LAs. Assignment is the only editable option on a Centralised policy.

!	**Important Note** Intune LAs can assign only their organisation's scoped Groups to a Centralised Compliance policy. Intune LAs can't remove groups that are not scoped to their organisation.

4.7.4 Device Compliance and Conditional Access

Device Compliance policies will mark a device as 'non-compliant' according to the (time) setting configured in the 3 postures. When the user of a device scoped for device compliance signs in – and the device is NOT compliant – user sign in will be blocked and the user will be required to remediate the 'non-compliance' items.

Such items might include 'device password does not meet requirements' and so forth.

It is recommended that organisations initially test the combined assignment of device compliance policies and conditional access prior to mass-population release.

!	**Important Note** Conditional Access policies relate to users (assignment). Device Compliance will be assessed for Intune-managed devices, however users' 'un-managed' devices or personal devices will not be affected)

4.7.5 Centralised iOS/iPad OS Compliance Policies Configuration Settings

These are the configuration settings enabled for each Posture for iOS/iPadOS devices:

Compliance Setting	Policy	Baseline	Enhanced	Restricted
Email				
	Unable to set up email on device	Not Configured	Not Configured	Not Configured
Device health				
	Jailbroken devices	Block	Block	Block
	Require the device to be at or under the device threat level	Not Configured	Not Configured	Not Configured
Device Properties				
	Minimum OS version	iOS 14	iOS 15	iOS 15
	Maximum OS version	Not Configured	Not Configured	Not Configured
	Minimum security patch level	Not Configured	Not Configured	14.x
Microsoft Defender for Endpoint				
	Require the device to be at or under the machine risk score	Not configured	Not configured	Not configured
System Security				

	Required Password to unlock mobile devices	Require	Require	Require
	Simple passwords	Not Configured	Block	Block
	Minimum password length	4	6	6
	Require password type	Numeric	Numeric	Alphanumeric
	Number of non-alphanumeric characters in password	Not Configured	Not Configured	0
	Maximum minutes after screen lock before password is required	Not Configured	Not Configured	Immediately
	Maximum minutes of inactivity before password is required	5 Minutes	2 Minutes	Immediately
	Number of days until password expires	Not Configured	90 days	60 Days
	Number of passwords required before user can reuse a password	5	10	20
Device Security				
	Restricted apps	Not Configured	Not Configured	Not Configured
Action for noncompliance				
	Mark device noncompliant	After 15 Days	Immediately	Immediately
	Send push notification to end user	15 Days	3 Days	Immediately
	Send Email to end user	15 Days	10 Days	5 Days
	Remotely lock the noncompliant device	Not Configured	Not Configured	Not Configured
	Retire the noncompliant device	Not Configured	Not Configured	Not Configured

4.7.6 Centralised MacOS Compliance Policies Configuration Settings

Baseline-Central-MacOS-Compliance Policy: a device must apply the following rules to be considered compliant:

Baseline Compliance Policy	Settings	Value
Device Health	Require system integrity protection	Required
Device Properties		
Operating System Version	Minimum OS version	14.0
	Maximum OS version	N/A
	Minimum OS build version	N/A
	Maximum OS build version	N/A
System Security	**Password**	
	Require a password to unlock devices.	Require
	Simple passwords	Block

	Minimum password length	8
	password type	Alphanumeric
	number of non-alphanumeric characters in password	1
	Maximum minutes of inactivity before password is required	5
	Password expiration (days)	365
	Number of previous password to prevent reuse	5
Encryption	Require encryption of data storage on device	Require
	Firewall	Enabled
Device Security	Incoming connections	Block
	Stealth Mode	Enabled
Gatekeeper	Allow apps downloaded from these locations	Mac App Store and identified developers
Microsoft Defender for Endpoint	Require the device to be at or under the machine risk score	Not configured
Actions for noncompliance	Mark device noncompliant	Immediately
	Send email to end user	Immediately

4.7.7 Centralised Android Compliance Policies Configuration Settings

These are the configuration settings enabled for each Posture for Android devices:

Compliance Setting	Policy	Baseline	Enhanced	Restricted
Microsoft Defender for Endpoint				
	Require the device to be at or under the machine risk score	Not configured	Not configured	Not configured
Device health				
	Require the device to be at or under the device threat level	Not configured	Not configured	Not configured
Google Play Protect				
	SafetyNet Device Attestation	Not Configured	Check Basic Integrity	Check Basic Integrity & certified devices
Device Properties				
	Minimum OS version	8	10	11
	Maximum OS version	Not Configured	Not Configured	Not Configured
	Minimum security patch level	Not Configured	2020-08-01	2022-05-02

Compliance Setting	Policy	Baseline	Enhanced	Restricted
System Security				
	Required Password to unlock mobile devices	Require	Require	Require
	Require Password type	Numeric	Numeric	Numeric Complex
	Minimum password length	4	6	6
	Maximum minutes of inactivity before password is required	5 Minutes	1 Minute	Immediately
	Number of days until password expires	Not Configured	90 days	60 Days
	Number of passwords required before user can reuse a password	5	10	20
Encryption				
	Require encryption of data storage on device	Require	Require	Require
Device Security				
	Intune App runtime integrity	Not Configured	Not Configured	Not Configured
Action for noncompliance				
	Mark device noncompliant	After 15 Days	Immediately	Immediately
	Send push notification to end user	15 Days	3 Days	Immediately
	Send Email to end user	15 Days	10 Days	5 Days
	Remotely lock the noncompliant device	Not Configured	Not Configured	Not Configured
	Retire the noncompliant device	Not Configured	Not Configured	Not Configured

4.7.8 Centralised Windows 10/11 Compliance Policies Configuration Settings

These are the configuration settings enabled for each Posture for Window 10/11 devices:

Compliance Setting	Policy	Baseline	Enhanced	Restricted
Device health				
	Require BitLocker	Require	Require	Require
	Require secure boot to be enabled on the device	Require	Require	Require
	Require code integrity	Require	Require	Require

Compliance Setting	Policy	Baseline	Enhanced	Restricted
Device Properties				
OS version	Minimum OS version	10.0.19042.1645 (20H2)	10.0.19043.1645 (21H1)	10.0.19044.1645 (21H2)
	Maximum OS version	Not Configured	Not Configured	Not Configured
	Minimum OS version for mobile devices	Not Configured	Not Configured	Not Configured
	Maximum OS version for mobile devices	Not Configured	Not Configured	Not Configured
	Valid OS Builds	Not Configured	Not Configured	Not Configured
Configuration Manager Compliance				
	Require the device compliance from configuration manager	Not Configured	Not Configured	Not Configured
System Security				
Password				
	Required Password to unlock mobile devices	Not Configured	Not Configured	Not Configured
	Simple passwords	Greyed Out	Greyed Out	Greyed Out
	Minimum password length	Greyed Out	Greyed Out	Greyed Out
	Require password type	Greyed Out	Greyed Out	Greyed Out
	Maximum minutes of inactivity before password is required	Greyed Out	Greyed Out	Greyed Out
	Number of days until password expires	Greyed Out	Greyed Out	Greyed Out
	Number of passwords required before user can reuse a password	Greyed Out	Greyed Out	Greyed Out
	Require password when device returns from idle state (Mobile and Holographic)	Greyed Out	Greyed Out	Greyed Out
Encryption				
	Require encryption of data storage on device	Require	Require	Require
Device Security				
	Firewall	Require	Require	Require
	Trusted Platform Module (TPM)	Require	Require	Require
	Antivirus	Require	Require	Require

Compliance Setting	Policy	Baseline	Enhanced	Restricted
	Antispyware	Require	Require	Require
Defender				
	Microsoft Defender Antimalware	Not Configured	Require	Require
	Microsoft Defender Antimalware minimum version	Not Configured	Not Configured	Not Configured
	Microsoft Defender Antimalware security intelligence up to date	Not Configured	Require	Require
	Real-time protection	Not Configured	Require	Require
Microsoft Defender for Endpoint				
	Require the device to be at or under the machine risk score	Not configured	Not configured	Not configured
Action for noncompliance				
	Mark device noncompliant	After 15 Days	Immediately	Immediately
	Send push notification to end user	N/A	N/A	N/A
	Send Email to end user	15 Days	10 Days	5 Days
	Remotely lock the noncompliant device	N/A	N/A	N/A
	Retire the noncompliant device	Not Configured	Not Configured	Not Configured

4.7.9 Centralised HoloLens Device Compliance Policy Configuration Settings

These are the configuration settings enabled for HoloLens 2 devices. There are not Posture for these types of devices due to the limit of settings supported on the HoloLens 2 themselves.

Compliance Setting	Policy	EMS-Central
Device health		
	Require BitLocker	Not Configured
	Require secure boot to be enabled on the device	Not Configured
	Require code integrity	Not Configured
Device Properties		
OS version	Minimum OS version	10.0.19041.1144
	Maximum OS version	Not Configured
	Minimum OS version for mobile devices	Not Configured
	Maximum OS version for mobile devices	Not Configured
	Valid OS Builds	Not Configured
Configuration Manager Compliance		
	Require the device compliance from configuration manager	Not Configured
System Security		
Password		
	Required Password to unlock mobile devices	Not Configured
	Simple passwords	Not Configured
	Minimum password length	Not Configured
	Require password type	Not Configured
	Maximum minutes of inactivity before password is required	Not Configured
	Number of days until password expires	Not Configured
	Number of passwords required before user can reuse a password	Not Configured
	Require password when device returns from idle state (Mobile and Holographic)	Not Configured
Encryption		
	Require encryption of data storage on device	Not Configured

Device Security		
	Firewall	Not Configured
	Trusted Platform Module (TPM)	Not Configured
	Antivirus	Not Configured
	Antispyware	Not Configured
Defender		
	Microsoft Defender Antimalware	Not Configured
	Microsoft Defender Antimalware minimum version	Not Configured
	Microsoft Defender Antimalware security intelligence up-to-date	Not Configured
	Real-time protection	Not Configured
Microsoft Defender for Endpoint		
	Require the device to be at or under the machine risk score	Not Configured
Action for noncompliance		
	Mark device noncompliant	Immediately

4.7.10 Centralised Apple-Shared Devices Compliance Policies Configuration Settings

These are the configuration settings enabled for each Posture for Shared iOS/iPadOS devices:

Compliance Setting	Policy	EMS-Central
Email		
	Unable to set up email on device	Not Configured
Device health		
	Jailbroken devices	Blocked
	Require the device to be at or under the device threat level	Not Configured
Device Properties		
	Minimum OS version	iOS 14
	Maximum OS version	Not Configured
	Minimum security patch level	Not Configured
Micorosoft Defender for Endpoint		
	Require the device to be at or under the machine risk score	Not Configured
System Security		
	Required Password to unlock mobile devices	Not Configured
	Simple passwords	Not Configured
	Minimum password length	Not Configured
	Require password type	Not Configured
	Number of non-alphanumeric characters in password	Not Configured
	Maximum minutes after screen lock before password is required	
	Maximum minutes of inactivity before password is required	Not Configured
	Number of days until password expires	Not Configured
	Number of passwords required before user can reuse a password	Not Configured
Device Security		
	Resticted apps	Not Configured
Action for noncompliance		
	Mark device noncompliant	Immediately
	Send push notification to end user	Not Configured
	Send Email to end user	Not Configured
	Remotely lock the noncompliant device	Not Configured
	Retire the noncompliant device	Not Configured

4.7.11 Centralised Android-Shared Devices Compliance Policies Configuration Settings

These are the configuration settings enabled for each Posture for Shared Android devices:

Compliance Setting	Policy	EMS-Central
Microsoft Defender for Endpoint		
	Require the device to be at or under the machine risk score	Not Configured
Device health		
	Require the device to be at or under the device threat level	Not Configured
Google Play Protect		
	SafetyNet Device Attestation	Not Configured
Device Properties		
	Minimum OS version	8
	Maximum OS version	Not Configured
	Minimum security patch level	Not Configured
System Security		
	Required Password to unlock mobile devices	Not Configured
	Require Password type	Not Configured
	Minimum password length	Not Configured
	Maximum minutes of inactivity before password is required	Not Configured
	Number of days until password expires	Not Configured
	Number of passwords required before user can reuse a password	Not Configured
Encryption		
	Require encryption of data storage on device	Require
Device Security		
	Intune App runtime integrity	Not Configured
Action for noncompliance		
	Mark device noncompliant	Immediately
	Send push notification to end user	Not Configured
	Send Email to end user	Not Configured
	Remotely lock the noncompliant device	Not Configured
	Retire the noncompliant device	Not Configured

4.8 Intune Feature Updates and Servicing Schedule

Microsoft issue updates and enhancements to Intune and Azure AD technology in ‘Service Releases’, globally, on a periodic basis. These features will be released into to the NHSmail Intune Tenant, in the new service administration model.

The NHSmail Intune Live Service Team will issue any forward notices of change for organisations to:

- Support readiness for new feature adoption
- Updates to Minimum Operating system requirements for Device Compliance and App Protection Policies
- Plan readiness activities for features or devices that need to be deprecated or removed.

!	**Important Note** Updates to the centrally managed Device Compliance and App Protection policies will be driven by new OS releases and other factors including new policy features required by the solution design.

These forward notices of any changes will be communicated to all Intune LAs at onboarded organisations, as outlined in the NHSmail Intune Terms of Reference (ToR) document:

Any tenant-wide changes affecting every organisation on the NHSmail Intune platform, changes in terms or general notices will be communicated to all onboarded organisations.

These will be communicated to the Intune LAs and it is expected that they will communicate the update as appropriate within their organisation to ensure continuity of service.

!	**Important Note** If additional features, enhancements, or integrations are required for a local organisation, Intune LAs should raise a service request via Helpdesk Self-Service (option: Other) for further assessment by the NHSmail Intune Live Service Team.

4.9 Windows Group Policy Analytics

Group Policy analytics is a feature that lets admins analyse on-prem Group Policy Objects (GPO) and uses Intune to find and replace you on-prem GPOs.

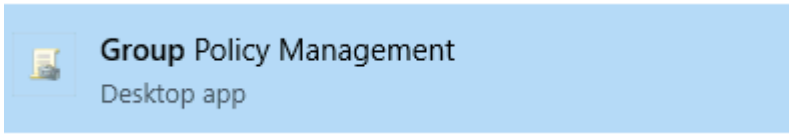
This tool can also be extremely helpful when transitioning from on-prem domain to a cloud only approach for Windows devices. As well as the added benefit of helping in resolving conflicts between Group Policy Objects (GPO) and Microsoft Intune policy, which can arise when migrating devices to Intune.

When you import a GPO, Intune automatically analyses the Group Policy and shows the policy elements that are available as supported configurations as Intune CSP. This works only for policies applicable to Windows 10/11 computers.

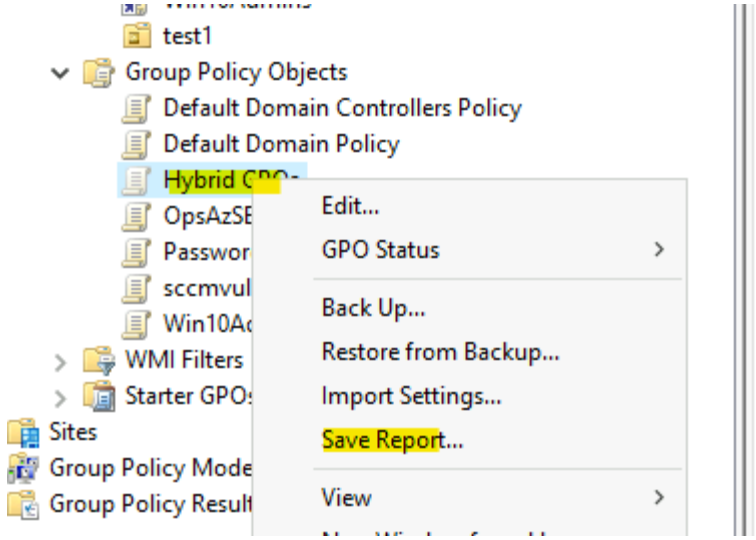
4.9.1 Importing GPOs

1. Export the desired GPOs from the On-Premises Active Directory to a .xml file using GPMC.msc

2. Launch Group Policy Management App

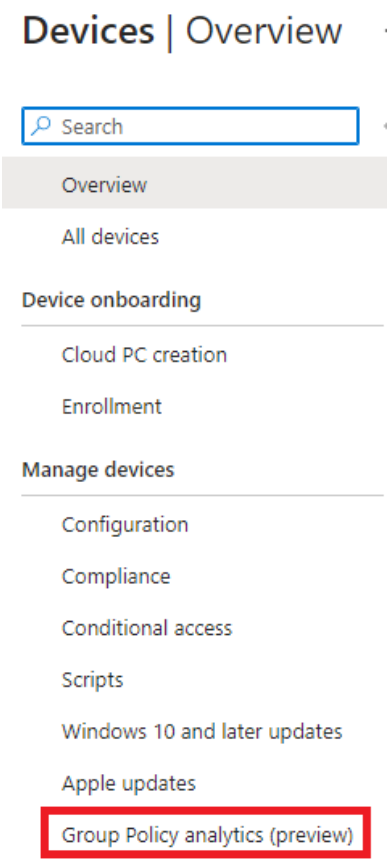


3. Navigate to the Group Policy setting to export. Select right-click on the settings, then select “Save Report” option.

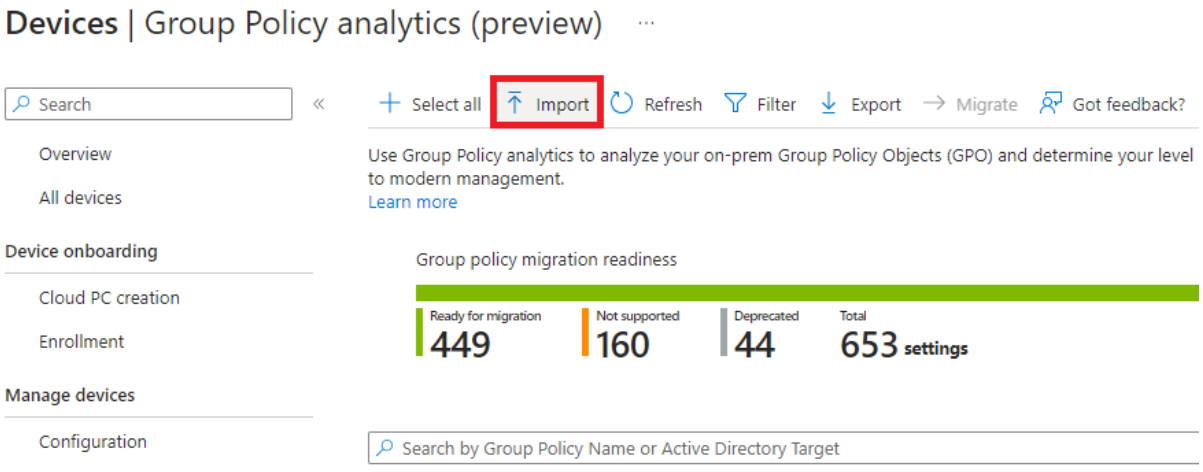


4. Save the file in a location where you can import it to Microsoft Intune.

5. Sign in to https://intune.microsoft.com/. Navigate to Devices > Group Policy Analytics

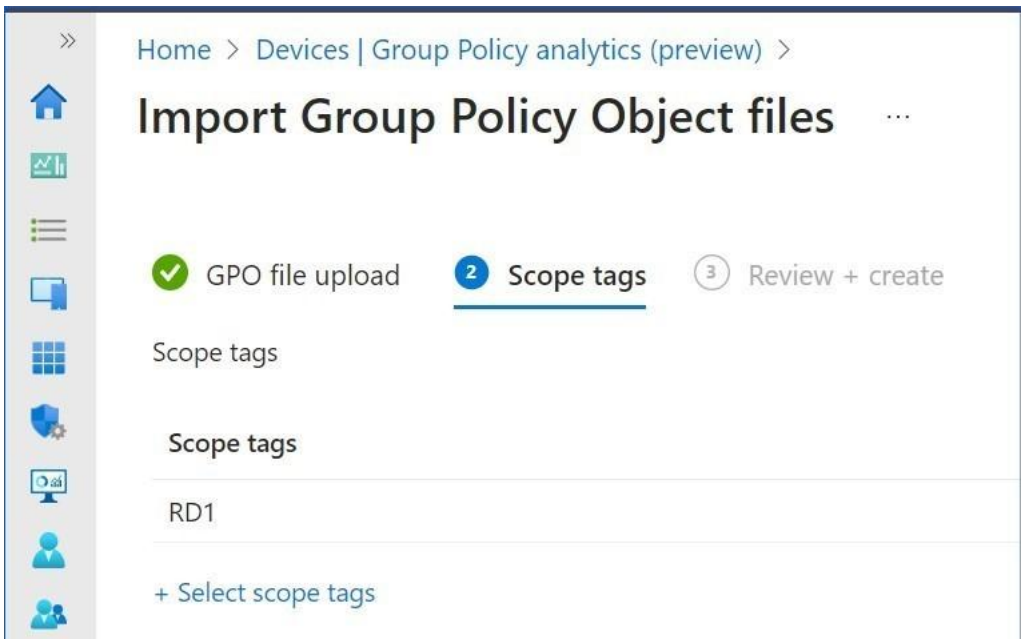


6. Select Import option and select the GPO file (xml) exported in step 1)



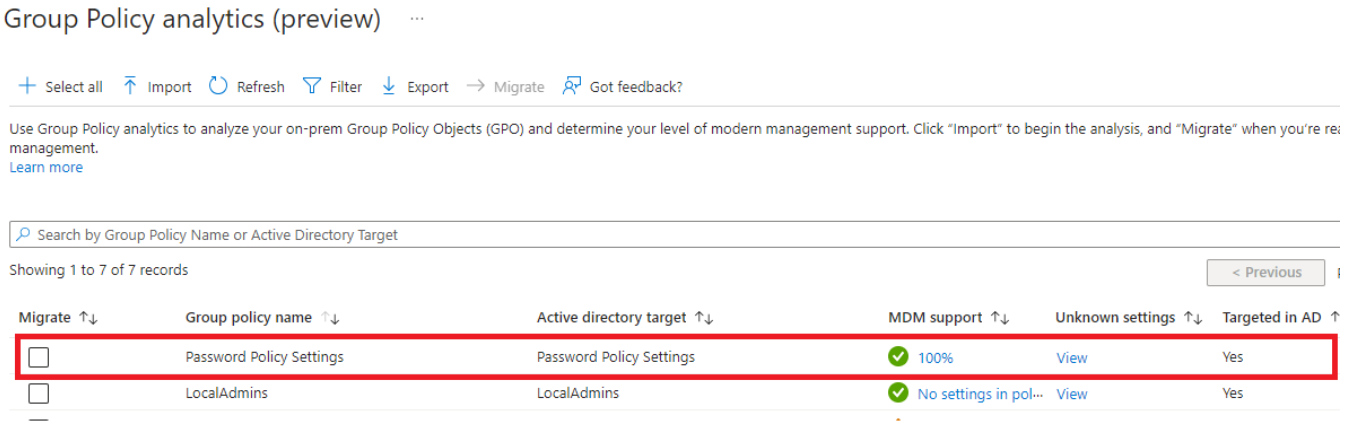
7. Once the file is uploaded, select Next.

8. The scope tag for your organisation is populated automatically. Select Next > Create.



!	**Note:** Scope tags assigned to your organisation are automatically applied when you import the GPOs.

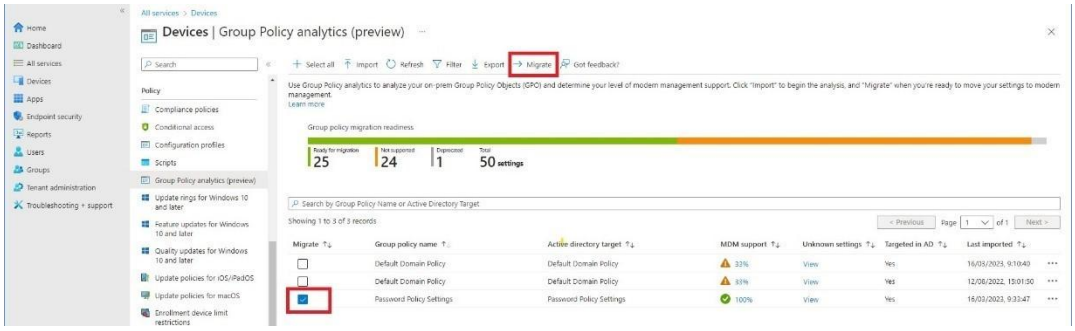
9. The GPO will be listed after the imported is completed.



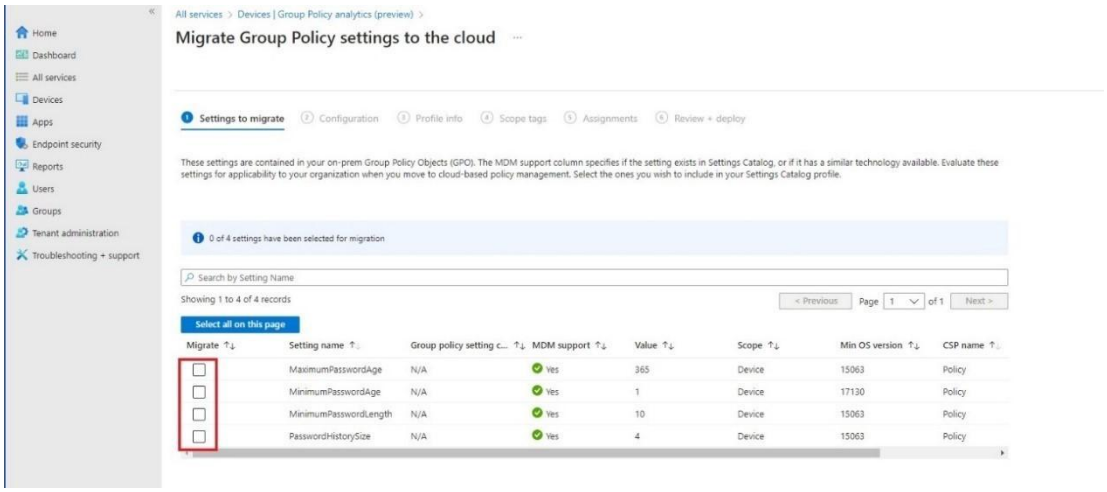
!	**Note:** The percentage under the MDM Support column will automatically update to reflect any changes. Items showing 'MDM Support' warning icons indicate settings that are partially supported via Intune CSP/Settings (or in some cases not at all).

4.9.2 Migrating GPOs

1. To migrate the policy select check the policy to migrate then select the "Migrate" button.

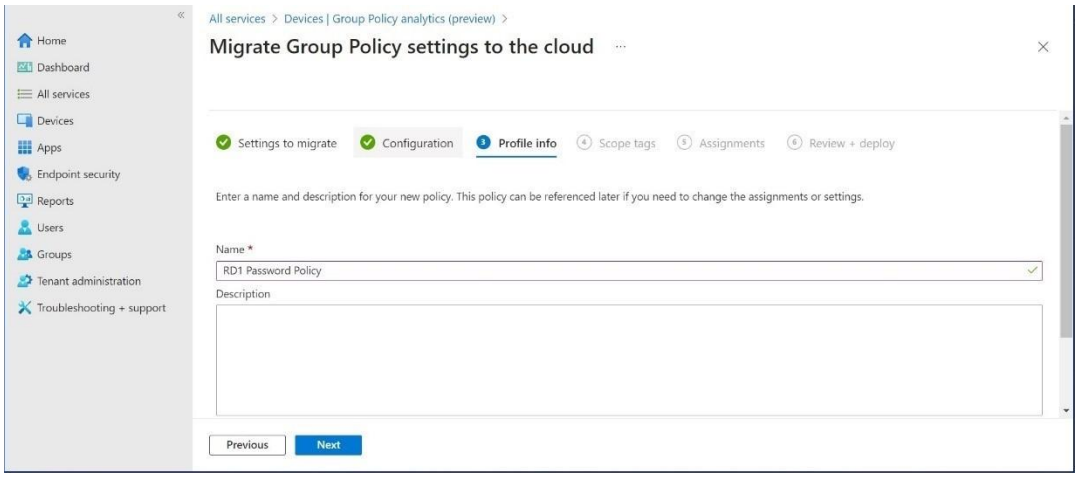


2. Select the settings to migrate. You can see “select all on this page” and all the whole policy will migrate. Click Next

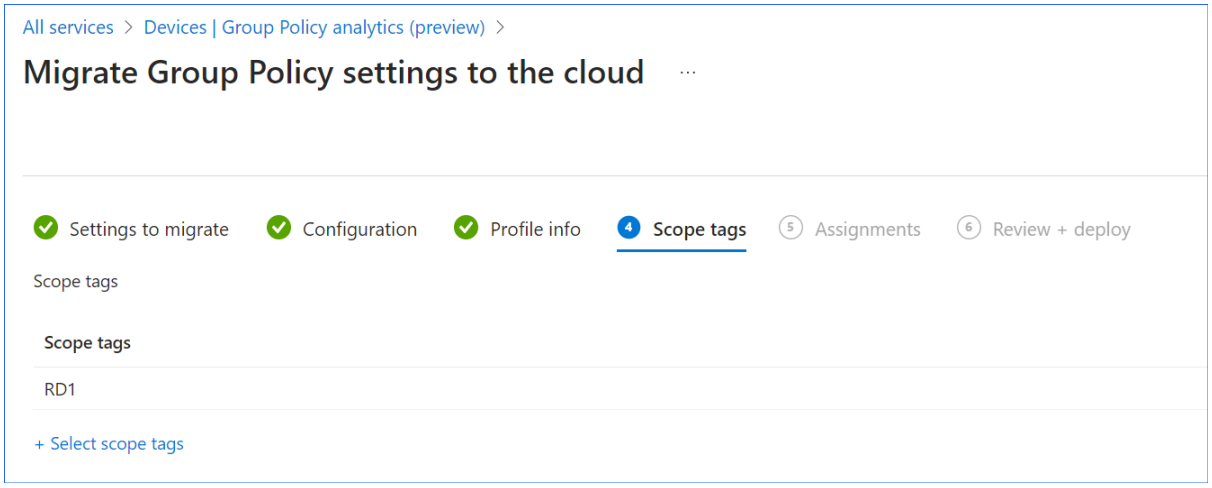


3. The configuration page provides the description and lists all the selected GPO policies from the previous page with the settings of individual policies.

4. Enter the name of the Configuration Profile e.g., “Password Policy” > Next.



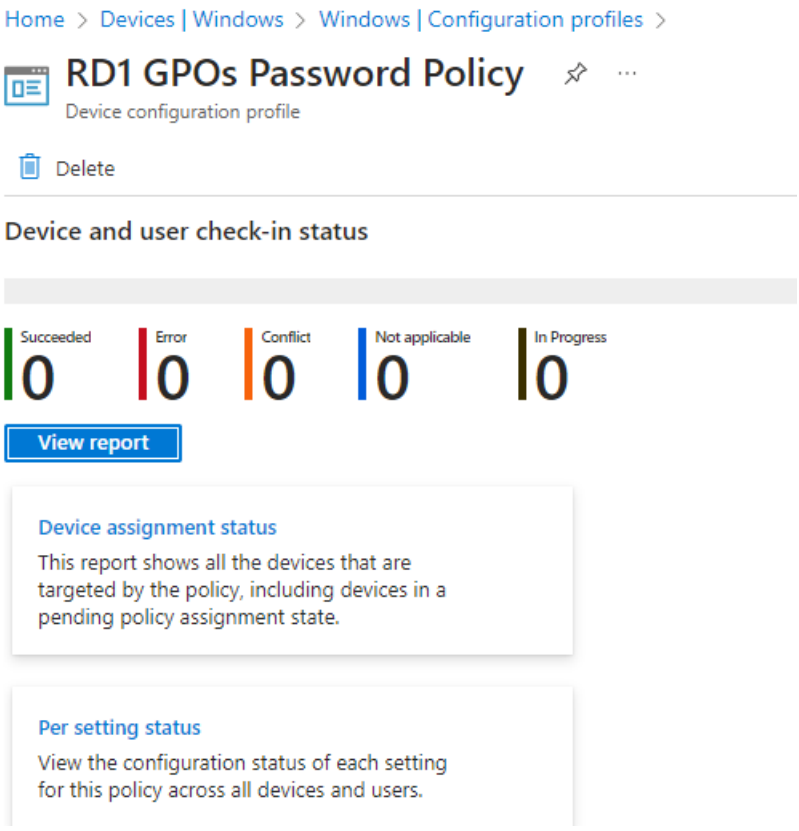
5. The organisation Scope tag is automatically populated to the new profile.



6. Under Assignments, select groups and then choose Select groups to add. Click Next.

7. On the Review + Deploy page, verify, and confirm all the configurations to migrate to Intune. Click on the Deploy button to complete the process.

8. Once the policy is migrated, a new device configuration profile is created.



4.10 Reporting

There are various forms of reporting in the Intune Tenant which allow Intune LAs to monitor all the devices they have enrolled into Intune. Intune LAs can view

reports providing an insight into device compliance, device health and device trends.

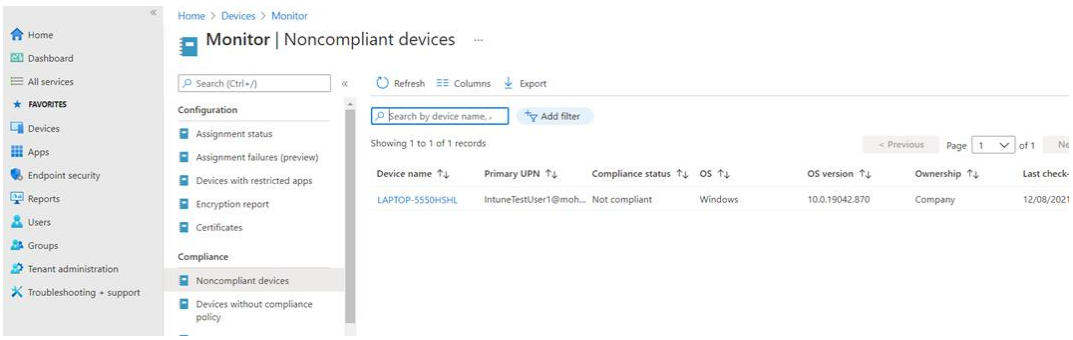
The initial Intune Reporting dashboard view is generic for the tenant and will show an overall summary of all devices within the tenant. However, in the devices page of Intune, Intune LAs can run exports to see the overall number of devices owned only by their organisation.

!	**Important Note** Due to the NHSmail Intune tenant being a single tenant containing multiple organisations, in some monitoring and reporting views, Intune LA can view aggregate data across the tenant (data belonging and pertaining to other organisations). This data is limited in scope and is read-only. The data which may be visible includes: • Device names • UPNs of assigned users Organisations **must** treat any such data as confidential.

4.10.1 Noncompliant Devices Report

To view a report detailing all devices which are noncompliant, please follow the steps below:

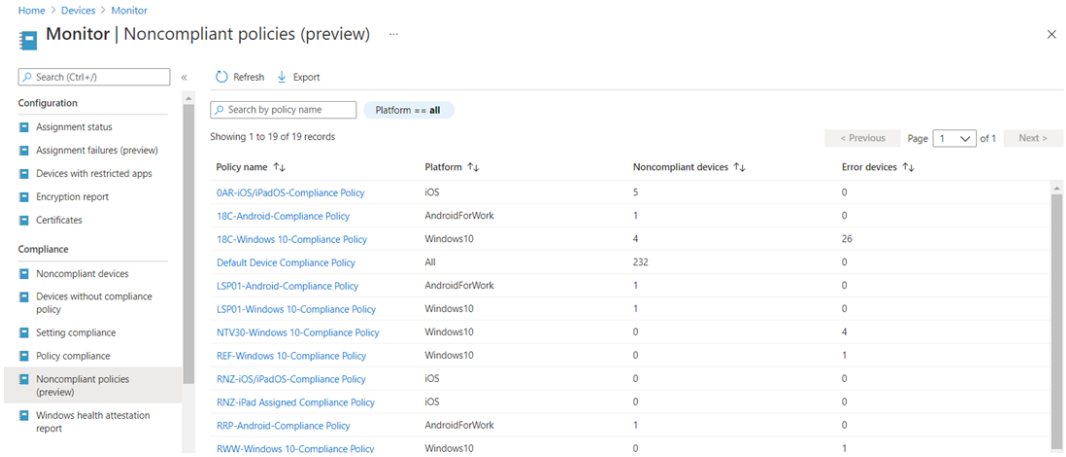
1. Sign into Microsoft Intune admin center.
2. Select **Devices > Monitor > Noncompliant devices**.



4.10.2 Noncompliant Policies Report

Intune LAs can also view reports that will help troubleshoot policies that have conflicts or errors. To view a report detailing all policies that are noncompliant, please follow the steps below:

1. Sign into Microsoft Intune admin center.
2. Select **Devices** > **Monitor** > **Noncompliant policies**.



When an Intune LA generates the report, it will display a list of compliance polices that have an error or devices that have been highlighted as noncompliant. Intune LAs will be able to view specific polices and be able to filter and sort across the various records.

When viewing the report, Intune LAs can select a policy to view device compliance policies applied to devices in a noncompliant or error state.

!	**Important Note** There are various reporting tools under the monitoring section in the Intune Tenant. Below is a link that covers the various tools. Please note: Due to the RBAC roles, not all Intune reporting functionality is available. https://docs.microsoft.com/en-us/mem/intune/fundamentals/reports

4.11 Items created when onboarding

When an organization is onboarded to the shared tenant, the following items will be created automatically.

4.11.1 Groups

- <ODS>.sg.Intune-Admins
- <ODS>.sg.Intune-Users
- <ODS>.sg.Intune-Users-MAM
- <ODS>.sg.Intune-Users-Conditional-Access
- <ODS>.sg.Intune-Android-Devices
- <ODS>.dsg.Intune-Android-Shared-Devices
- <ODS>.dsg.Intune-Apple-Devices
- <ODS>.dsg.Intune-Apple-Shared-Devices

- <ODS>.dsg.Intune-Windows 10-Devices
- <ODS>.dsg.Intune-Hololens2-Devices

4.11.2 Scope tag

A scope tag using the Orgs ODS code will be created, this can be found by going to:

Tenant Administration > Roles > Scope tags

4.11.3 Role assignments

Organisation will have the assignments created in the following RBACs:

- EMS-Global-RBAC-Role:

  This will be assigned to the group <ODS>.dsg.Intune-Admins

- EMS-Trust-RBAC-Role:

  This will be assigned to the group <ODS>.dsg.Intune-Admins

4.11.4 Device configuration profile

The following Windows Device Configuration profile will be created:

- <ODS>-Windows 10 - ATP Defender Trust Tagging

5. iOS /iPadOS and MacOS Enrolment and Management

This section will outline the process Intune LAs will need to follow and complete to successfully enrol an iOS, iPadOS or MacOS device.

It is important that Intune LAs assign all devices to the Intune MDM tenant via ABM before handing them to end users. If devices have not been assigned, end users will be unable to use their devices to complete tasks.

Specifically, this section will cover:

- Centralised configuration profile policies. It is advisable to use them however, custom RBAC roles enable Intune LAs to create, change, amend or remove their own custom configurations for their Organisations.
- What you will need to do to maintain the iOS, iPadOS or MacOS environment.
- The steps to show how groups are assigned to the policies that are in place.

- The naming standards that we have implemented for creating groups and it is advised that you follow.
- How to create configuration profiles with examples.

5.1 Hardware and Software Requirements

Prior to enrolling any iOS or iPadOS devices onto Intune the following minimum Mac, iPhone or iPad specifications should be validated:

- Apple iOS 14.0 and later
- Apple iPadOS 14.0 and later
- Devices reset for use are not currently part of another ABM.

Recommendation / Recommended Use

It is recommended to upgrade devices iOS/iPadOS 14 or later and to ensure devices have the latest security patches. This is also a requirement of the centralized enhanced and restrictive device compliance policies.

5.2 Apple Tokens and Certificates

This section will outline the process Intune LAs will need to follow to create, manage and support Apple tokens.

5.2.1 Apple MDM Push Certificate

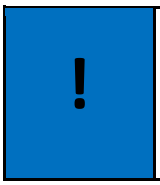
Within the Intune portal you may see the Apple MDM push certificate. Intune LAs do not need to do anything to configure this as this has been configured centrally.

The Apple MDM Push Certificate is a pre-requisite to enable management of iOS and iPadOS via Intune. The certificate establishes a trusted connection between Intune and Apple devices.

Intune LAs can enrol their devices using Device Enrolment Program.

Managed Centrally

The Apple MDM push certificate is managed centrally.



Important Note

The Apple MDM Push certificate and ABM are relevant only to the enrolment of iOS and iPadOS devices.

5.2.2 ABM Connection to NHSmail Intune

All organisations onboarded onto the NHSmail Intune platform, who wish to enrol iOS or iPadOS devices onto the platform will need to ensure that their ABM is linked into NHSmail Intune.

5.2.3 What is Apple Business Manager?

Apple Business Manager (ABM) is the Apple portal that enables enterprises to simplify and automate the bulk management and deployment of corporate-owned Apple devices, including iOS and iPadOS. ABM provides an integration with Intune to allow secure and simplified user enrolment of devices.

To allow users to successfully enrol iOS/iPadOS devices, Intune LAs will need to download the Apple Device Enrolment (ADE) token from the Apple Business Manager (ABM) portal. This token will allow Intune to sync information about the Apple Device Enrolment (ADE) devices that an organisation manages. In addition, the token allows Intune to upload Enrolment Profiles to Apple as well as assign devices to those profiles.

5.2.4 ABM Link Prerequisites

Before linking your organisation's ABM into NHSmail Intune, you should be aware of the following prerequisites:

- Organisations wanting to enrol Apple devices (iOS iPhones and iPadOS iPads) will require those devices to exist in an Apple Business Manager (ABM) instance already.
- Organisations will be needed to associate their vendor management portals with Intune (e.g., connect ABM with NHSmail Intune)

!	**Important Note** Intune Live Service team will support the connecting of ABM to NHSmail Intune, this is an available Service Request once your organisation has been onboarded.

!	**Important Note** • When connecting your organisation's ABM into NHSmail Intune, the Apple ID used to connect into Intune should have **either** the Administrator role or the Device Enrolment Manager (DEM) role assigned to it in ABM.

	• Please do not have both roles assigned to the Apple ID being used to connect into Intune as this may cause a conflict.

- Location terms and conditions should be accepted to enable deployment of applications.
- Domain verification should be pre-configured (if required, Apple does enable the use of a default domain)
- Management of Apple Business Manager (ABM) for iPads and iPhones are to be maintained by LAs (including Apple IDs).
- The NHSmail Intune platform is not supporting the management of any Apple devices which are not enrolled into ABM.
- The NHSmail Intune platform is not supporting the management Apple Configurator.

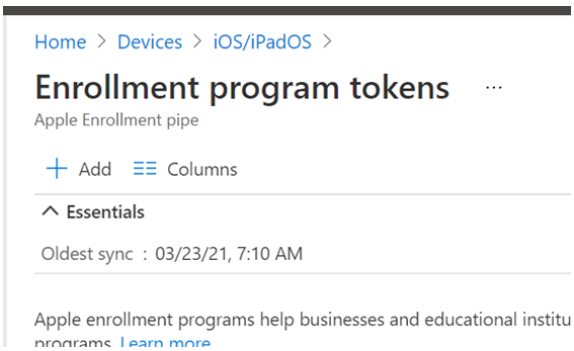
!	**Important Note** When onboarding a Multi Org and you are adopting the Model 2 approach, LAs will need to configure multiple MDM servers within a single ABM tenant which allows the organisation to segregate the devices into “containers”. Info via: Apple – Multiple MDM servers

5.2.5 Linking your ABM to NHSmail Intune

!	**Important Note** Intune LAs must ensure that during the connection process linking your organisation’s ABM and Intune the naming standards shown below are followed for the ADE token: <ODS>-ABM-Production

Please follow the steps below if you wish to link your organisation’s ABM into NHSmail without help:

1. Navigate to the following: **Devices** > **iOS/iPadOS** > **iOS/iPad Enrolment** > **Enrolment Program Tokens**.

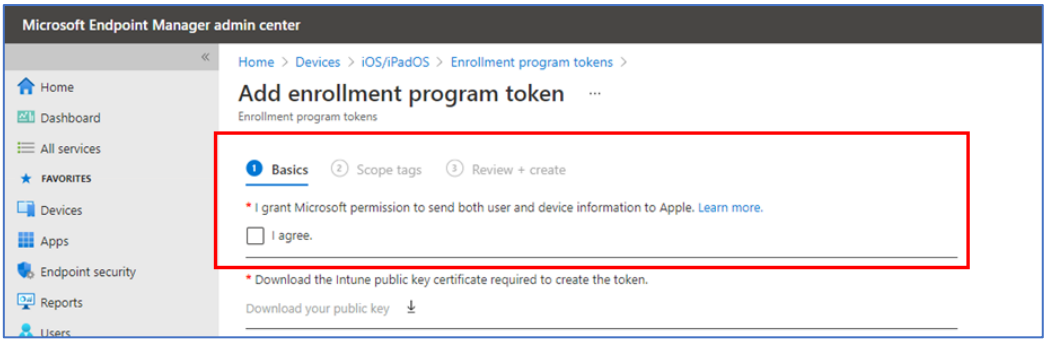


x

Important Note

As part of the Intune and ABM connection, a token exchange process serves as a mechanism to facilitate the connection between the two systems.

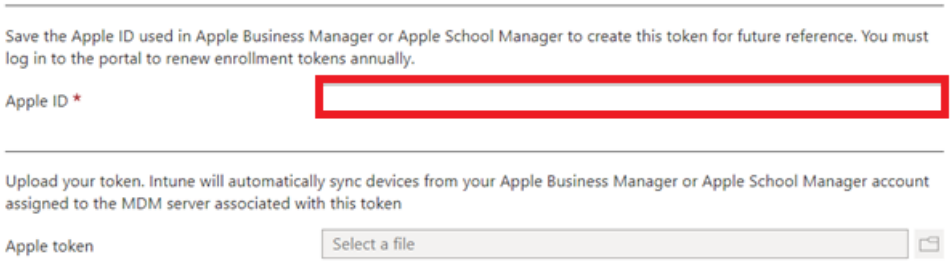
2. Select **I agree** to grant Microsoft permissions and then download the Intune 'Public Key'.



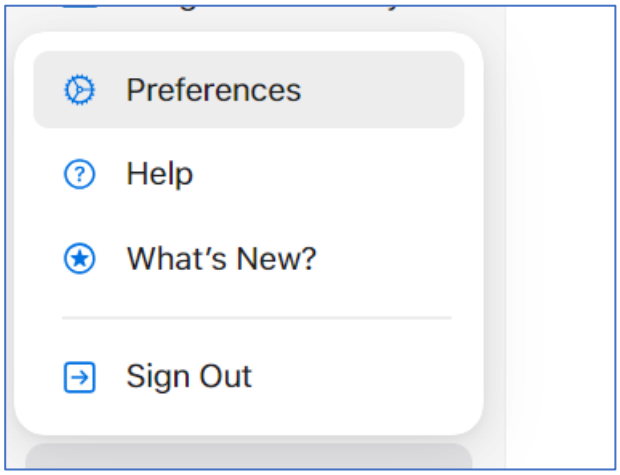
3. Enter the Apple ID from the ABM instance that will be connected.

Recommendation / Recommended Use

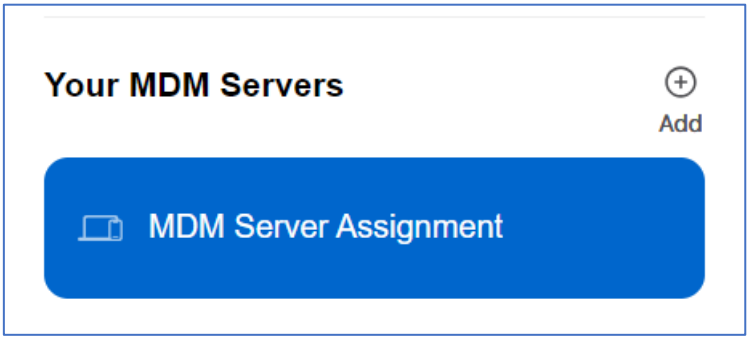
It is recommended that you use a shared Apple ID/mailbox for the connection process. If a shared mailbox is not used, it is still possible to renew the ADE Token via another administrative account within the ABM. If there any issues with renewing the token, Intune LAs should contact Apple Support.



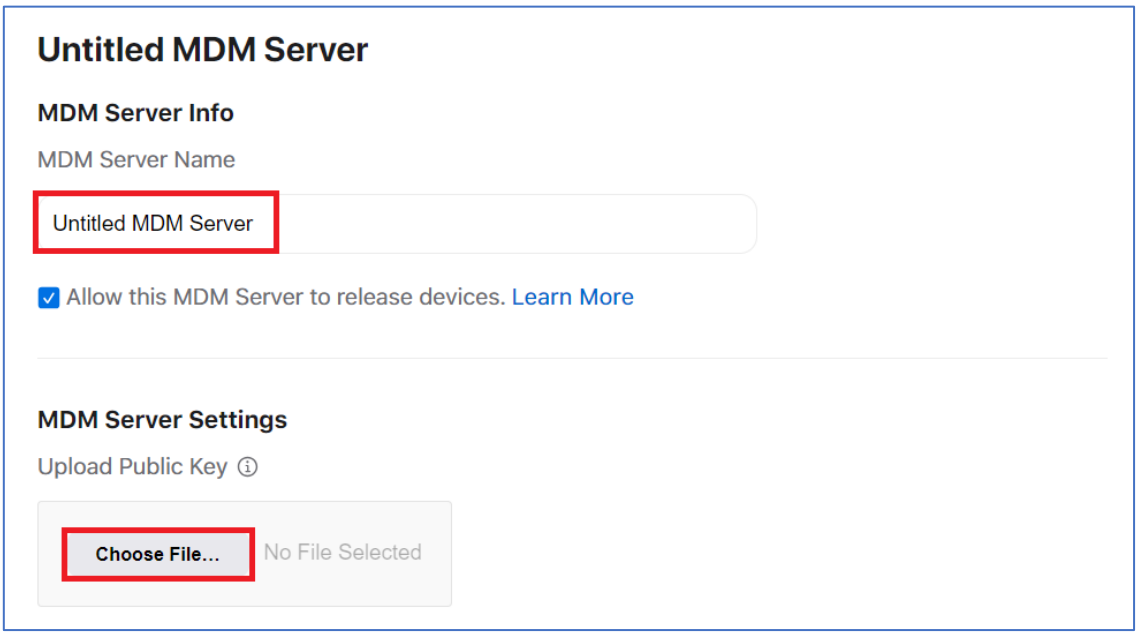
4. Log into the ABM portal and click your Username on the bottom left. Then select **'Preferences'.**



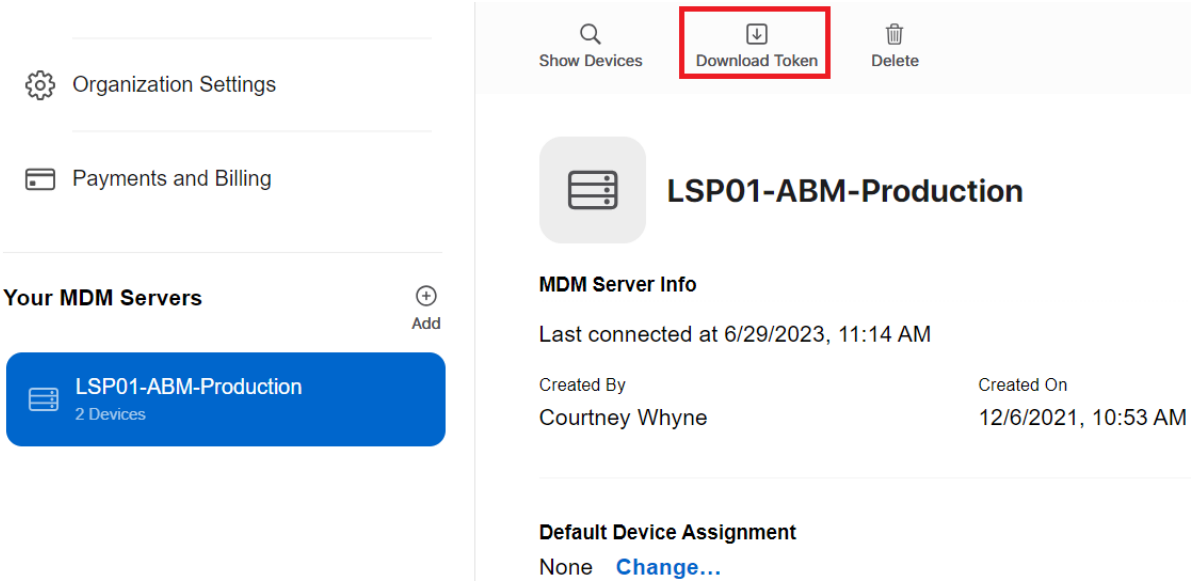
5. In the 'MDM Server Assignment' section, click '**Add'** to add a new MDM server.



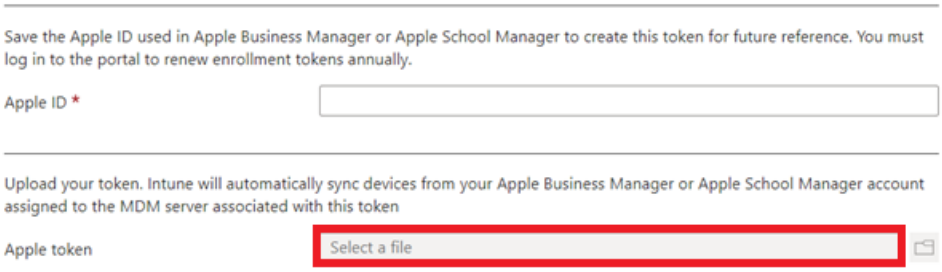
6. Upload Public Key from Intune and give the Server a name: **<ODS>-ABM-Production.**



7. Download the Token from ABM by selecting **Download Token** and then selecting **Download Server Token**.



8. Upload the ABM token file into Intune and then once done click next twice, before finally clicking create.



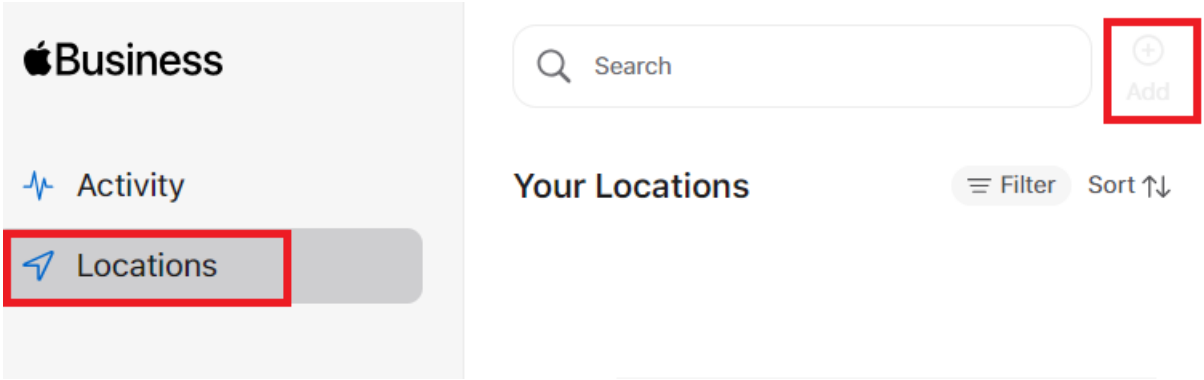
Once this has been completed successfully, you should be able to enrol your iOS or iPadOS devices.

!	**Important Note** When downloading the ADE and VPP token it's best recommended saving this token in a secure location. This will allow you to re-use the token in future should you have issues with the token.

5.2.6 Add A New Location

!	**Important Note** Only one token is needed to manage iOS or iPadOS apps

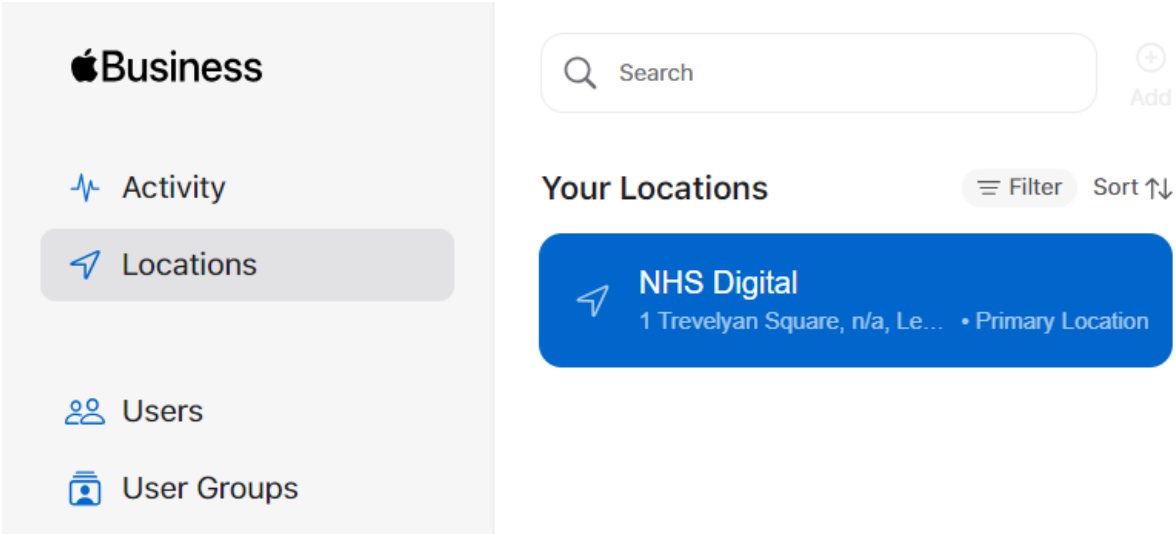
1. Click Locations in the sidebar, then click the Add (+) button.



2. Enter the information for your new location then click **Save**.

You must enter the location name (<ODS>-VPP-Token) and address. Phone number and website URL are optional.

3. Verify that the new location appears in the list of existing locations.



5.2.7 VPP Token Connection to NHSmail Intune

Location tokens are volume purchase licences that were commonly known as Volume Purchase Program (VPP) tokens. Location tokens are used to assign and manage licences purchased using Apple Business Manager. Content Managers can purchase and associate licences with location tokens they have

permissions to in Apple Business Manager. These location tokens are then downloaded from Apple Business Manager and uploaded in Microsoft Intune. Microsoft Intune supports uploading multiple location tokens, from multiple ABM instances. Each token is valid for one year.

Microsoft Intune can help organisations manage apps purchased through the VPP program by:

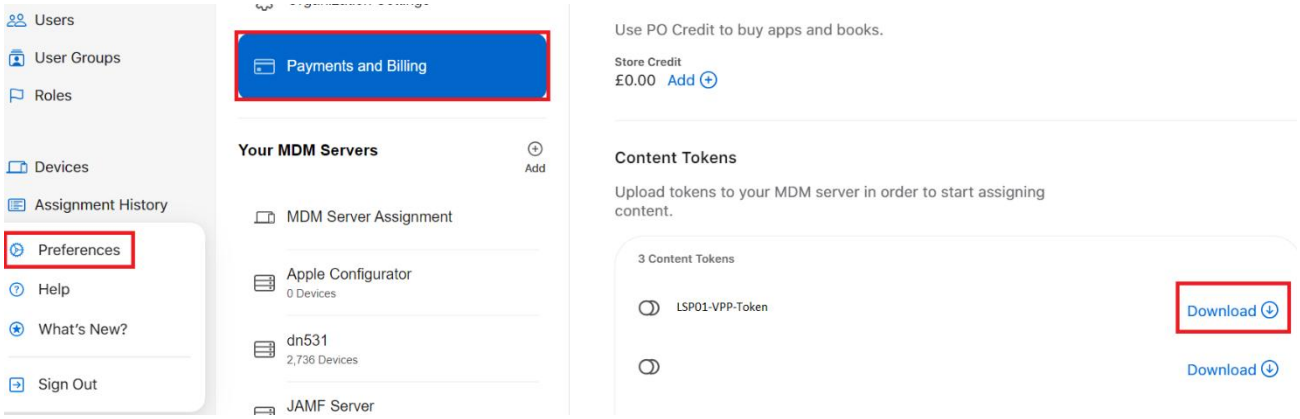
- Synchronizing location tokens that are downloaded from Apple Business Manager.
- Tracking how many licences are available and have been used for purchased apps.
- Monitor app installs up to the number of licences you own.

!	**Important Note** As part of the Onboarding Process a new “Location” must be created in ABM and the VPP token must be added from the organisation’s ABM into Intune. The connection process is a one-time setup. Admins will be required to assign licences to the Company portal app in ABM, to the NHS Intune tenant. This ensure that users can enrol with “User Affinity”.

!	**Important Note** The naming standard show below must be followed when connecting the VPP token to Intune. <ODS>-VPP-Token

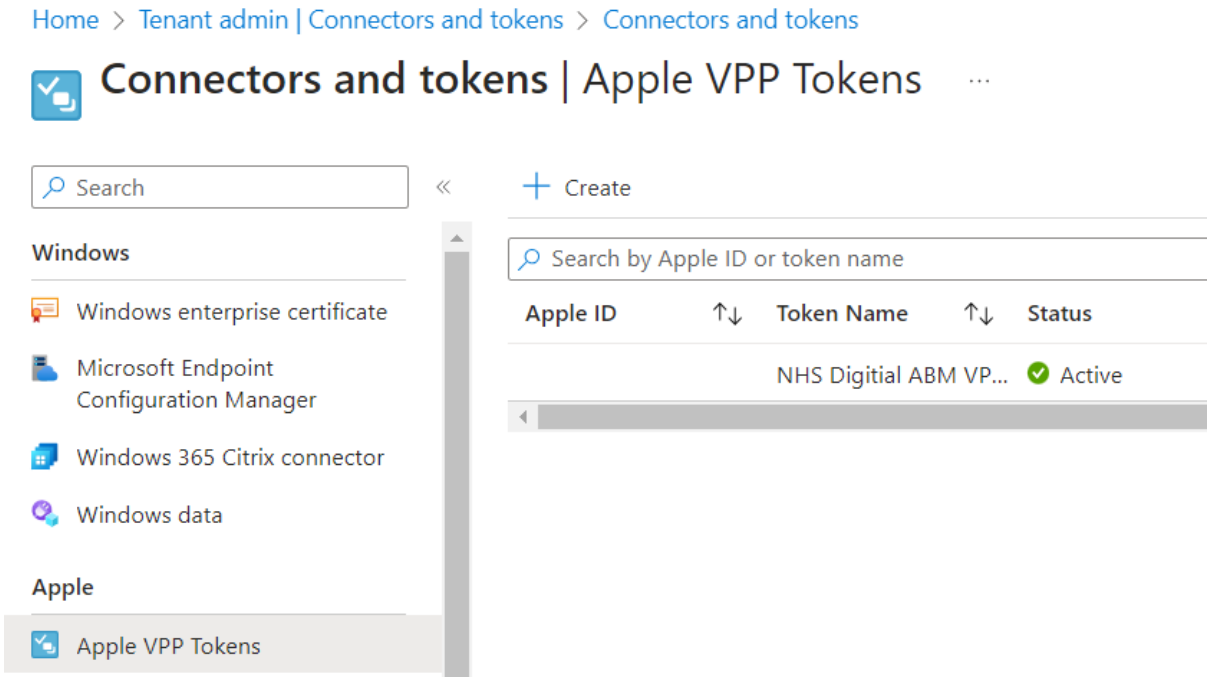
!	**Important Note** VPP tokens expire every 365, It is the LAs responsibility to renew this.

1. In Apple Business Manager, click **Preferences** > **Payments and Billing**. Under **Server Tokens**, click on the new VPP Token to download and save.

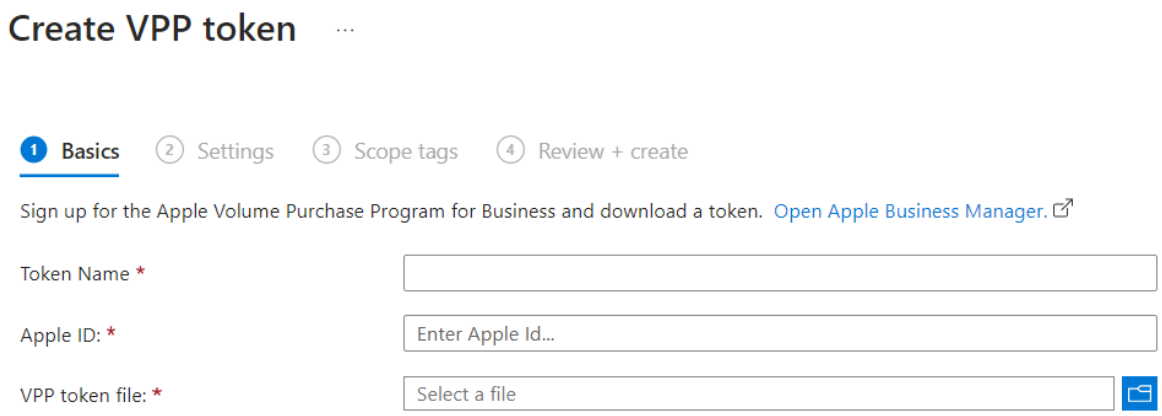


2. In Intune, navigate to: **Tenant Administration > Connectors and Tokens > Apple VPP tokens**.

This will be required to connect your ABM VPP licences into Intune. As part of the enrolment process users must have Company Portal VPP licences available.



3. Select **Create**.



4. **Enter your organisation's name with the correct ODS prefix**, <ODS>-VPP-Token.

4.1.1 The "Apple ID" can be the same Apple ID used to connect your ABM to Intune.

4.1.2 Export a VPP token file from ABM and import into Intune.

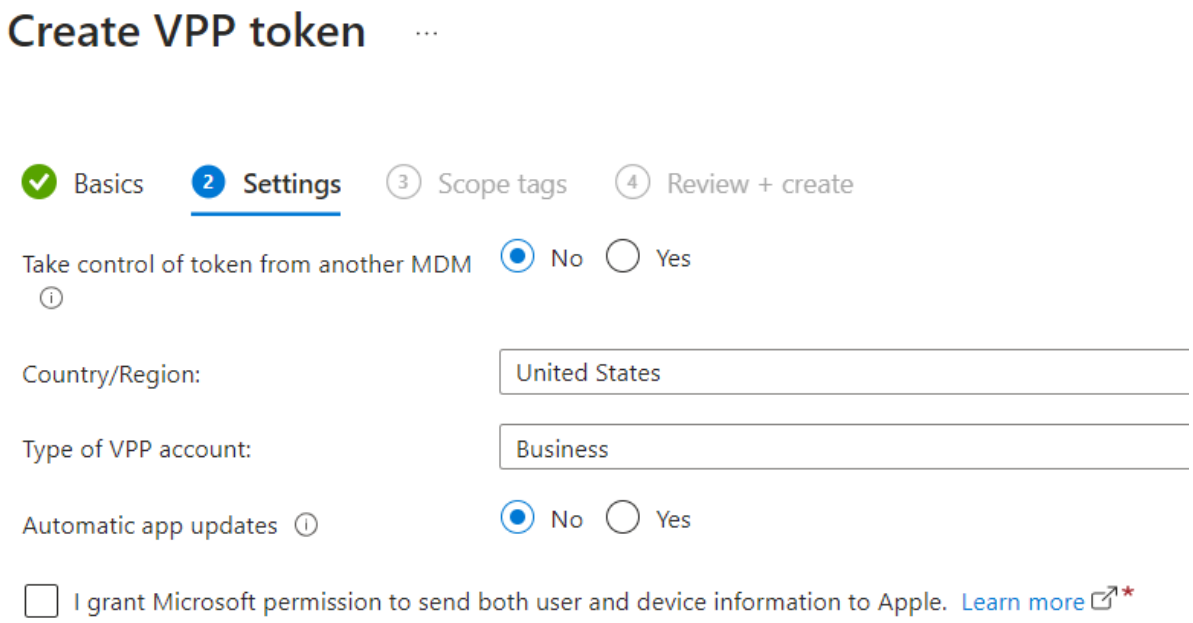
5. Complete the settings page as shown in the example below:

5.1.1 Take Control of token from another MDM = **No**

5.1.2 Country/Region = **United Kingdom**

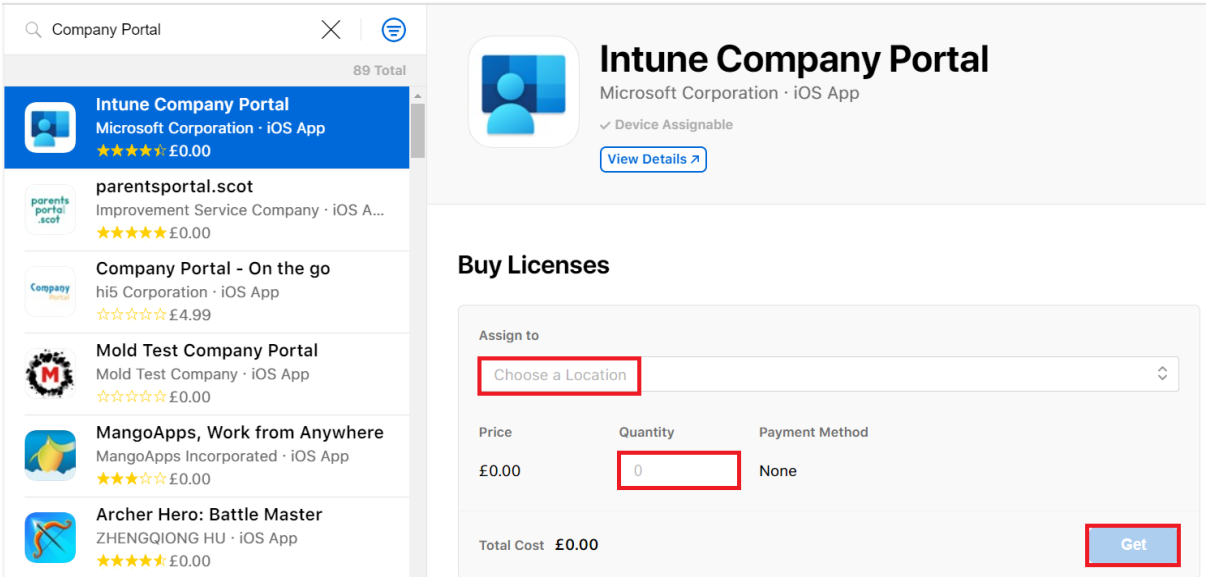
5.1.3 Automatic Updates = **Yes**

5.1.4 Select the tick box to complete the connection process.



6. Assign Intune Portal licence in ABM.

Click on **Apps and books > Search for Intune > Select Intune Company Portal > Choose the new location for Intune > Select Licence quantity > Get**.



5.2.8 Renewing the ABM Token

Critical Notes that will require action.

ABM tokens expire every 365 days. This token will need to be renewed and this is the responsibility of the Intune LAs.

Important Note

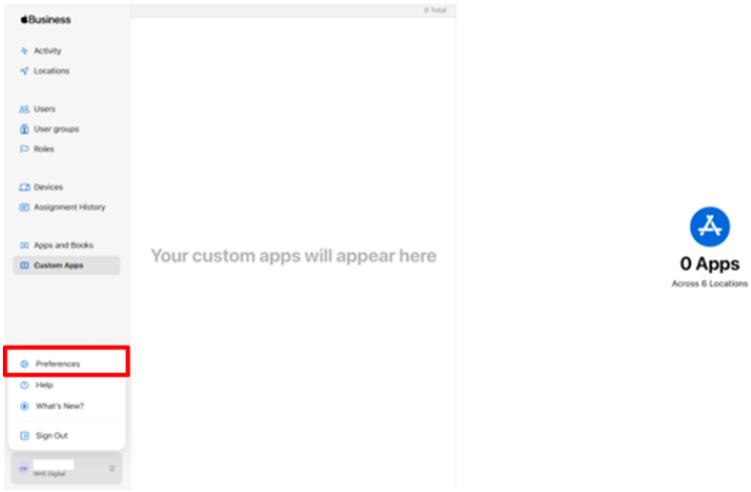
Please do not select the generate a new token for Apple Business Manager option, all your devices are linked to the original token. Generating a new token will mean that any device associated to the original token will need to be enrolled onto the Intune Central Platform.

Please reach out to the Intune Live Service team if you require any support.

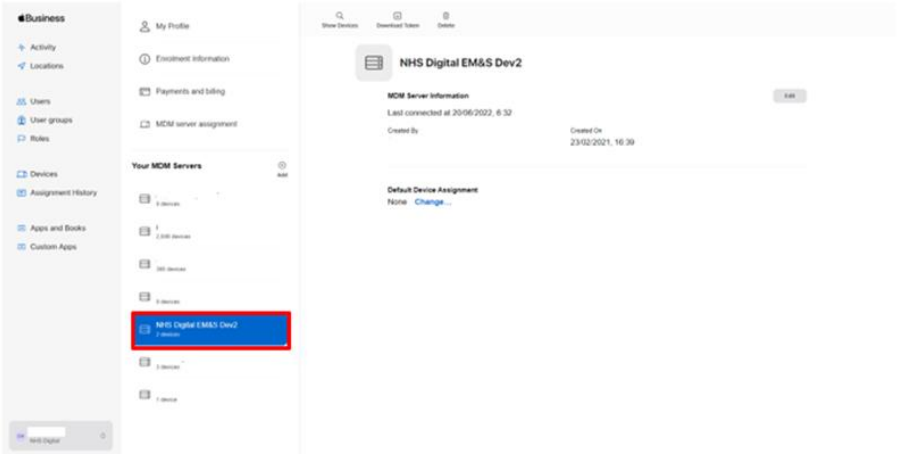
Please follow the steps detailed below to renew your ABM token:

1. Go to business.apple.com and sign in with an account that has an Administrator or Device Enrolment Manager role.

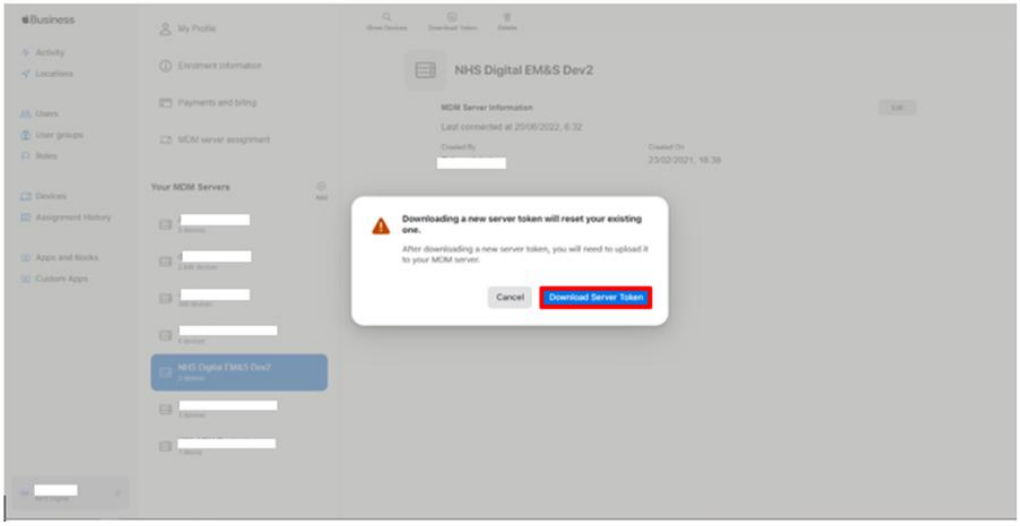
2. Click your Username on the bottom left and select '**Preferences'**.



3. Under the 'Your **MDM Servers**' section, select the MDM server associated with the token file that you want to renew.



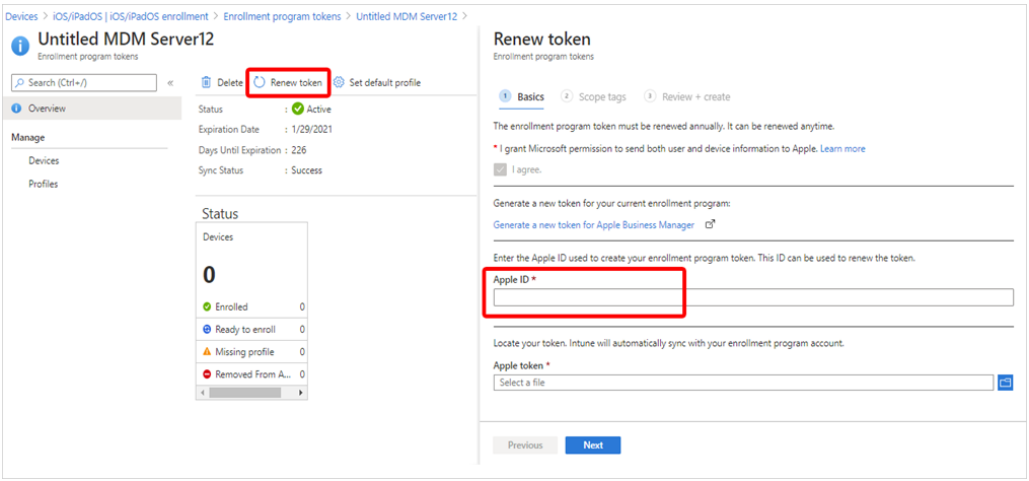
4. Select **Download Server Token**.



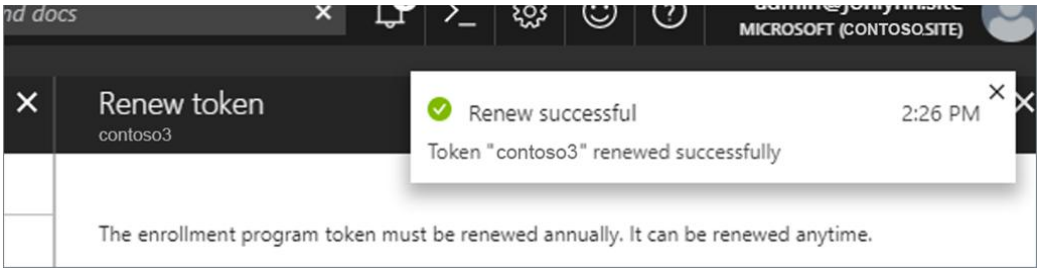
Important Note

Don't select **Download Server Token** if you don't intend to renew the token. Doing so will invalidate the token being used by Intune (or any other MDM solution). If you already downloaded the token, continue with the next steps until the token is renewed.

5. After you download the token, go to Microsoft Intune admin center. Select **Devices > iOS/iPadOS > iOS/iPadOS Enrolment > Enrolment program tokens**. Select the token.
6. Select **Renew token**. Enter the **Apple ID** used to create the original token (if it's not automatically populated):



7. Upload the newly downloaded token.
8. Select **Next** to go to the **Scope tags** page. Assign scope tags if you want to.
9. Select **Renew token**. You'll see a confirmation that the token is renewed:

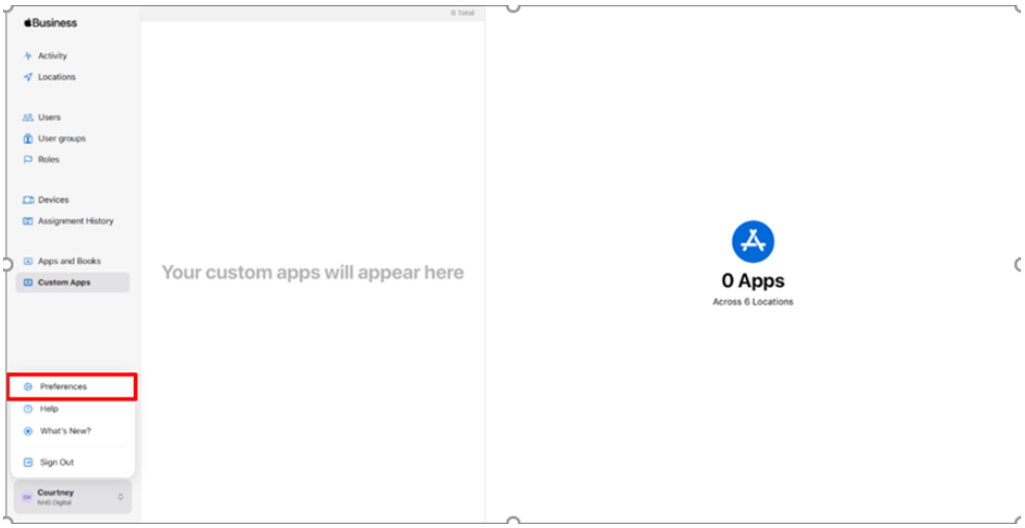


5.2.9 Renewing the VPP Token

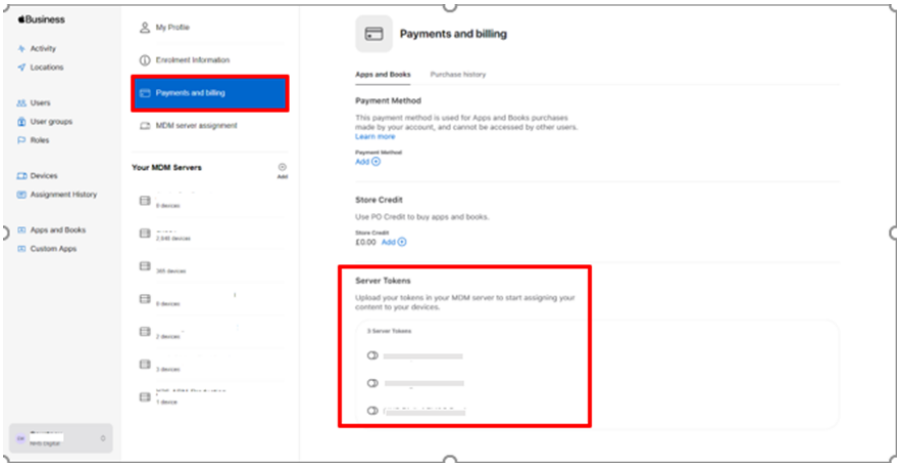
Critical Notes that will require action.

VPP tokens expire every 365 days. This token will need to be renewed and this is the responsibility of Intune LAs.

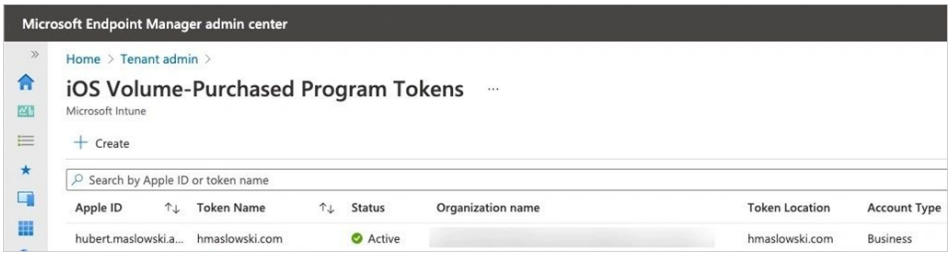
1. Download new **VPP Token** from the **Apple Business Manager** (business.apple.com) by selecting **Preferences** (by clicking your Username on the bottom left).



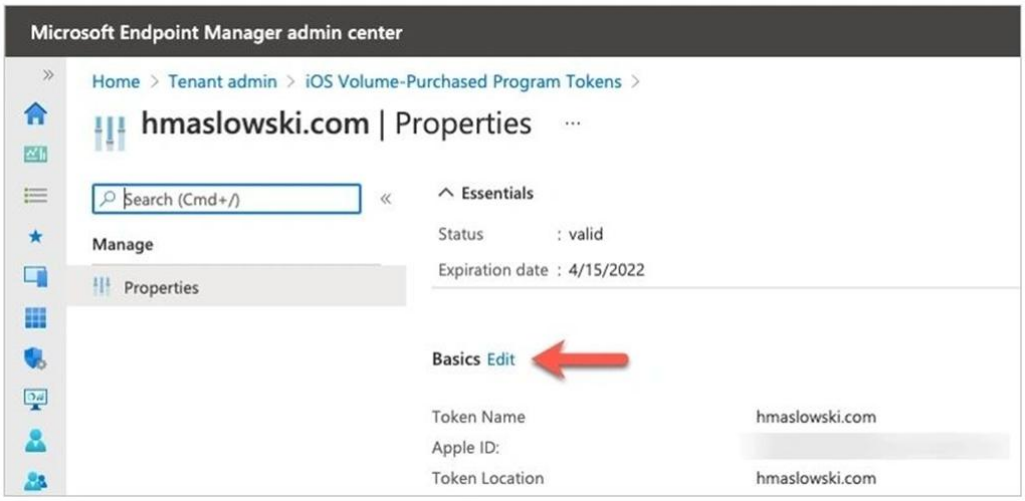
2. Select '**Payments and Billing**'. Download the relevant token under the 'Server Tokens' section.



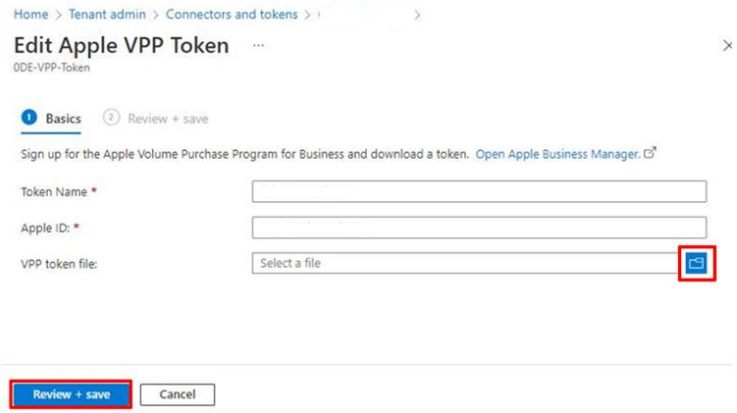
3. When you obtain a new **VPP Token** file (.vpptoken), open the Microsoft Intune console (endpoint.microsoft.com) and go to **Tenant administration – Connector Status** to choose **VPP Token**.



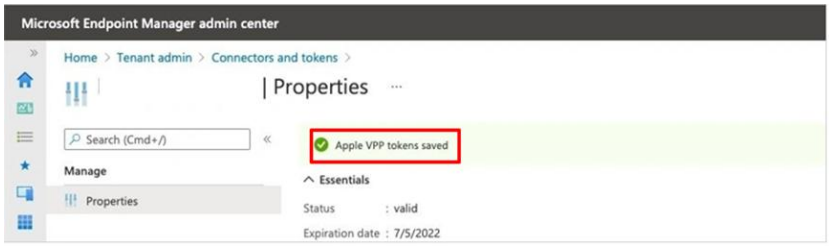
4. Select the **VPP Token** location you want to renew and press **Edit** (no renew button).



5. Upload your VPP token file (Token Name and Apple ID will be automatically populated already). Once you have done this click '**Review and save**'.

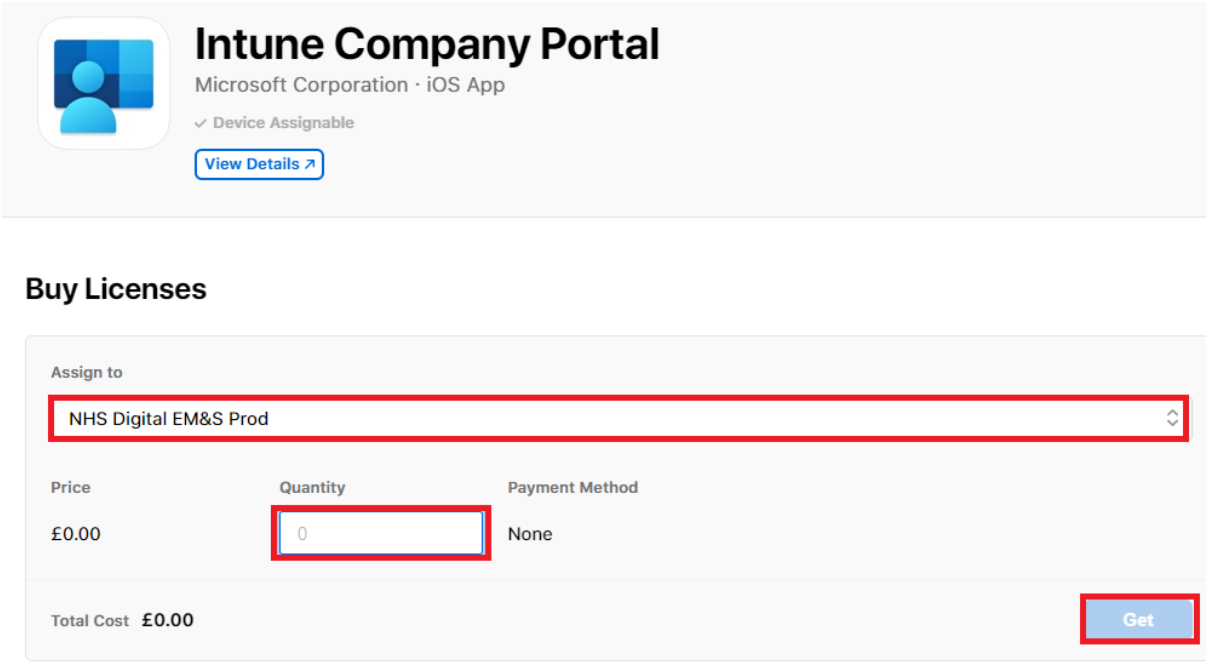


6. You should now see 'Apple VPP tokens saved' which means you have successfully renewed your VPP token.

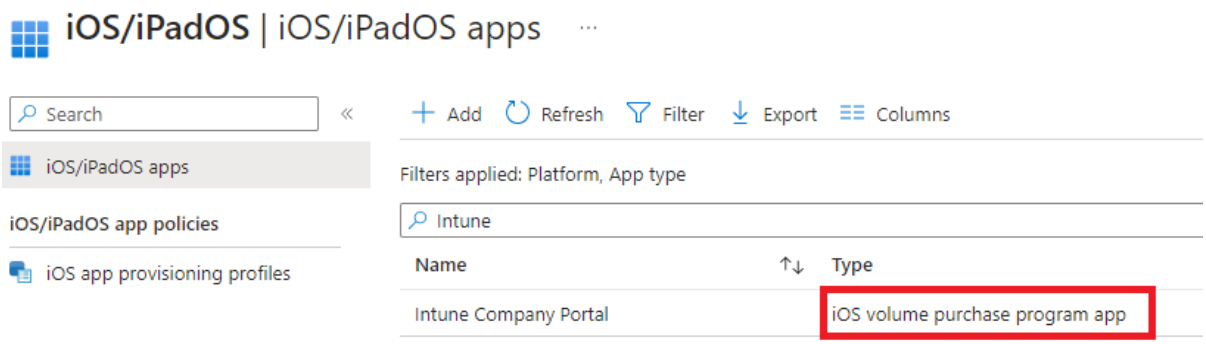


5.3 iOS/iPadOS and MacOS Application Management VPP App

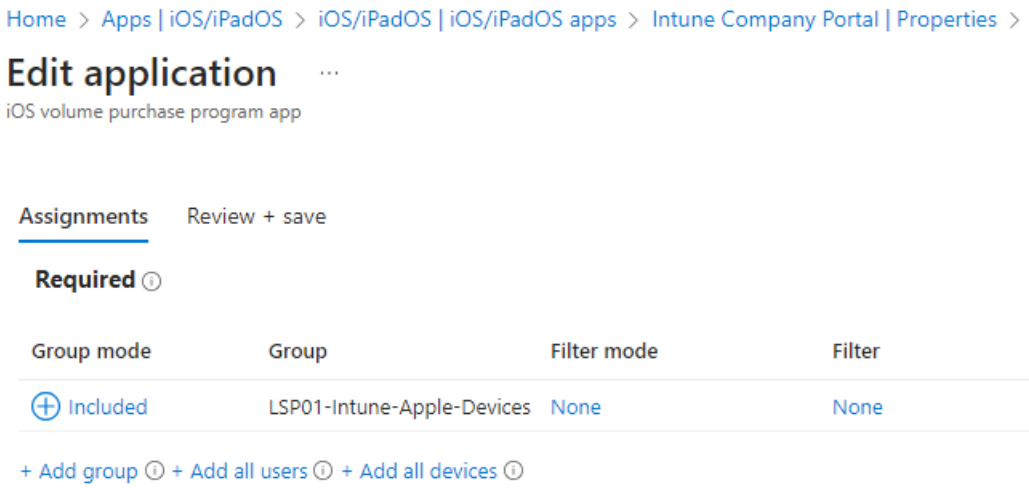
1. In ABM Click on **Apps and books > Search for and select the required app > Assign to Intune > Select Licence quantity > Get**.



2. Allow some time for the VPP token to sync the changes, then Navigate to **Apps > iOS/iPadOS Apps > Search for and select the required app (Be sure to select the iOS Volume Purchase Program App).**



3. Open the app and select **Properties**
4. **Assignments** > **Edit >** Select the relevant groups



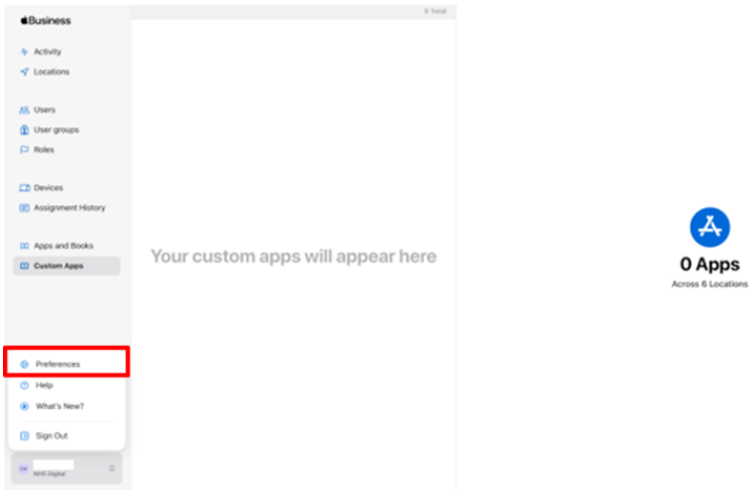
5. **Review and Save**

	Critical Notes that will require action ABM tokens expire every 365 days. This token will need to be renewed and this is the responsibility of the Intune LAs. **Please do not select the generate a new token for Apple Business Manager option, all your devices are linked to the original token.** Generating a new token will mean that any device associated to the original token will need to be re-enrolled onto the Intune Central Platform.

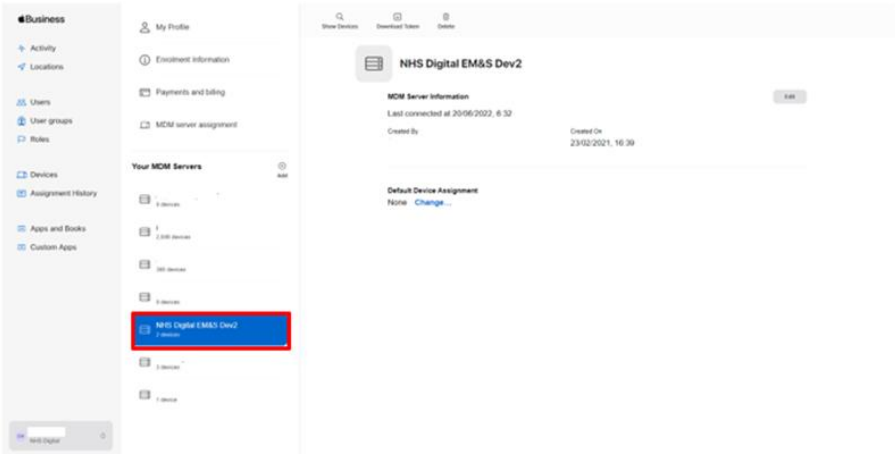
!	**Important Note** **Please reach out to the Intune Live Service team if you require any support.**

Please follow the steps detailed below to renew your ABM token:

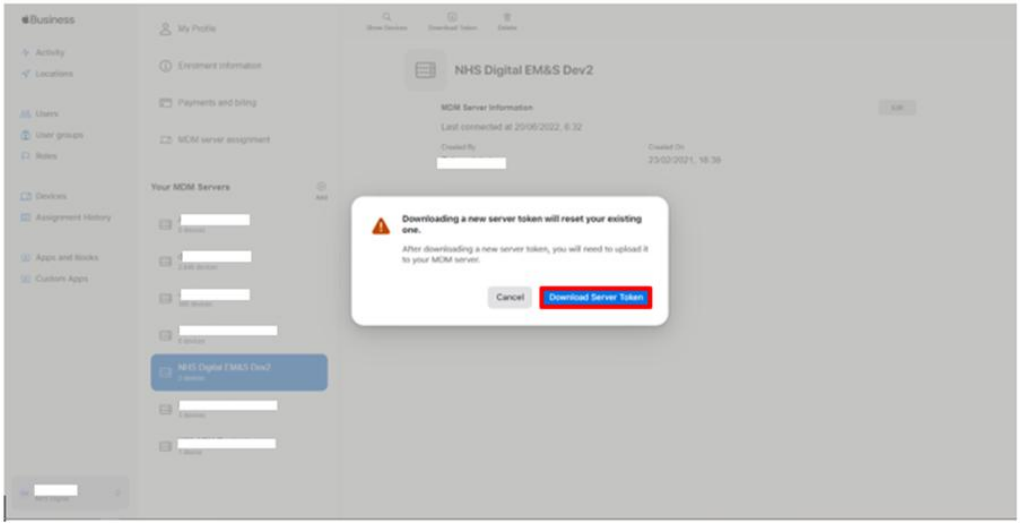
10. Go to business.apple.com and sign in with an account that has an Administrator or Device Enrolment Manager role.
11. Click your Username on the bottom left and select '**Preferences'**.



12. Under the 'Your **MDM Servers**' section, select the MDM server associated with the token file that you want to renew.



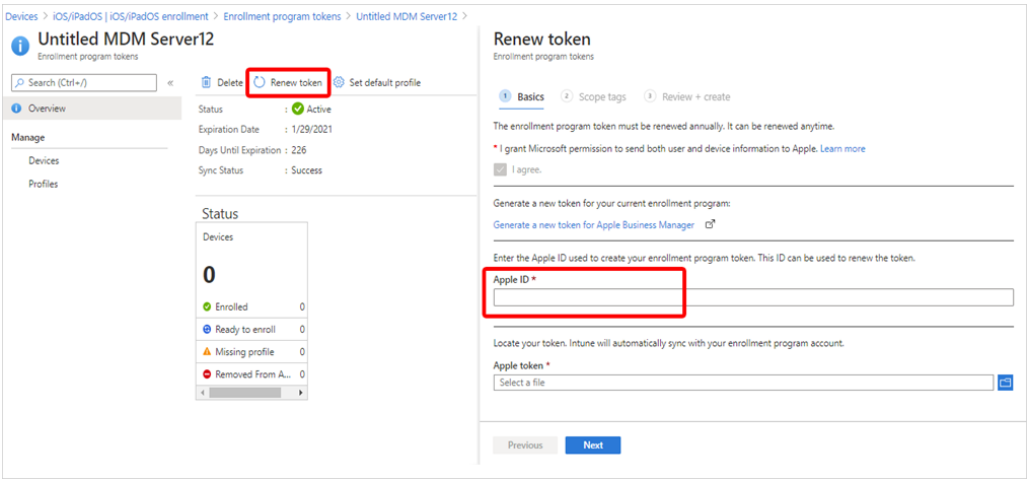
13. Select **Download Server Token**.



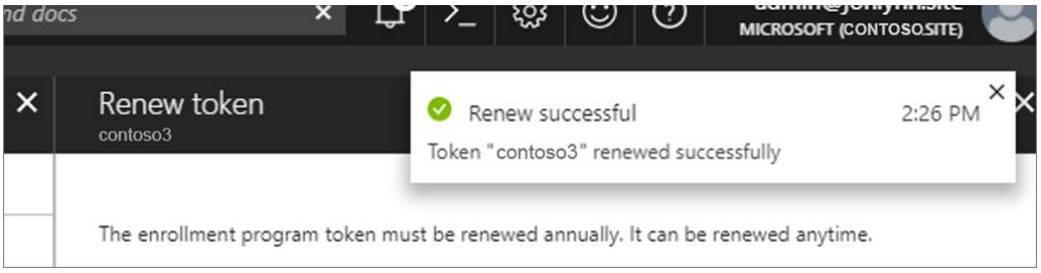
Important Note

Don't select **Download Server Token** if you don't intend to renew the token. Doing so will invalidate the token being used by Intune (or any other MDM solution). If you already downloaded the token, continue with the next steps until the token is renewed.

14. After you download the token, go to Microsoft Intune admin center. Select **Devices > iOS/ iPadOS/ MacOS> iOS/ iPadOS/ MacOS Enrolment > Enrolment program tokens**. Select the token.
15. Select **Renew token**. Enter the **Apple ID** used to create the original token (if it's not automatically populated):



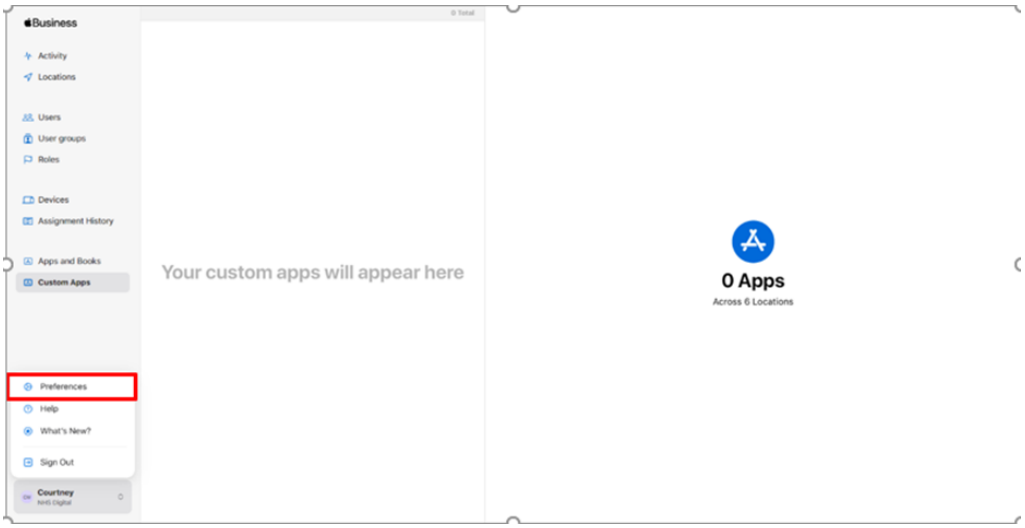
16. Upload the newly downloaded token.
17. Select **Next** to go to the **Scope tags** page. Assign scope tags if you want to.
18. Select **Renew token**. You'll see a confirmation that the token is renewed:



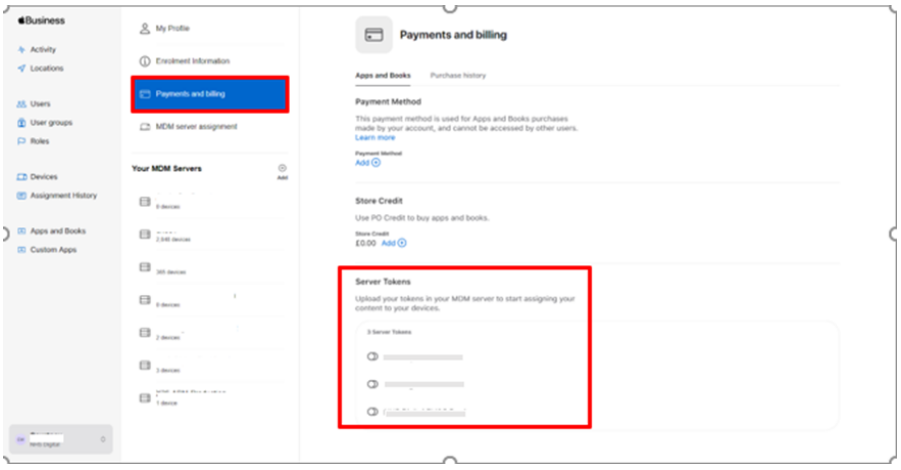
Critical Notes that will require action

VPP tokens expire every 365 days. This token will need to be renewed and this is the responsibility of Intune LAs.

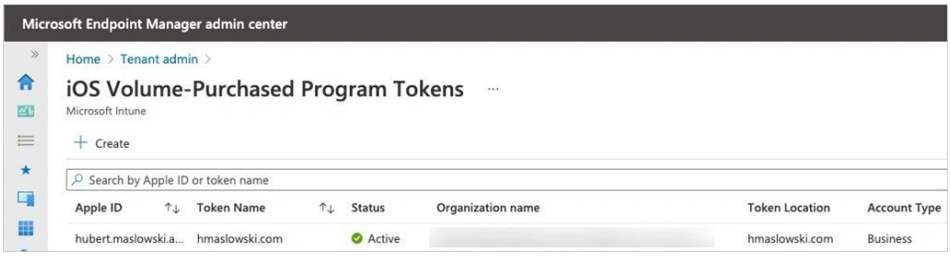
7. Download new **VPP Token** from the **Apple Business Manager** (business.apple.com) by selecting **Preferences** (by clicking your Username on the bottom left).



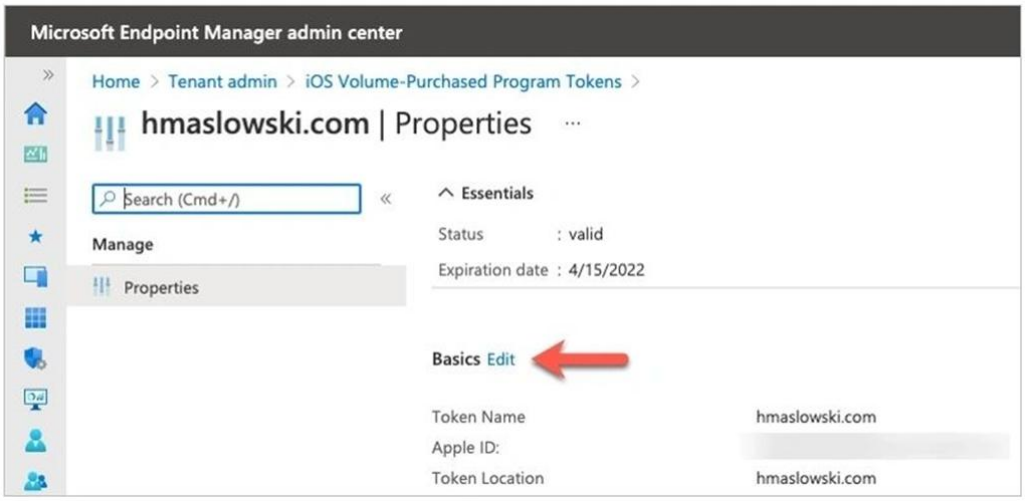
8. Select '**Payments and Billing**'. Download the relevant token under the 'Server Tokens' section.



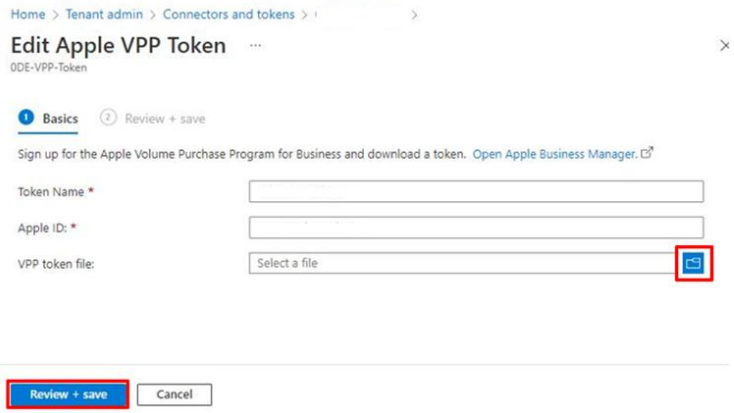
9. When you obtain a new **VPP Token** file (.vpptoken), open the Microsoft Intune console (endpoint.microsoft.com) and go to **Tenant administration – Connector Status** to choose **VPP Token**.



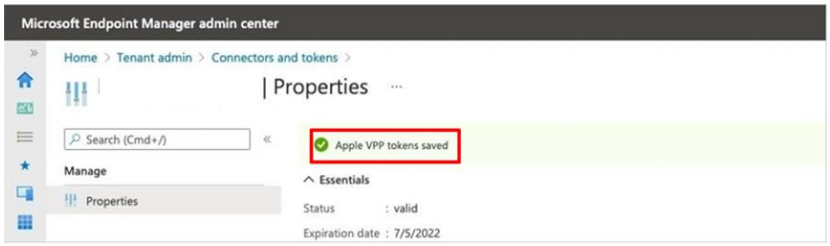
10. Select the **VPP Token** location you want to renew and press **Edit** (no renew button).



11. Upload your VPP token file (Token Name and Apple ID will be automatically populated already). Once you have done this click '**Review and save**'.



12. You should now see 'Apple VPP tokens saved' which means you have successfully renewed your VPP token.



5.3.2 MacOS App management

Company Portal: To oversee device management, install optional applications, and access resources protected by Conditional Access on MacOS devices associated with user affinity, users are required to install and log in to the Company Portal app. This app will be installing Company Portal to the targeted device. Intune Local admin can assign their organization macOS device group from in the Intune Portal.

!	**Note:** An Intune Local admin can Add and managed their own macOS apps from Intune Portal. If they want to install the Company

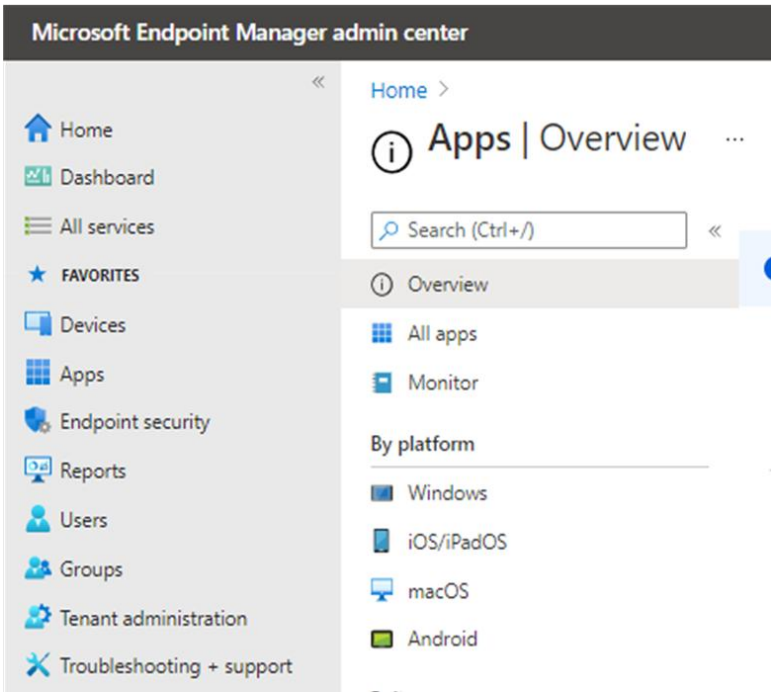
	Portal App, [please refer on how to add the Company Portal for macOS app.]

5.4. iOS/iPadOS Application Management iOS Store App

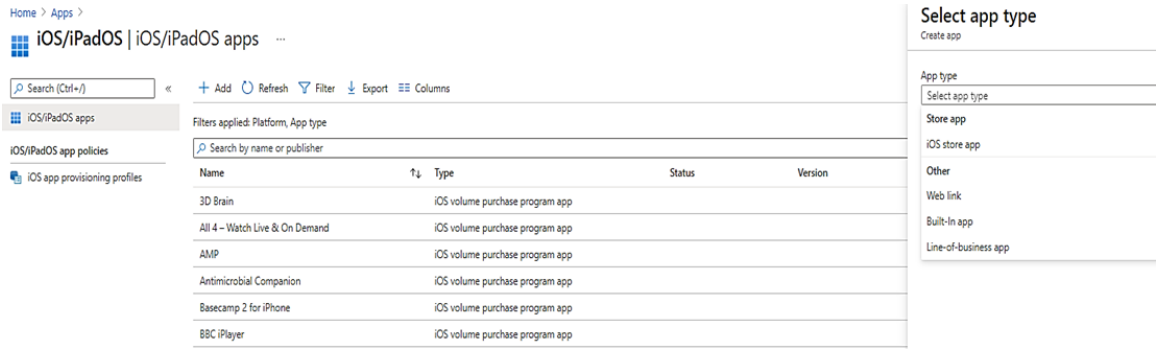
!	**Important Note** Using an iOS Store Apps will require users to authenticate with an Apple ID and it is recommended to use VPP apps.

In the Intune portal, LAs can push various iOS apps to enrolled iOS devices. This section below covers the steps to successfully deploy an iOS app to an iOS device via the Intune Portal.

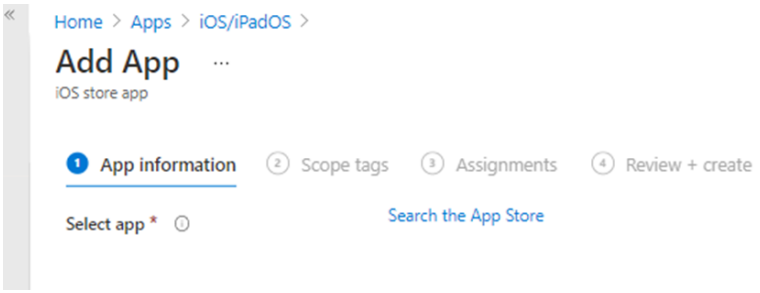
1. Sign into Endpoint Management.
2. Navigate to **Apps > iOS/iPadOS**.



3. Select **Add > Select iOS Store App > Select**.

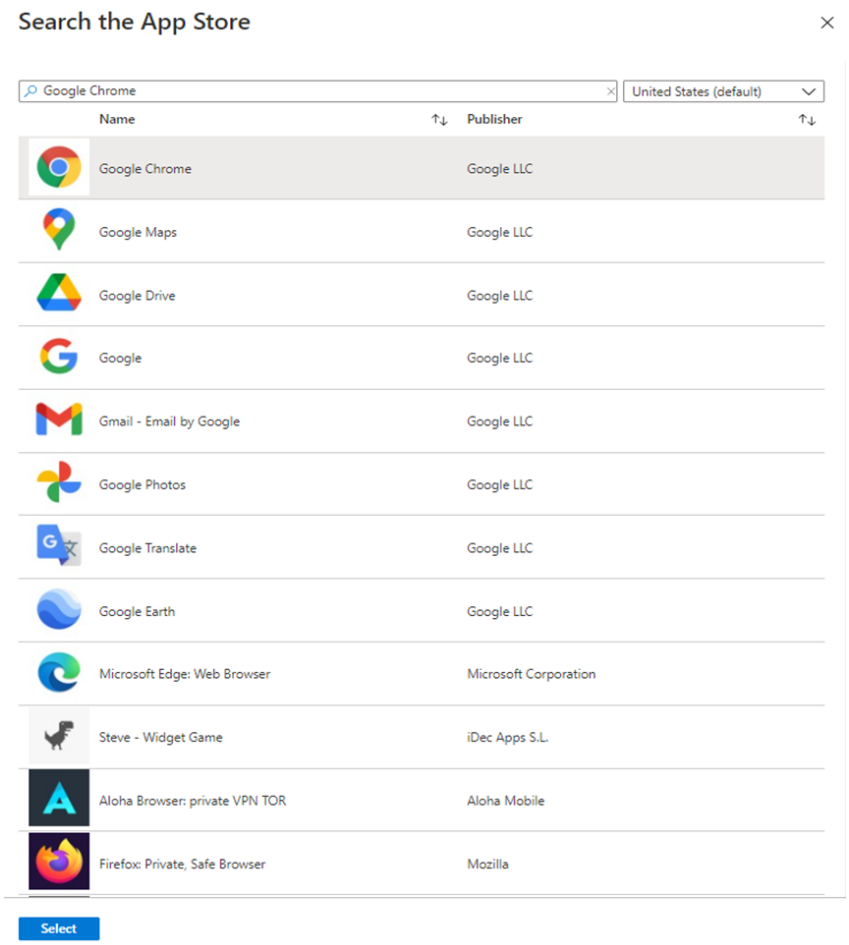


4. Select the **Search the App Store** option



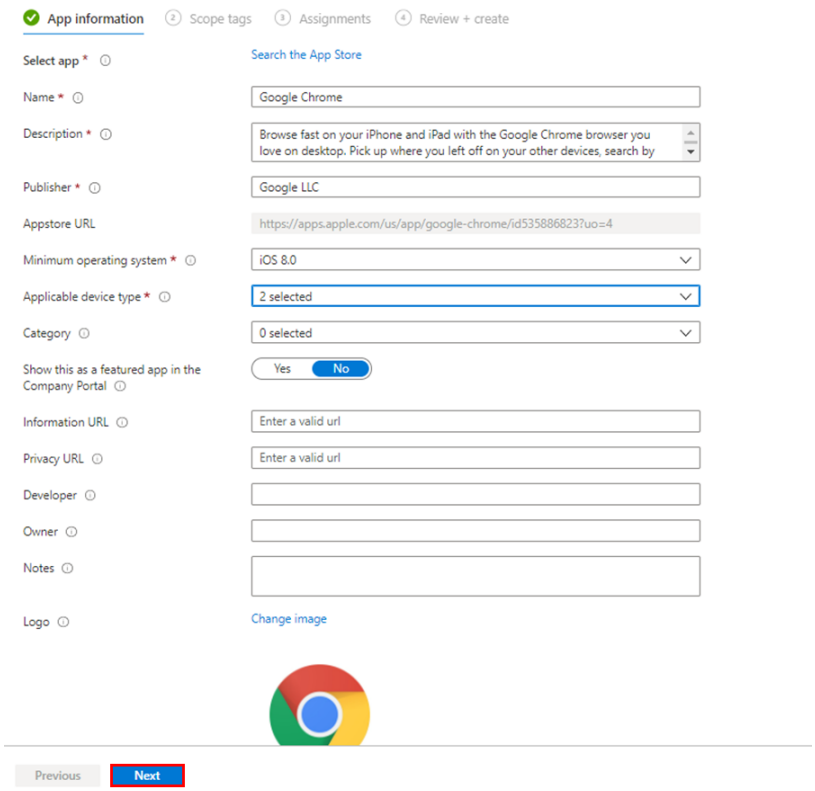
5. **Search for the app** to you want to deploy.

!	**Important Note** By default, the language will be set to United States, but this can be changed.

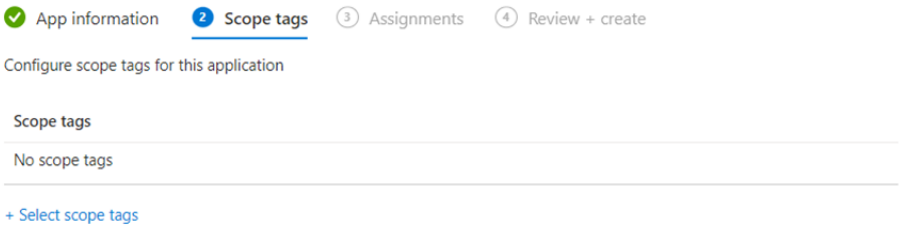


6. Select **Next**.

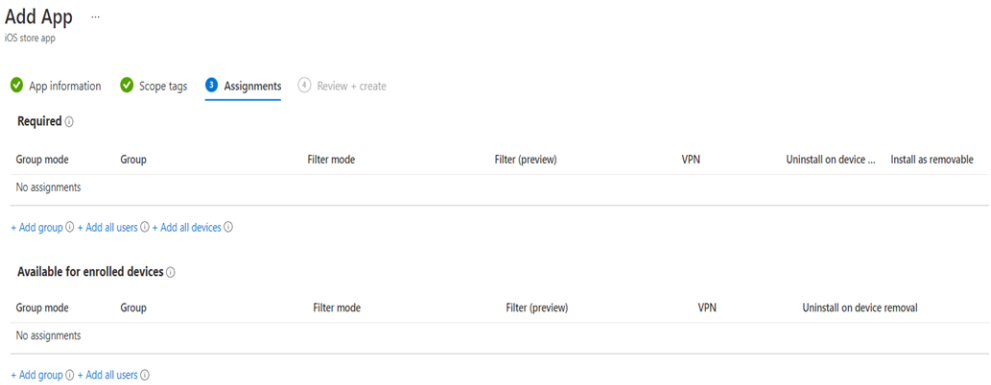
!	**Important Note** There are few default settings you can change, specifically: • Name of the app • Description of the app • Minimum Operating System • Applicable Device Type



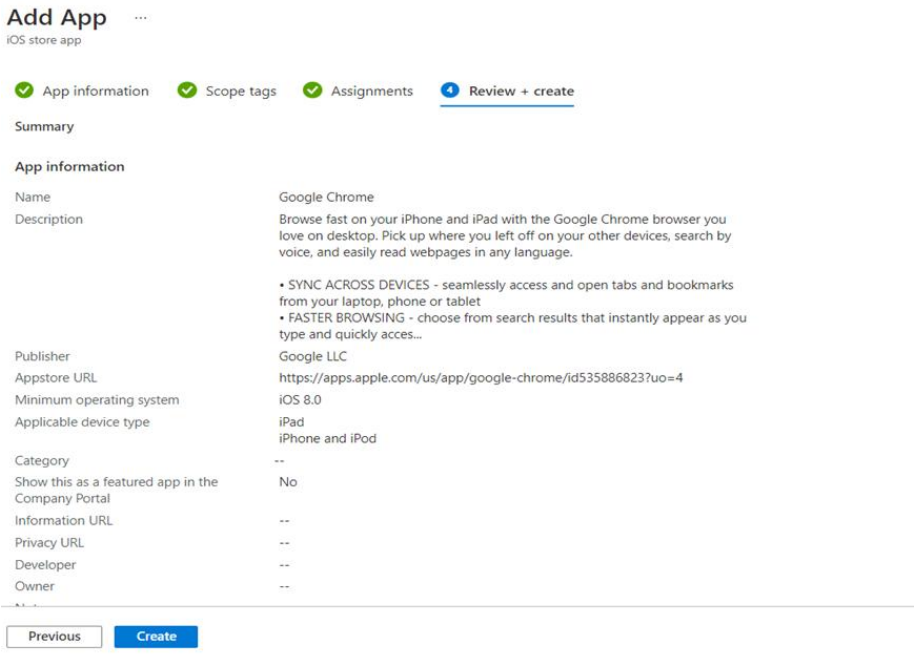
7. Select the relevant **scope tag**.



8. The select **Add Group** to apply the app to the relevant group.



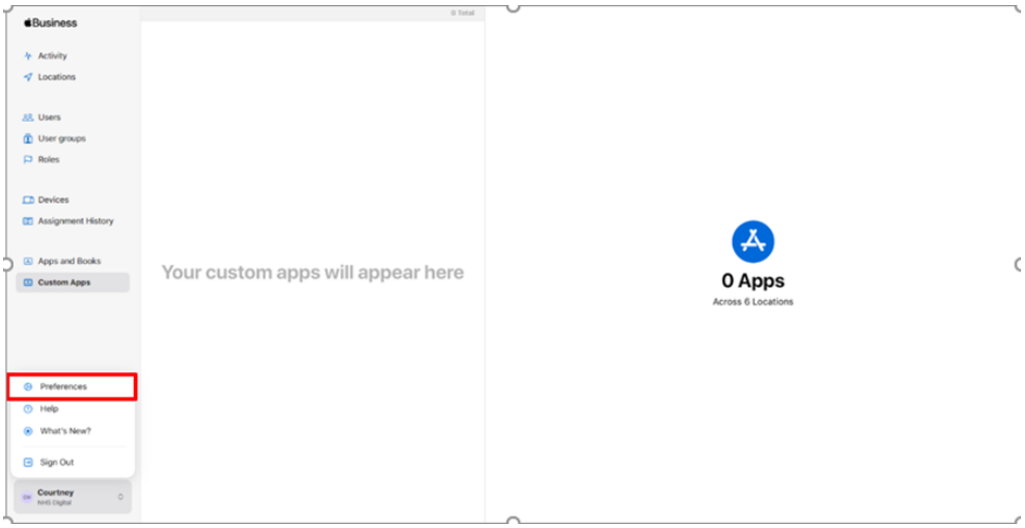
9. Select **Next > Create**.



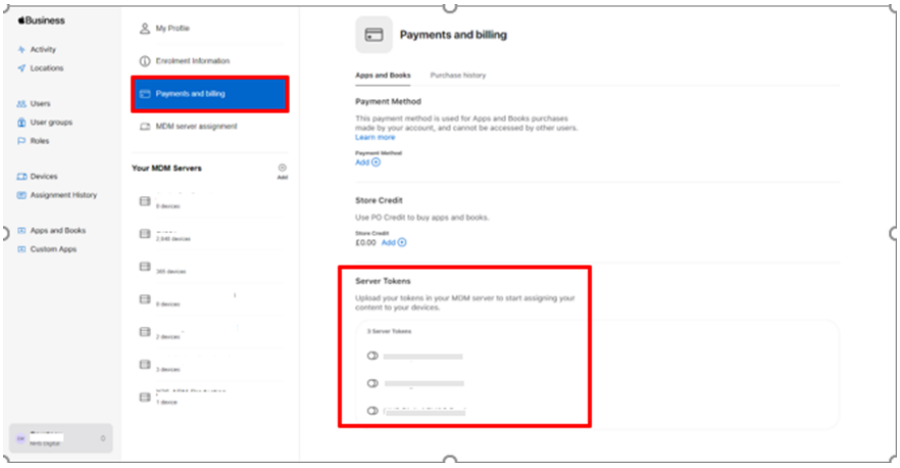
Critical Notes that will require action

VPP tokens expire every 365 days. This token will need to be renewed and this is the responsibility of Intune LAs.

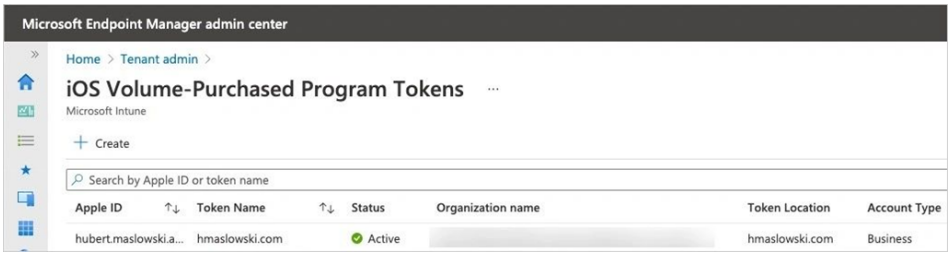
13. Download new **VPP Token** from the **Apple Business Manager** (business.apple.com) by selecting **Preferences** (by clicking your Username on the bottom left).



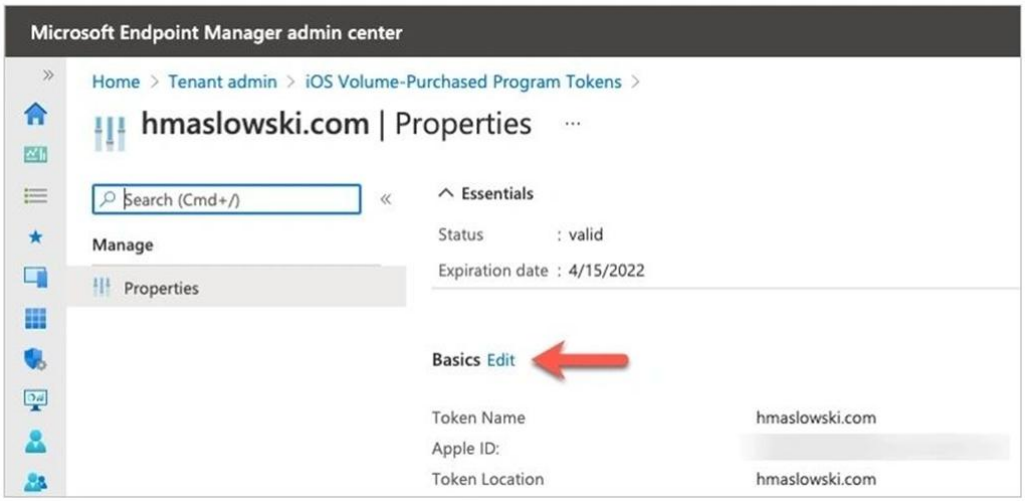
14. Select '**Payments and Billing**'. Download the relevant token under the 'Server Tokens' section.



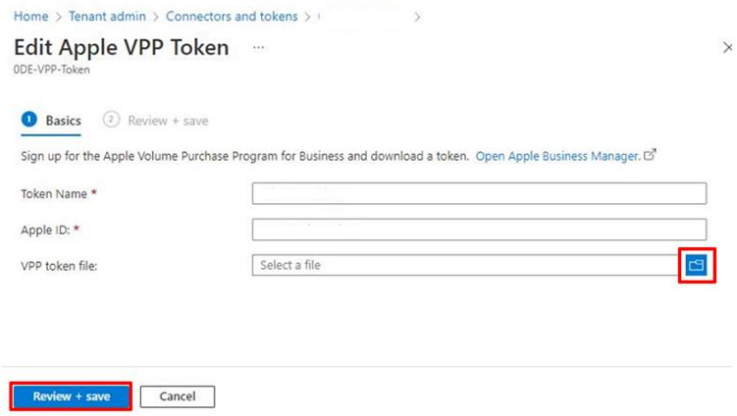
15. When you obtain a new **VPP Token** file (.vpptoken), open the Microsoft Intune console (endpoint.microsoft.com) and go to **Tenant administration – Connector Status** to choose **VPP Token**.



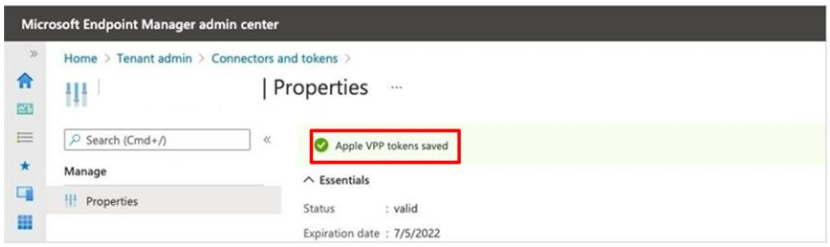
16. Select the **VPP Token** location you want to renew and press **Edit** (no renew button).



17. Upload your VPP token file (Token Name and Apple ID will be automatically populated already). Once you have done this click '**Review and save**'.



18. You should now see ‘Apple VPP tokens saved’ which means you have successfully renewed your VPP token.



5.4 Creating User Enrolment Profiles

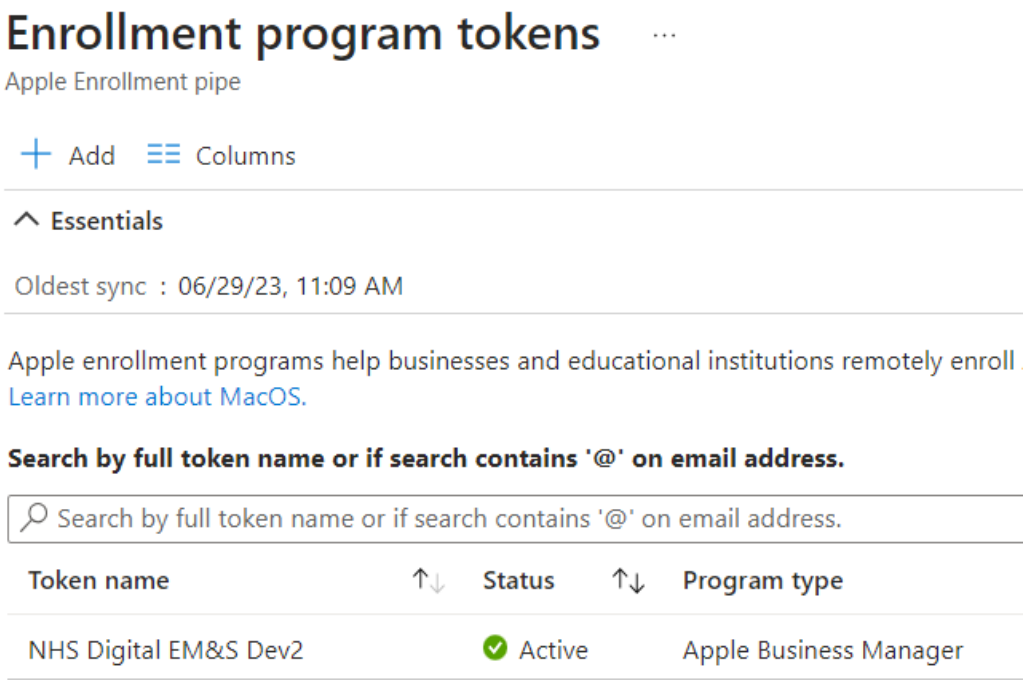
Once the Apple Device Enrolment token has been installed, enrolment profiles for the Apple Device Enrolment (ADE) devices can be created. These enrolment profiles define the experience and settings applied to a group of devices during the enrolment phase.

The following section details the steps to create and configure enrolment profiles.

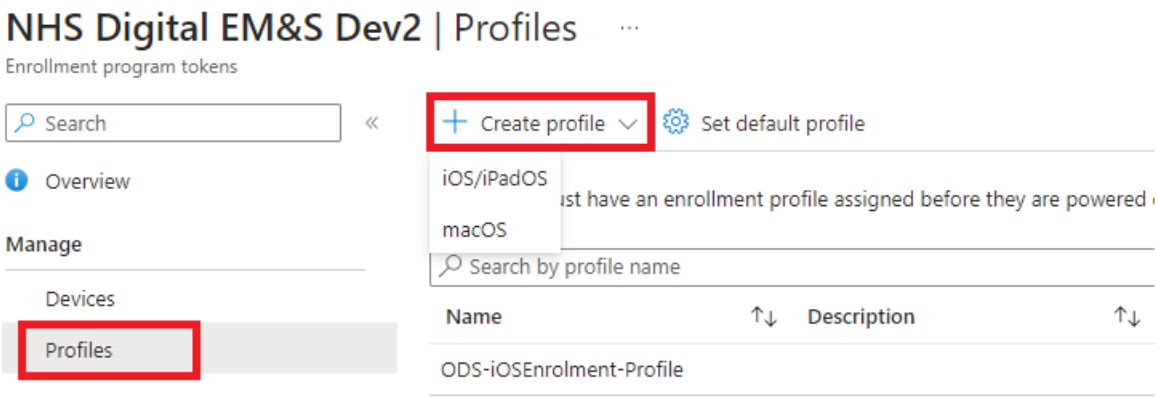
!	**Important Note** When entering a new profile name please follow the correct standard – ‘Trust ODS Code -Device Type Enrolment Profile’ e.g., <ODS>-Shared Device-iOSEnrolment-Profile <ODS>-iOS-Enrolment-Profile

!	**Important Note** Each new enrolment profile will require an AAD Dynamic group to be created, to pull devices into their relevant groups. This is required to ensure devices can be managed within the Intune Portal. If you require a dynamic group to created or amended, please raise a service request via Helpdesk Self-Service.

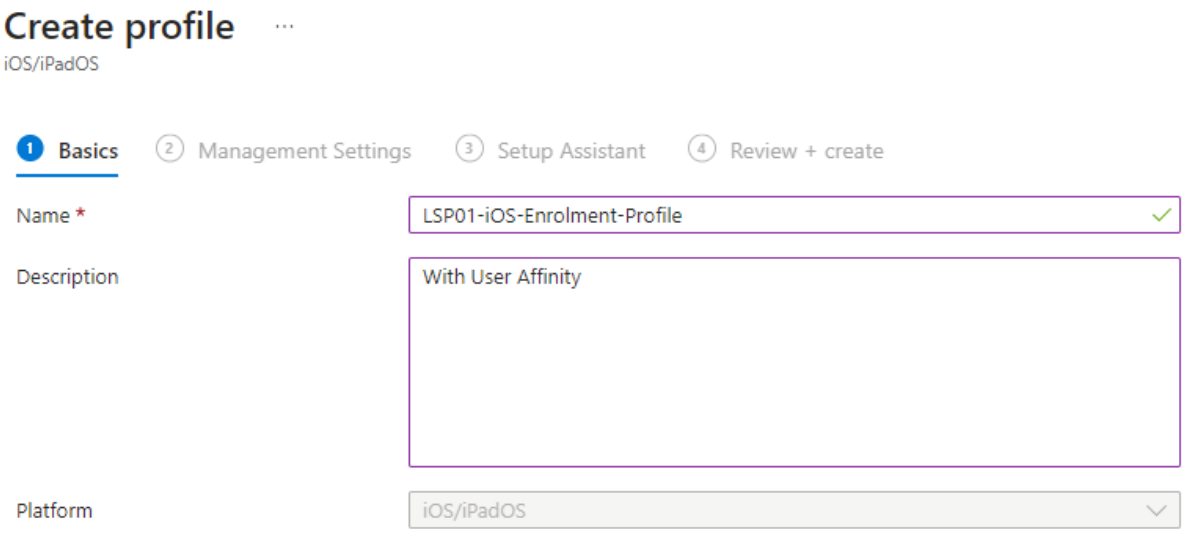
1. Navigate to: **Devices > Apple> iOS/iPadOS > iOS/iPadOS Enrollment > Enrollment Program Token** to connect your ABM instance to Intune.



2. Select **Profiles** > **Create Profile**



3. Enter the relevant **Profile Name**.



5.4.1 iOS User Enrolment Affinity Options

Intune provides two different user affinity options during enrolment. The key differences between the two options are highlighted as follows:

- Enrol with User Affinity:
    - This option allows users to enrol using their Azure AD nhs.net credentials and is designed for a single user use case.
- Enrol Without User Affinity
    - This option is shared/kiosk mode device mode and does not require the Company Portal app.

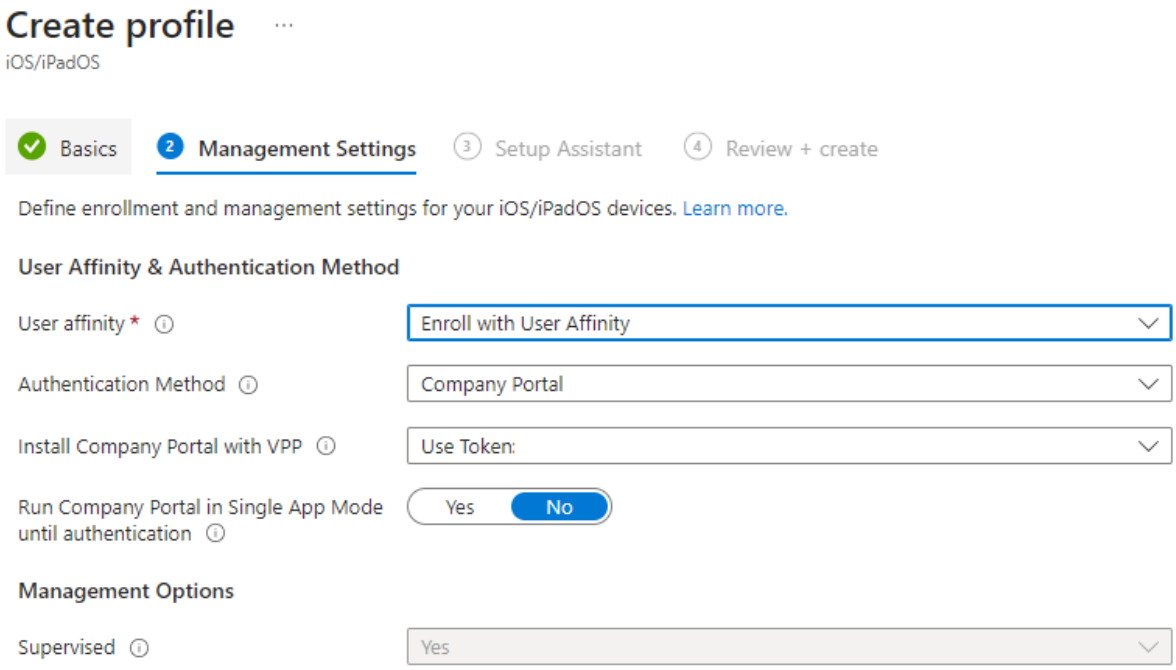
5.4.2 iOS Single User Device Enrolment

The following section details the steps to enrol devices with User Affinity.

!	**Important Note** The settings configured in this profile will determine end users' experience after their device is reset and they progress through the enrolment process.

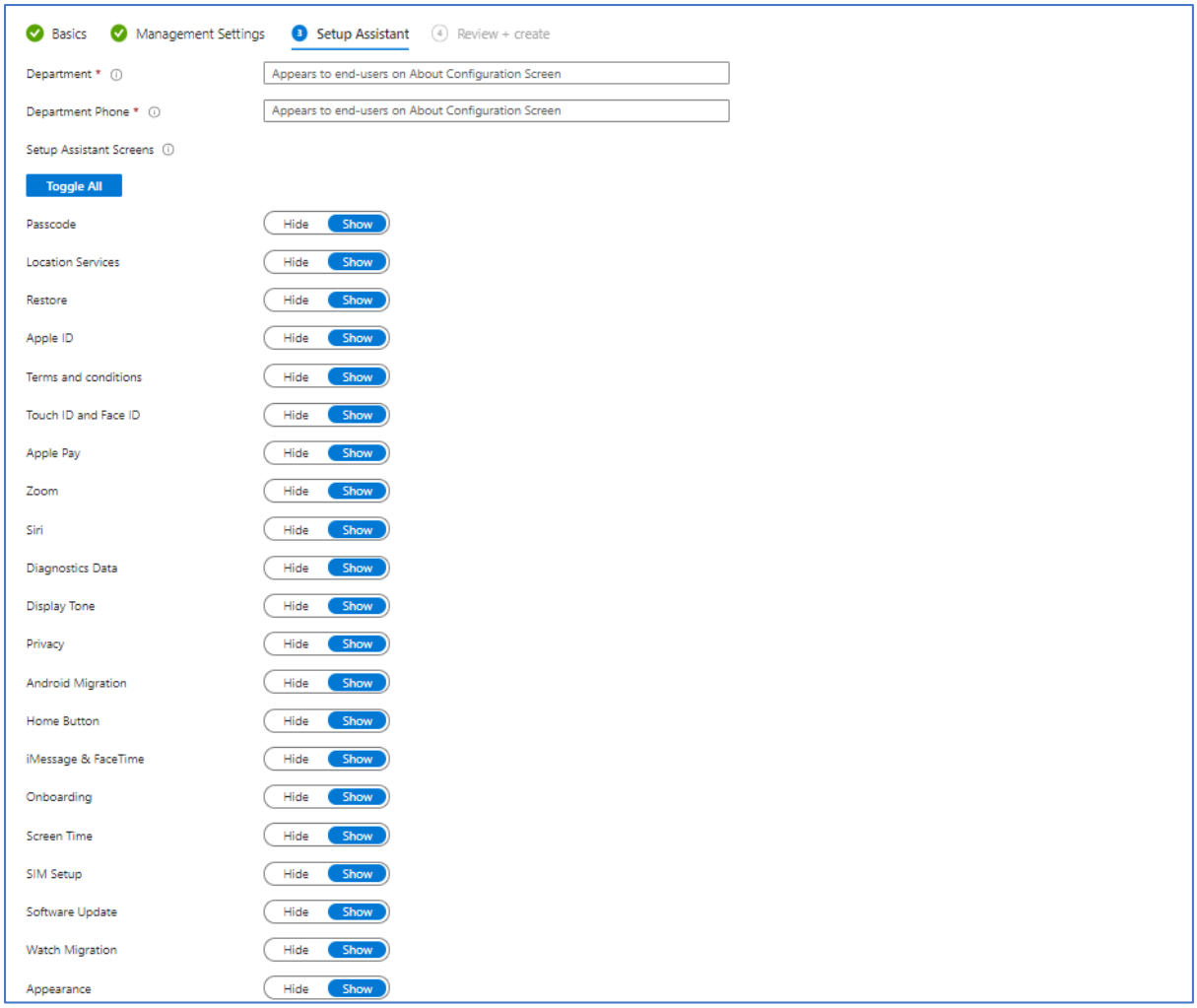
1. Select **Enrol with User Affinity** for single user devices and ensure all details are completed as shown on the screenshot below, and then select **Review + save**.

!	**Important Note** For the 'Device Name Template' Please see the following name standard: <ODSCode>-{{DEVICETYPE}}-{{SERIAL}}



!	**Important Note** End users will be required to authenticate via the 'Company Portal App' when they are enrolling their devices. It is therefore important that Company Portal VPP licences are assigned to Intune.

2. **Configure** the **Apple Setup Assistant**.

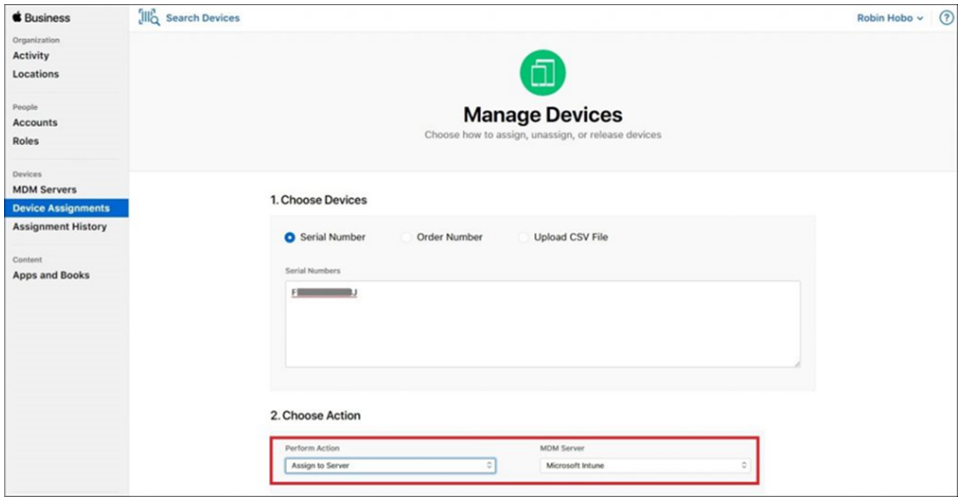


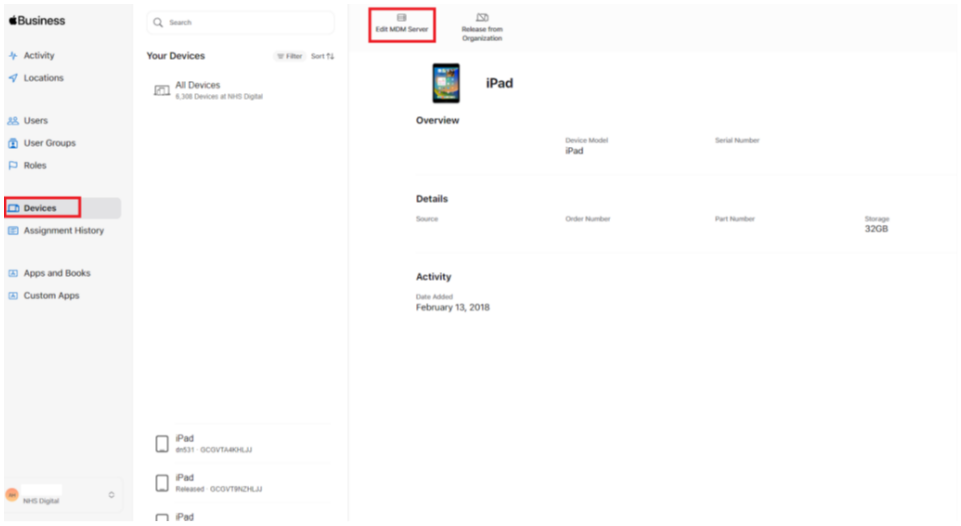
Critical Notes that will require action.

The "Apple ID" page needs to be set to "Hidden" from the Setup Assistant. This is to prevent users from being prompted to enter Apple IDs during the enrolment process. As the primary method of authentication to AAD is via Company Portal, it is expected that users sign in with their nhs.net credentials in the Company Portal app.

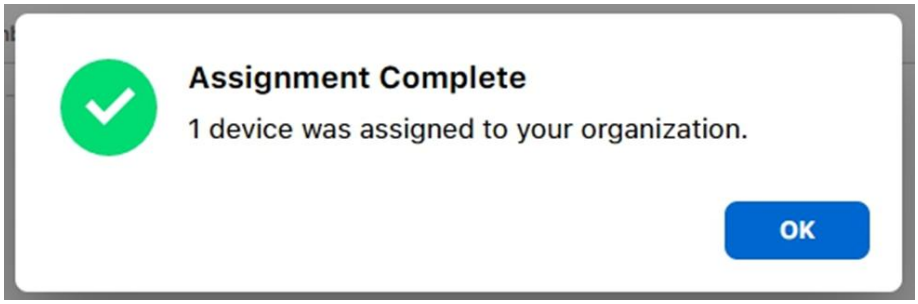
Users can choose to connect their Apple ID after their enrolment.

3. Next, open the **ABM Tenant** to add devices.

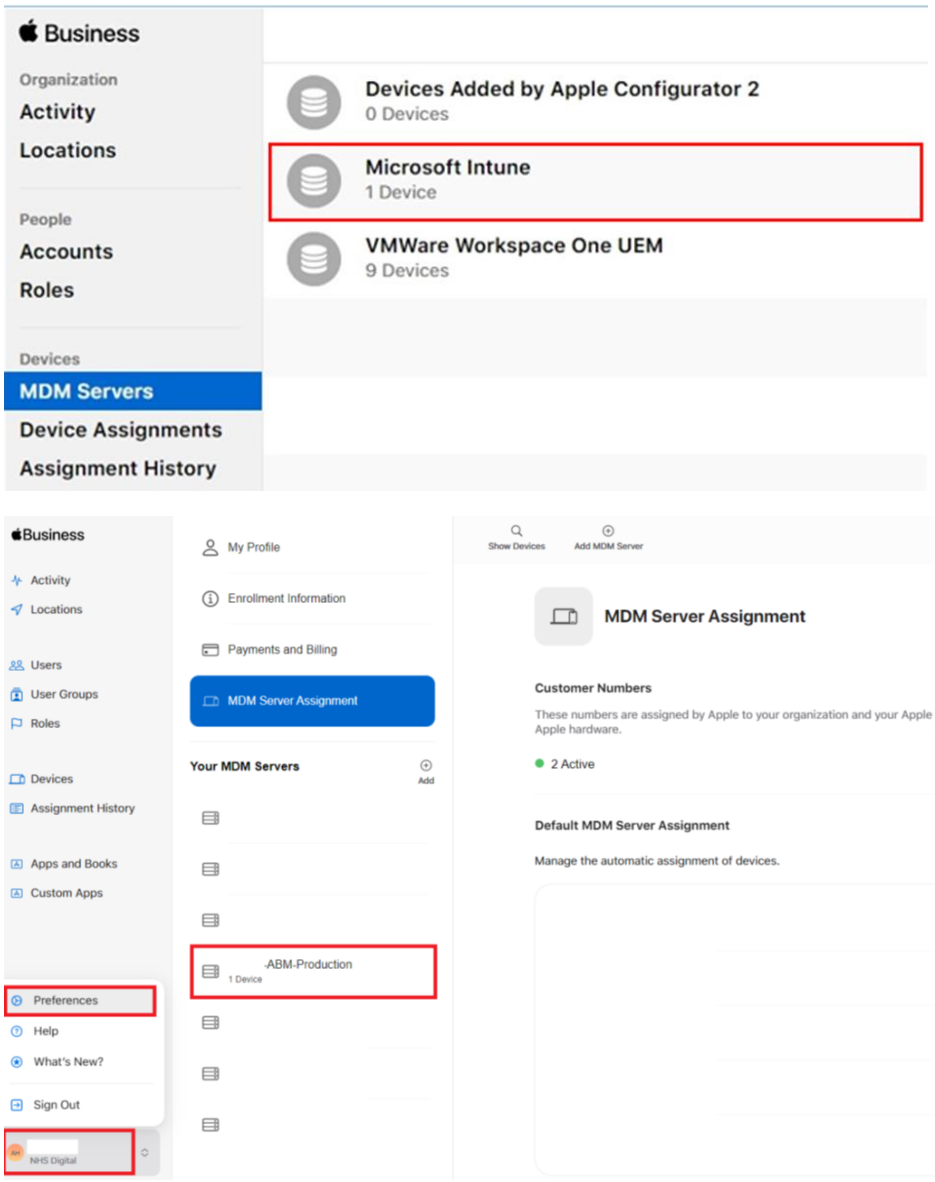




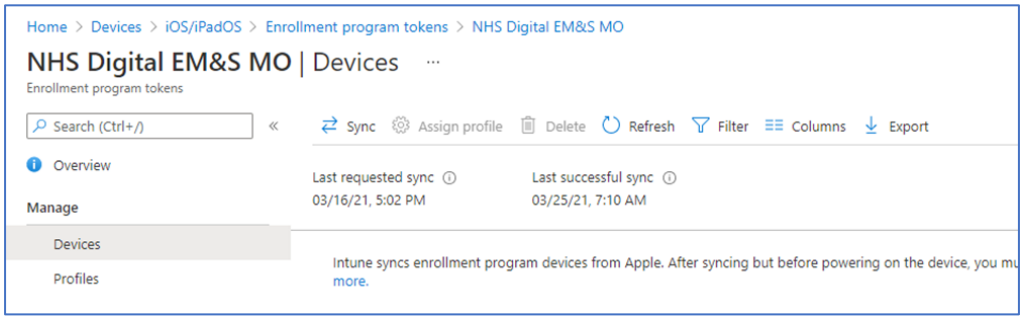
4. Once device has been assigned **a completion notification** should appear.



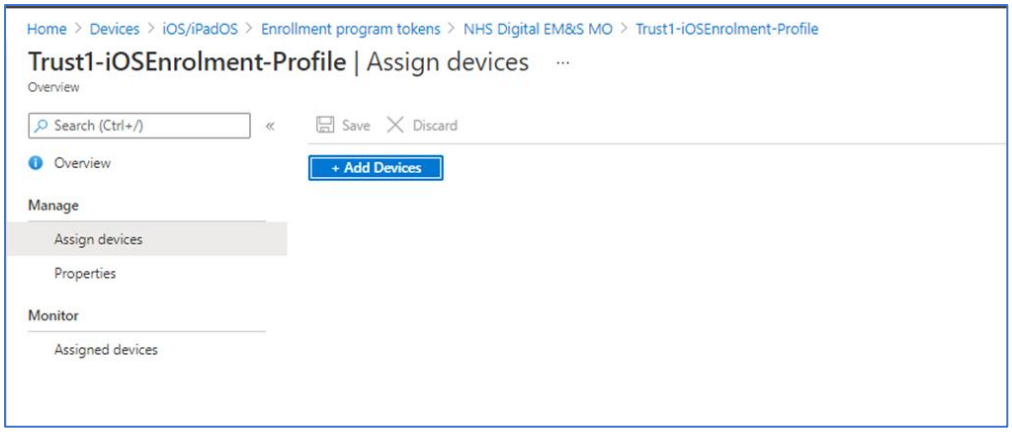
5. Once the device has been assigned to Intune this should update on the MDM servers Page in ABM.



6. Once you have confirmed that the device has updated (and is showing) on the MDM Servers page, **open the Intune Enrolment Program Token page** and **Sync the devices**.



7. **Assign the devices** to the profile you have created to complete the link.



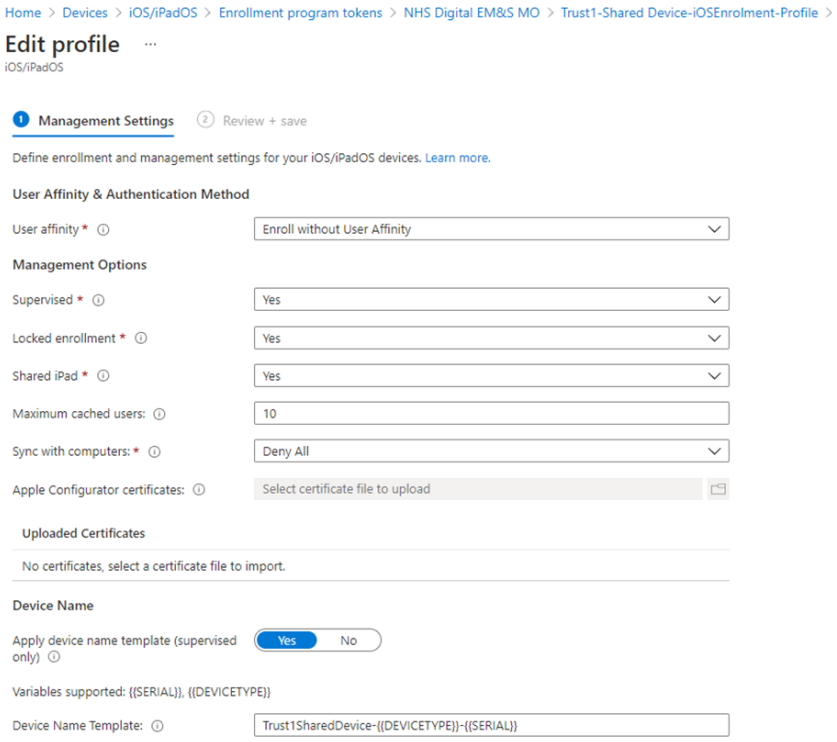
!	**Important Note** iOS devices cannot be assigned to specific users, however, when the user logs in their UPN will be added to the device which will be visible to LAs in Intune.

5.4.3 iOS, iPadOS Shared Device Enrollment

!	**Important Note** SharePoint, Teams and Outlook apps are unsupported on iOS and iPadOS shared devices.

The process for setting up ‘shared mode’ for iOS and iPadOS is similar to that of a user affinity profile. Whilst the same device enrolment process is followed, it is necessary to create a separate Enrolment Profile for Shared Devices. The process below describes the steps required to enrol a shared iOS/iPadOS device via an Intune Enrolment profile:

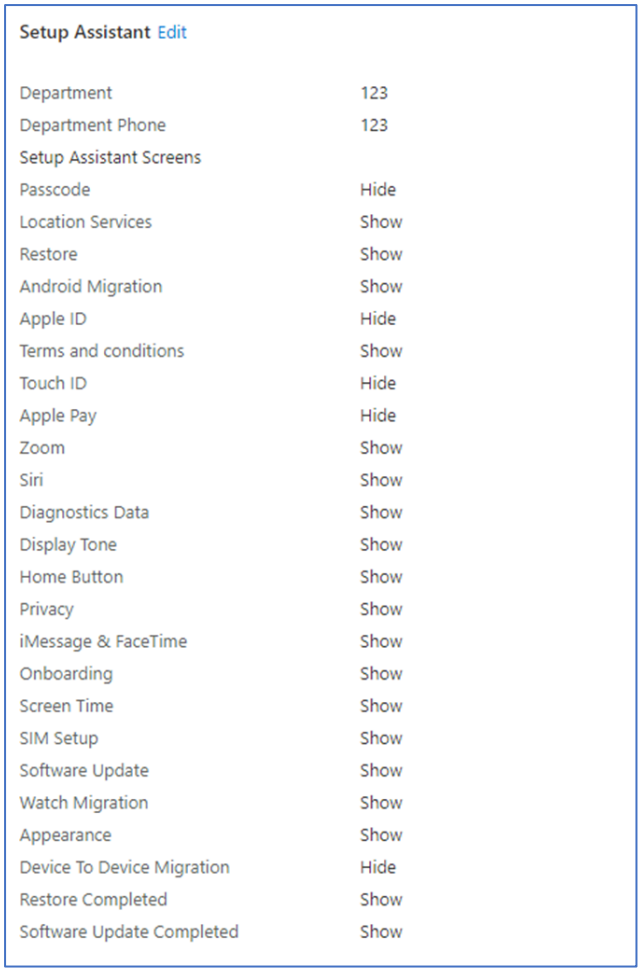
1. Select the Enrol without User Affinity option, then enter your ‘<ODS>-SharedDevice-{{DEVICETYPE}}-{{SERIAL}}’



!	**Important Note** It is important to follow the correct naming standard – ODS CodeSharedDevice-{{DEVICETYPE}}-{{SERIAL}}'. Example: Trust1SharedDevice-{{DEVICETYPE}}-{{SERIAL}}

2. Please change the following settings to 'Hide':

- Passcode
- Apple ID
- Touch ID
- Apple Pay
- Device to Migration



Setup Assistant Edit

Department	123
Department Phone	123
Setup Assistant Screens	
Passcode	Hide
Location Services	Show
Restore	Show
Android Migration	Show
Apple ID	Hide
Terms and conditions	Show
Touch ID	Hide
Apple Pay	Hide
Zoom	Show
Siri	Show
Diagnostics Data	Show
Display Tone	Show
Home Button	Show
Privacy	Show
iMessage & FaceTime	Show
Onboarding	Show
Screen Time	Show
SIM Setup	Show
Software Update	Show
Watch Migration	Show
Appearance	Show
Device To Device Migration	Hide
Restore Completed	Show
Software Update Completed	Show

!

Important Note

When setting up an enrolment profile for a Shared Device there are several settings that need to change compared to a standard device enrolment profile.

It is recommended that the following settings are set to ‘Hide’:

- Passcode
- Touch ID
- Device to Device Migration

Intune LAs can choose to disable more settings if required.

5.4.4 MacOS User Enrolment Profiles

Organizations will need to create an enrollment profile for MacOS profile, like that of iOS User Affinity profile as per following steps:

!	**Note:** The settings configured in this profile will determine end users' experience after their device is reset and they progress through the enrolment process.

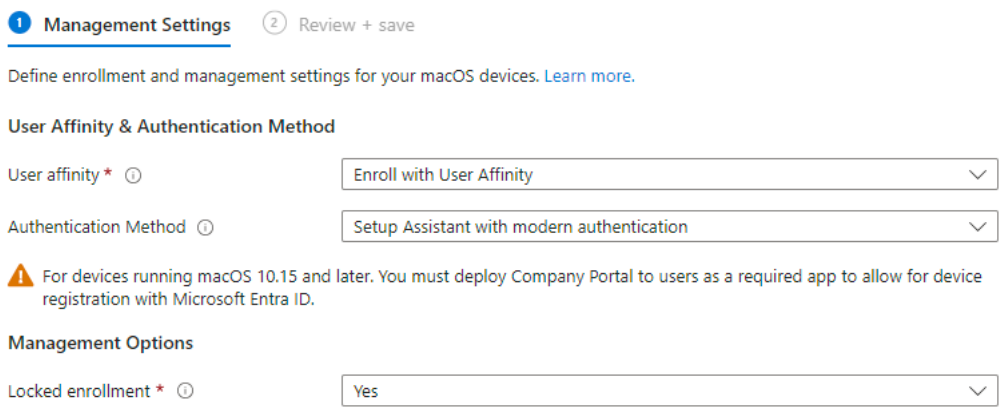
1. Navigate to **Devices** > **macOS** > **macOS enrollment.**
2. Select Enrolment program tokens and select your organization token.

!	**Note:** All organizations onboarded onto the NHSmail Intune platform, who wish to enroll MacOS devices onto the platform will need to ensure that their ABM is linked into NHSmail Intune. Please raise a SR with the Intune Live Support Team for further assistance.

3. Select **Profiles** > + Create **profile > macOS.**
4. Enter the name of the Profile and description e.g., ODS- MacOS Enrolment Profile. Ensure you follow the correct format described. > **Next.**

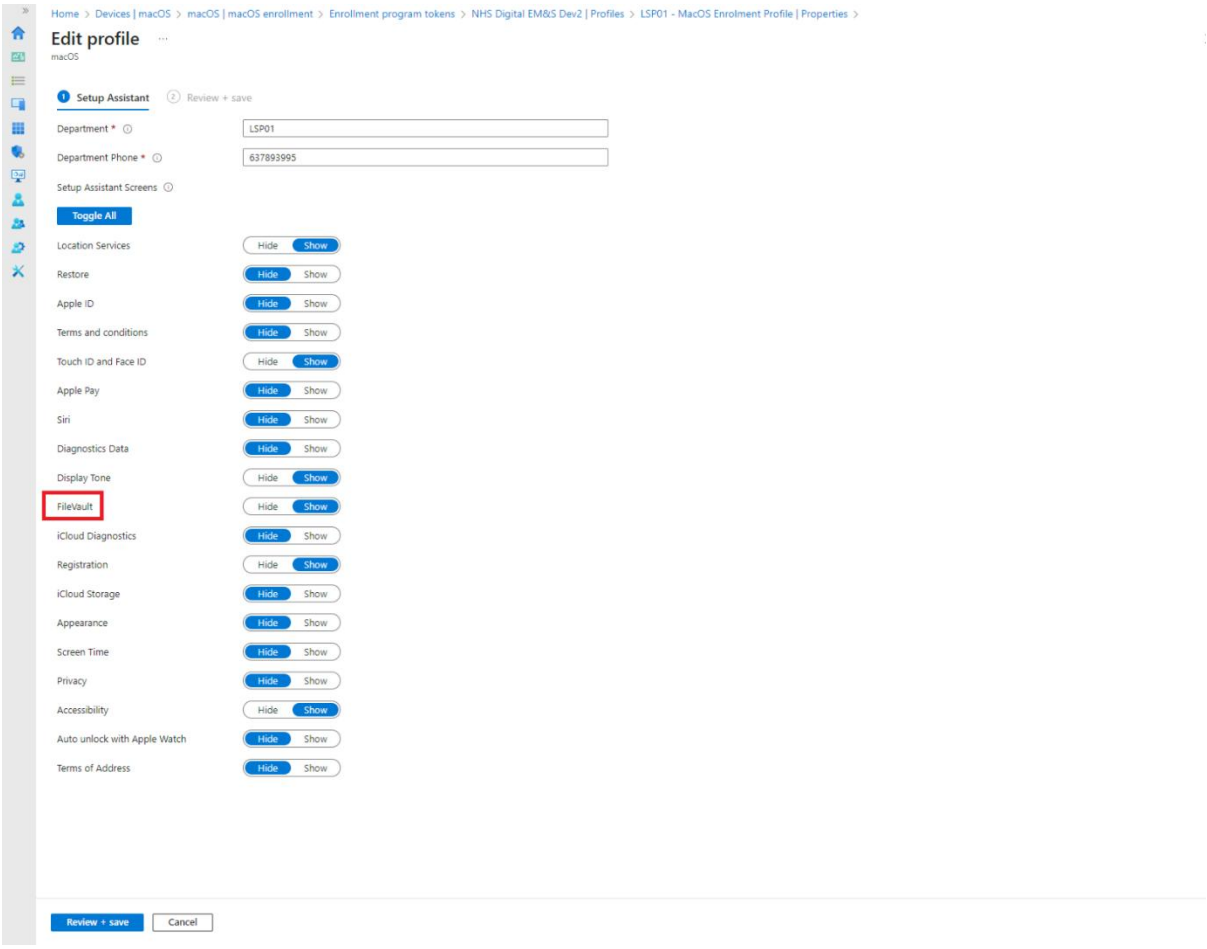
!	**Note:** If Organizations want to create more than one enrolment profile, they can do it. To link it to a dynamic Group, raise a SR with the Intune Live Support team.

5. Select the below options:
   1. User affinity: Enrolment with User affinity
   2. Authentication Method: Setup Assistant with modern authentication
   3. Locked enrolment: Yes
6. Select **Next**



!	**Note:** Locked enrolment will remove end-user the ability to delete the management profile from the device.

7. Enter the following information:
   1. Department
   2. Department phone
   3. Setup Assistance Screen: toggle the options the organization wants the user to have access to.
8. Select **Review + save.**



!	**Note:** FileVault must be set to “show” to allow user to encrypt their device.

9. Select **Save.**

!	**Note:** The enrolment profile is linked with the Dynamic Group **ODS.dsg.Intune-MacOS-Devices** created per each Intune Organization. To create additional dynamic groups, please raise a Service Request with the Intune Live Support Team.

5.4.5 Setup Assistant with modern authentication

Setup Assistant with modern authentication is supported on devices running iOS/iPadOS 13.0 and later.

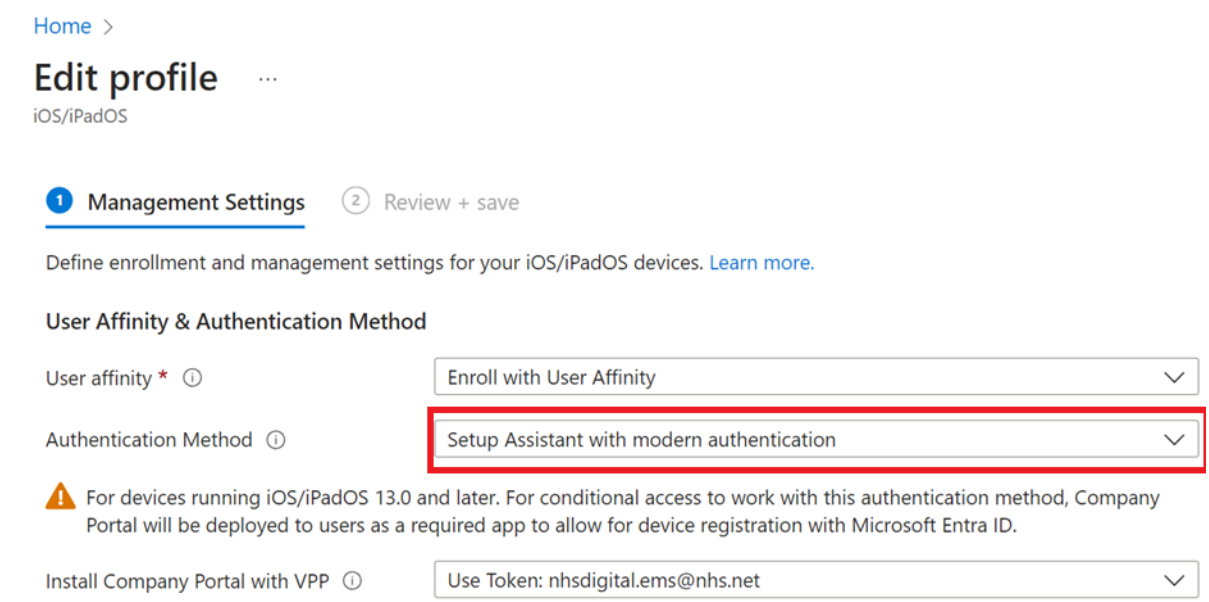
JIT registration is supported with the following enrolment types:

- Apple automated device enrolment: For enrolments that use Setup Assistant with modern authentication as the authentication method.

To move to Setup Assistant with Modern Auth for Automated Device Enrolment, you can either:

1. Edit your existing ADE policy to use the “Setup Assistant with modern authentication” for authentication.

See the screen below for where you’ll select this in your exiting profile.



Alternatively, you can create a new enrolment profile set to use Setup Assistant with Modern Authentication as follows:

2. Setting up the “Setup Assistant with Modern Authentication” method Enrolment Profile

You can create an enrolment profile for automated device enrolment. A device enrolment profile defines the settings applied to a group of devices during enrolment.

a. In Microsoft Intune admin centre, go to **Devices** > **Enrolment**.
b. Select the **Apple** tab.
c. Choose **Enrolment Program Tokens**.
d. Choose a token, and then select **Profiles**.
e. Select **Create profile** > **iOS/iPadOS**.
f. For **Basics**, give the profile a **Name** and **Description** for administrative purposes. Users don't see these details.
g. Select **Next**.
h. In the **User Affinity** list, select an option that determines whether devices with this profile must enroll with or without an assigned user.
i. Set Authentication Method to **Setup Assistant with modern authentication.**
j. Select **Review + Save** tab.

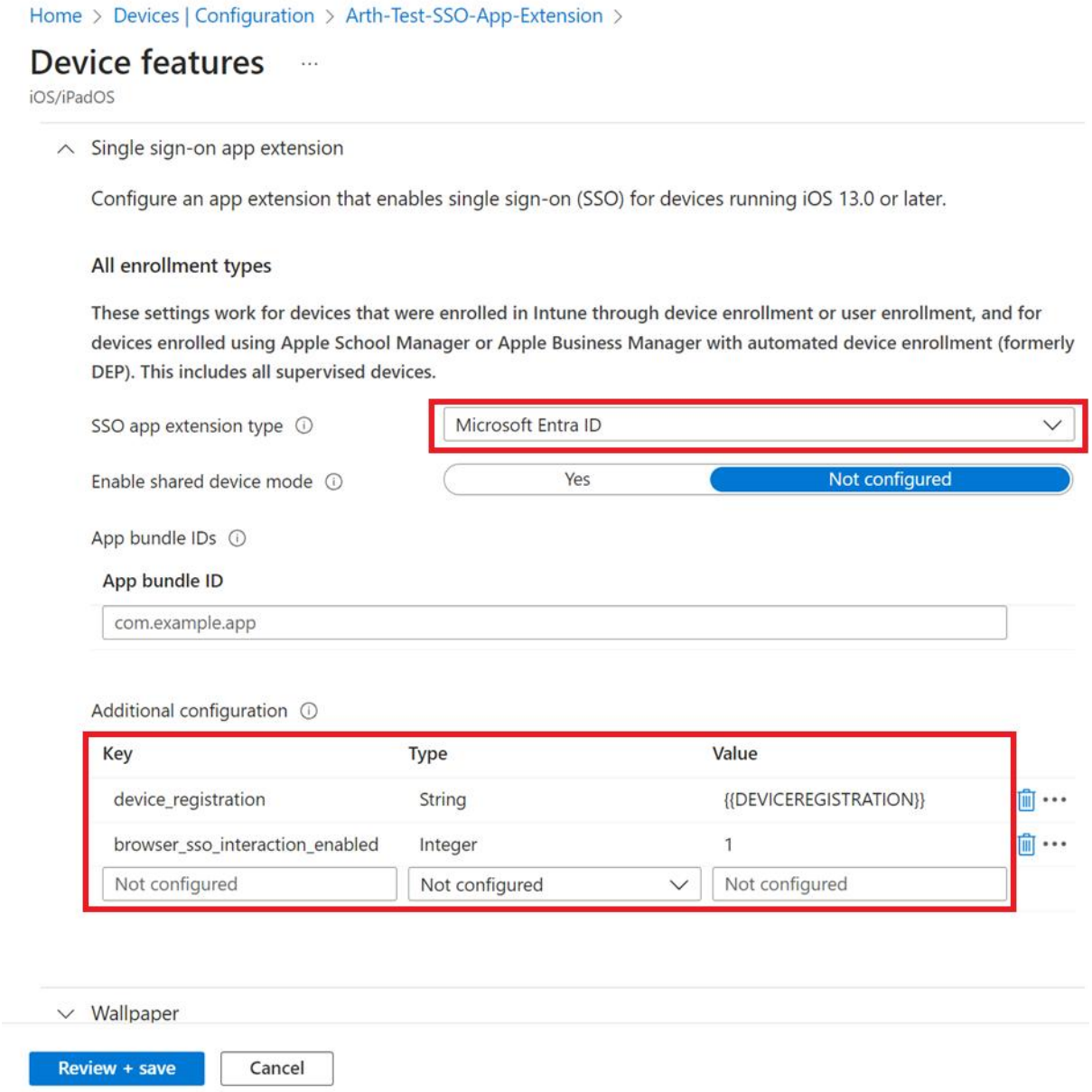
!	**NOTE:** All existing enrolments are unaffected because they have already been authenticated and enrolled. We recommend Intune Local Admin to use Modern Authentication moving forward.

Setting up the device configuration for JIT Registration for ADE

1. Create a device configuration policy under the Microsoft Endpoint Manager admin centre > Devices | iOS/iPadOS > Configuration Profiles > Templates > Device features > Category > Single sign-on app extension.
    a. Set the SSO app extension type to Microsoft Entra ID
    b. All Microsoft applications are automatically part of the iOS/iPadOS Microsoft Entra ID SSO app extension policy.
    c. Add all the App bundle IDs for non-Microsoft apps that you want SSO to be established on.
        i. After the end users first sign in, the user will be automatically signed into any Microsoft app and non-Microsoft app that’s part of the SSO extension policy.
    d. Add the required key value pair under the additional configuration.
        i. Key: device_registration
        ii. Type: String
        iii. Value: {{DEVICEREGISTRATION}}

    e. We recommend adding the key value pair that enables SSO within the Safari browser for all apps in the policy as well. (Recommended Values)

i. Key: browser_sso_interaction_enabled
1. Type: Integer
iii. Value: 1



2. Once these configuration steps are completed, the user will be able to proceed with the device's setup and registration. To fully enrol the device with Intune and establish user device affinity, they simply need to power on the device, navigate the Setup Assistant pages, and authenticate with their Azure AD credentials. When a user launches a managed Microsoft Office app, SSO is automatically enabled. We recommend that the end user sign into Teams first for the most up-to-date and streamlined experience.

5.5 iOS Configuration Policies

This section will describe the different Centralised Configuration Profile policies that configure iOS and iPadOS devices. The Centralised policies are "**Device Restrictions**" type. Intune LAs don't have rights to modify any settings on the Centralised policies however they are able to create their custom Configuration Profile Policies for their organisation.

We have also recommended how to assign policies to groups. Once the policy has been assigned to a particular group, all the iOS devices in that group will have that policy applied to it.

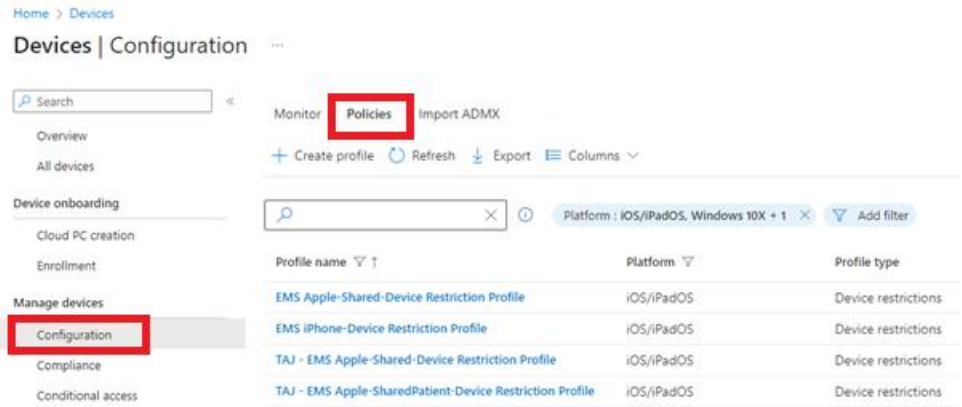
Examples of recommended policies are shown below, however Intune LAs do have the rights to change the various polices that may suit a particular organisation. For a detailed breakdown of the recommended policy settings, please see Appendix.

!	**Important Note** Any deviation from the Centralised settings and configuration should be done with consideration and prior testing. Organisations are solely responsible for changes made by their Intune LAs that have been provided with Intune RBAC permissions.

5.5.1 EMS iOS/iPadOS Device Restriction Profile Policies

There 2 Centralised iOS/iPadOS device restriction policies that Organisation can utilize as Baseline:

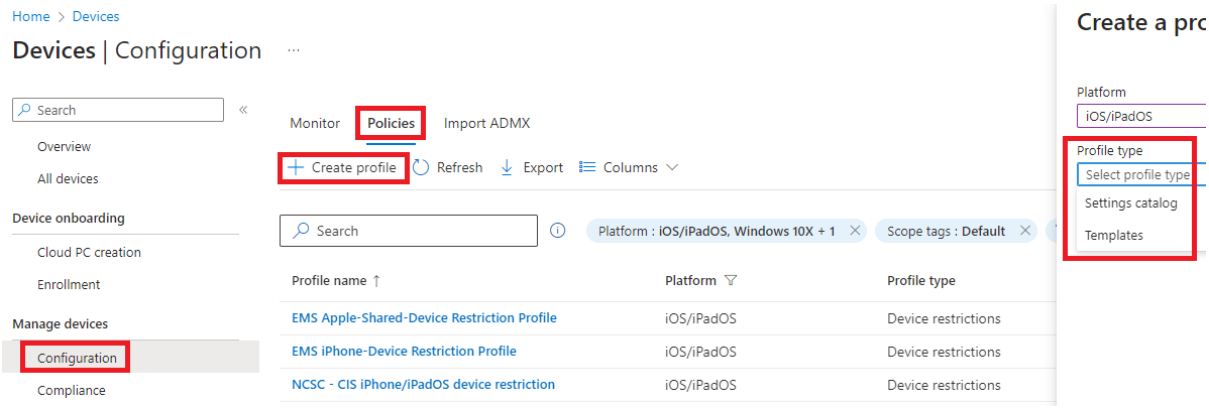
- EMS iPhone-Device Restriction Profile
- EMS Apple-Shared-Device Restriction Profile



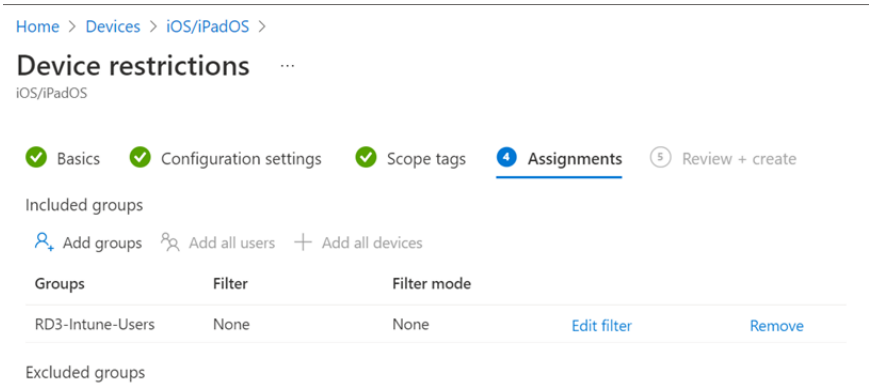
Detailed configuration settings for each Profile can be found in the Appendix of this document.

5.5.2 Creating an iOS/iPadOS Configuration Profile for your Organisation

1. Navigate to the following: **Devices > Configuration > Policies > Create Profile**.



2. Select the Profile Type: Templates or Setting catalog.
3. Enter the name and description. It is important to add the ODS in the name of the policy.
4. Enter the configuration Settings to the correspondent policy.
5. Under **Assignments**, add the users or devices group to apply the configuration profile.



6. Once you have chosen the correct options, select **Review + save**.

!	**Important Note** Any deviation from the Centralised settings and configuration should be done with consideration and prior testing. Organisations are solely responsible for changes made by their Intune LAs that have been provided with Intune RBAC permissions.

5.5.3 MacOS Configuration Profile

!	**Note:** Intune Local Admins can create their own configuration profiles to tailor their organization's requirements.

The following device configuration profiles are available if Organizations want to adopt one or more these policies:

5.5.3.1 EMS – MacOS - Activate FileVault

Configure and manage MacOS FileVault disk encryption. FileVault is a whole-disk encryption program that is included with macOS. With Intune you can deploy policies that configure FileVault, and then manage recovery keys on devices that run macOS 10.13 or later.

This policy is applied to devices in two stages. First, the device is prepared to enable Intune to retrieve and back up the recovery key. This action is referred to as escrow. After the key is escrowed, the disk encryption can start.

!	**Note:** MacOS devices with Apple silicon or an Apple T2 Security Chip, is encrypted automatically.

Escrow of keys enables Intune Local admins to rotate keys to help protect devices, and users to recover a lost or rotated personal recovery key. After Intune escrows the personal recovery key:

- Intune Local Admins can manage and rotate the FileVault recovery keys for any managed macOS device, by using the Intune encryption report.
- Intune Local Admins can view the personal recovery key for only managed macOS devices that are marked as *corporate*. They can't view the recovery key for personal devices.
- For a macOS device that has its FileVault encryption managed by Intune, end users can retrieve their personal recovery key (FileVault key) from the following locations, using any device:
    - Company Portal website (https://portal.manage.microsoft.com/)
    - iOS/iPadOS Company Portal app
    - Android Company Portal app
    - Intune app

The end-user will be prompted to enable the encryption automatically. If this action is not completed, the device will not be compliant.

!	**Note:** Intune can't manage FileVault disk encryption on a macOS device that was encrypted by a device user, unless you apply FileVault policy through Intune. For more information, please refer to Encrypt macOS devices with FileVault disk encryption with Intune.+

The following endpoint settings are enabled in this device configuration profile:

EMS - Activate FileVault	Settings
Enable FileVault	Yes
Escrow location description of personal recovery key	To retrieve a lost or recently rotated recovery key, sign in to the Intune Company Portal website from any device.

Personal recovery key rotation	12 months
Hide recovery key	Yes
Disable prompt at sign out	Yes
Number of time allowed to bypass	3
Firewall	
Enable Firewall	Yes
Block all incoming connections	No - if set to yes, will disable Stealth mode
Enable stealth mode	Yes
Gatekeeper	
Allow apps downloaded from these locations	Mac App Store and identified developers
Do not allow user to override Gatekeeper	Yes

5.5.3.2 EMS - MacOS - Device Features

Enforce the requirement to use username and password text fields while disabling content caching. Please see detailed settings below:

EMS – macOS – Device Features	Settings
Login Items	
Add the files, folders, and custom apps that will launch at login	/Applications/Company Portal.app
Login Windows	
Require username and password text fields	Yes
Disable user login from Console	Yes

5.5.3.3 EMS - MacOS - Device Restriction

Applied restrictions to the devices as per description below:

EMS – macOS – Device Restriction	Settings
App Store, Doc Viewing, Gaming	
Block adding Game Center friends	Yes
Block Game Center	Yes
Block multiplayer gaming in the Game Center	Yes
Built-in apps	
Block Safari AutoFill	Yes
Block Apple Music	Yes
Block spotlight suggestions	Yes
Block file transfer using Finder or iTunes	Yes
Cloud and Storage	
Block iCloud Keychain sync	Yes
Block iCloud desktop and documents sync	Yes

Block iCloud document and data sync	Yes
Block iCloud Mail backup	Yes
Block iCloud Contact Backup	Yes
Block iCloud Calendar Backup	Yes
Block iCloud Reminder Backup	Yes
Block iCloud Bookmark Backup	Yes
Block iCloud Notes Backup	Yes
Block iCloud Photos backup	Yes
Block Handoff	Yes
Connected devices	
Block AirDrop	Yes
Block Apple Watch auto unlock	Yes
General	
Block dictation	Yes
Block content caching	Yes
Block screenshots and screen recording	Yes
Defer software updates	Not configured
Block modification of wallpaper	Yes
Block users from erasing all content and settings on device	Yes
Allow activation lock	Yes
Password	
Require password	Yes
Required password type	Alphanumeric
Number of non-alphanumeric characters in password	1
Minimum password length	8
Block simple passwords	Yes
Maximum minutes after screen lock before password is required	5 minutes
Maximum minutes of inactivity until screen locks	Immediately
Password expiration (days)	365
Prevent reuse of previous passwords	5
Maximum allowed sign-in attempts	11
Lockout duration	30
Block password AutoFill	Yes
Block password proximity requests	Yes
Block password sharing	Yes

5.5.3.4 EMS - MacOS - Disabling Guest Users

Disable the capability of adding Guest users.

EMS – macOS – Disabing Guest Users	Settings

Disable Guest Account	True

5.5.3.5 EMS - MacOS - Prevent FileVault from Being Disabled

As per description, prevent end user from disabling FileVault.

EMS – macOS – Prevent FileVault from being disabled	Settings
Prevent FileVault From Being Disabled	True

5.5.3.6 EMS - MacOS - Enable Microsoft SSO

Activating the Microsoft Enterprise SSO plug-in allows for single sign-on (SSO) access to applications and websites utilizing Microsoft Entra ID for authentication. The following prerequisites must be met:

- The device is managed by Intune.
- The device must support the plug-in: macOS 10.15 and newer
- The Microsoft Company Portal app must be installed and configured on the device.

EMS – macOS – Enable Microsoft SSO	Settings	
SSO app extension type	Microsoft Entra ID	
App bundle IDs	com.apple.Safari	
	com.microsoft.OneDrive	
	com.microsoft.edgemac	
	com.microsoft.teams	
Additional configuration		
AppPrefixAllowList	String	com.microsoft. , com.apple.
browser_sso_interaction_enabled	Integer	1
disable_explicit_app_prompt	Integer	1

5.6 iOS Personal Device Enrolment

Personal device enrolment allows users with their own devices to securely access the NHS.net connect tenant

The required features are enabled to allow enrolment capabilities for users of personal mobile devices as:

IOS/iPad - Personal Enrolment with Company Portal

No Administrator intervention or pre-configuration is required by Local Organisations to support enrolment, there being automation to scope enrolled devices to specific ODS codes

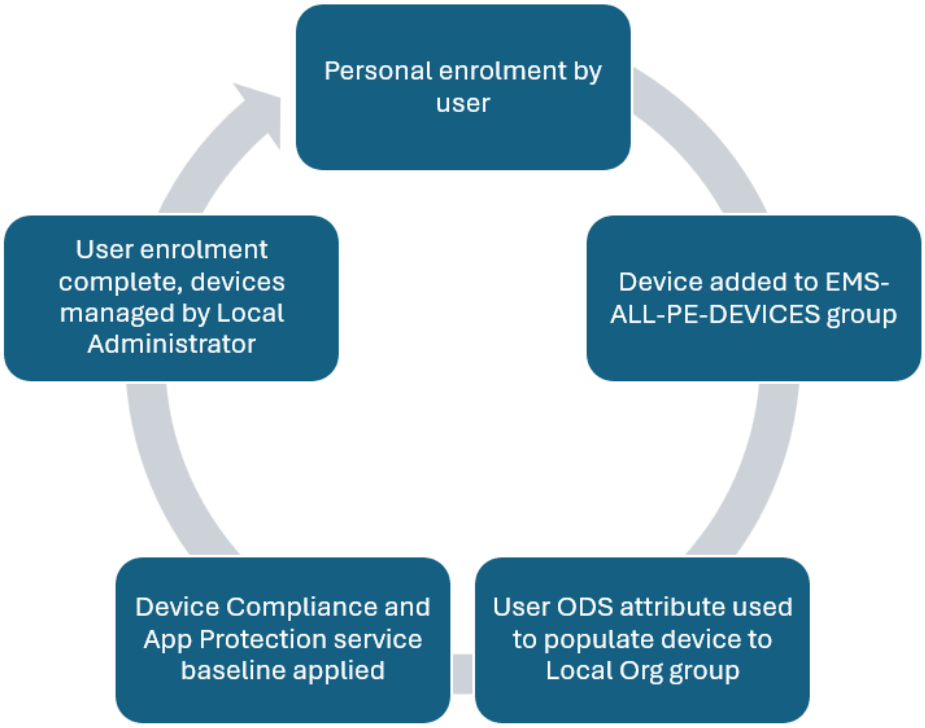
Personal Intune enrolment methods:

Since Personal enrolment is enabled, iOS/iPadOS personal devices can be enrolled via the Company Portal method. Local Administrators can advise users to follow the standard personal-enrolment process, per Microsoft's user guidance:

Microsoft Personal Apple Mobile enrolment video

Users can un-enrol and re-enrol personal devices without Local Administrator intervention.

The following diagram describes the enrolment, scoping and baseline configuration process for personal enrolment devices:



Once personal devices are enrolled and configured, the following groups are used for scoping and to apply the fundamental configurations.

EMS-ALL-PE-DEVICES

This dynamic device group populates any mobile device enrolment *(rule: device.deviceOwnership -eq "Personal"*). Service automation that creates and then scopes the device into a Local Organisation assignment group, based on the User's ODS attribute:

ODS.sg.Intune-iOS-PE-Devices

Contains all Personal-enrolled iOS/iPadOS Devices for a Local Organisation

!	**Important Note:** If a user moves to another organisation, the personal device will not automatically un-enrol but will be added to the destination Local Org device group as above.

Local Administrators can use the 'PE-Devices' groups to assign policy to Personally-enrolled devices if required, however user-assigned methods should be favoured.

EMS-MDM-USER-SCOPE

This 'global' group is used to assign the following Intune Service Security Baselines which align with existing App Protection policies, but use specific device compliance policies. The mandatory policies applied to users of personal devices in this group are:

Device Compliance:

Global-Baseline-iOS-PE-Compliance-Policy-R1

App Protection:

Global-Baseline-APP-Managed-iOS/iPad-R1
Global-Baseline-APP-Unmanaged-iOS/iPad-R1

The EMS-MDM-USER-SCOPE group contains Local Organisation 'Intune Users' groups, 'ODS.sg.Intune-Users', and so Local Administrators should apply required apps, configurations and policy for users as such.

5.6.1 iOS Personal Device Enrolment Restriction

Although Personal Device Enrolment is allowed by default for all Organizations, Organizations can continue to block Personal Device Enrolment via a Service Request to have their ODS.sg.intune-Users group added to the iOS Device Enrolment Restriction Policy (iOS-PE-Restriction).

Once an Organization is in a position to allow Personal Device Enrolment, a Service Request can be made to have their ODS.sg.intune-Users group removed from the iOS Device Enrolment Restriction Policy (iOS-PE-Restriction). This will then allow end users to enroll their Personal Devices and access NHS Resources safely and securely.

5.7 iOS Defender for Endpoint

Local Admins can automatically on-board Mobile Devices to Microsoft Defender XDR. By deploying the Defender App to iOS and then applying an App Configuration policy to the same, devices can be automatically tagged. In doing so, mobile devices will be visible in the XDR UI.

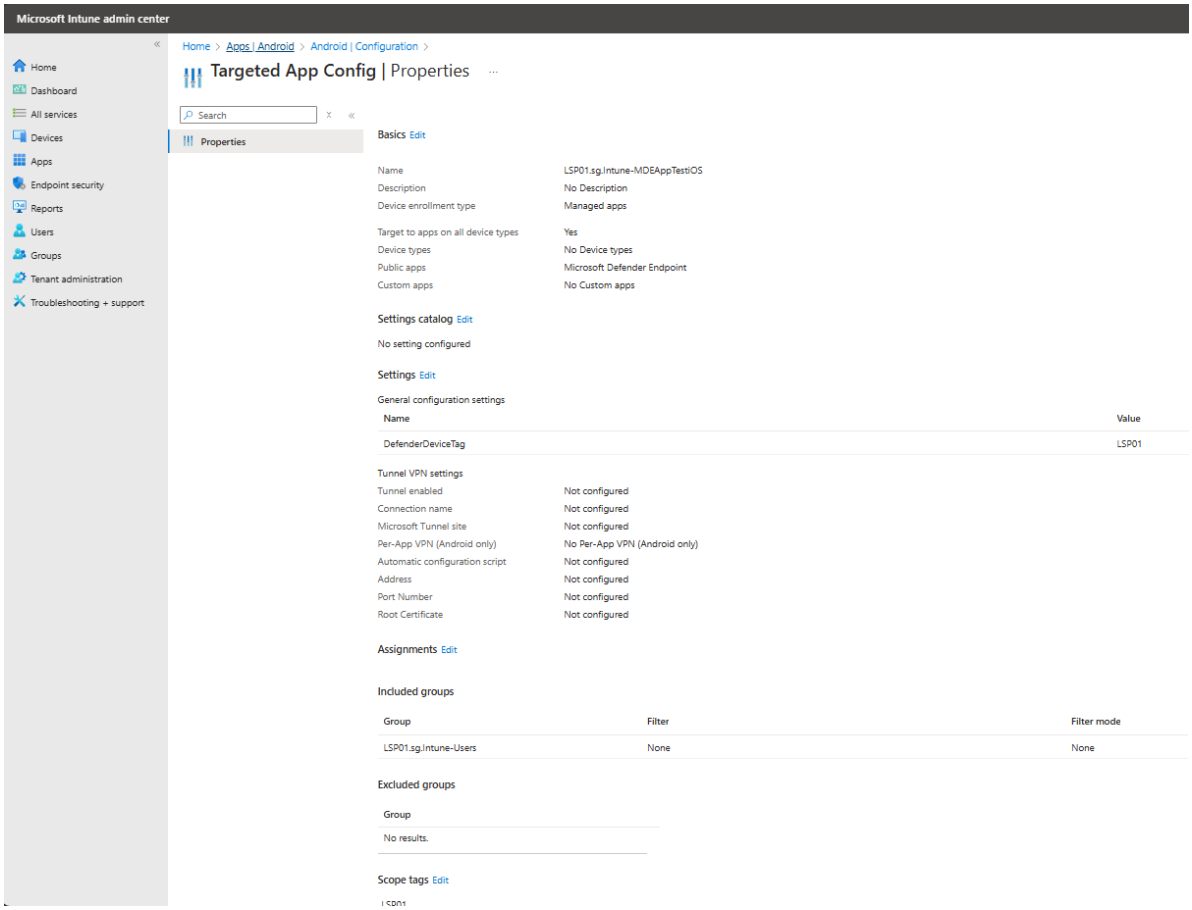
Device Tagging can be applied to Managed Devices & Managed Apps. The following outlines the process for modifying both Managed Device Tagging and Managed Apps Tagging for Microsoft Defender for Endpoint.

!	**Note:** Policies can be created via a service request and these steps are guidance on how the policies can be modified / amended to suit an Orgs needs.

5.7.1 Modifying Managed App Tagging

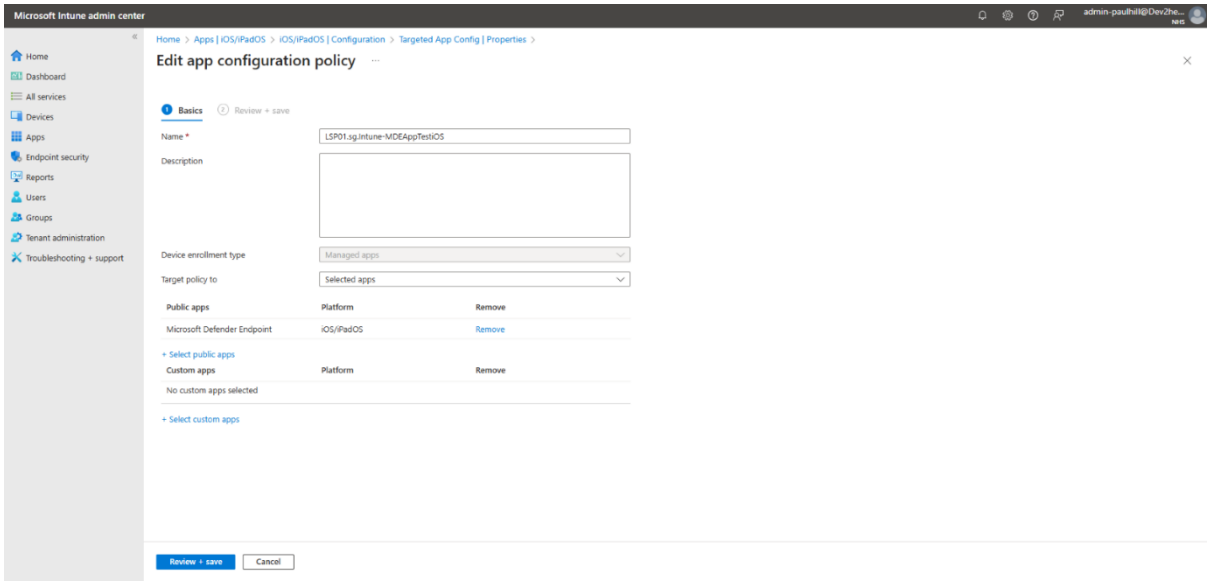
1. From Intune, navigate to Apps > iOS/iPadOS > Configuration
2. Search for the Policy, click on it and go top Properties.
3. The sections that can be modified are;
    - Basics

- Settings Catalog
- Settings
- Assignments
- Scope tags



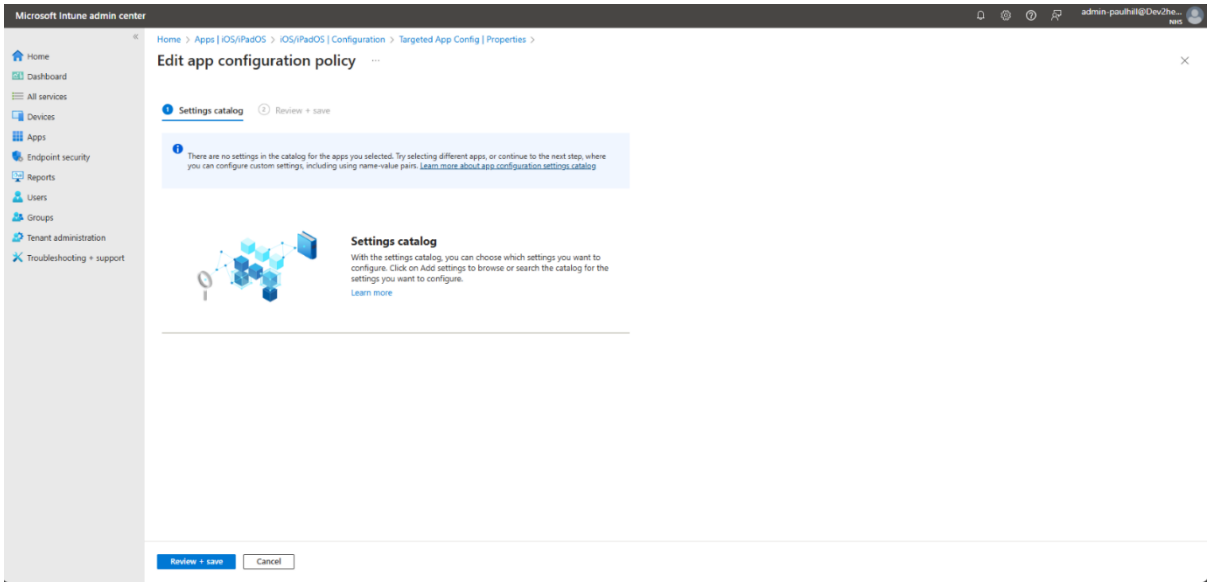
Edit Basics settings

1. Click Edit next to Basics
2. The policy name and description can be modified
3. It is not recommended to modify the targeted apps as the policy is already configured to the Defender App.
4. Click Review + save to save the modifications.



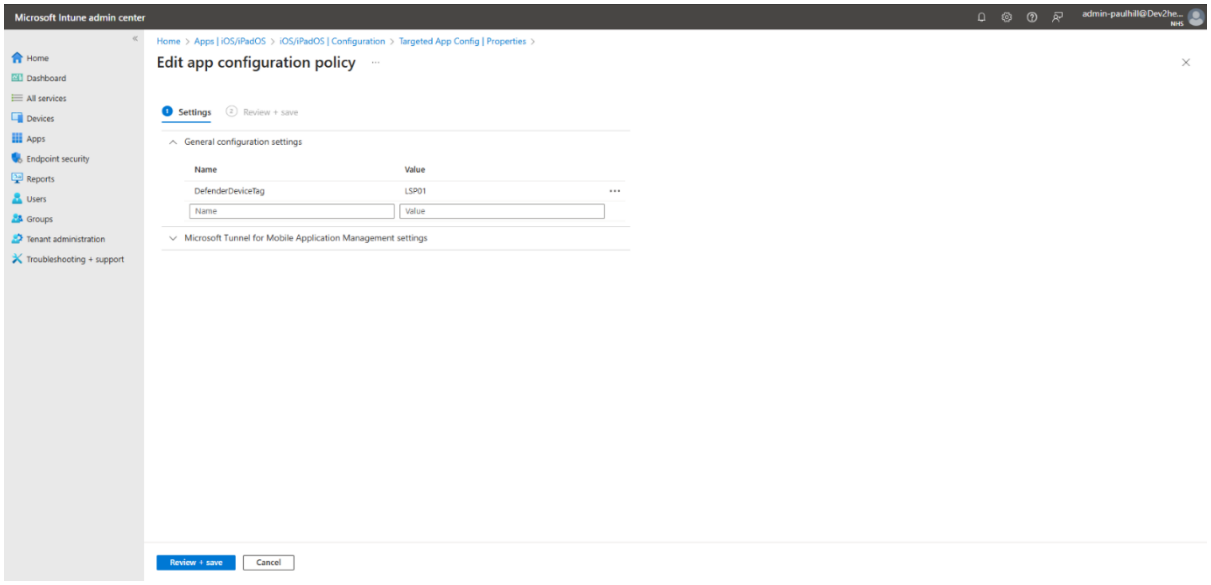
Edit Settings catalog

1. There are no settings for this particular app that can be modified.



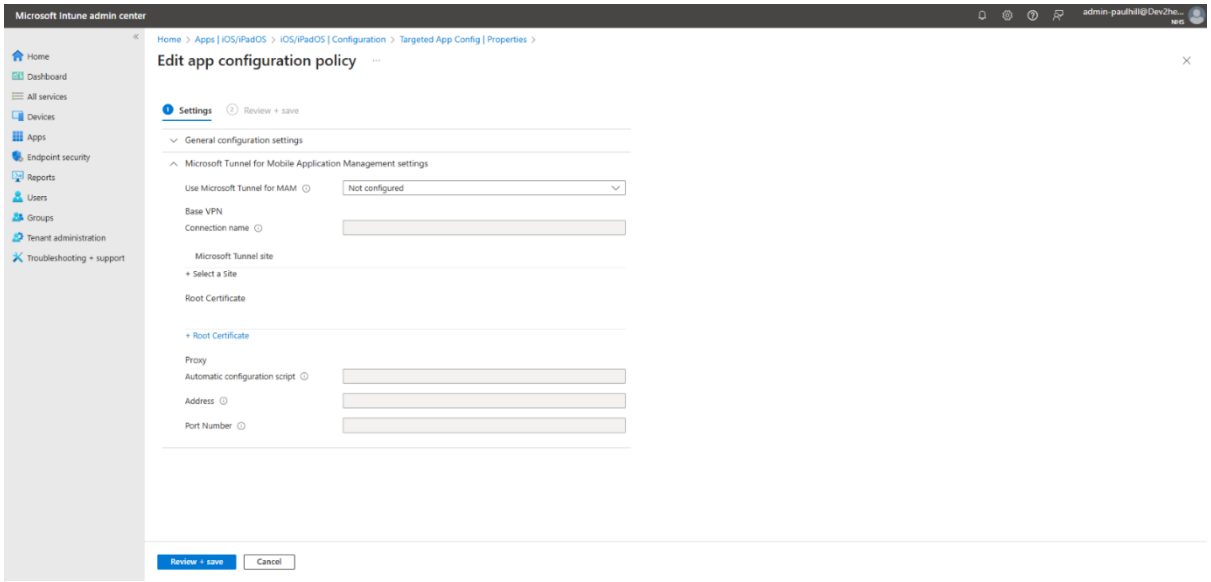
Edit Settings

1. It is not recommended to modify the General configuration settings as the policy has already been configured to the correct Name and Value for Defender and the Organization ODS.



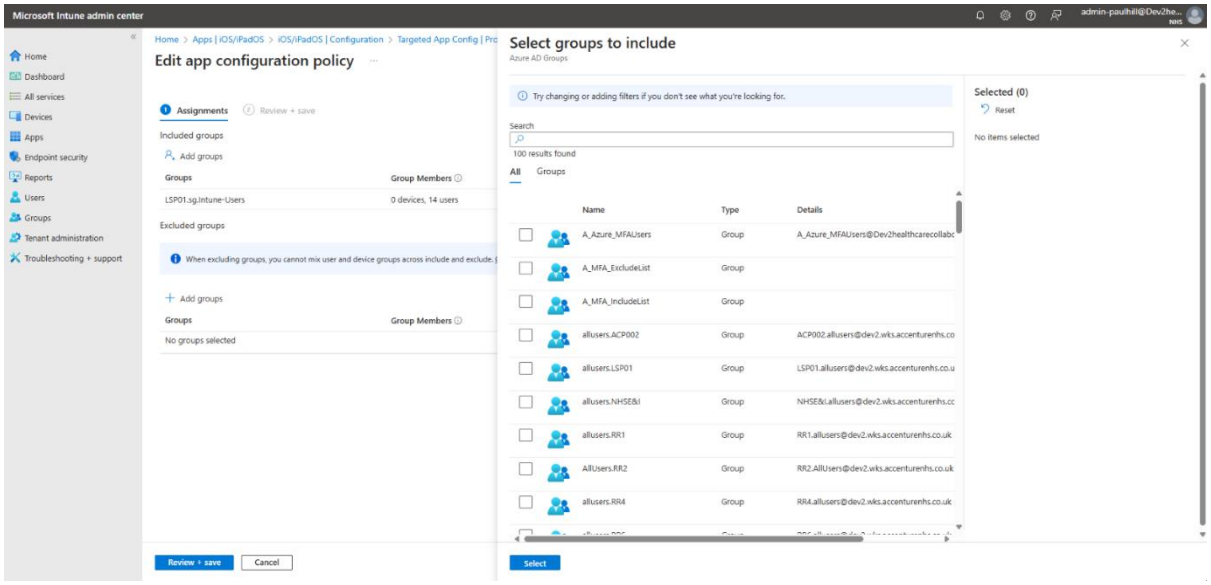
2. If required, Tunnel for MAM can be configured in the Microsoft Tunnel for Mobile Application Management Settings.

3. Configure the Tunnel as required and click Review + save to save the modifications.



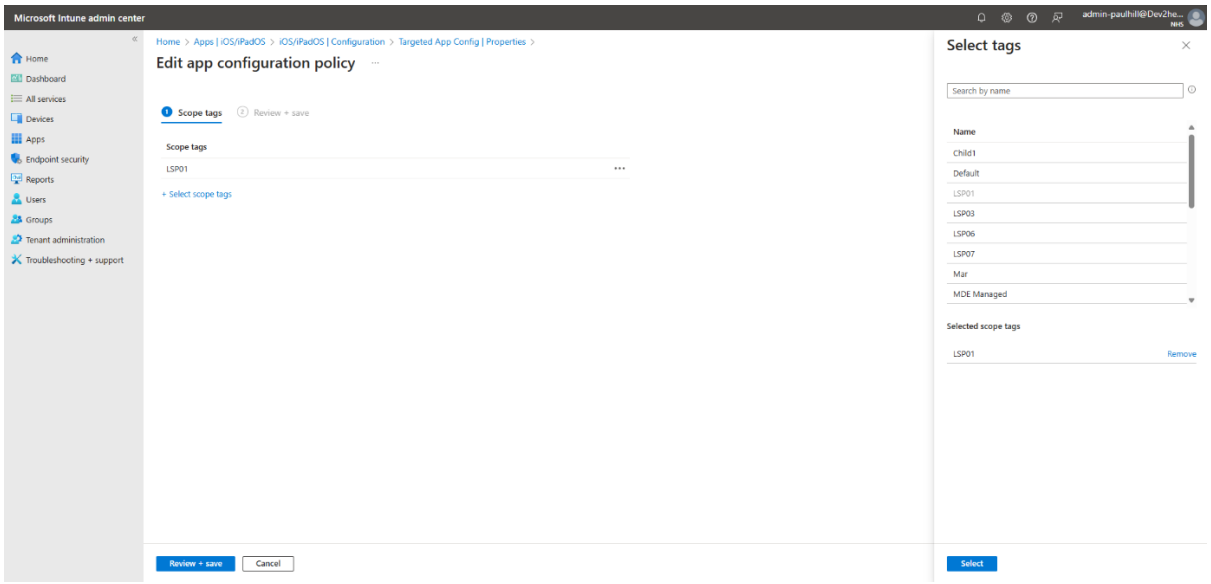
Edit Assignments settings

1. Click + Add Groups in either of the Include groups or Exclude groups sections to add groups that should be included or excluded from the policy.
2. Groups added to the Include groups section will have the Defender policy applied.
3. Groups added to the Exclude groups section will be exempt from the policy.



Edit Scope tags

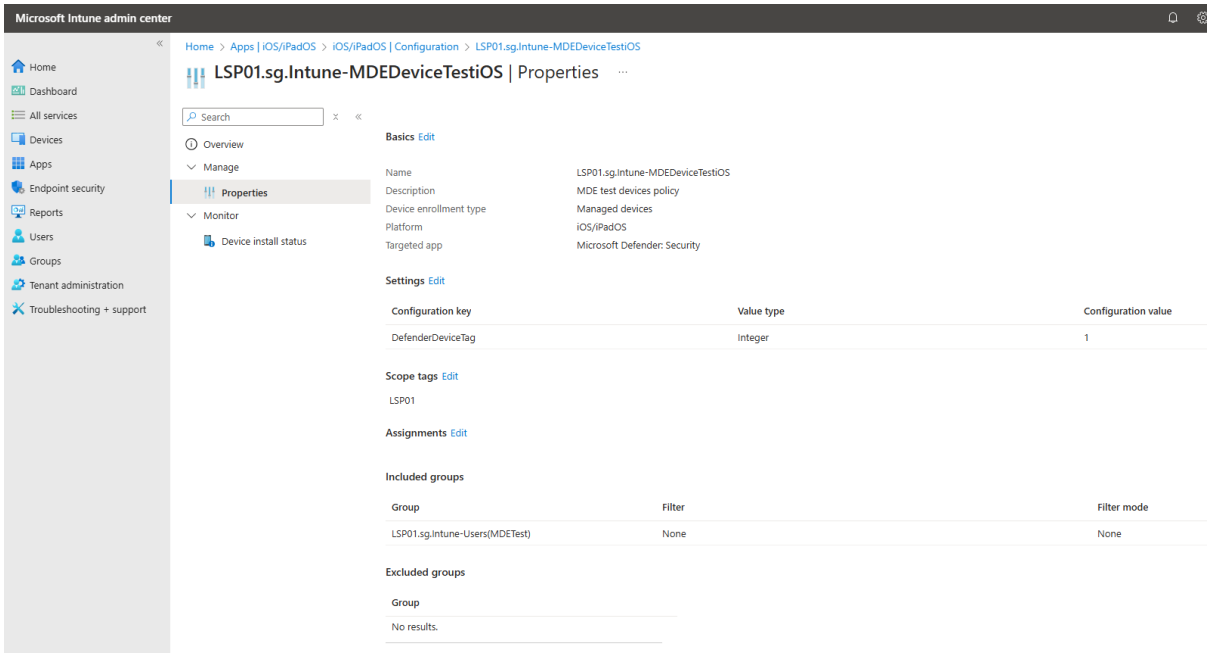
1. It is not recommended to modify the Scope tags as the policy has already been configured to include the Orgs ODS.



=-poklm,n -=[pl

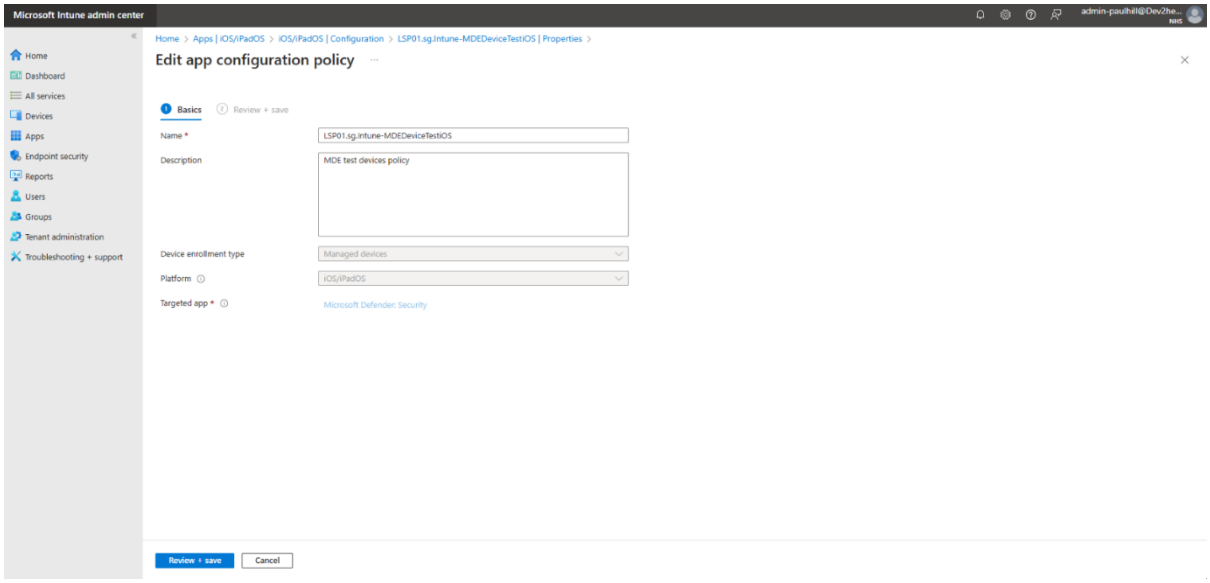
5.7.2 Modifying Managed Device Tagging

1. From Intune, navigate to Apps > iOS/iPadOS > Configuration
2. Search for the Policy, click on it and go top Properties.
3. The sections that can be modified are;
    - Basics
    - Settings
    - Scope tags
    - Assignments



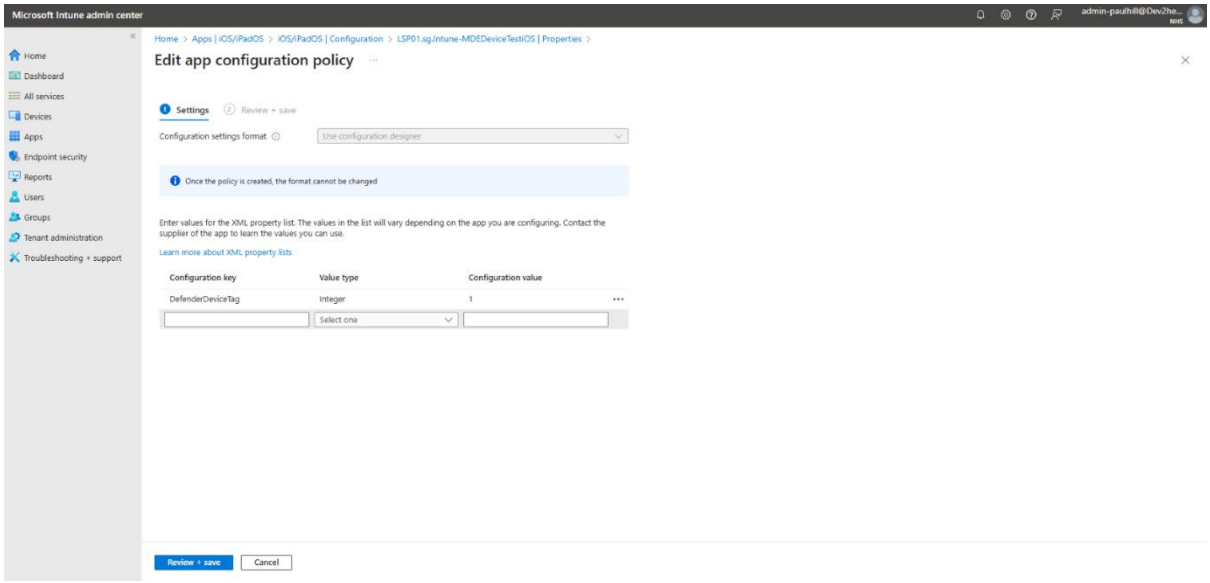
Edit Basics settings

1. The Policy Name and Description can be modified
2. Click Review + save to save the modifications



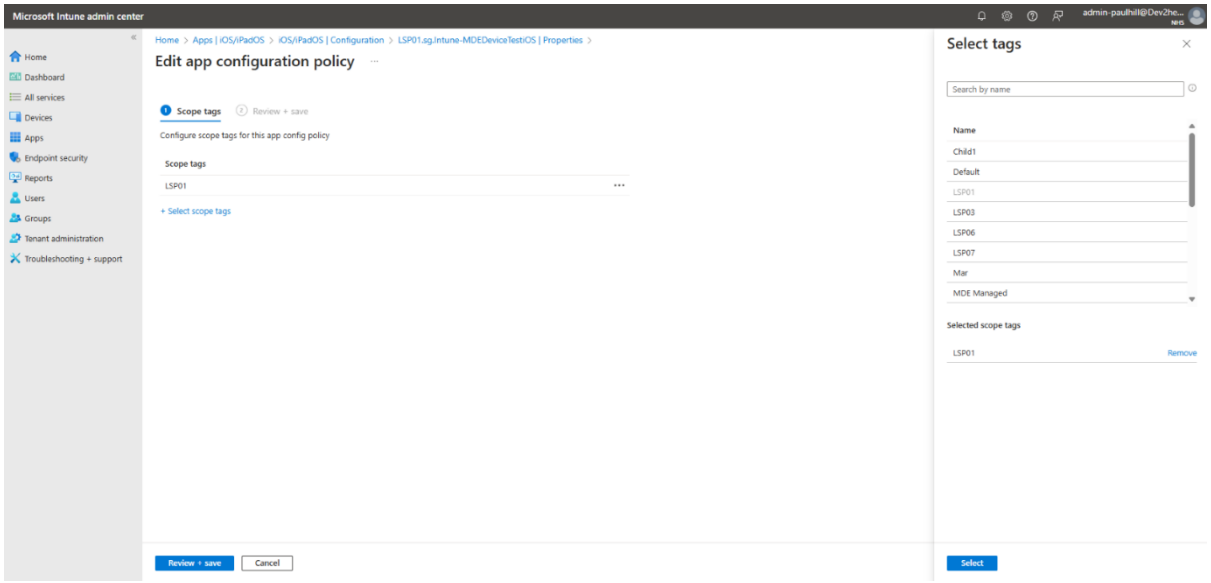
Edit Settings

1. It is not recommended to modify any setting in the Settings section as the policy has already been configured to the Defender App.



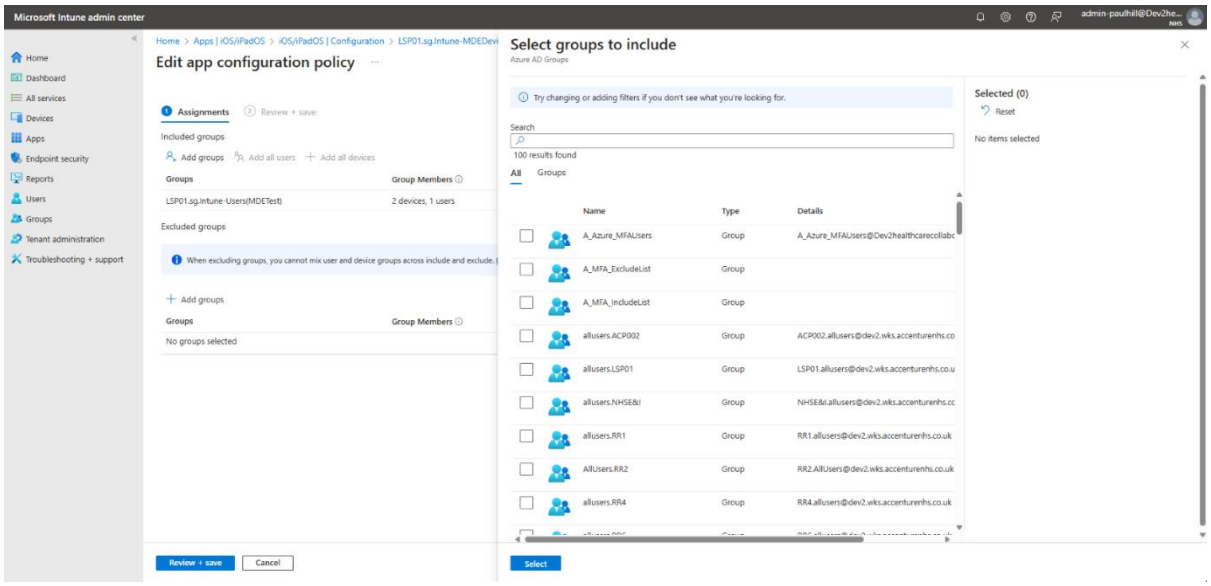
Edit Scope Tags

1. It is not recommended to modify the Scope tags as the policy has already been configured to include the Orgs ODS.



Edit Assignments settings

1. Click + Add Groups in either of the Include groups or Exclude groups sections to add groups that should be included or excluded from the policy.
2. Groups added to the Include groups section will have the Defender policy applied.
3. Groups added to the Exclude groups section will be exempt from the policy.



5.8 Retiring/Unenrolling iOS/iPadOS

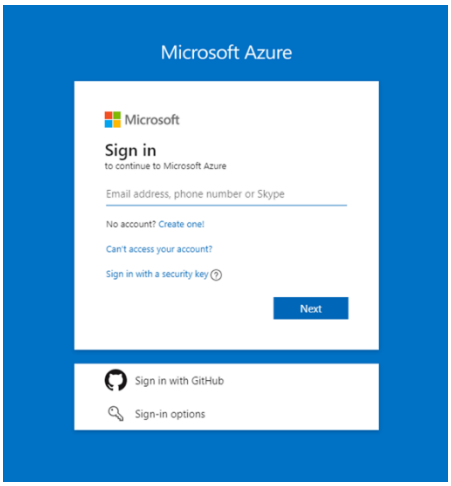
With delegated RBAC controls Intune LAs have the permissions to remotely wipe and remove iOS/iPadOS and Android devices from the NHSmail Intune platform. This action should be performed only as a last resort for devices experiencing issues

and Intune LAs are not required to seek support from the Intune Live Service Team to complete this action.

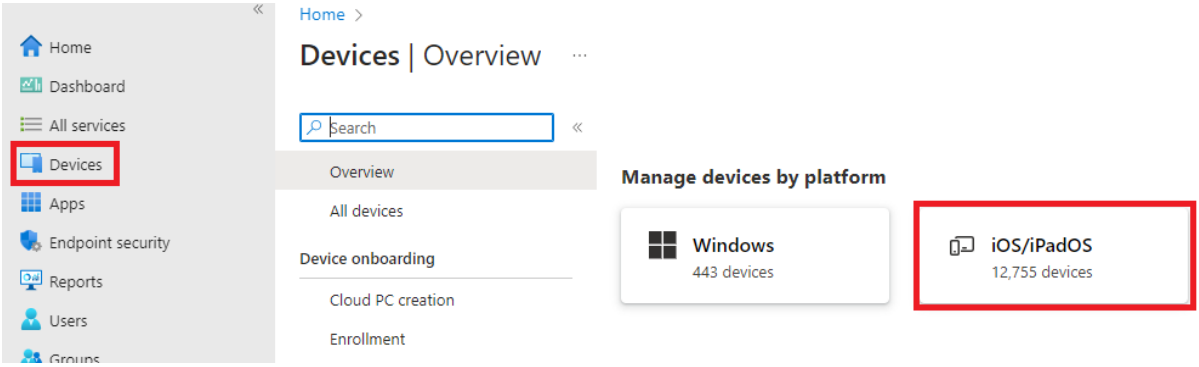
5.8.1 Wiping an iOS/iPadOS

Devices can be wiped through the Intune Portal by following the below steps:

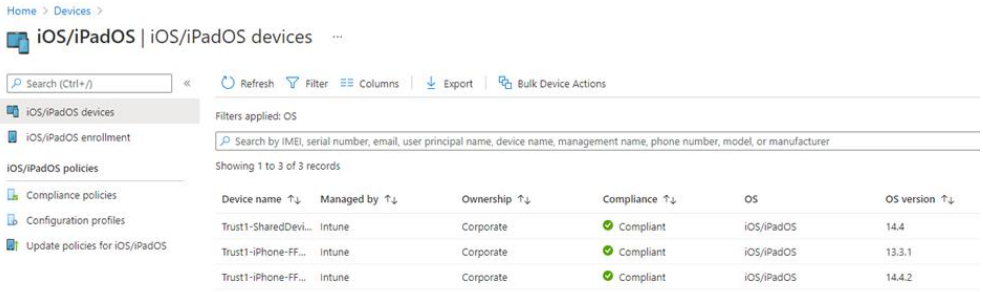
1. **Sign into** the Intune Portal.



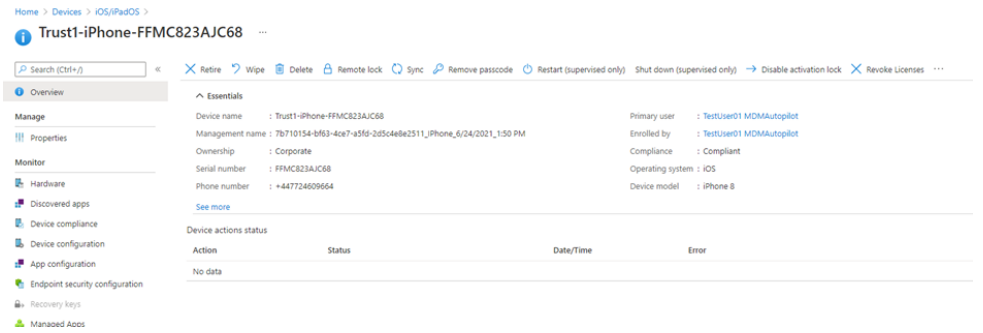
2. Select the **Devices** page.



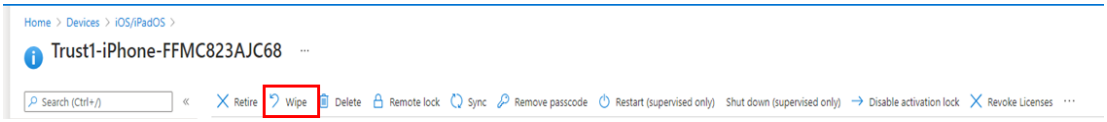
3. **Find** the device that you would like to be wiped.



4. **Select** the device to be wiped.

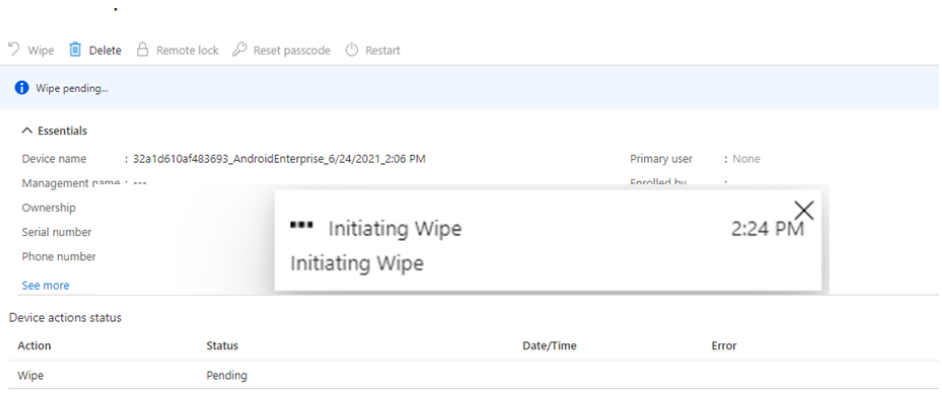


5. You be presented with a list of options at the top of the page. Select **Wipe** to factory reset the device and remove all data.



6. You will be prompted to confirm that you want to wipe the device. Select **Yes**.

7. The device will now begin wiping.



8. After the wipe has been initiated the device will be removed from the Portal.

5.9 MacOS Shell scripts

- **DowngradeUsertoStandard:** This script will downgrade the Local admin account setup during the device initial setup, if this is completed by the end user, to a standard account.

!	**Note:** Intune local adminis are responsible for establishing and maintaining a Local Admin account on their macOS devices under their supervision

5.10 Update policies for macOS

EMS - macOS - Software update: policy that enable software updates on the macOS Devices.

EMS – macOS – Software Update	Settings
Critical updates	Install immediately
Firmware updates	Install immediately
Configuration file updates	Install immediately
All other updates (OS, built-in apps)	Install immediately
Schedule type	Install immediately

6. Android Device Enrolment and Management

This section will outline the process you will need to follow and complete to successfully enrol an Android device.

In summary, this section covers:

- What is currently in place: there are Centralised Profile settings, and it is advised that you follow these. However, custom RBAC roles enable Intune LAs to create their own configuration profile policies.
- Details on device and software requirements required prior to enrolling any Android device.
- Details about the RBAC model and how this enables Intune LAs to change policies.
- What you will need to do to maintain the Android environment.
- The steps to show how groups are assigned to the policies that are in place.
- The naming standards that we have implemented for creating groups and it is advised that you follow.
- How to create configuration profiles with examples.
- How to deploy an application to a Fully Managed Android device.

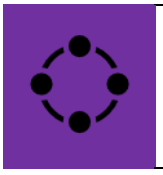
Android Enterprise which was previously known as ‘Android for Work’ is a platform managed by Google which allows Android devices and Apps to be managed by Intune.

Intune allows organisations to set up a separate Android Enterprise Profiles, enabling them to manage their devices as well as their apps. Google Android Enterprise provides for 4 types of enrolment profiles.

!	**Important Note** The NHSmail Intune solution provides enrolment via 2 main Google Android Enterprise enrolment profiles: 1. Android Enterprise - Corporate-owned Fully Managed user devices 2. Android Enterprise Dedicated Devices (Shared Device mode) This will involve scanning the QR code on an Android device when enrolling the device into Intune.

	A 3rd enrolment token is also available for Google Zero Touch devices.

Enrolment Type	Description	Available?
Android Enterprise - Corporate-owned, fully managed user devices	For corporate-owned, single user devices used exclusively for work and not personal use. Admins can manage the entire device and enforce policy controls unavailable to personally owned/corporate-owned work profiles.	Yes
Android Enterprise - corporate-owned devices with work profile	For corporate-owned, single user devices intended for corporate and personal use.	No
Android Enterprise Dedicated	For corporate-owned, single use devices, such as digital signage, ticket printing, or inventory management. Admins lock down the usage of a device for a limited set of apps and web links. It also prevents users from adding other apps or taking other actions on the device.	Yes
Android Enterprise - personally owned device with work profile	For personal devices granted permission to access corporate data. Admins can manage work accounts, apps, and data. Personal data on the device is kept separate from work data and admins don't control personal settings or data.	No
Samsung Knox Mobile Enrolment (KME)	Samsung Knox is available for Organisations that want to use it via Intune. Please refer to Samsung Knox Mobile Enrolment (KME) for full details on how to enable it.	Yes



Managed Centrally

Both the managed Google Play account/connector and enrolment profiles are managed centrally. Intune LAs are unable to edit these.

6.1. Hardware and Software Requirements

Prior to enrolling any Android devices onto Intune the following minimum device and software specifications should be validated.

Device and software requirements:

- Android devices must run Android OS 8.0 and above
- Newer, lower specification Android phones that run the Android ‘go’ version are not supported for Android Enterprise ‘Fully Managed’ enrolment.
- Android device must have a functioning camera to scan the QR enrolment code.
- Devices must run a distribution of Android that has Google Mobile Services (GMS) connectivity.
- Devices must have GMS available and must be able to connect to GMS.

Critical Notes that will require action

Device updates for Android devices are the responsibility of organisations.

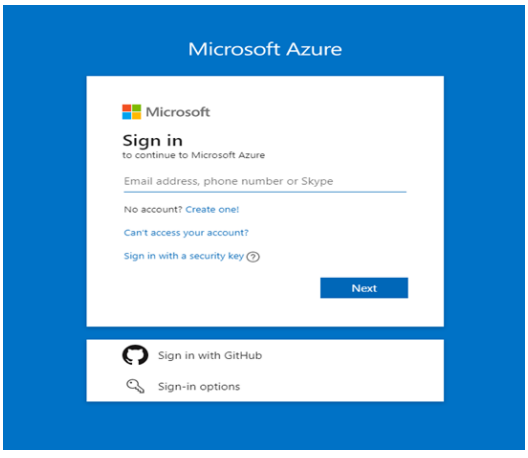
6.2 Single and Shared Android Enrolment

This section will outline the process you will need to follow and complete to successfully enrol an Android device.

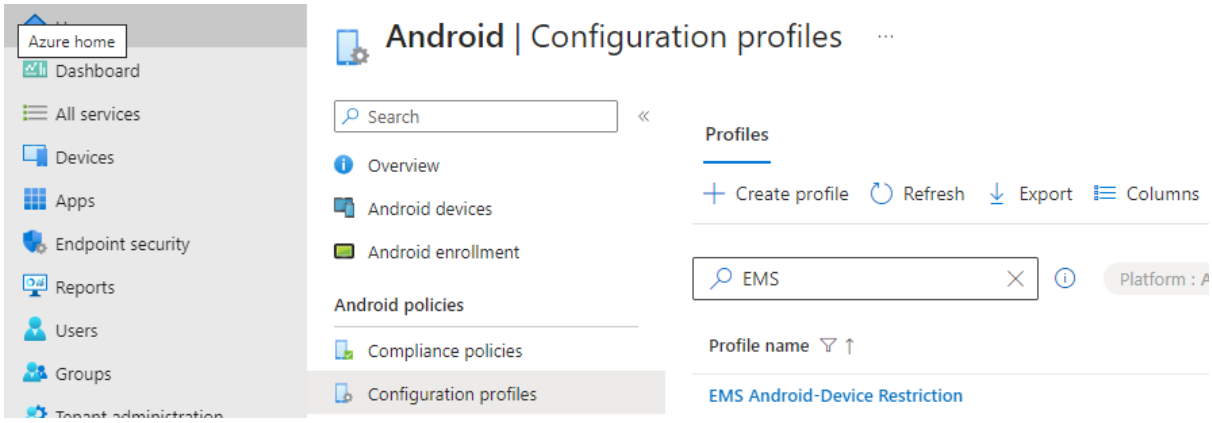
6.2.1 Single User Android Device Enrolment

The following steps will cover some of the pre-configurations required to enrol an Android device.

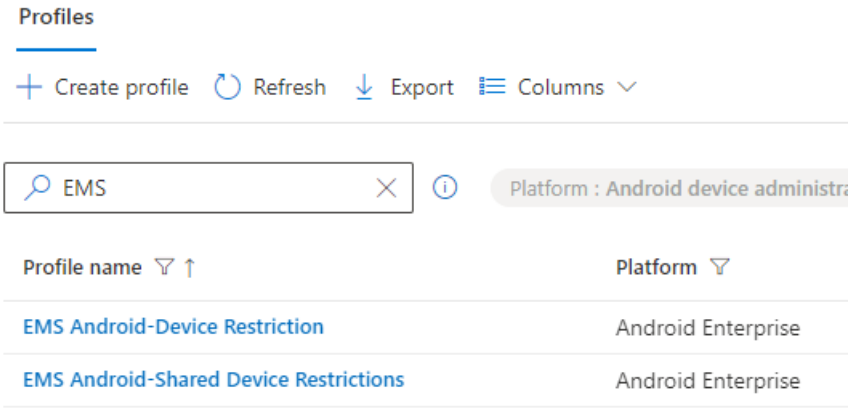
1. **Login** into the Intune Portal: https://endpoint.microsoft.com/



2. Next, navigate to **Devices > Android > Configuration Profile** to setup the Android Configuration Profiles. This will need to be done before a user enrols.

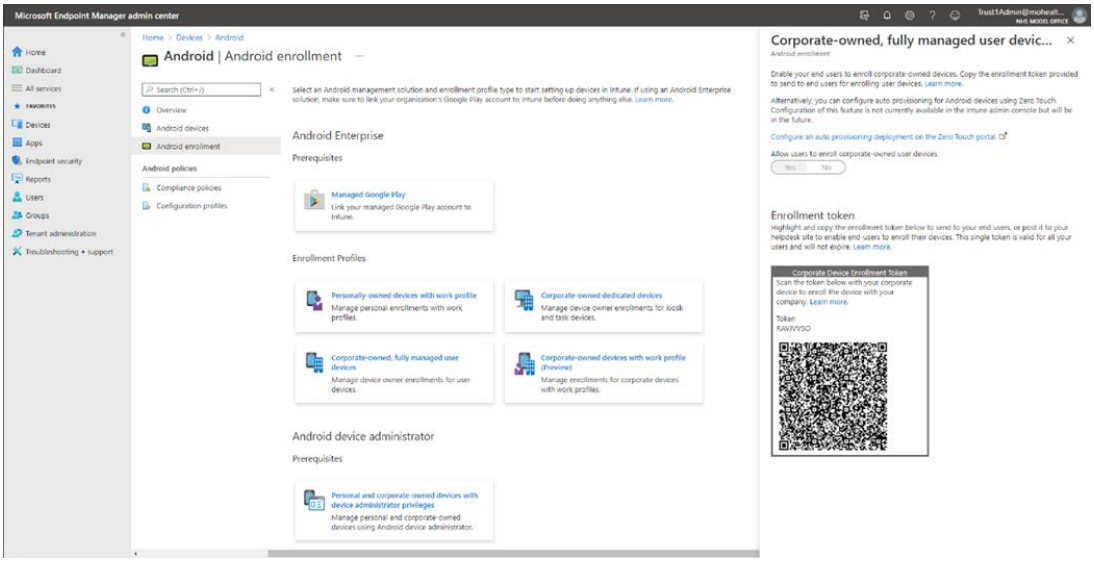


3. There will be a set of Centralised configuration policies that are already in place, and you will have to the ability to use them if you like. Alternately, Intune LAs can create their own custom Configuration Profile Policies.



!	**Important Note** Ensure that you add your local org user group to the assignments. Otherwise, policies and apps will not get pushed to end users.

4. Once devices profiles have been added, you can then forward the enrolment token to users. Navigate to **Devices > Android > Android Enrolment > Corporate Owned, Fully Managed user** to see the QR code.

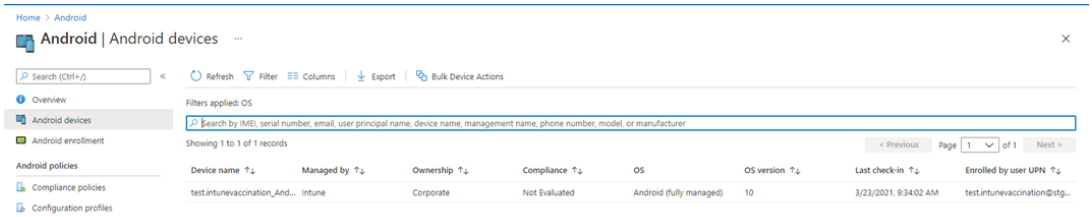


5. Send the QR code to the user.

> **Important Note**
>
> End users should only enrol **corporate devices** onto Intune using the QR code. Please ensure that end users at your organisation are aware that **they should not be enrolling any personal, private devices onto Intune using the QR code**.

> **Important Note**
>
> Android 8.0 and above is required to use the QR enrolment method.
>
> It is recommended that all devices are regularly updated to the latest Android version to ensure that they have the latest security patches.

6. End users' devices should then populate in the devices section in Intune. **Devices > Android > Android Devices**.



6.2.2 Shared Device Android Enrolment

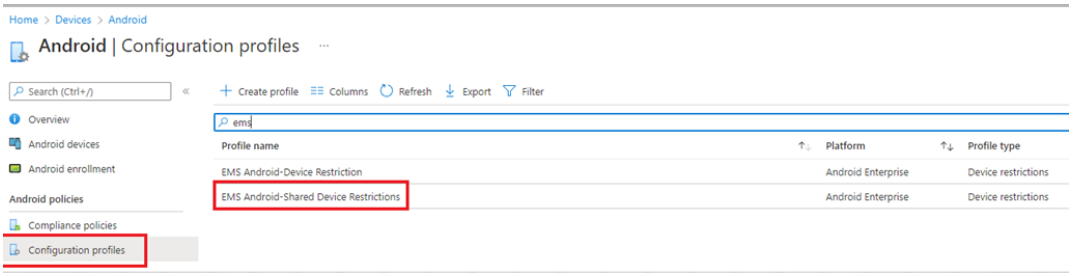
!	**Important Note** LAs will need to raise a service request to create shared device enrolment token.

The setup of Android shared mode is a very similar process to the setup process required for a standard single user device. Please follow the same process for enrolling a standard device.

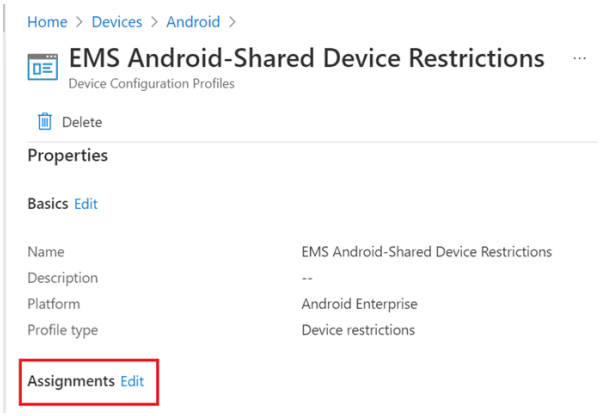
There are a few differences in the setup and it's important to note that there will be a separate enrolment profile for the shared devices. If you want to set up a shared device, you will need to apply **the Centralised shared device enrolment profile** to that group.

The steps below highlight the actions required to setup a shared device and how this is different to enrolling a single user device.

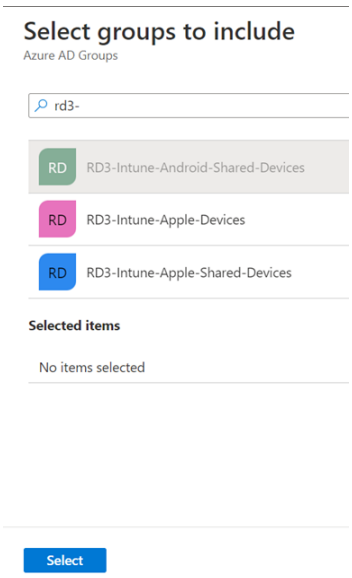
1. Navigate to: **Device > Android > Configuration Polices**.



2. Select "**EMS Android-Shared Device Restrictions**" and then navigate to **Assignments > Edit**:



3. Select **Add groups** > select the Azure AD group that contain Users/Shared-Android-Devices for your Organisation **> Select**:



4. Select **Review + save > Save** to finish the assignment of the group to the **EMS Android-Shared Device Restrictions**.

6.3 Android Configuration Profiles

This section will describe the different Centralised Configuration Profile policies that configure Android devices. The Centralised policies are "**Device Restrictions**" type. Intune LAs don't have rights to modify any settings on the Centralised policies however they are able to create their custom Configuration Profile Policies for their Organisation.

In addition, this section will cover how assign see the Centralised polices that we have recommended as well how to assign policies to group. Once the policy has been assigned to a particular group, all the Android devices in that group will have that policy applied to it.

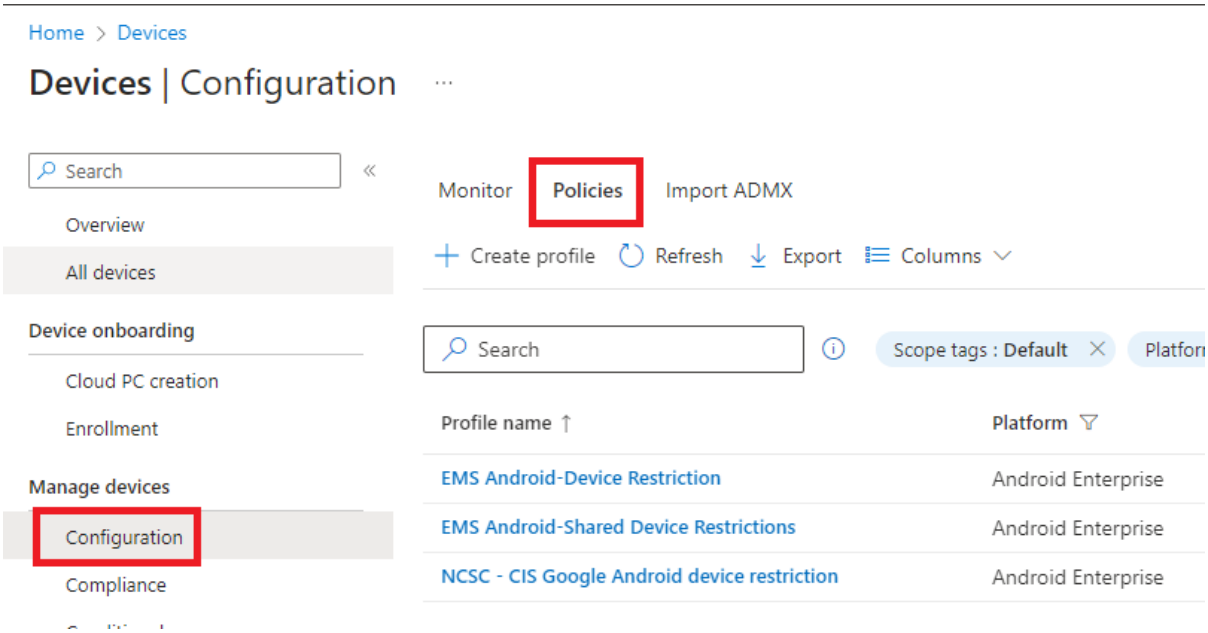
For a full list of recommended Android policy settings, please see Appendix.

!	**Important Note** Please see this link for a detailed list of all the device restriction polices and what they do. This will highlight what polices you may need to enable to resolve an issue that you have. https://docs.microsoft.com/en-us/mem/intune/configuration/device-restrictions-android-for-work

6.3.1 EMS Android Device Restriction Profiles

There 2 Centralised Android device restriction policies that an Organisation can utilize as Baseline:

- EMS Android-Device Restriction
- EMS Android-Shared Device Restrictions



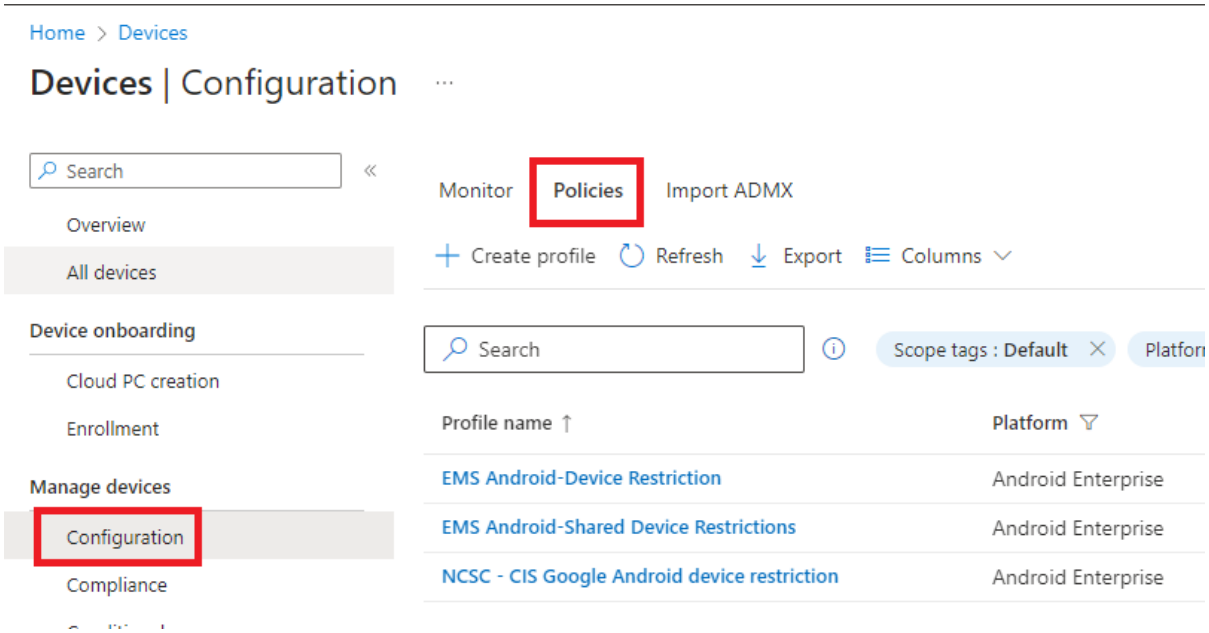
Detailed configuration settings for each Profile can be found in the Appendix of this document.

6.3.2 Creating an Android Device Configuration Profile

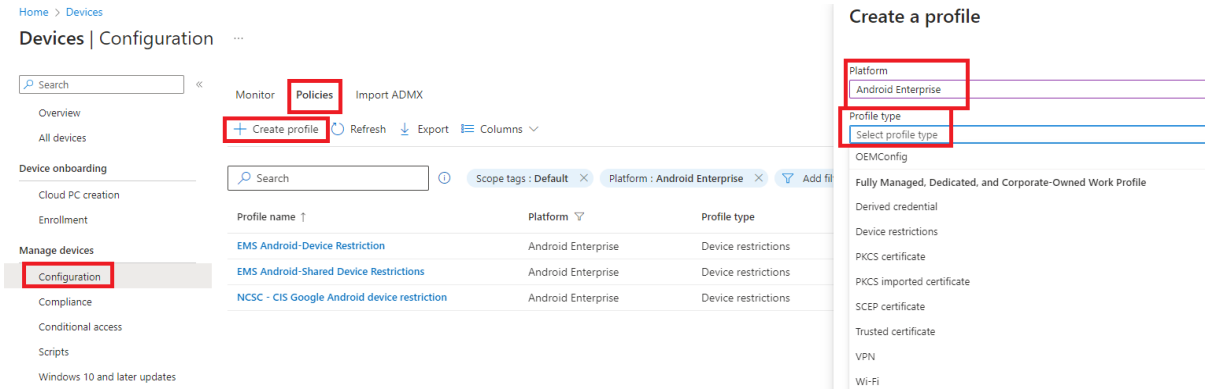
Below are instructions that detail how to create configurations policies to fit your organisation.

!	**Important Note** Any deviation from the Centralised configuration profiles should be done with consideration and prior testing. Organisations are solely responsible for changes made by their Intune LAs that have been provided with Intune RBAC permissions.

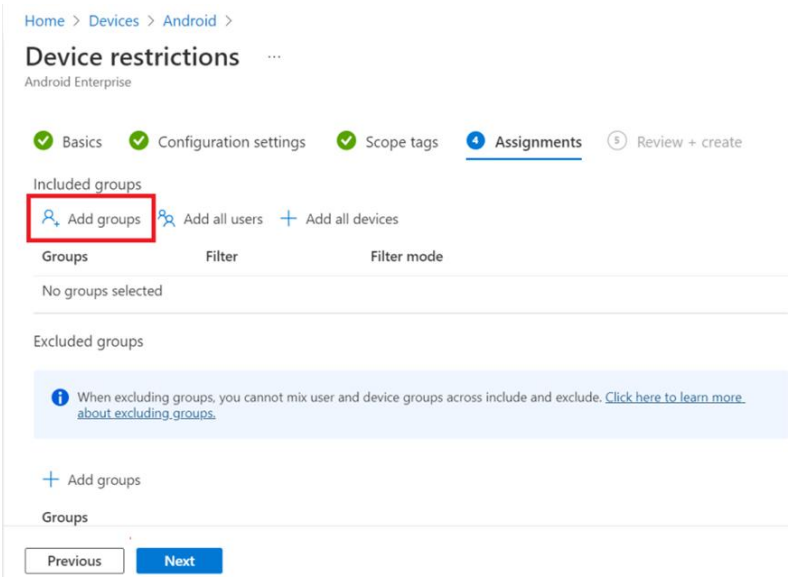
1. Navigate to the following: Devices > Configuration > Policies > **+ Create Profile**:



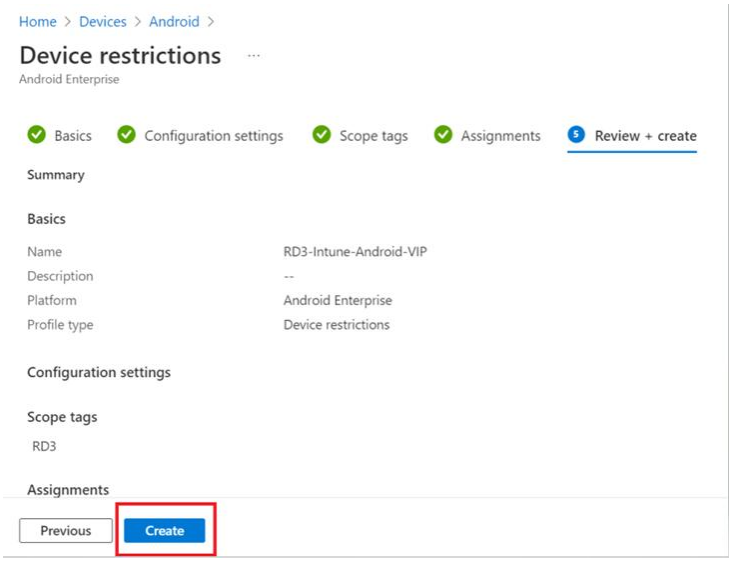
2. Then select **Android Enterprise**. Under Profile Type, select the desired type e.g., Device Restrictions > **Create**



3. Enter a Name and Description for the configuration Profile. It is important to add the ODS in the name of the policy.
4. Enter the configuration Settings to the correspondent policy
5. Under **Assignments**, add the users or devices Azure AD group to apply the configuration profile selecting "**Add groups**" > **Next**



6. Under **Review + create**, review the settings that you want to apply and then click Create.



6.4 Android Application Management

The below steps will cover the actions that are required to deploy an application to a Fully Managed Android Device.

!	**Important Note** • The Managed Google Play Store is the sole method of app deployment for Android Enterprise devices. This is a central store, so it is possible for common apps e.g., Outlook to already be approved within the environment. • Intune LAs should not be concerned if they see another organisation assigned to the same application. • Intune LAs have permissions beyond the scope of their own organisation. Intune LAs **should not unapprove/delete any**

app that is already approved within the Google Play Store. Apps can be assigned be selecting the app and assigning your AAD Group.

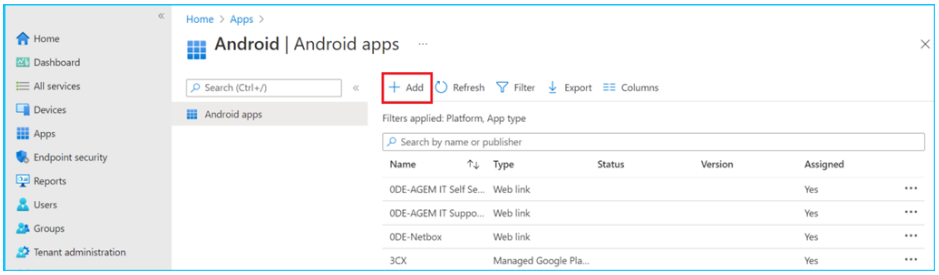
- Any deleted application can be approved and imported again.

Important Note

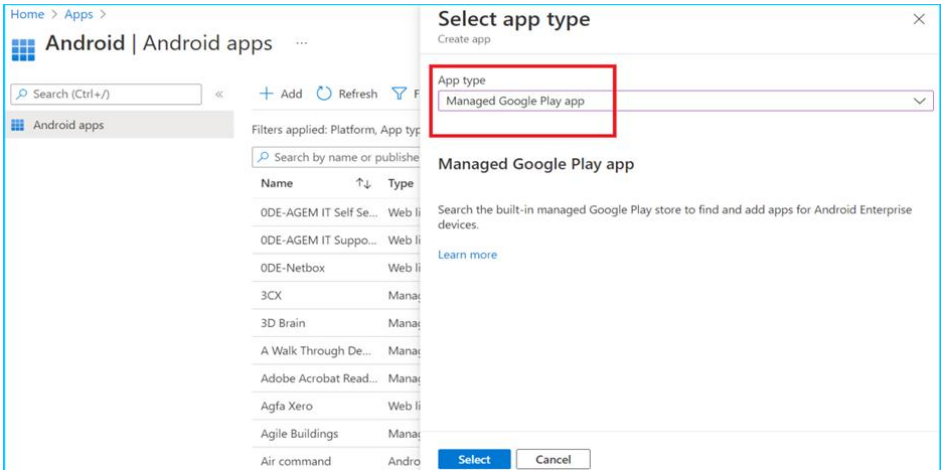
Intune LAs **should not unassign the default scope tag from Android apps**. This will remove the ability for other Intune LAs within Intune to assign apps to their organisation.

The default scope tag can be readded.

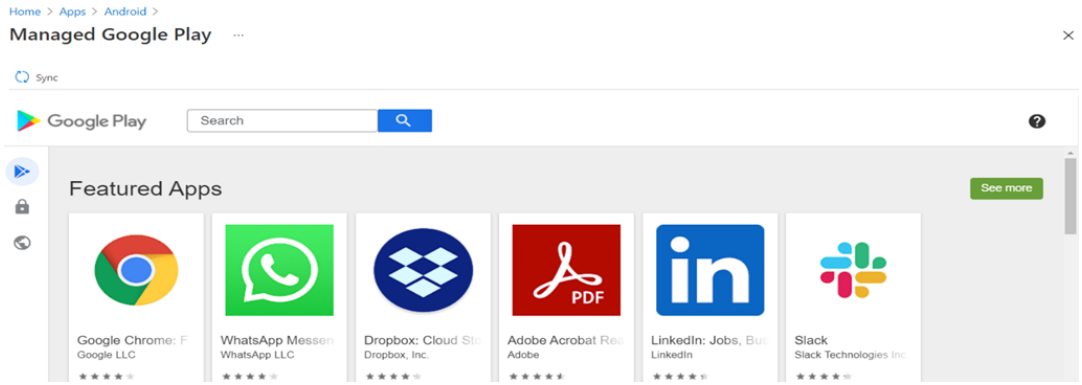
1. Navigate to **Apps** > **Android** and Select **Add**:



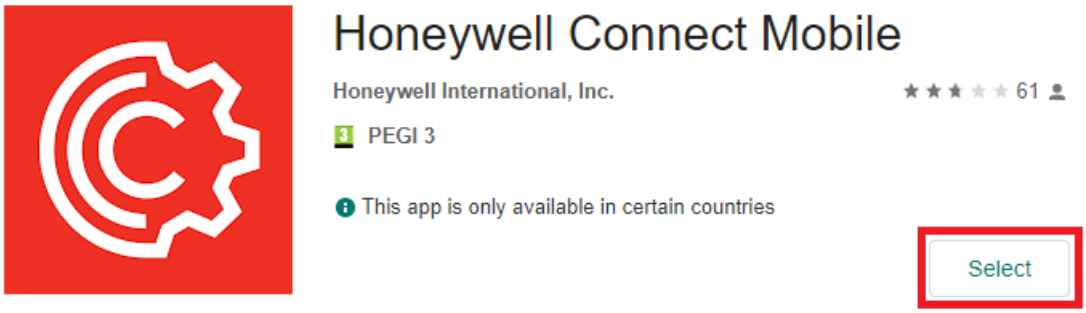
2. Select the **Managed Google Play App** option under the app type option.



3. **Select** the app you wish to deploy.

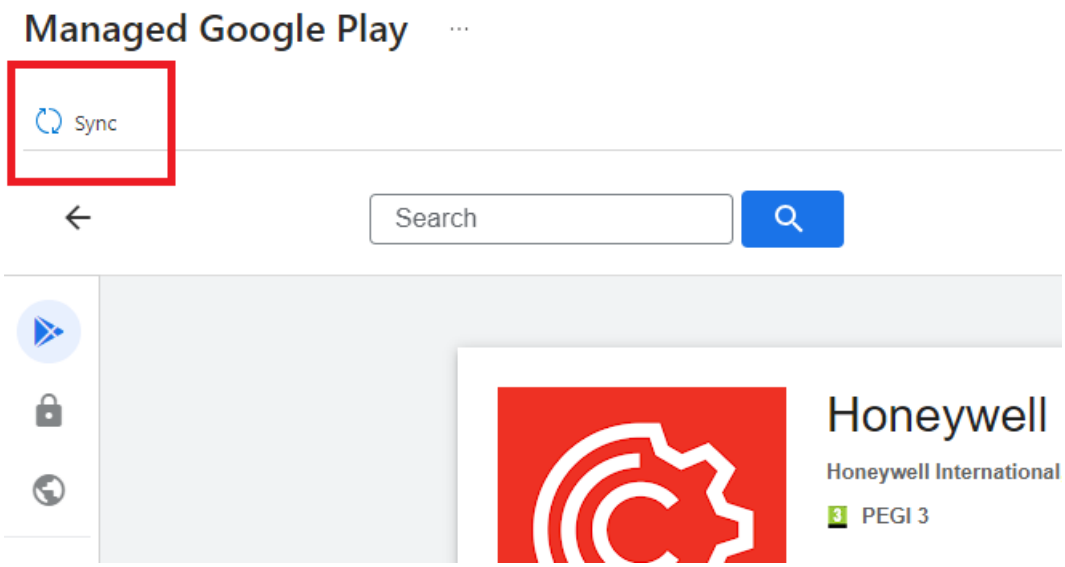


4. Press Select

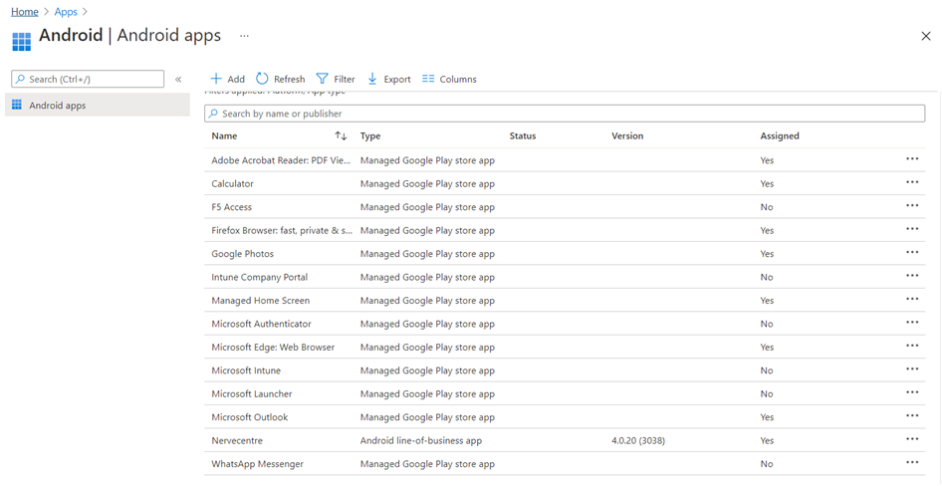


!	**Important Note** Although it may appear as though nothing has happened, this is by design. Press Select once and move on to step 5.

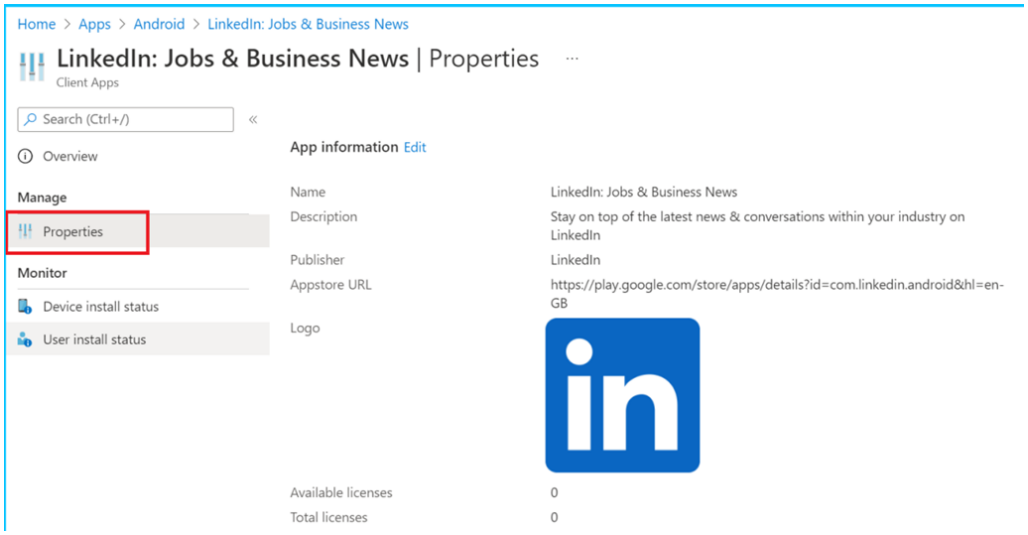
5. Select **Sync** under **Managed Google Play**



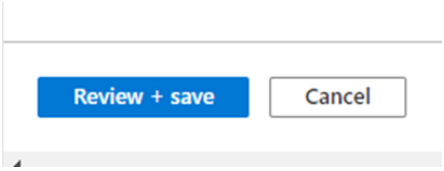
6. Navigate back to the apps section: Under **Apps > Android**, and the approved app should now be showing:



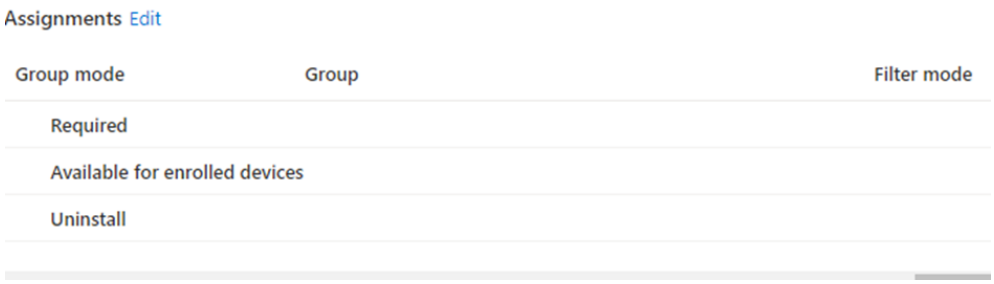
7. **Select the app** you want to assign to the group and then select **Properties**.



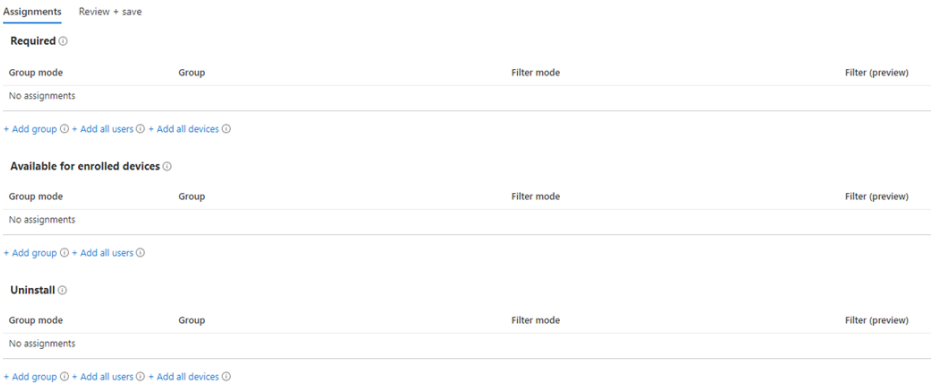
8. Then, select the **Review + save** button.



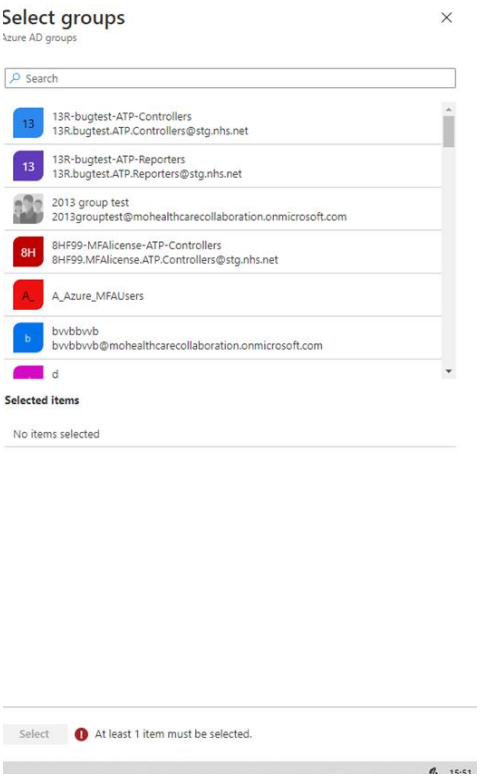
9. Next, select the **Edit** button next to Assignments.



10. Click on the **Add Group** option under the **Required** heading.



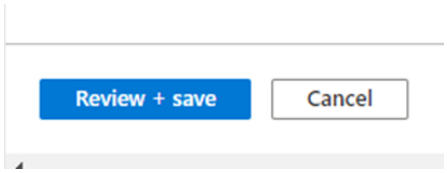
11. On the search tab on the left-hand side find the group you want to apply and then click **Select**.



Important Note

Although Intune LAs can see other groups, Intune LAs will only be able to assign groups which are covered under their RBAC role.

12. Next, select the **Review + save** button.



Important Note

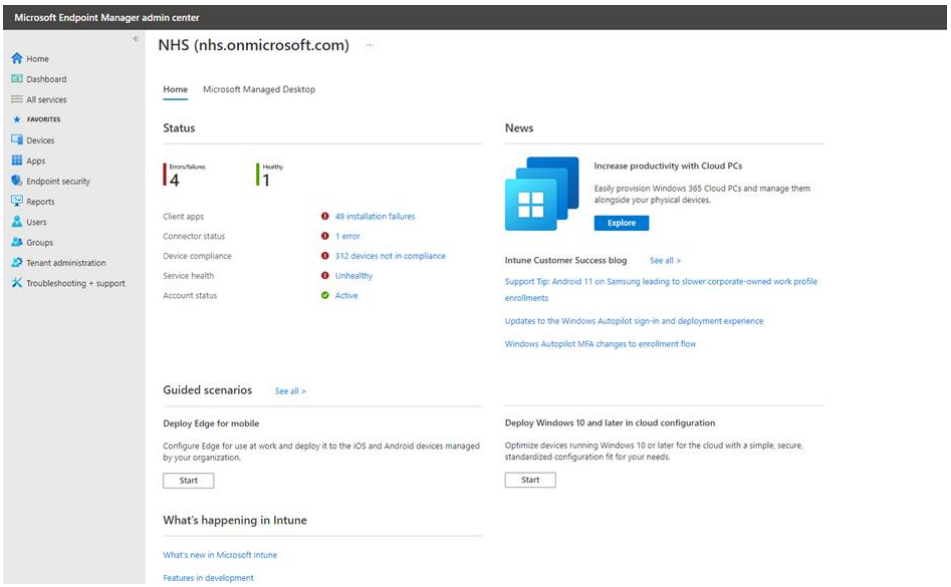
Intune LAs will not be able to amend any AAD Group which is assigned to an Android app which does not belong to their organisation.

6.4.1 Android Custom Apps

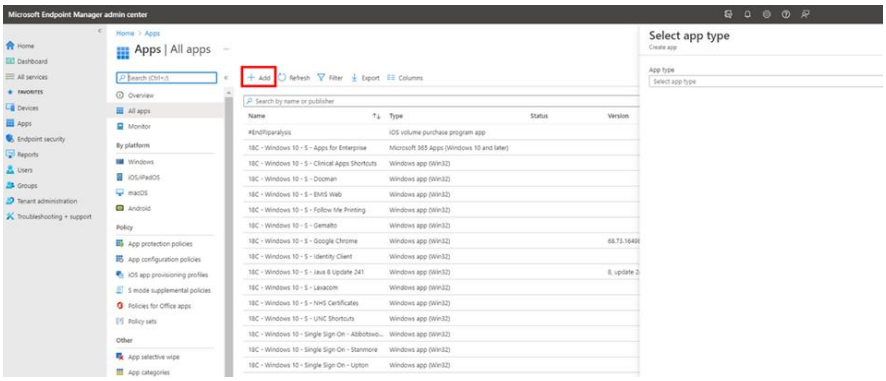
Android Custom Apps are those which have been custom-developed and could also be private applications; these can be uploaded to the Intune platform and managed by Intune LAs.

!	**Important Note** When enabling Custom Apps which contain sensitive information Intune LAs should use their organisations' scope tags to ensure data protection and privacy is maintained. An Android Package Kit (APK) is the file format used by the Android OS for distribution and installation of mobile apps. The installation and any subsequent application update files can be obtained from the app publisher or developer.

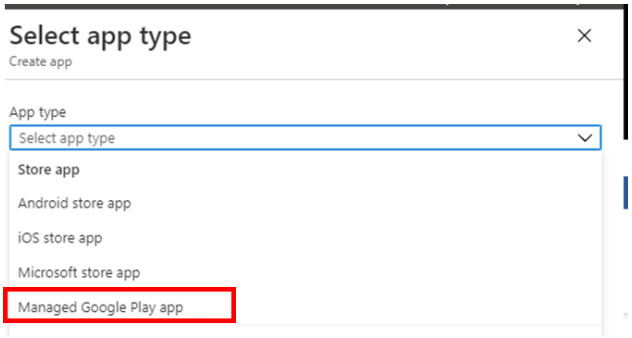
1. Sign into the **Microsoft Intune** admin centre.



2. Select **Apps > All apps > Add**.

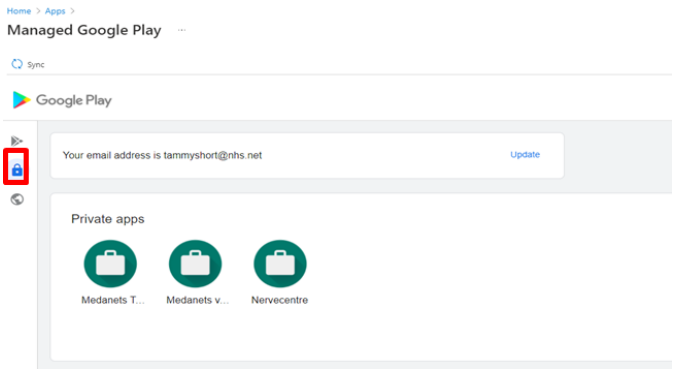


3. In the **Select app type** pane, under the available Store app types, select **Managed Google Play app**.

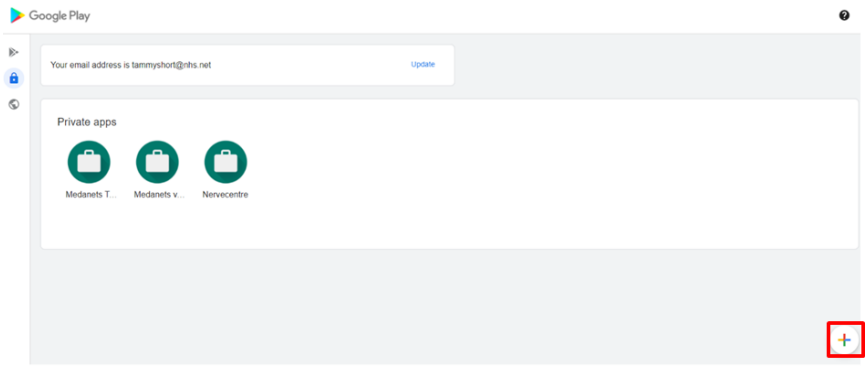


4. Click **Select**. The **Managed Google Play** app store is displayed within Intune.

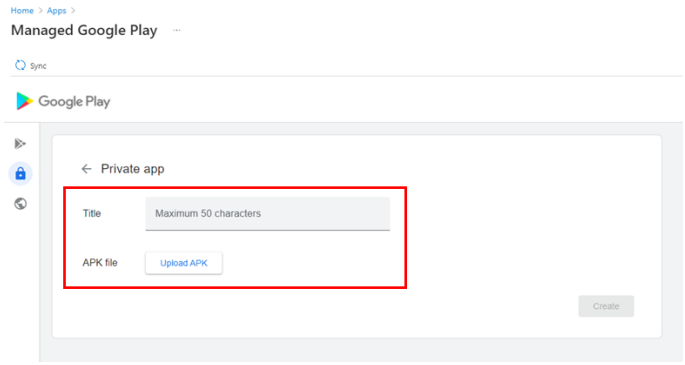
5. Select **Private apps** (next to the lock icon) in the Google Play window.



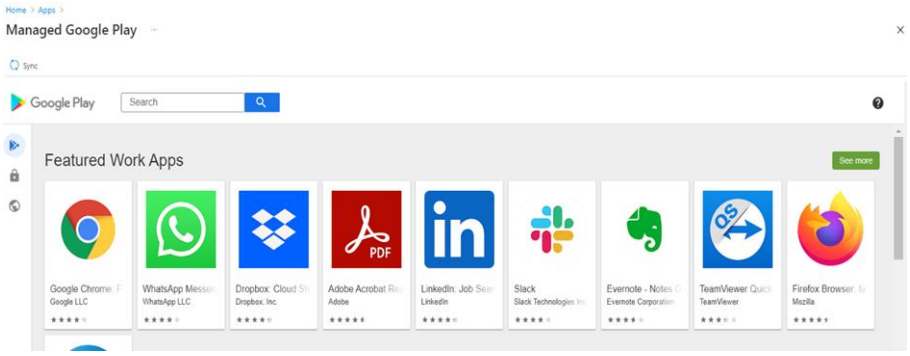
6. Click the "**+**" button at the lower right to add a new app.



7. Add an app **Title** and click **Upload APK** and add the **APK app package**.



8. Click **Create**.
9. Close the **Managed Google Play** pane if you are done adding apps.
10. Click **Sync** on the App pane to sync with the Managed Google Play service.



6.4.2 Android private or paid for apps

Developers can make private or paid for apps available to the tenant. This may cover scenarios where the developer has built a custom app but would prefer to manage updates though the Managed Google Play store, rather than send out a new .APK every update, or when an Org is required to purchase an enterprise version of an app, not currently available to the tenants Managed Google Play Store.

To do this, Organisations will need to provide an Organisation ID and Organisation Tenant Name to the developer.

LAs should raise a Service Request specifically asking for the Managed Google Play Store Organisation ID and Organisation Tenant Name

6.5 Samsung Knox Mobile Enrolment (KME)

This section will cover how to setup Samsung Knox mobile enrolment with Intune.

Samsung Knox Mobile Enrolment (KME) is a Zero Touch provisioning solution. This solution fully automates the enrolment of new, or factory reset devices into an MDM solution like Microsoft Intune. Intune LAs should ensure end users turn on their corporate-owned Android device and connect to a Wi-Fi network.

!	**Important Note** Once the Samsung Knox enrolment process starts, the process cannot be cancelled until the enrolment is completed. This service is only available for Samsung devices.

6.5.1 Prerequisites

Before starting Samsung Knox Mobile Enrolment with Intune LAs should ensure they have the following prerequisites in place:

- A Microsoft Intune environment up-and-running with at least one Corporate-owned enrolment profile enabled such as dedicated devices or fully managed user devices.
- Samsung devices with Knox 2.8 or higher.
- A Samsung Knox account
- Samsung Knox Enterprise runs on Android version (8) Oreo and above.

!	**Important Note** If an organisation wishes to use Samsung Knox for device management, they will need a Samsung Knox Enterprise account and Intune LAs will need a Samsung Knox tenant configured.

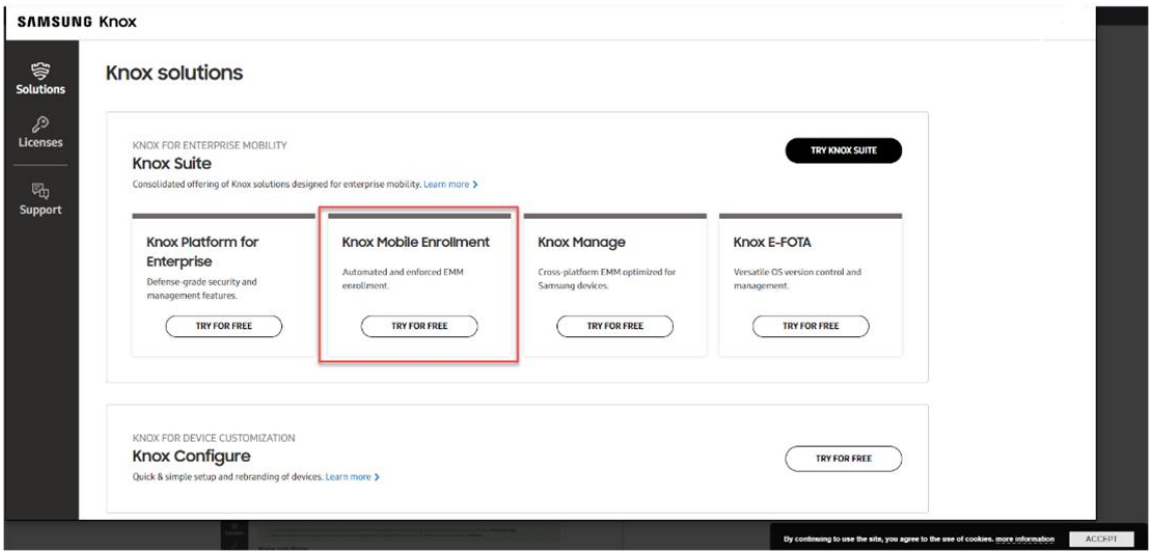
The Knox platform for enterprise solution comes in a two-tiered offering:

1. **Knox platform for Enterprise: Standard** Edition
    - Standard Edition offers free additional policies you can use to provide enhanced security, manageability, and usability over your Samsung device fleet. The standard edition is free.
2. **Knox platform for Enterprise: Premium Edition**
    - Knox Premium Edition (KPE) offers Secure Container for encrypting and decrypting data and protects corporate data on a device with government-certified data encryption technology. There is a charge to the premium edition.

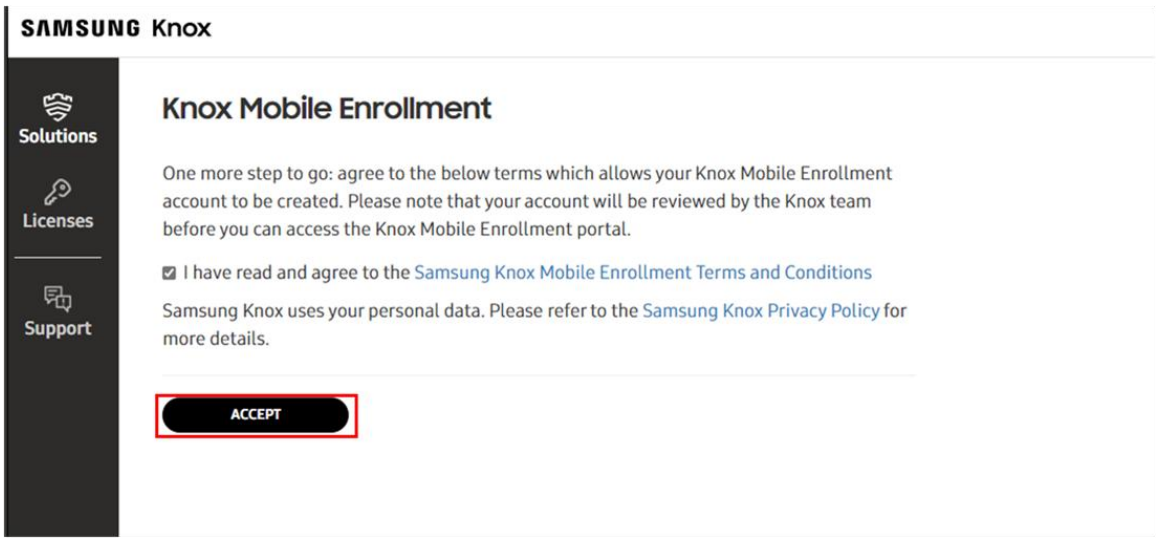
6.5.2 Knox Mobile Enrolment

The following steps below are instructions on how to start the Knox Mobile enrolment.

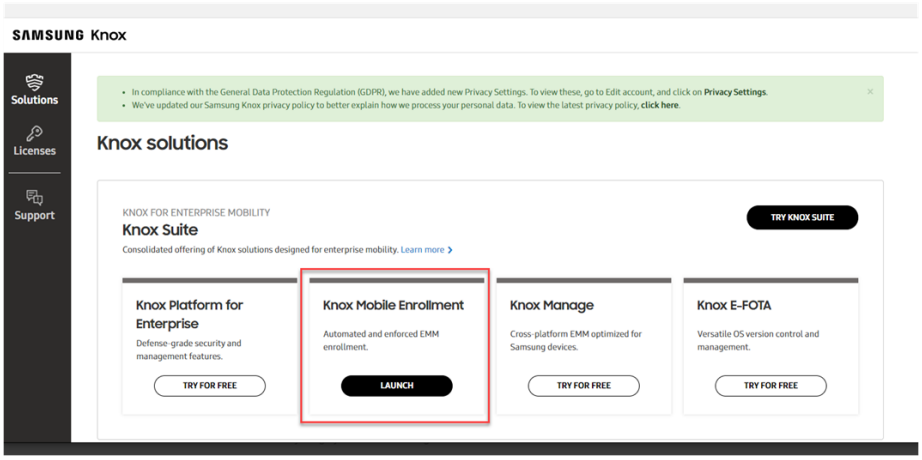
1. Navigate to the following URL: https://central.samsungknox.com/
2. On the **Solutions** page, click **Knox Mobile Enrolment**.



3. Select **I have read and agree to the Samsung Knox Mobile Enrolment Terms and Conditions** (if you do) and click **Accept**.



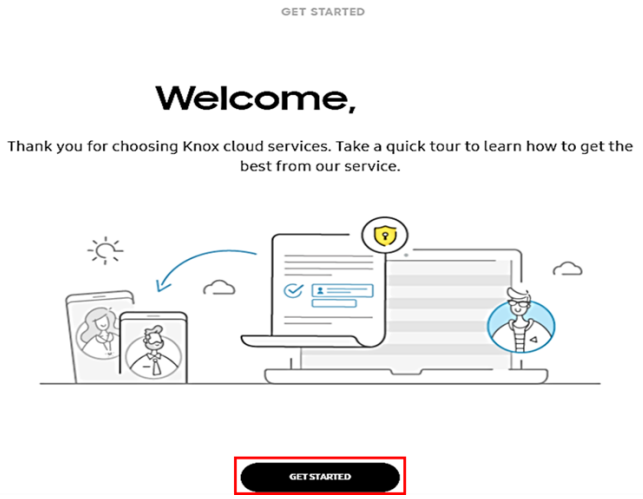
4. In most cases your request will have the status **PENDING** for a short time. In some cases, this status may show for a few hours. Once activated, you can click **Launch**.



6.5.3 Create an MDM Profile

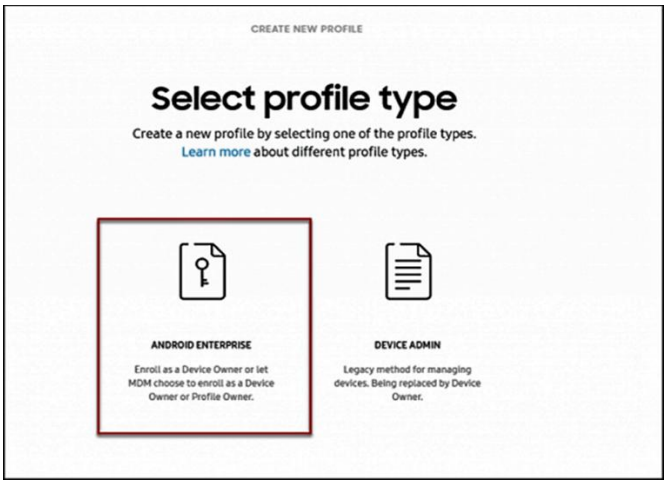
Once you have activated the Knox Mobile Enrolment, you can create an MDM profile. Below are step by step instructions on how to create an MDM profile.

1. If this is the first time you have logged in, you will see the message below. Click Get Started.



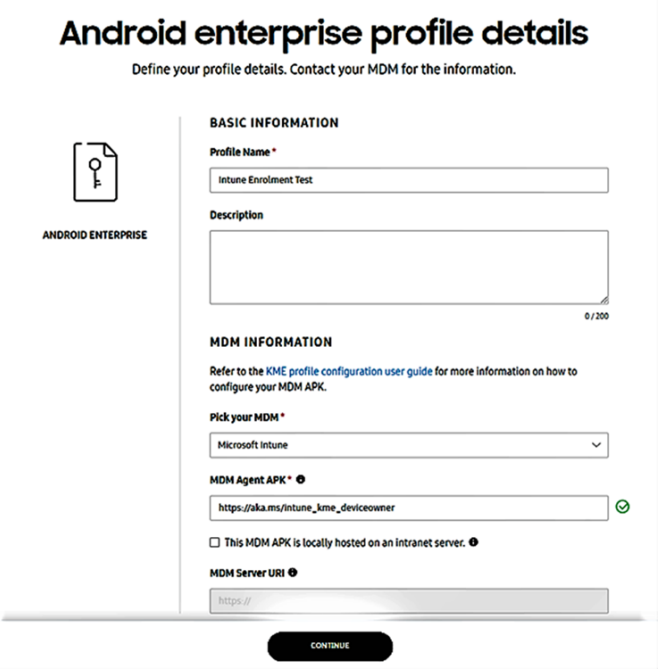
2. Open the MDM Profiles page and click Create Profile.

3. Next, select Android Enterprise.

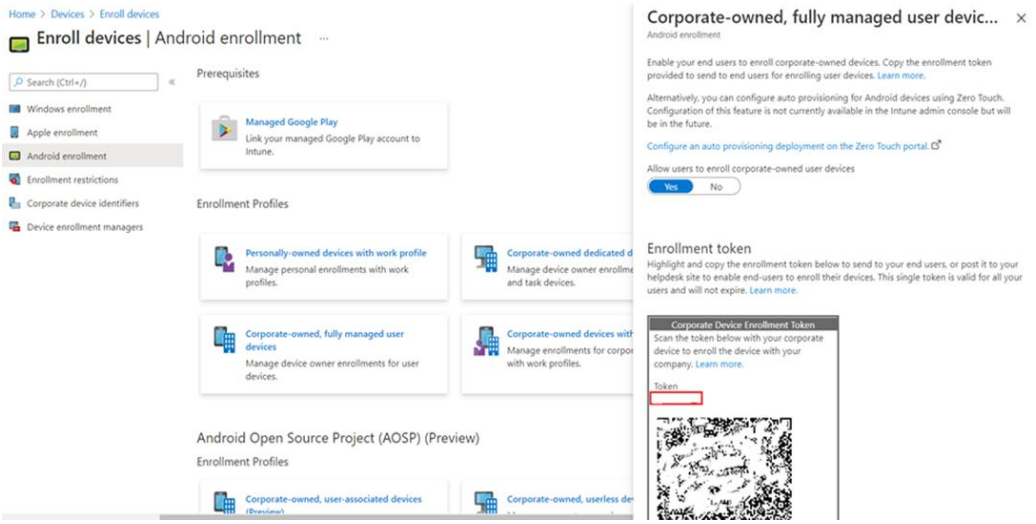


4. Please follow the instructions below to complete this step:
5. Give this MDM Profile a Profile Name and a Description (optional).

6. Select Let MDM choose to enrol as a Device Owner or Profile Owner (changed since Android 11)
7. Select Microsoft Intune as your MDM solution.
8. Fill in the following MDM Agent APK: https://aka.ms/intune_kme_deviceowner



9. Leave everything else as default and click Continue.
10. Open a new browser tab and navigate to the Microsoft Intune admin center.
11. Open your corporate-owned device enrolment profile and copy the Token (see screenshot below).



12. Now, go back to the Samsung Knox admin portal.
13. Fill in the following Custom JSON Data: {"com.google.android.apps.work.clouddpc.EXTRA_ENROLLMENT_TOKEN": "your Intune MDM Profile token code"}

14. Replace [your Intune MDM Profile token code] with the Token copied in previous step.
15. Fill in your Company Name and leave everything else default.
16. Click Create.

6.5.4 Samsung Knox Connection to Intune

Samsung Knox is a proprietary security framework pre-installed on most Samsung mobile devices. Its primary purpose is to provide organisations with a toolset for managing work devices, such as employee mobile phones or interactive kiosks.

The Knox platform for Enterprise solution provides a robust set of features on top of the core Android Enterprise platform, to fill security and management gaps and meet the strict requirements of highly regulated industries.

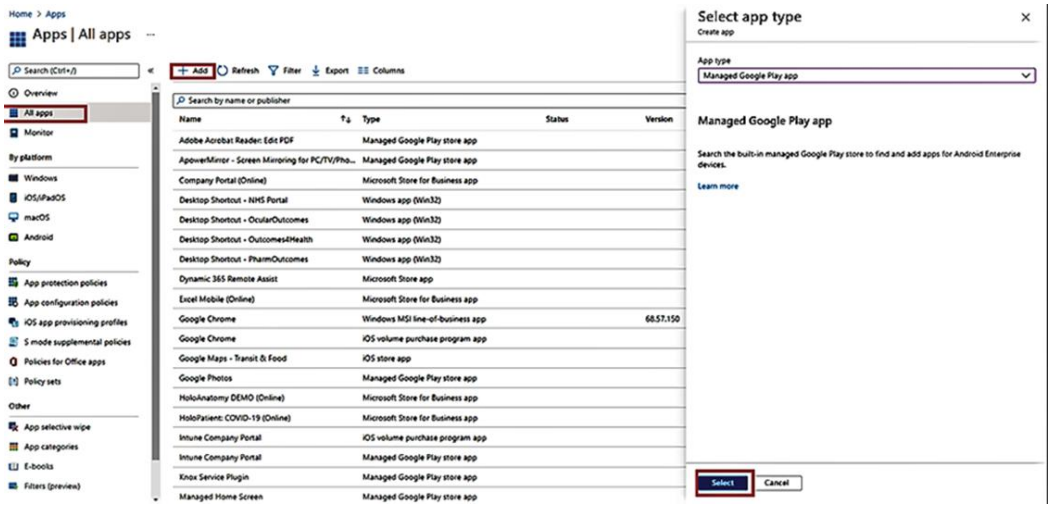
!	**Important Note** Knox Service Plugin is an OEMConfig app developed by Samsung for enabling enterprise devices to access advanced security configurations, restrictions and features as soon as they become available.

6.5.5 Configuring Knox Service Plugin

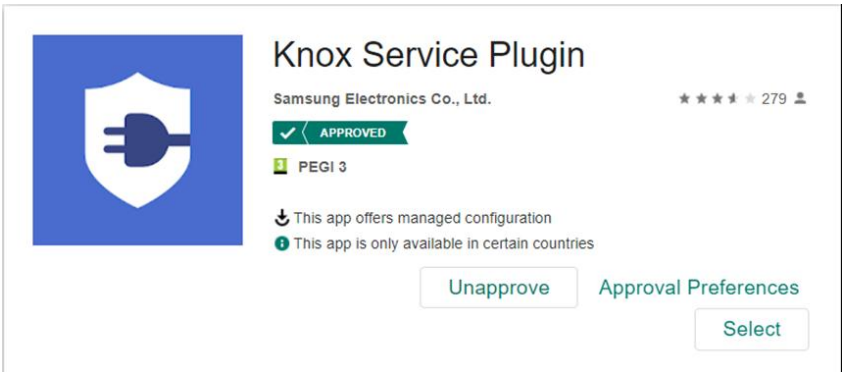
This section will provide instructions on how to configure the Knox Service plugin.

!	**Important Note** This step is optional. Cusont Applications are managed in the Google Play Store which automatically deploys applications. In the Managed Google Play Store, applications are central, once an application has been approved by an Intune LA, the application is approved for all organisations on the Intune tenant and is accessible to all Intune LAs.

1. Within the Intune console, navigate to **Apps > Android Apps > Add**.
2. Set the App type to **Managed Google play app** and click **select**.



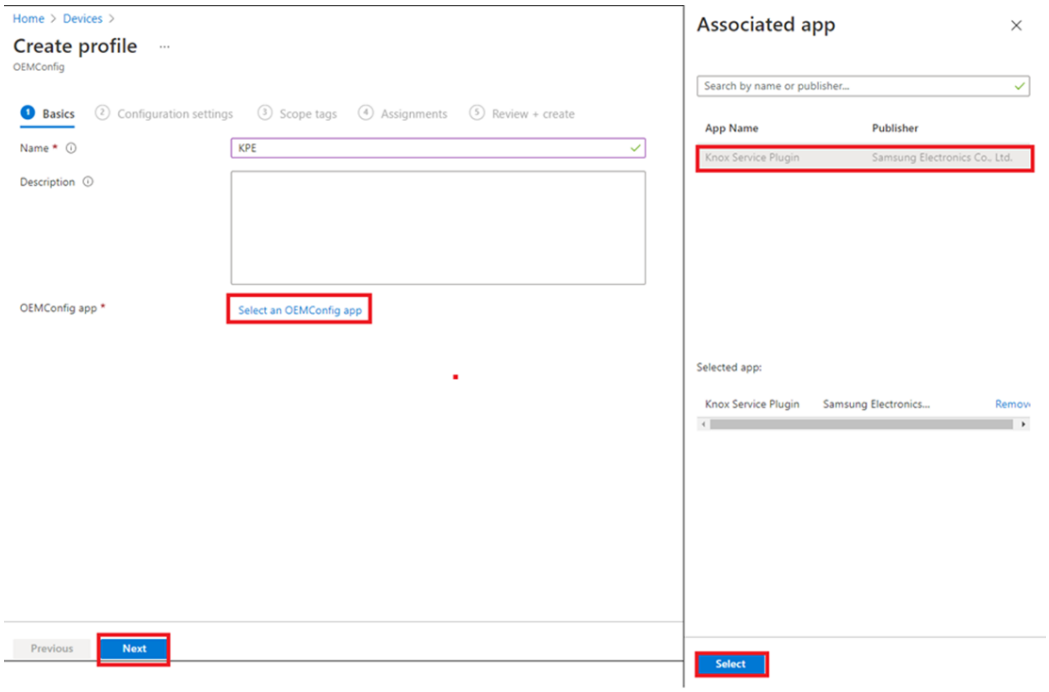
3. Search for and **approve** the Knox Service plugin.



4. Navigate to: **Device > Android > Configuration Profiles**.
5. Click **Create Profile**.

6. Set the platform to **Android Enterprise**.
7. Set the profile to **OEMConfig**.
8. Click **Create**.

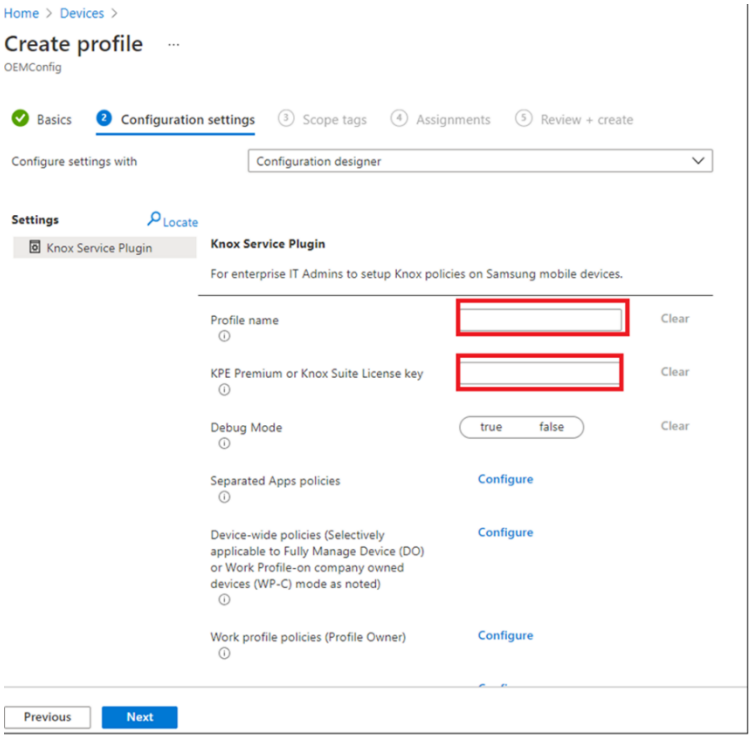
9. To create a profile, complete the relevant fields: **Name, Description** (optional) and select an **OEMConfig app**.
10. Search for and select the **Knox Service Plugin**.
11. Click **Select** and then **Next**.



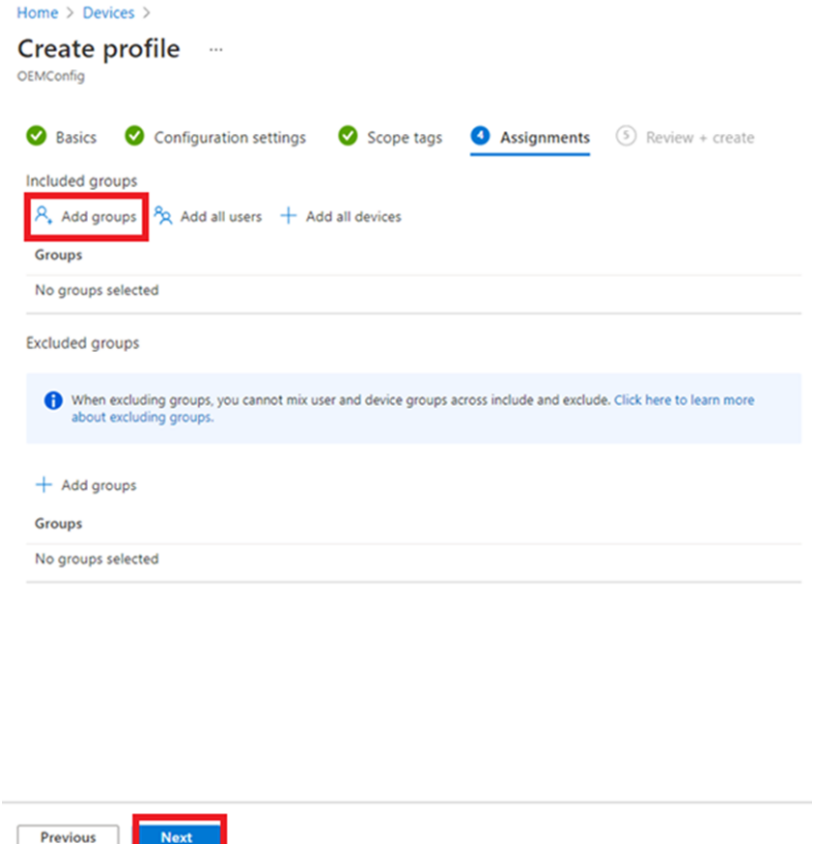
Important Note

To make use of the KPE features, enter your KPE licence key. This can be found in your Samsung Knox portal.

12. Enter a **profile name**.
13. Enter your **KPE licence key**.
14. Set your **desired configurations** and select **Next**.



15. On the **Assignments** tab, choose a **group** to assign the app and select **Next**.



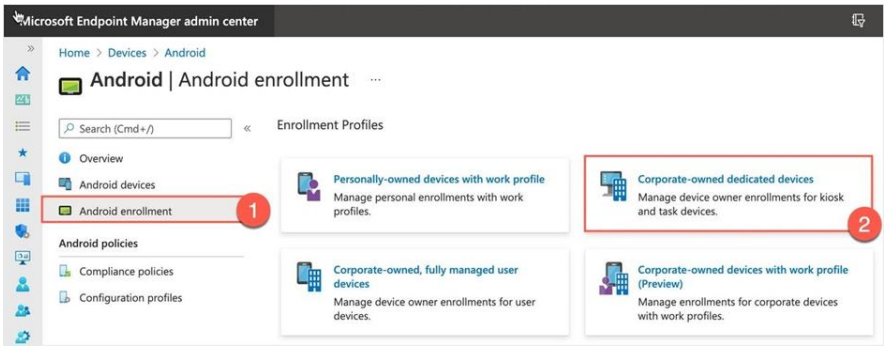
16. Click **Create**.

6.6 Zebra Mobility Extensions

6.6.1 How to Enrol Zebra device with Intune Configuration

!	**Important Note** LAs will need to raise a service request to create shared device enrolment token. The service request should contain the requested name of the token and name of a group to link the token to.

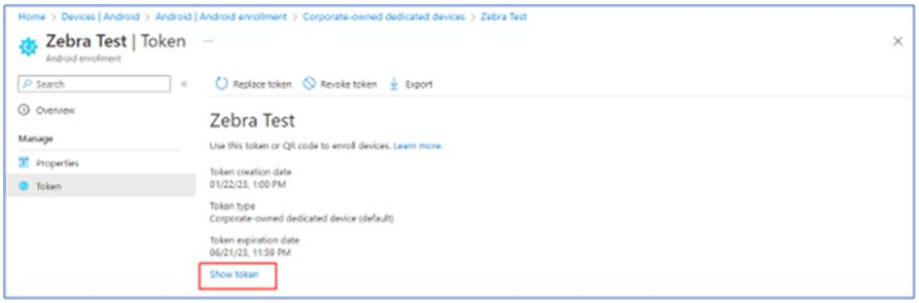
1. Create an enrolment **token**.
    - Navigate to Devices > Android > Android enrolment > Corporate-owned dedicated devices.



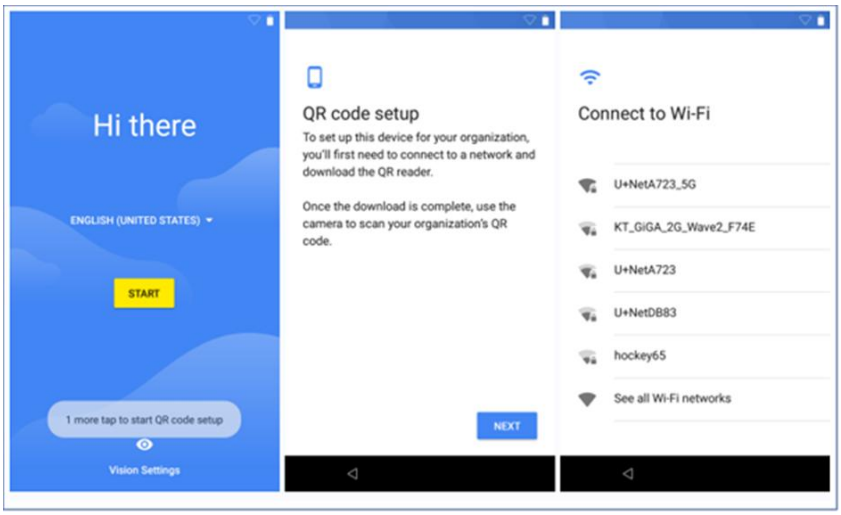
From here, you can **Create Profile** with one of the two available **Token types** that allow enrolling a device in two different ways (default or shared mode):

- **Corporate-owned dedicated device (default)** - device enrolment without a user account; the device is not associated with any end-user
- **Corporate-owned dedicated device with Azure AD shared mode (preview)** - same as above, and additionally, in this enrolment flow, a Microsoft Authenticator app is installed, and AAD Shared device mode allows for sign-in and sign-out between users/apps.

- The Enrolment QR code can be shown from Token > Show Token

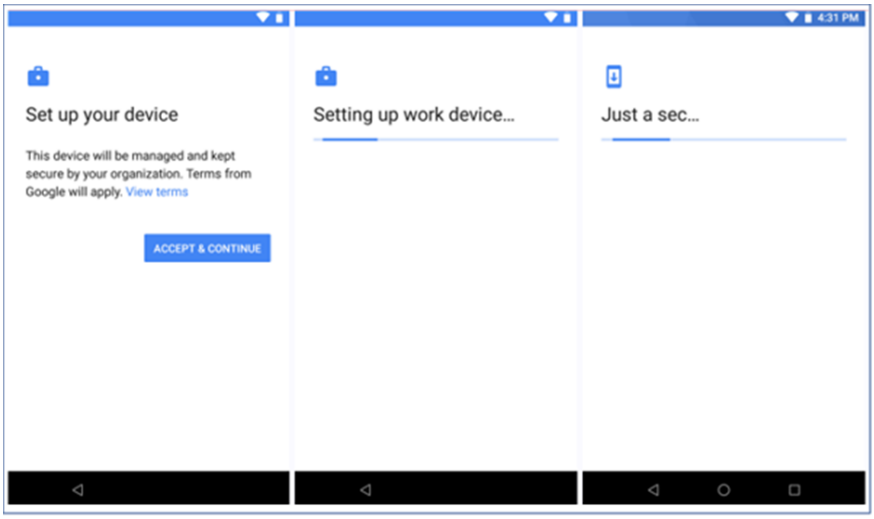


2. Prepare the Zebra Android device and perform a **factory reset status**. (Either from setting the menu or installing the factory reset file via recovery mode). Refer to Performing a Factory Reset on Android Devices.
3. Enrol a Zebra Android device with QR code
    - The first bootup will show the Google setup wizard.
    - Tap **Hi there** six times.
    - Select **Next** for QR code setup.
    - Connect the WiFi network so you can download and install the QR code reader app through the Internet.

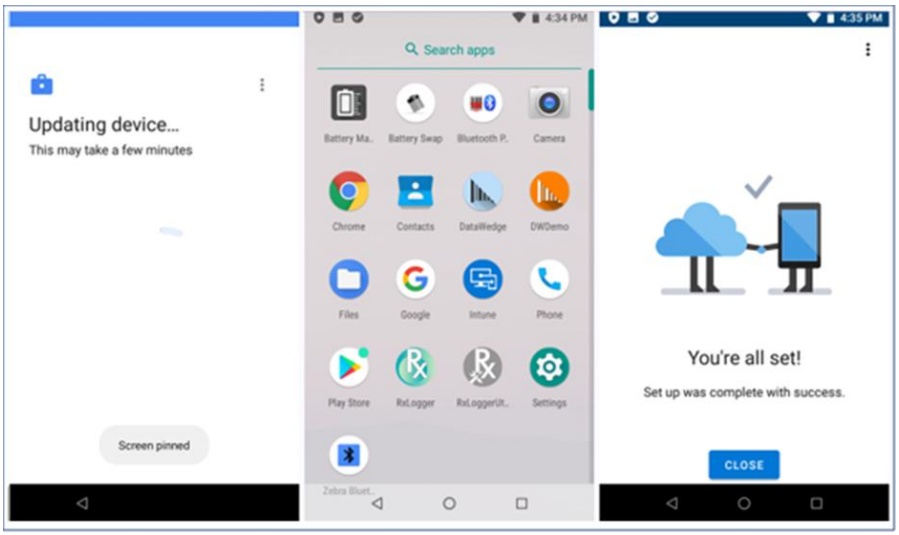


    - Once you connect to WiFi, the Rear Camera enables the QR code reader's preview.
    - Scan the enrolment QR code from your token of the console

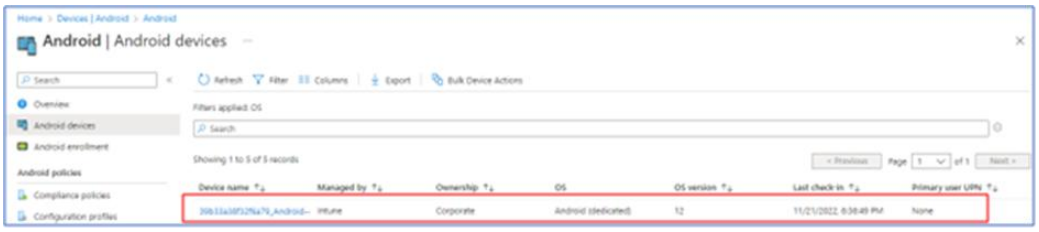
    - Select Accept and Continue



- Wait for a while, and the **Intune app** will be installed shortly.



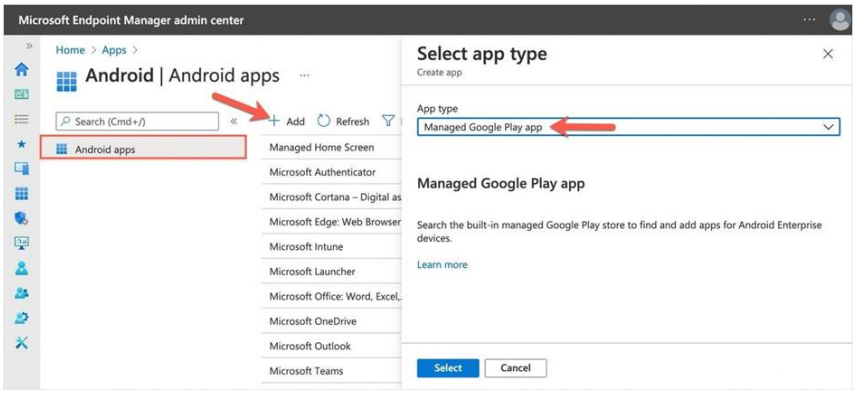
4. Check the device is enrolled from **Devices > Android > Android devices**.



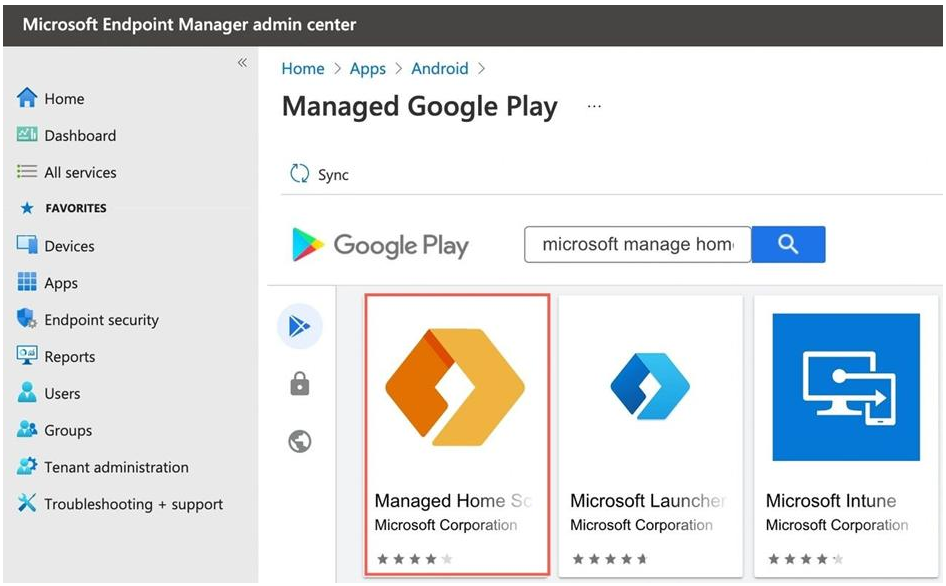
6.6.2 Configuring Zebra's OEMConfig on a dedicated, shared device

1. Configuring the Managed Home Screen (MHS) app:

   - **Managed Home Screen (MHS)** is an Android application available for use through **Managed Google Play** and can be easily added to the **Microsoft Intune admin centre** (endpoint.microsoft.com)

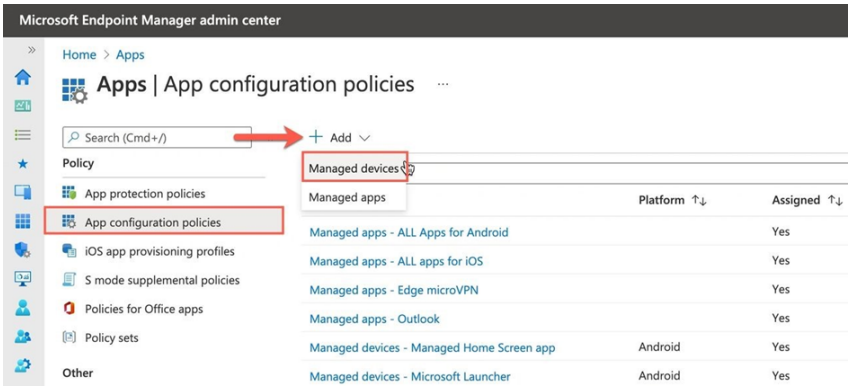


- Add the **MHS app** for Sync and assign it to the AAD Dynamic Group created earlier as **Required** for installation.



!	**Important Note** The same steps should be repeated if you want to add other apps, for example, Zebra's OEMConfig app used later in this guide.

2. Create an App Configuration Policy for the MHS app:
    - Device enrolment type: Managed devices
    - Platform: Android Enterprise
    - Profile Type: Fully Managed, Dedicated, and Corporate-Owned Work Profile Only
    - Targeted app: Managed Home Screen

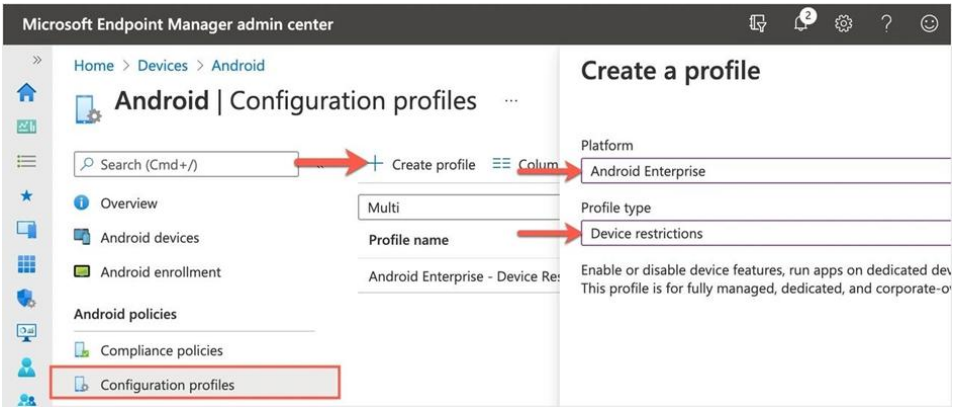


Configure the **MHS app** by using one of two available methods:

- **Configuration designer** allows you to configure settings with an easy-to-use UI that lets you toggle features on or off and set values.
- **JSON data** allows you to define all possible configuration keys using a JSON script.

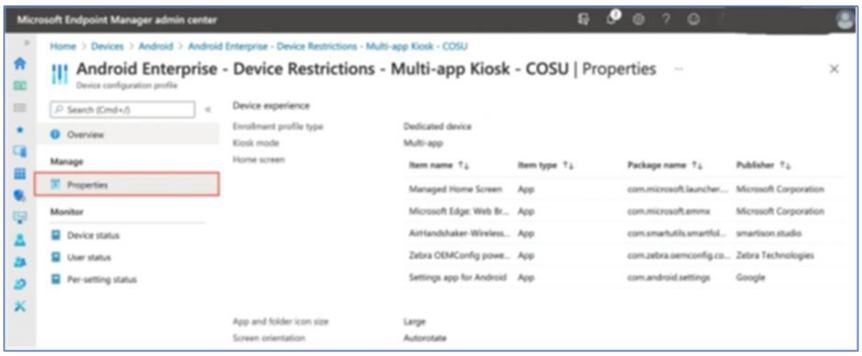
3. Configuring the Multi-app Kiosk configuration

When configured in multi-app kiosk mode, the **MHS app** is automatically launched as the default home screen on the device and appears to the end-user as the only home screen app. Create a new profile Android Enterprise- Device restrictions in the Microsoft Intune console (endpoint.microsoft.com).



Under profile Properties - Device experience configures:

- Enrolment profile type: **Dedicated device**
- Kiosk mode: **Multi-app**
- Home screen: (specify a list of apps for display

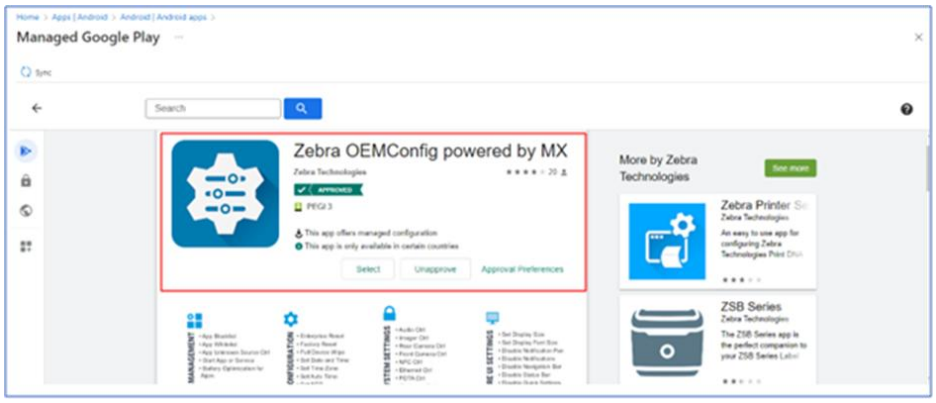


!	**Important Note** The Multiple app kiosk mode locks the device to run multiple apps defined to be launched from the Managed Home Screen (MHS) app. You must first approve and assign the MHS app from the client app's workload to use this mode.

Deploy this Device restriction profile to Zebra's Android Enterprise dedicated (COSU) devices with the MHS app installed.

4. Zebra's OEMConfig

OEMConfig and the Zebra schemas are available from the Google Play Store as an application called Zebra OEMConfig powered by MX.

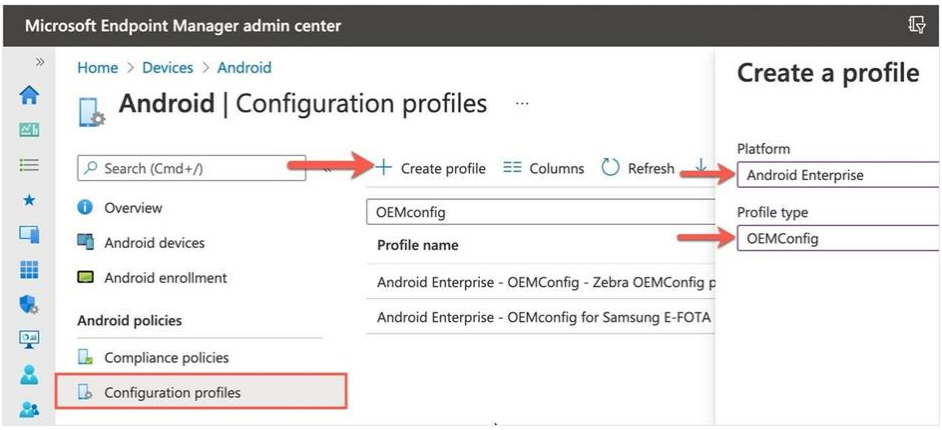


The first step is to add this app to the Microsoft Intune portal (endpoint.microsoft.com)

When the **Zebra OEMConfig app** is available in the console, deploy it as a **Required** app for installation on Zebra devices.

Also, a device **Configuration profile** is needed to manage configuration settings on Zebra:

- Platform: **Android Enterprise**
- Profile type: **OEMConfig**

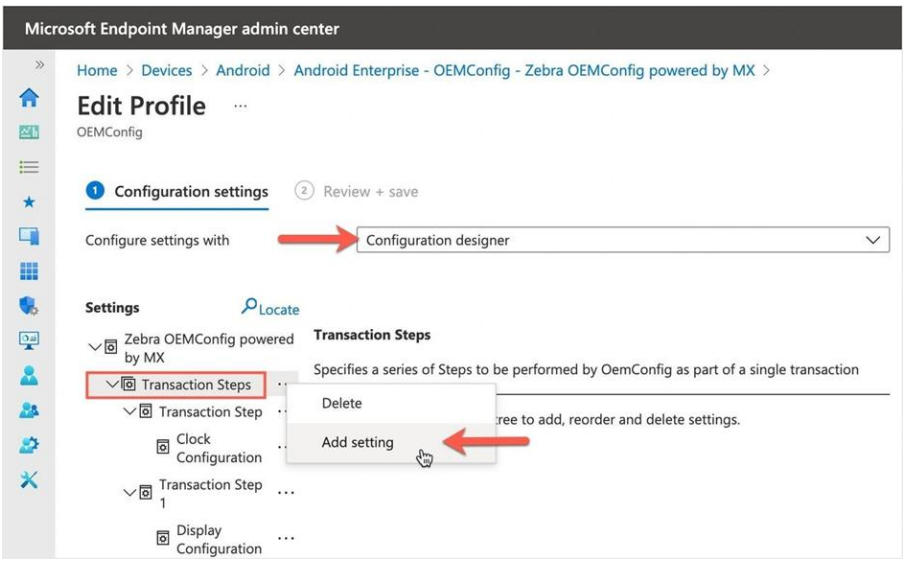


Important Note

You can create multiple OEMConfig profiles and assign them to the same device (this is not always possible with other OEMs), see how to deploy multiple OEMConfig profiles.

For the OEMConfig Profile, there are **two configuration methods** available:

- **Configuration designer** (displays configuration settings from the Zebra's app schema in an easy-to-follow graphical interface)
- **JSON editor** (opens a JSON editor for the app schema template, allowing to customize it with values for the different settings)



- **Transaction Steps** specify an order for the configuration settings you wish to perform on a device as part of an overall Transaction.

Any configuration setting that is not yet supported natively in Microsoft Intune for Zebra devices but is supported by OEM (Zebra) should be configurable via the OEMConfig app and Profile.

5. User Experience

Tested on a Zebra L10 Rugged Tablet (Android 10.0 and OEMConfig 10.1) and enrolled with a QR code as an Android Enterprise dedicated (COSU) with Azure AD shared mode.

On a new or factory-reset device, a user taps six times on the screen to launch the Camera app.

6.7 Google Zero Touch onboarding

!	**Important Note** Access to the Google Zero Touch (GZT) portal is granted to the Intune Support Team only. Intune LAs are responsible engaging their resellers directly.

6.7.2 Getting started

Once your organization has purchased zero-touch enrolment devices, you must provide your reseller the customer ID to onboard and register the devices for zero-touch enrolment in the Intune NHSMail tenant.
The customer ID is 1798912954 and the account's name is NHSMail.

!	**Important Note** To enrol a new Reseller, please raise a Service request with the Intune Live Support Team

6.7.3 Enrol an Android device with Android Zero-Touch

Google Zero Touch is supported in Intune for Corporate-owned, fully managed user devices and Corporate-owned dedicated devices. The enrolment process is the following:

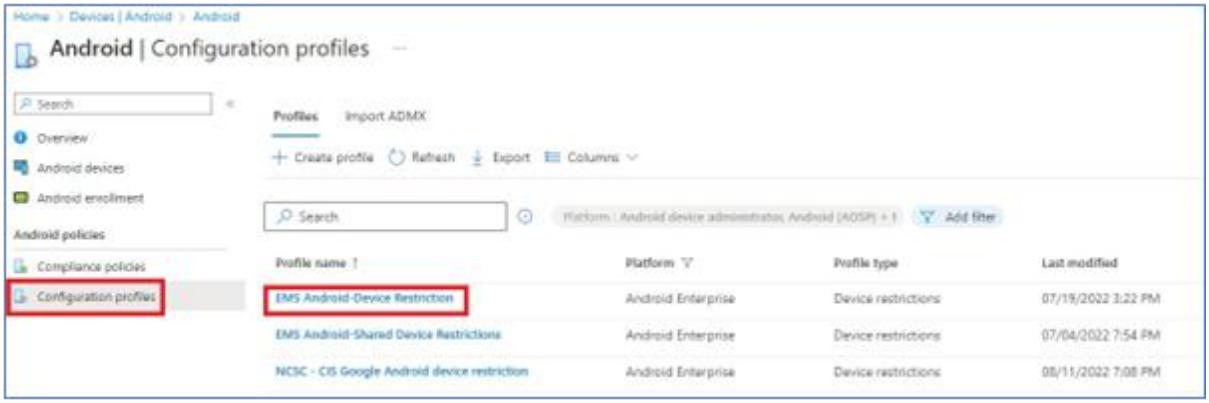
For Corporate-owned fully managed user devices

1. Your reseller will upload the devices bought for your Organization in the GZT Portal

2. The Intune Live Service Team will assign the configuration profile to these devices.

3. Once the previous step is complete, sign in to NHS Microsoft Intune admin center

4. Navigate to **Devices > Android > Configuration Profile** to assign the Android Configuration Profile to the user or devices group for your organization. This will need to be done before a user enrol the device.



5. There is a set of Centralised configuration policies already in place to adopt if required. Alternately, Intune LAs can create their own custom Configuration Profile Policies.

!	**Important Note** Ensure that you add your Trust user or devices group to the assignments. Otherwise, policies and apps will not get pushed to end users.

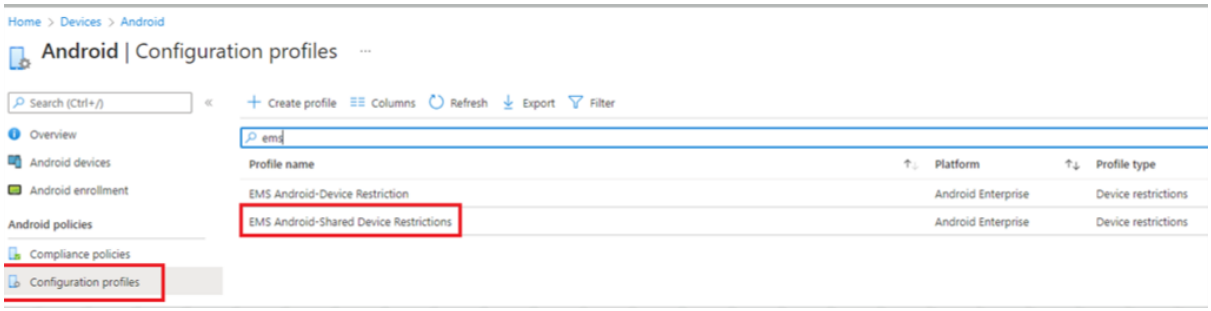
6. Intune LAs can assign the user or devices group to any of the centralized compliance policies and the applications that will be installed in the device during the enrolment.
7. Once the above steps are completed, devices could be dispatched to the end user who will be able to enrol the devices automatically.

Corporate-owned dedicated devices

1. Your reseller will upload the devices bought for your Organization in the GZT Portal

!	**Important Note** Intune LAs don't have rights to create Enrolment Profiles. Please raise a service request with the Intune Live support team to action this.

2. Once the enrolment token is created, Intune Live Support Team will create a configuration profile to these devices in the GZT portal.
3. Once the previous step is complete, sign in to NHS Microsoft Intune admin center
4. Navigate to **Devices > Android > Configuration Profile** to assign the Android Configuration Profile to the user or devices group for your organization. This will need to be done before a user enrol the device.



1. There is a set of Centralised configuration policies already in place. You could use them if you like. Alternately, Intune LAs can create their own custom Configuration Profile Policies.

!	**Important Note** Ensure that you add your Trust user or devices group to the assignments. Otherwise, policies and apps will not get pushed to end users.

2. Intune local admin can assign the user or devices group to any of the centralized compliance policies and the applications that will be installed in the device during the enrolment.
3. Once the above steps are completed, devices could be dispatched to the end user who will be able to enrol the devices automatically.

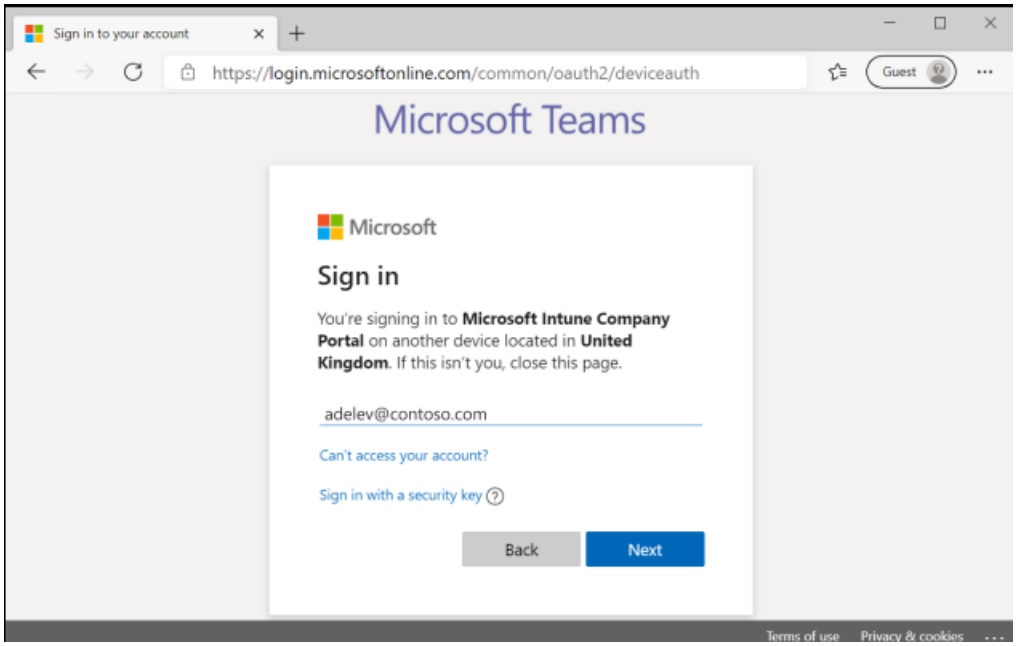
6.8 Android Teams Rooms Devices

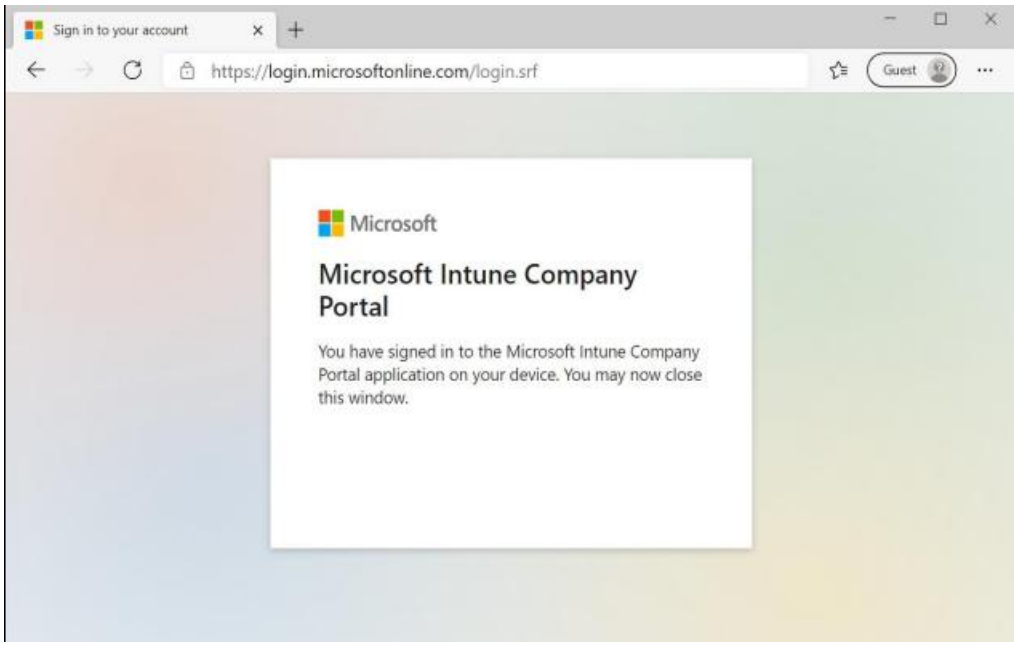
!	**Important Note**

When setting up an Android Teams Room device it may try to auto enrol on to the Intune platform. This can happen if your organisation is onboarded to the Intune platform or not.

Intune LAs will need to raise a service request via Helpdesk Self-Service – Providing the list of accounts they will need to use to log in to all of their Android Teams Rooms devices.

Once access has been confirmed by the Live Service team, continue to sign in and enrol the device.





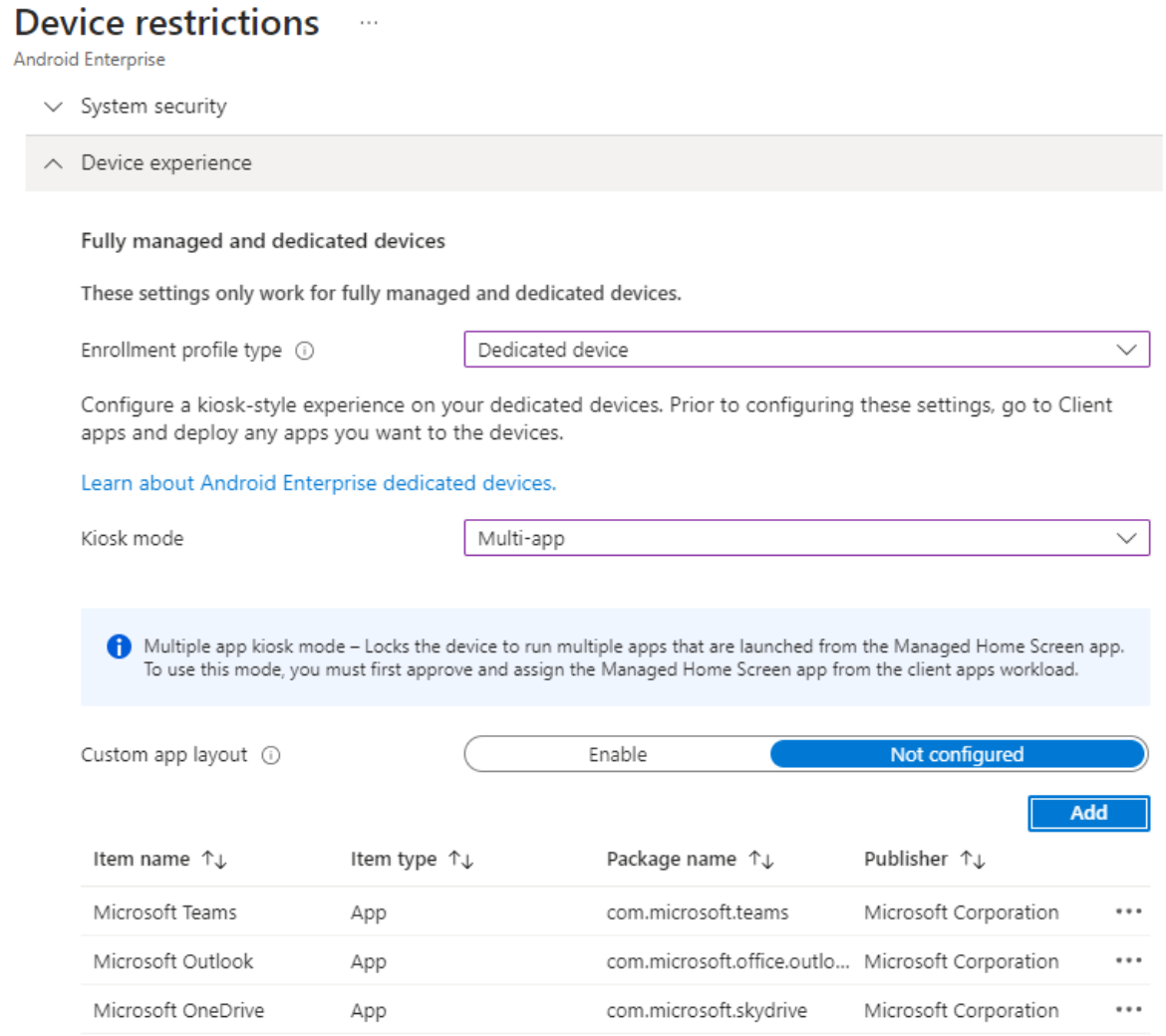
6.9 Managed Home Screen on Dedicated Device

Managed Home Screen also enables LAs to further customize, restrict, and troubleshoot their Intune-managed dedicated devices. Managed Home Screen is intended only for enrolled as an Android Enterprise dedicated device.

!	**Important Note** If you are looking for a similar solution on your Android Enterprise fully-managed devices, then LAs should use Microsoft Launcher for Enterprise.

6.9.1 Assign Device config and necessary apps

1. Prior to configuring the Managed Home Screen app, LAs should first assign all applications necessary and a Dedicated Device restrictions profile with the same applications referenced and any other restrictions LAs require.



2. At this point you can enroll devices into Intune and expect them to download any of the apps, policies and restrictions assigned, additionally the device will automatically lock in to and launch Managed Home Screen.

6.9.2 Assign Managed Device App Configuration Policy

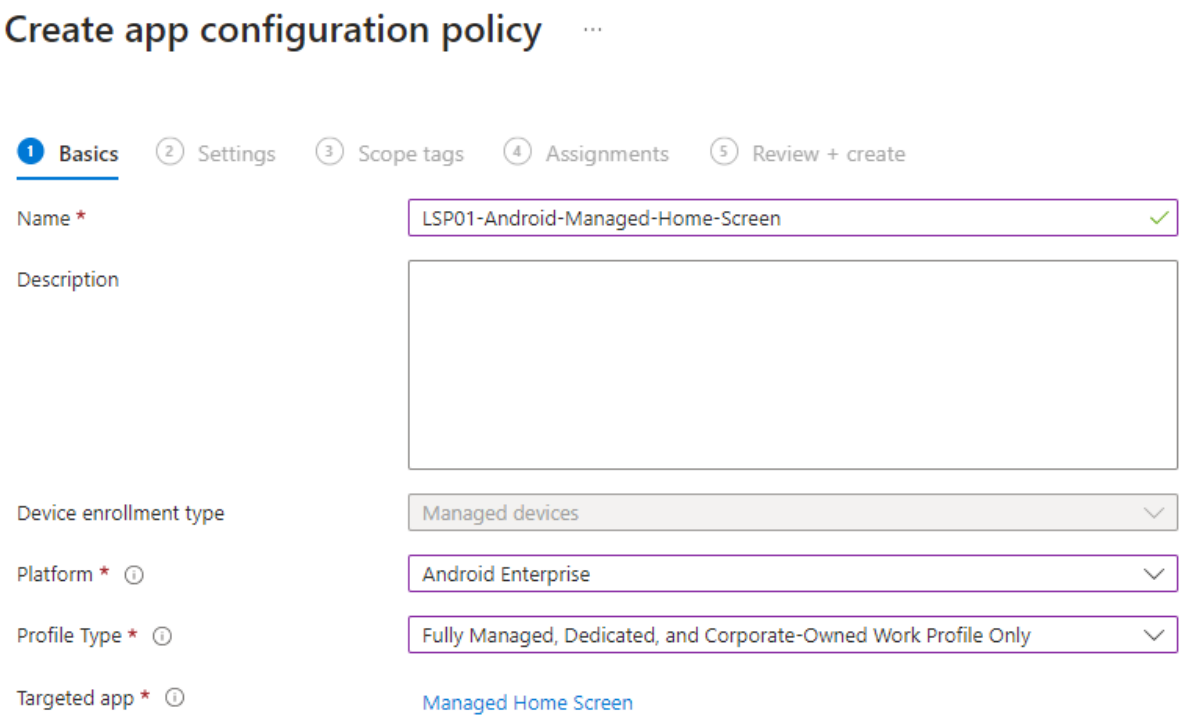
To take full advantage of all the settings Managed Home Screen has to offer, LAs should deploy a Managed Device App Configuration policy

1. Go to Apps > App Configuration Policies > Add > Managed Devices

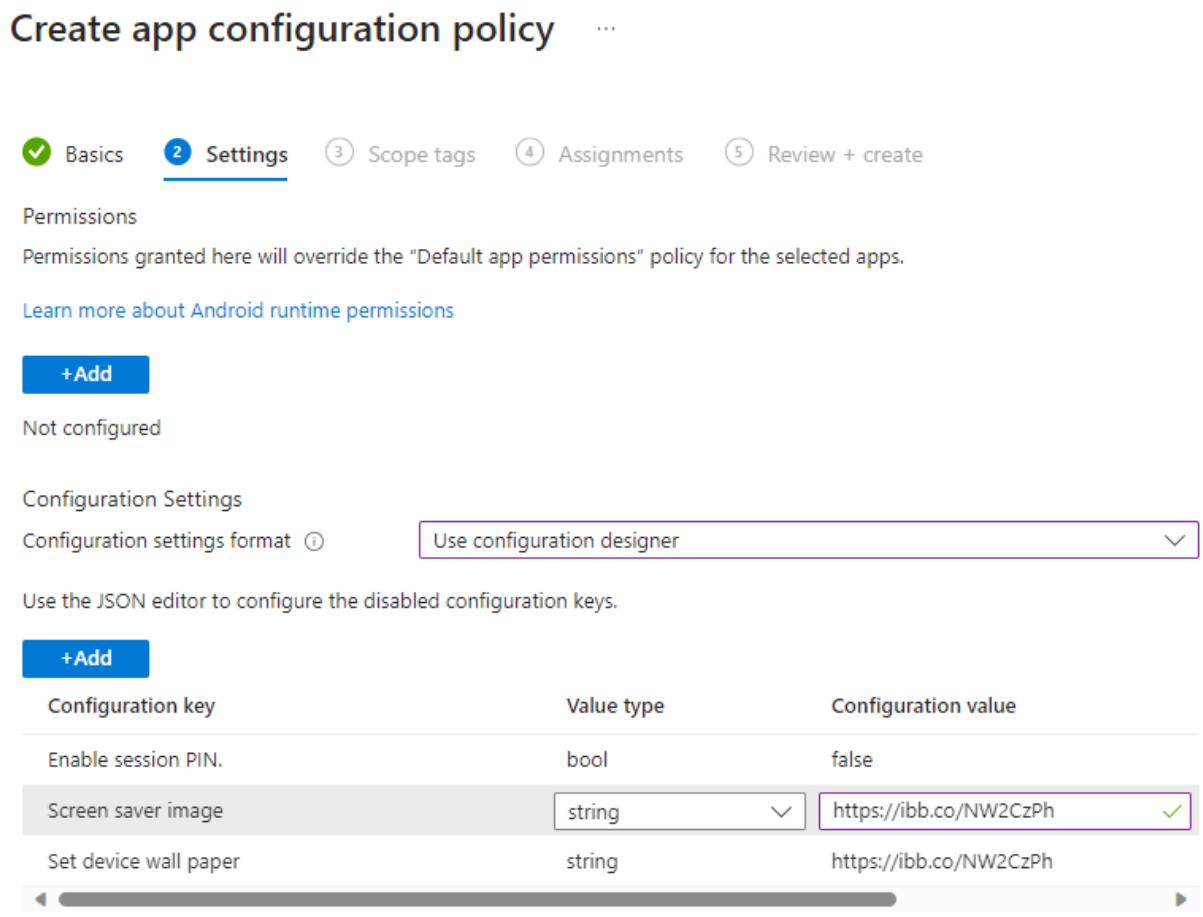
   Select a name > ODS-Android/iOS-AppName

Platform > Android Enterprise
Profile type > Fully Managed, Dedicated, and Corporate-Owned Work Profile Only

Targeted App > Managed Home Screen



2. LAs should add any permissions necessary for their organization.
3. Using Configuration designer > **Press** Add+. LAs can also opt to use the JSON Data.
4. Add any of the settings required from the blade that opens including any value requested such as URL or statement



5. Continue to **Review and Save** the Policy

6.9.3 Setting up the device

When all Apps, Configs and Managed Device App Configuration Policies have been created and assigned, enroll the Android device as a Dedicated device (see Shared Device enrollment).

After the device installs Managed Home Screen, it will auto launch and show all present with all the preset configurations.

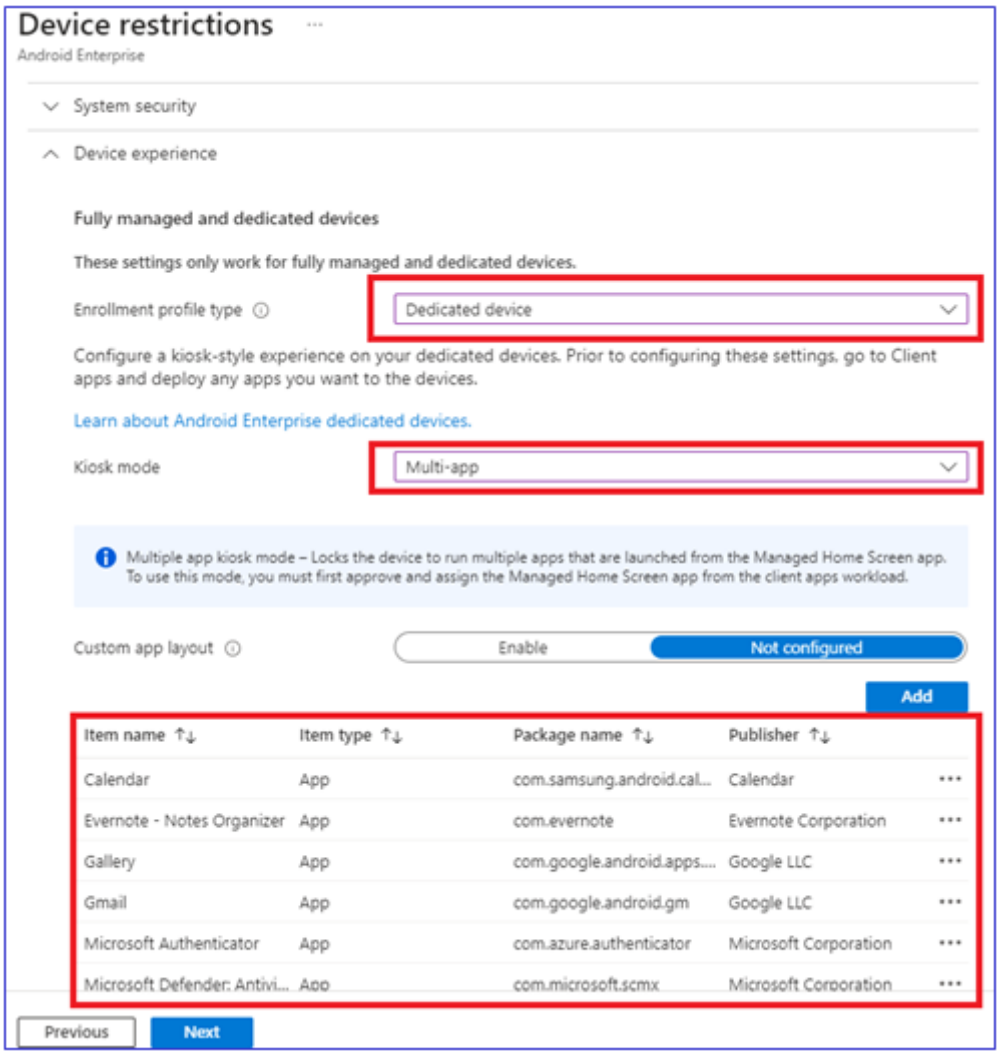
6.9.4 Updated Settings

Before the new features can be taken advantage of, first the app must be accompanied by a Device Configuration Restriction Policy and an App Configuration Profile targeting Managed Home Screen.

Create Device Configuration Profile

1. Go to **Devices** > **Device Configuration Policy** > **Android Enterprise** > **Device Restriction**
2. Select a name and description
3. Go to **Device Experience**, Enrollment type > **Dedicated Device**

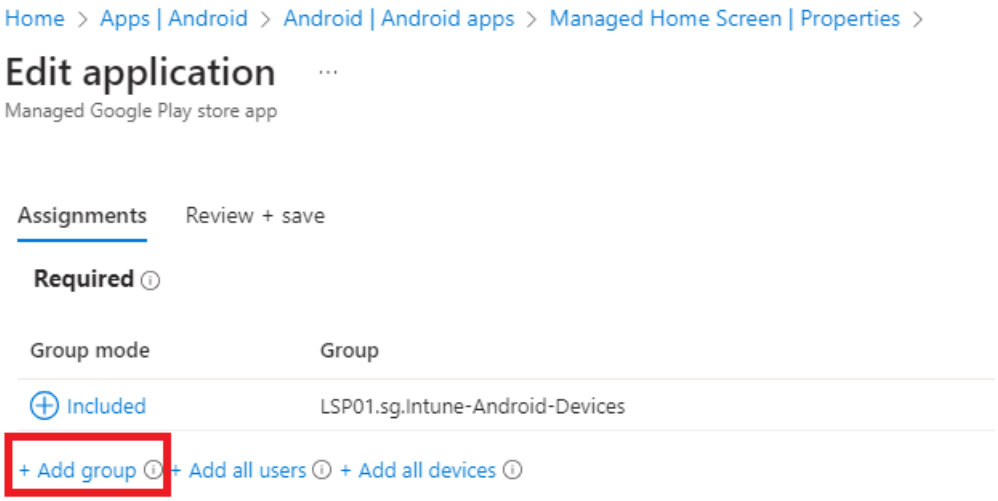
Kiosk Mode > **Multi App**, Select **Add** > Choose desired apps



4. **Review** and **Save.**

Assign Managed Home Screen App

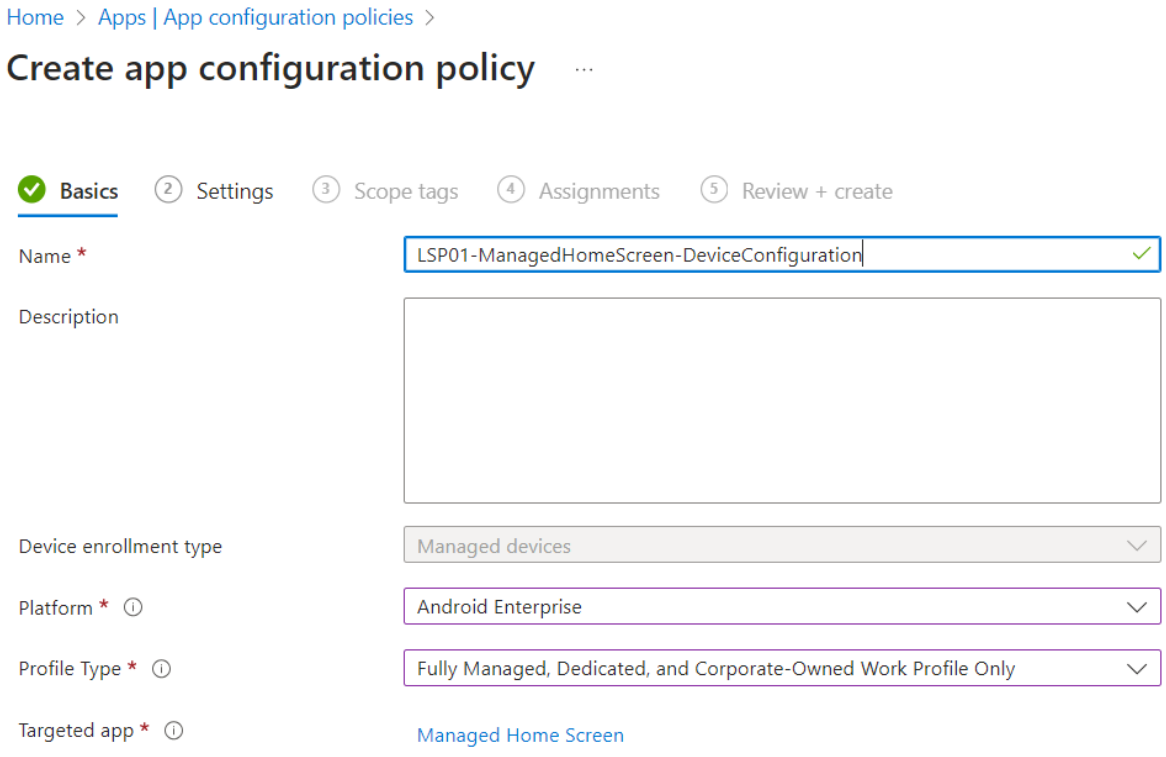
1. Go to Apps > Android > Search for and select **Managed Home Screen** > **Properties**
2. Under assignments select **Edit** > select **+Add Group** > Select desired group
3. **Review** and **Save**



Create App Configuration Profile

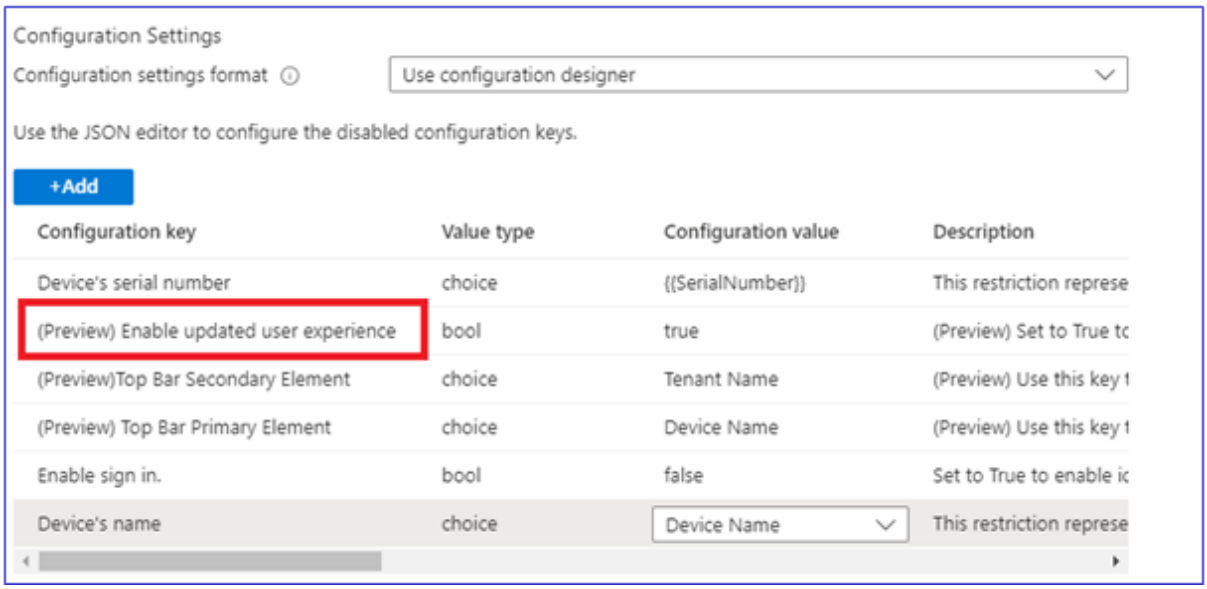
1. Go to **Apps** > **App configuration profiles** > **+Add** > **Managed Device** >

Select a name, a description. Select **Android Enterprise** > **Fully managed, Dedicated and Corporate-Owned Work Profile Only** > Targeted app, select **Managed Home Screen** > **Next.**



2. Settings > **Configuration settings format** > Select **Use configuration designer**
3. In order for the new settings to apply correctly, the first setting that must be enabled is **"Enable updated user experience"**.

4. Choose from the following settings:
   - Enable sign in.
   - Top bar primary element – Setting unavailable if "Enable sign in" is set to "**False":**
     - Device name
     - Tenant name
     - Serial number
   - Top bar secondary element
     - Device name – **"Device's name"** option must be set to **"Device Name"**
     - Serial number – **"Device's serial number"** option must be set to **"Serial Number"**
     - Tenant name
   - Devices name
   - Devices Serial number
   - Top bar User Name Style – Setting only available if "Enable sign in" is set to **"True"**
     - Display name
     - Last name, First name
     - First name, Last name
     - First name, Last initial
   - Show Managed Setting



5. Choose **Next**.
6. **Assignments** > **Included groups** > **Add necessary groups**
7. **Next** > **Review and create**

6.10 Android Personal Device Enrolment

Personal device enrolment allows users with their own devices to securely access the NHS.net connect tenant

The required features are enabled to allow enrolment capabilities for users of personal mobile devices as:

Android – Personal Owned Work Profile (POWP)

No Administrator intervention or pre-configuration is required by Local Organisations to support enrolment, there being automation to scope enrolled devices to specific ODS codes

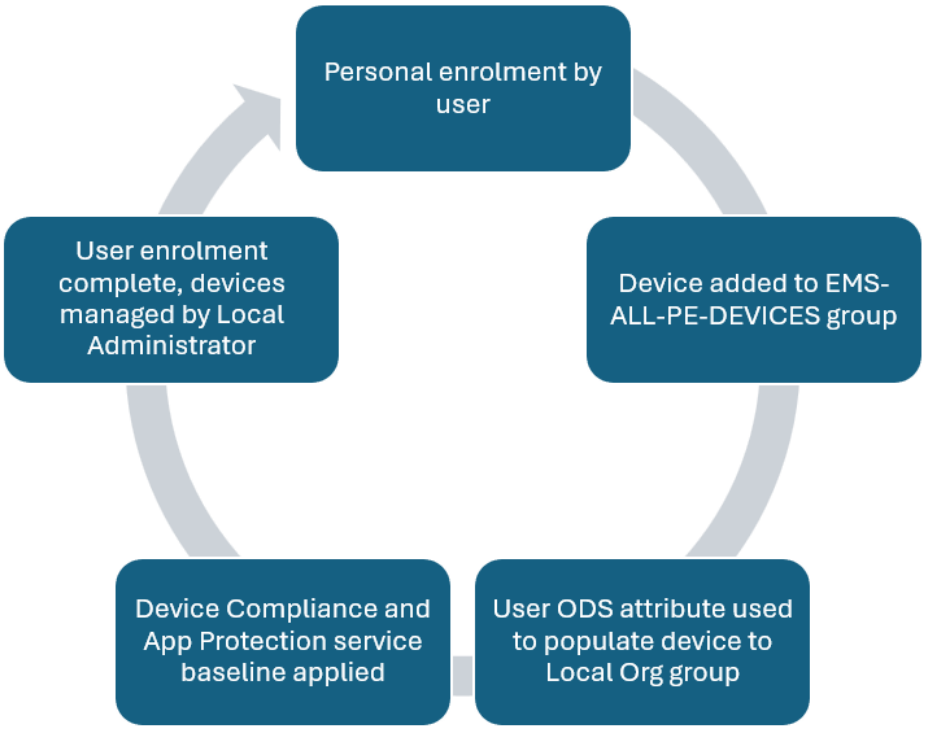
Personal Intune enrolment methods:

Since Android POWP is enabled, Local Administrators can advise users to follow the standard personal-enrolment process, per Microsoft's user guidance:

Microsoft Personal Android enrolment video

Users can un-enrol and re-enrol personal devices without Local Administrator intervention.

The following diagram describes the enrolment, scoping and baseline configuration process for personal enrolment devices:



Once personal devices are enrolled and configured, the following groups are used for scoping and to apply the fundamental configurations.

EMS-ALL-PE-DEVICES

This dynamic device group populates any mobile device enrolment *(rule: device.deviceOwnership -eq "Personal"*). Service automation that creates and then scopes the device into a Local Organisation assignment group, based on the User's ODS attribute:

ODS.sg.Intune-Android-PE-Devices

Contains all Personal-enrolled Android OS Devices for a Local Organisation

!	**Important Note:** If a user moves to another organisation, the personal device will not automatically un-enrol but will be added to the destination Local Org device group as above.

Local Administrators can use the 'PE-Devices' groups to assign policy to Personally-enrolled devices if required, however user-assigned methods should be favoured.

EMS-MDM-USER-SCOPE

This 'global' group is used to assign the following Intune Service Security Baselines which align with existing App Protection policies, but use specific device compliance policies. The mandatory policies applied to users of personal devices in this group are:

1. Device Compliance:

    a. Global-Baseline-Android-PE-Compliance-Policy-R1

2. App Protection:

    a. Global-Baseline-APP-Managed-Android R1
    b. Global-Baseline-APP-Unmanaged-Android-R1

The EMS-MDM-USER-SCOPE group contains Local Organisation 'Intune Users' groups, 'ODS.sg.Intune-Users', and so Local Administrators should apply required apps, configurations and policy for users as such.

6.10.1 Android Personal Device Enrolment Restriction

Although Personal Device Enrolment is allowed by default for all Organizations, Organizations can continue to block Personal Device Enrolment via a Service Request to have their ODS.sg.intune-Users group added to the Android Device Enrolment Restriction Policy (Android-PE-Restriction).

Once an Organization is in a position to allow Personal Device Enrolment, a Service Request can be made to have their ODS.sg.intune-Users group removed from the Android Device Enrolment Restriction Policy (Android-PE-Restriction). This will then allow end users to enroll their Personal Devices and access NHS Resources safely and securely.

6.11 Android Defender for Endpoint

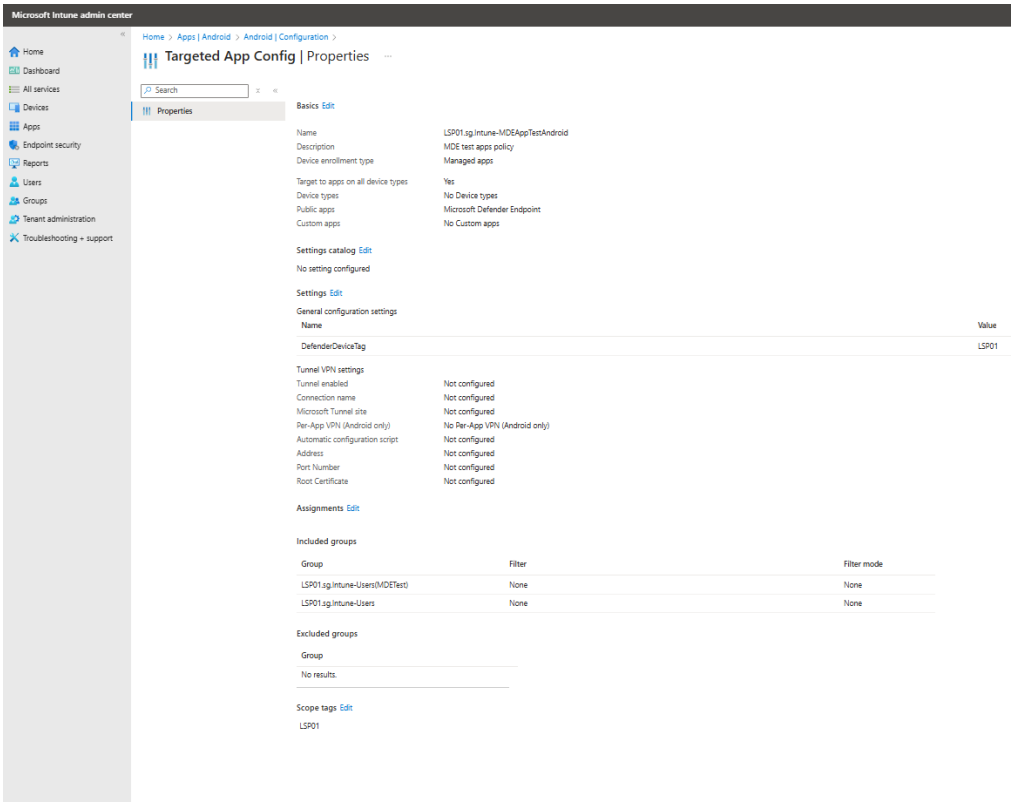
Local Admins can automatically on-board Mobile Devices to Microsoft Defender XDR. By deploying the Defender App to Android and then applying an App Configuration policy to the same, devices can be automatically tagged. In doing so, mobile devices will be visible in the XDR UI.

Device Tagging can be applied to Managed Devices & Managed Apps. The following outlines the process for modifying both Managed Device Tagging and Managed Apps Tagging for Microsoft Defender for Endpoint.

!	**Note:** Policies can be created via a service request and these steps are guidance on how the policies can be modified / amended to suit an Orgs needs.

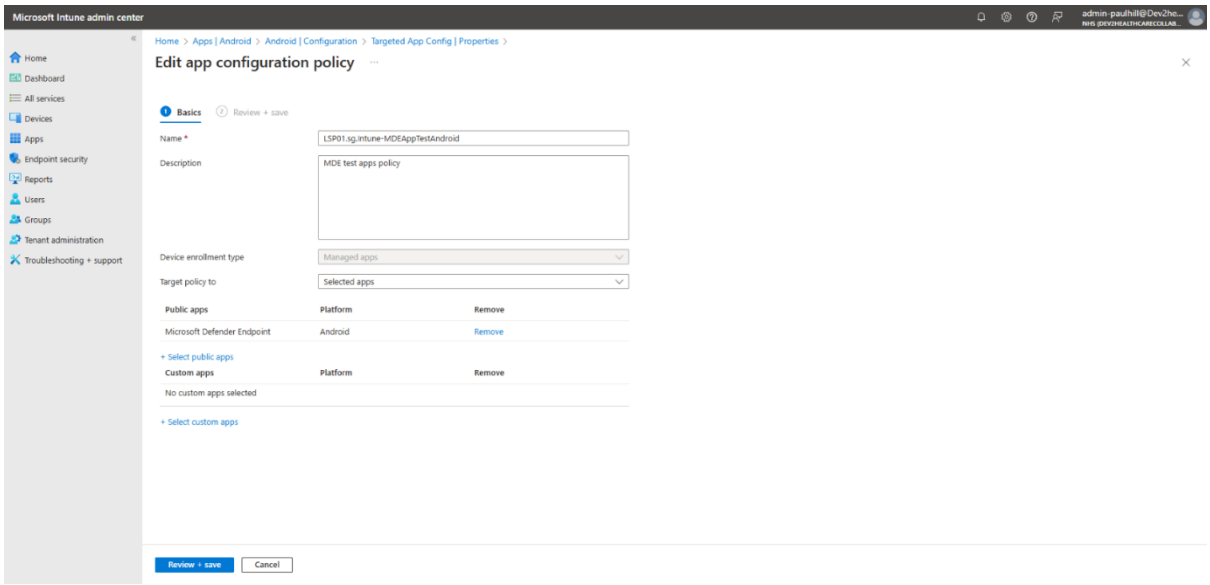
6.11.1 Modifying Managed App Tagging

1. From Intune, navigate to Apps > Android > Configuration
2. Search for the Policy, click on it and go top Properties.
3. The sections that can be modified are;
    - Basics
    - Settings catalog
    - Settings
    - Assignments
    - Scope tags



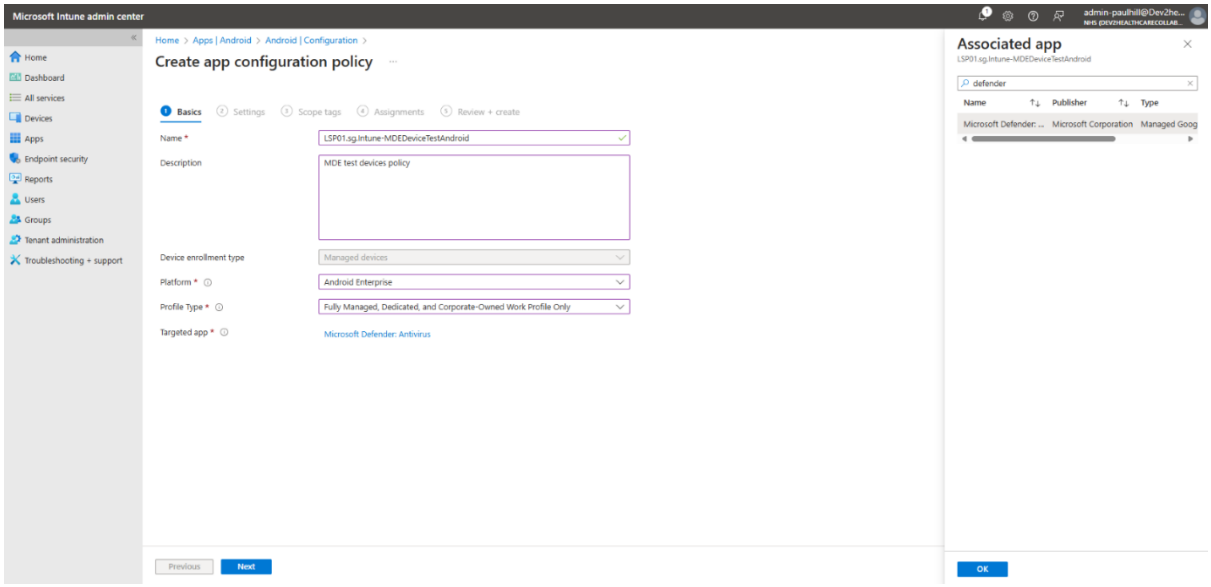
Edit Basics settings

1. Click Edit next to Basics
2. The policy name and description can be modified
4. It is not recommended to modify the targeted apps as the policy is already configured to the Defender App.
5. Click Review + save to save the modifications.



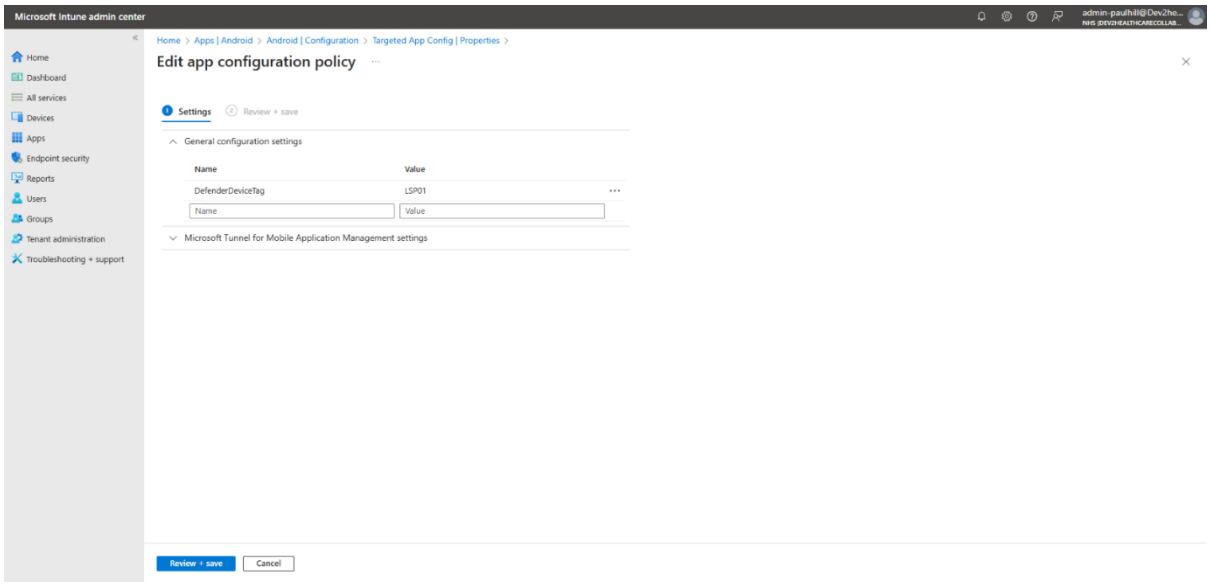
Edit Settings catalog

1. There are no settings for this particular app that can be modified.



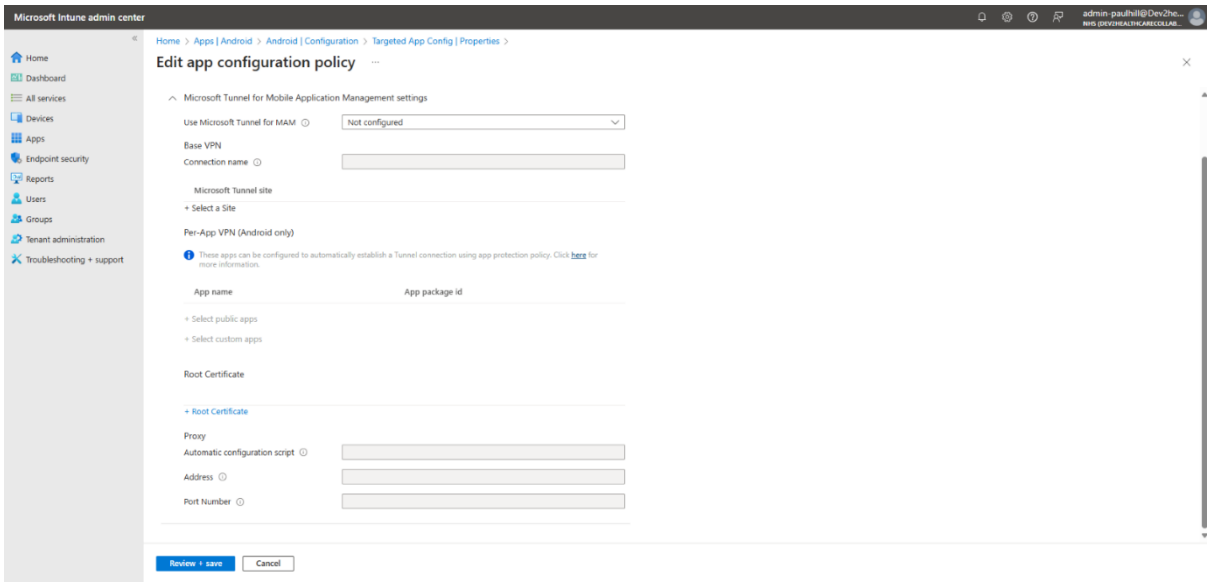
Edit Settings

1. It is not recommended to modify the General configuration settings as the policy has already been configured to the correct Name and Value for Defender and the Orgs ODS.



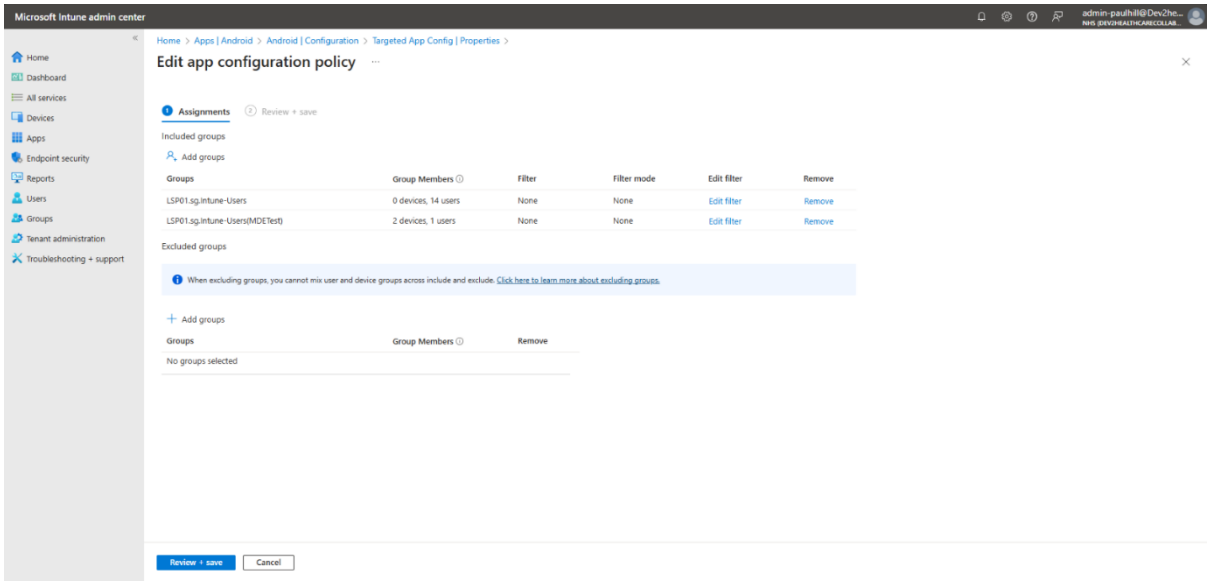
2. If required, Tunnel for MAM can be configured in the Microsoft Tunnel for Mobile Application Management Settings.

3. Configure the Tunnel as required and click Review + save to save the modifications.



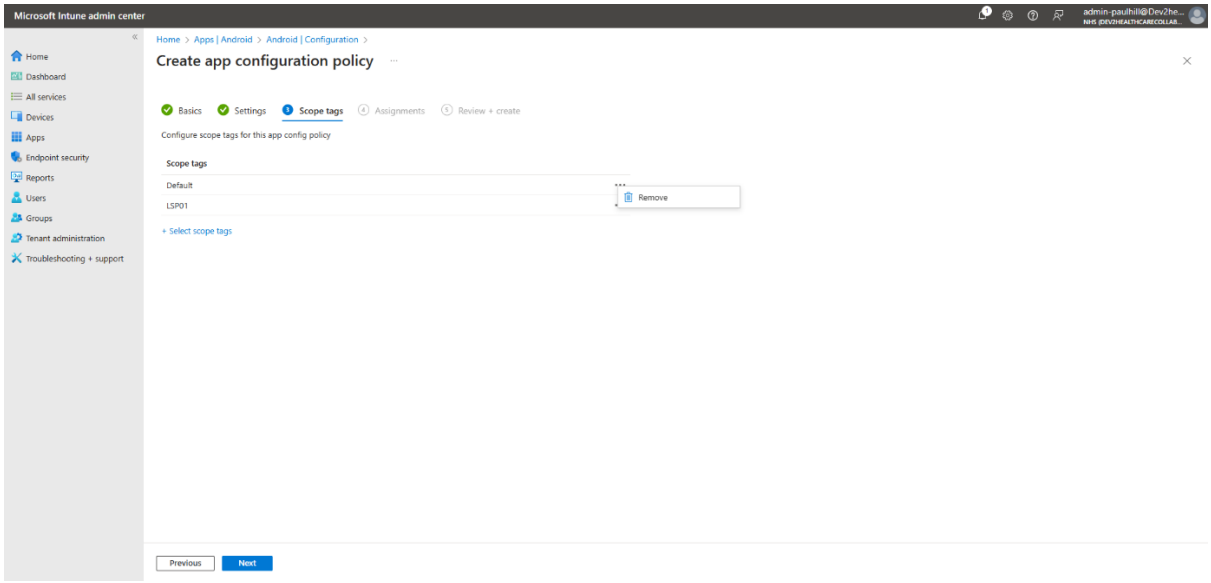
Edit Assignments settings

1. Click + Add Groups in either of the Include groups or Exclude groups sections to add groups that should be included or excluded from the policy.
2. Groups added to the Include groups section will have the Defender policy applied.
3. Groups added to the Exclude groups section will be exempt from the policy.



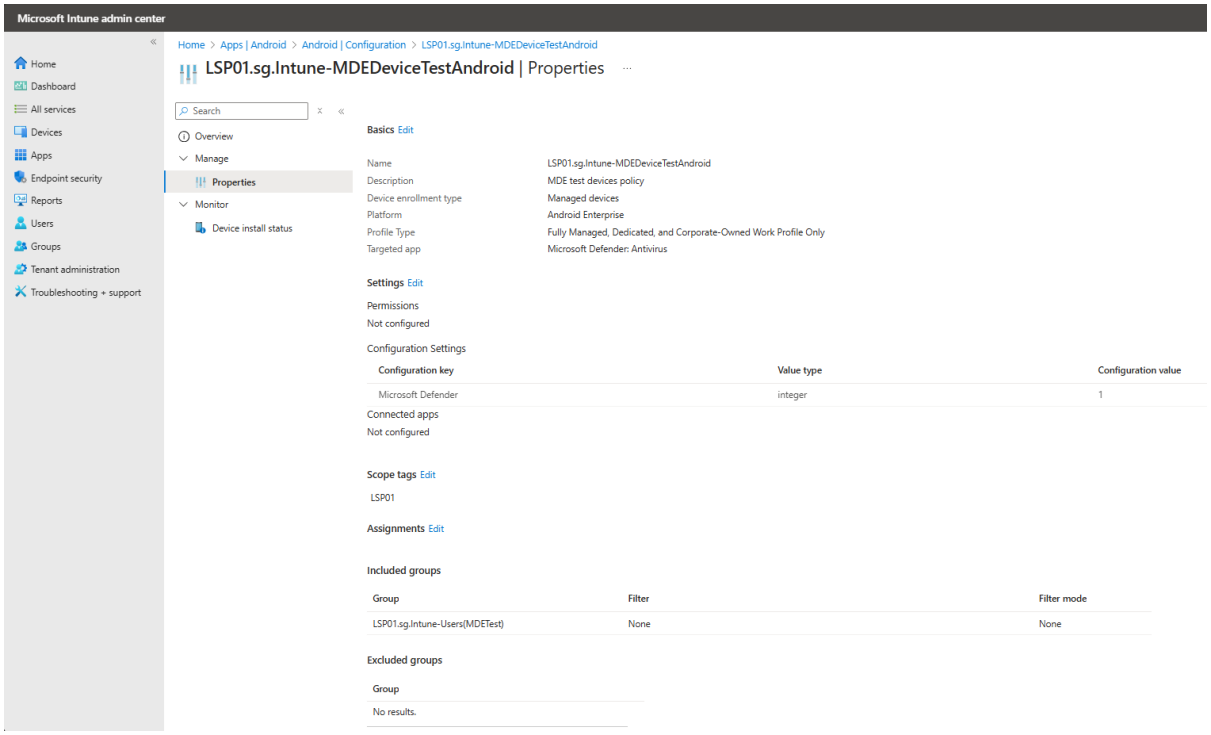
Edit Scope tags

1. It is not recommended to modify the Scope tags as the policy has already been configured to include the Orgs ODS.



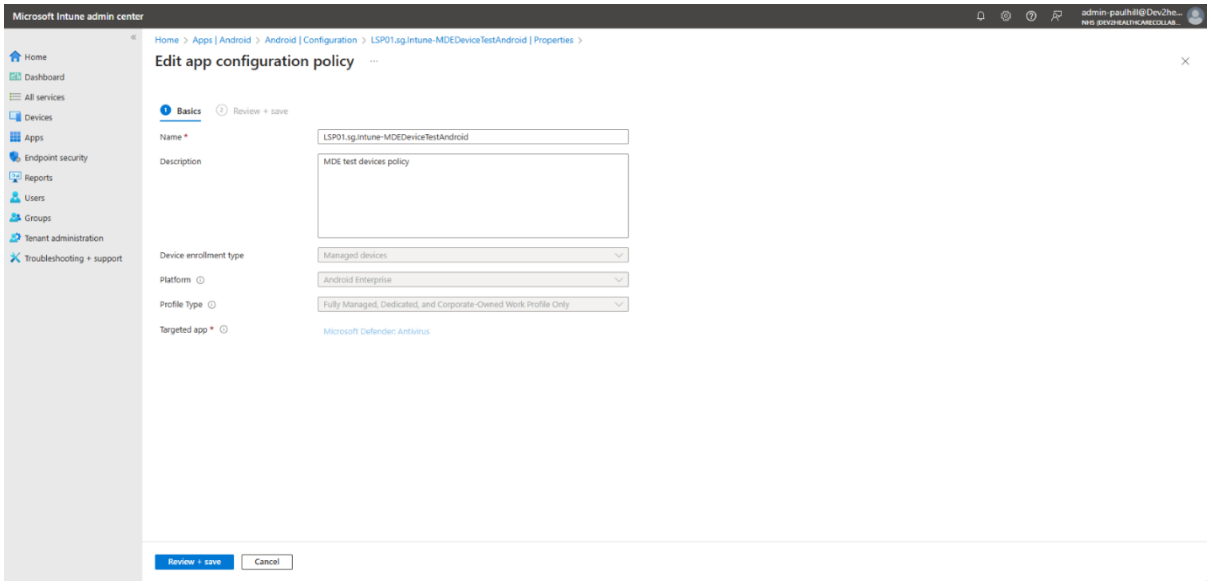
6.11.2 Modifying Managed Device Tagging

1. From Intune, navigate to Apps > Android > Configuration
2. Search for the Policy, click on it and go top Properties.
3. The sections that can be modified are;
   - Basics
   - Settings
   - Scope tags
   - Assignments


Microsoft Intune admin center
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Apps | Android > Android | Configuration > LSP01.sg.Intune-MDEDeviceTestAndroid
LSP01.sg.Intune-MDEDeviceTestAndroid | Properties
Search
Overview
Manage
Properties
Monitor
Device install status
Basics Edit
Name LSP01.sg.Intune-MDEDeviceTestAndroid
Description MDE test devices policy
Device enrollment type Managed devices
Platform Android Enterprise
Profile Type Fully Managed, Dedicated, and Corporate-Owned Work Profile Only
Targeted app Microsoft Defender: Antivirus
Settings Edit
Permissions
Not configured
Configuration Settings
Configuration key
Value type
Configuration value
Microsoft Defender
integer
1
Connected apps
Not configured
Scope tags Edit
LSP01
Assignments Edit
Included groups
Group
Filter
Filter mode
LSP01.sg.Intune-Users(MDETest)
None
None
Excluded groups
Group
No results.

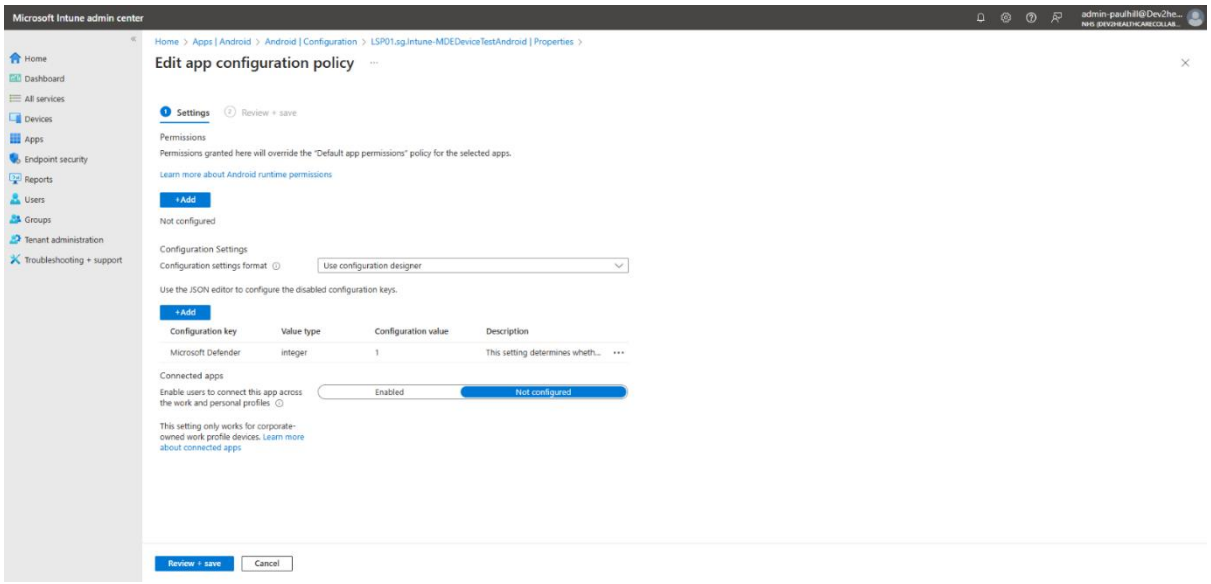
Edit Basics settings

1. The Policy Name and Description can be modified
2. Click Review + save to save the modifications



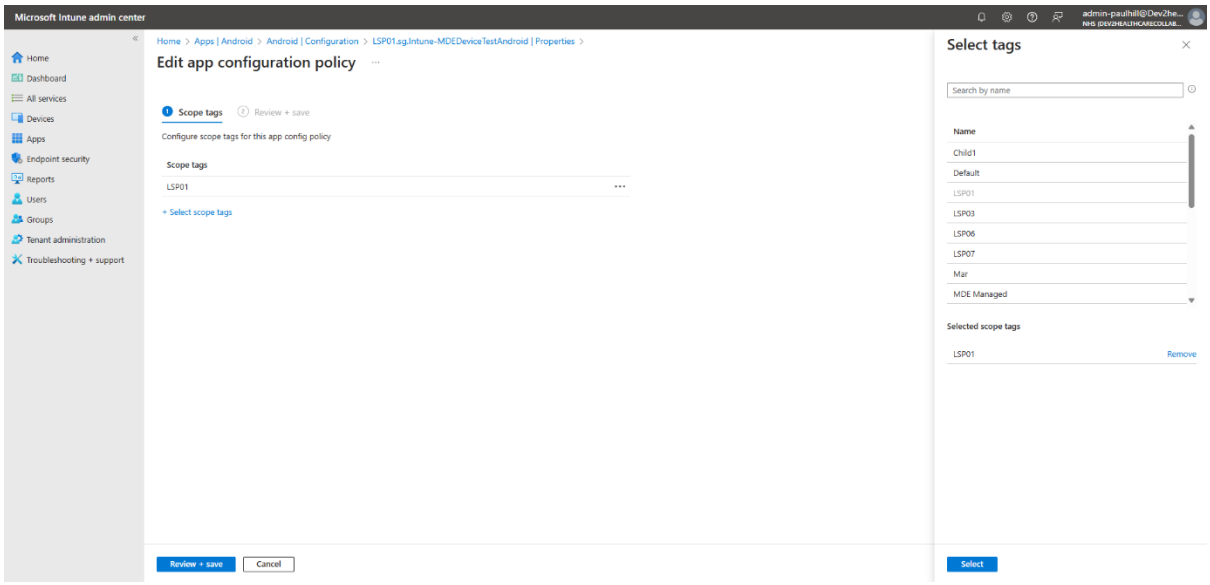
Edit Settings

1. It is not recommended to modify any setting in the Settings section as the policy has already been configured to the Defender App.



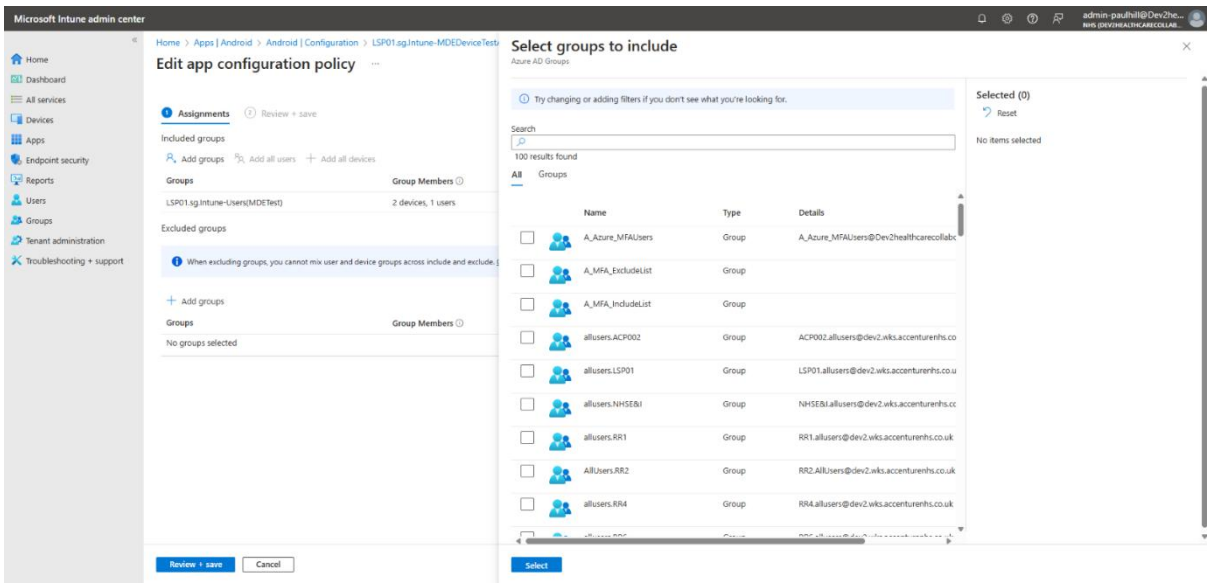
Edit Scope Tags

1. It is not recommended to modify the Scope tags as the policy has already been configured to include the Orgs ODS.



Edit Assignments settings

1. Click + Add Groups in either of the Include groups or Exclude groups sections to add groups that should be included or excluded from the policy.
2. Groups added to the Include groups section will have the Defender policy applied.
3. Groups added to the Exclude groups section will be exempt from the policy.



6.12 Naming of Android Device

When new shared or fully managed Enterprise Android devices are enrolled on to the Intune tenant, they will be automatically renamed ready to standard naming convention, for example:

"*LSP01-AndroidEnterprise-USERNAME-RZ8NC0VYP2X*"

!	**Important Note** LAs keeping an external tracker of devices should log the Serial number rather than the initial Android Device name, as this changes some time after enrollment due to the renaming script.

6.12.1 Renaming existing enrolled android devices

To rename existing enrolled android devices with the standard naming structure, Intune LAs must send a service request outlining the groups containing the devices they want to rename with the new format.

Once the groups are identified a member of the Intune Live Support team will populate a CSV. file with the group names and run the custom build PowerShell script to rename the existing devices.

The resulting naming format for Each Android Device enrolment type are:

- **Fully Managed Devices:** "ODS-OS-First Name-Last Name-Serial Number".
- **Dedicated (Shared) Devices:** "Enrollment profile–OS-Serial Number".

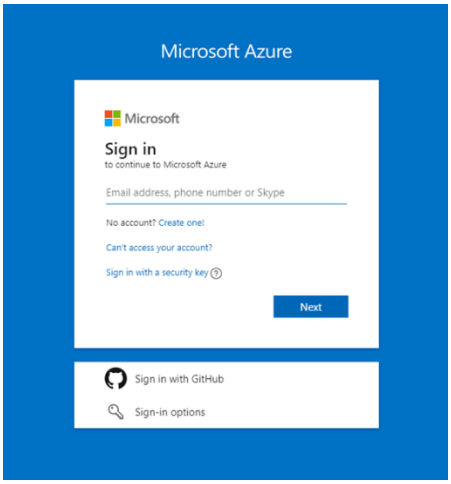
6.13 Retiring/Unenrolling Android

With delegated RBAC controls Intune LAs have the permissions to remotely wipe and remove iOS/iPadOS and Android devices from the NHSmail Intune platform. This action should be performed only as a last resort for devices experiencing issues and Intune LAs are not required to seek support from the Intune Live Service Team to complete this action.

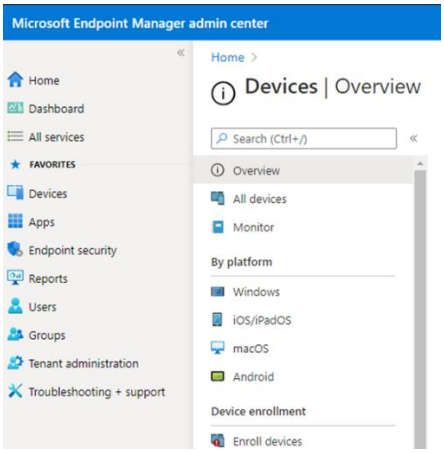
6.13.1 Wiping an Android device

Devices can be wiped through the Intune Portal by following the below steps:

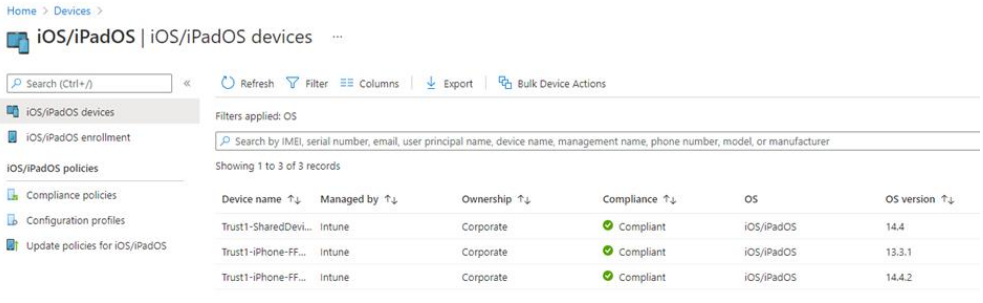
1. **Sign into** the Intune Portal.



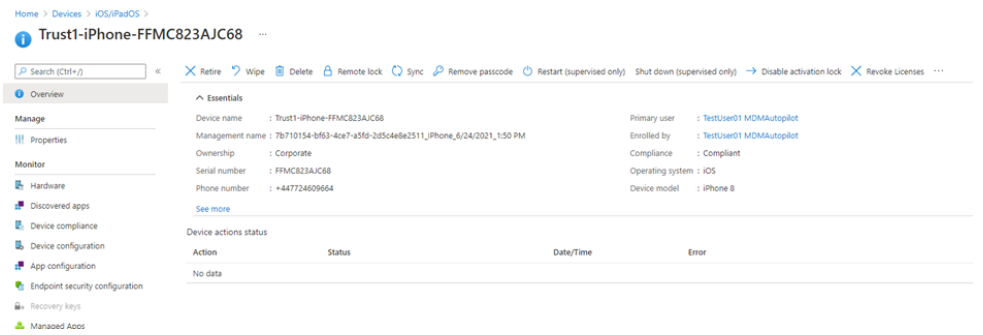
2. Select the **Devices** page.



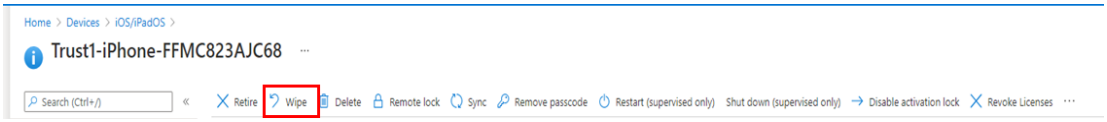
3. **Find** the device that you would like to wipe.



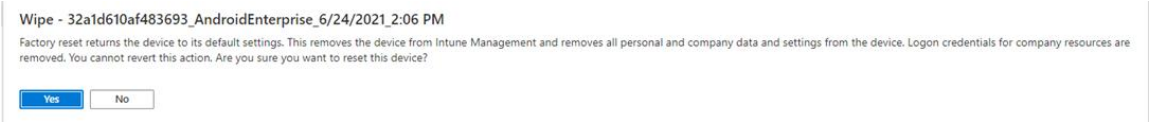
4. **Select** the device to be wiped.



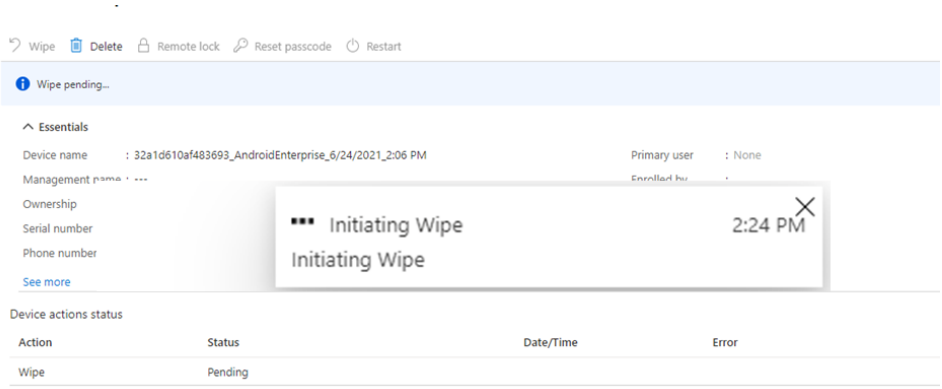
5. You be presented with a list of options at the top of the page. Select **Wipe** to factory reset the device and remove all data.



6. You will be prompted to confirm that you want to wipe the device. Select **Yes**.



7. The device will now begin wiping.



8. After the wipe has been initiated the device will be removed from the Portal.

!	**Important Note** Android Devices may still be visible in the Portal even after they have been wiped/retired. This is a known issue for Android devices.

7. Mobile Application Management (MAM)

Intune Mobile Application Management (MAM) allows Intune Local Administrators to manage and protect corporate data within an application.

Intune supports two MAM configuration types:

- **MAM without Enrolment (MAM-WE)**:
    - Manage apps using MAM and app protection policies on the devices that are not managed by any MDM solution.
- **MAM + MDM**:
    - Manage apps using MAM and app protection policies on devices that are enrolled with Intune (MDM). While Intune MDM protects at the device level, MAM and app protection policies protect at the application level.

!	**Important Note** Users need to have an M365 E3 licence assigned to their AAD accounts for MAM to work. Intune LAs are responsible for the provision of this licencing.

7.1 NHSmail Application Protection Policies

An additional layer of security is provided by application protection policies on Intune. App protection policies (APP) are rules that ensure an organisation's data remains safe or contained in a managed app. Many productivity apps, such as the Microsoft Office apps, can be managed by Intune MAM.

There are 6 default App Protection Policies available in Intune NHSmail. These policies have 3 different postures with a different level of complexity. These postures cover these platforms:

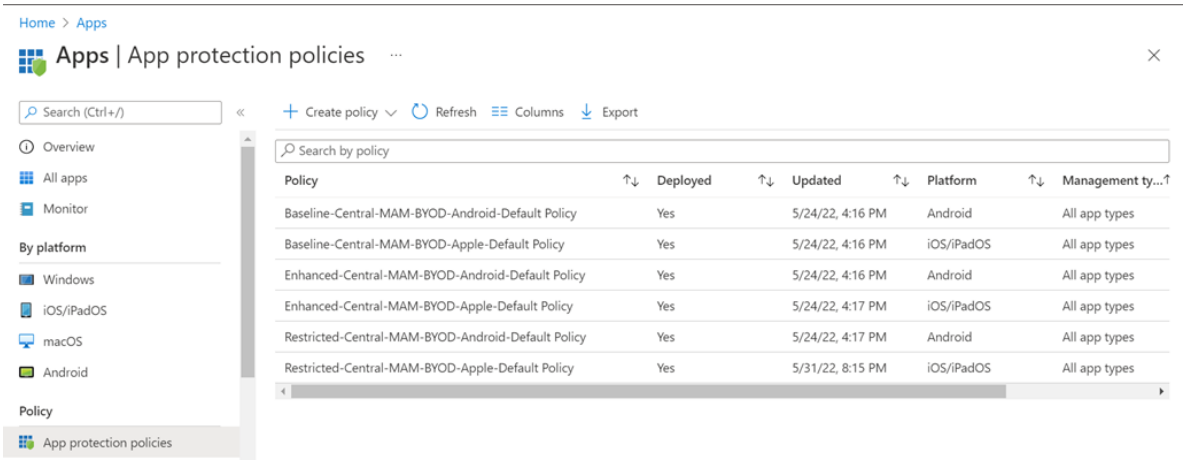
- Enrolled and Personal iOS/iPadOS devices.
- Enrolled and Personal Androids devices.

!	**Important Note** Windows & macOS Personal Devices cannot be enrolled in Intune. To protect corporate data on Personal devices, we recommend using App Protection Policies to protect Corporate Windows and macOS devices.

- **Baseline**: enterprise basic data protection. It is recommended as the minimum data protection configuration for an enterprise device.
- **Enhanced**: A more restrictive. It is recommended for devices where users access sensitive or confidential information. This configuration is applicable to most mobile users accessing corporate data.
- **Restrictive**: Provides the most secure data protection. It is recommended for devices run by an organisation with a larger or more sophisticated security team, or for specific users or groups who handle highly sensitive data.

!	**Important Note** App protection policies can be assigned to an organisation's AAD users security group only. **Device Groups are not supported for these policies**. Intune LAs must add the users to the group using the Security Group Management App.

This is the overview of the Centralised App Protection Policies in Intune NHSmail:



7.2 Assigning App Protection Policies

Organisations can assign any of the centralised app protection policies to their orgs Intune groups. They can also select more than one policy, however the scope of the Azure AD group should be different e.g., if an Intune LAs assigns <ODS>.sg-Intune-Users group to Restricted-Central-MAM-BYOD-Android-Default Policy and Baseline-Central-MAM-BYOD-Android-Default Policy, the most restrictive setting of any conflict will take precedent.

Recommendation / Recommended Use

App protection policy settings can be found below. We recommend reading these articles before assigning a policy:

iOS/iPadOS app protection policy settings - Microsoft Intune | Microsoft Docs

Android app protection policy settings - Microsoft Intune | Microsoft Docs

Validate your app protection policy setup - Microsoft Intune | Microsoft Docs

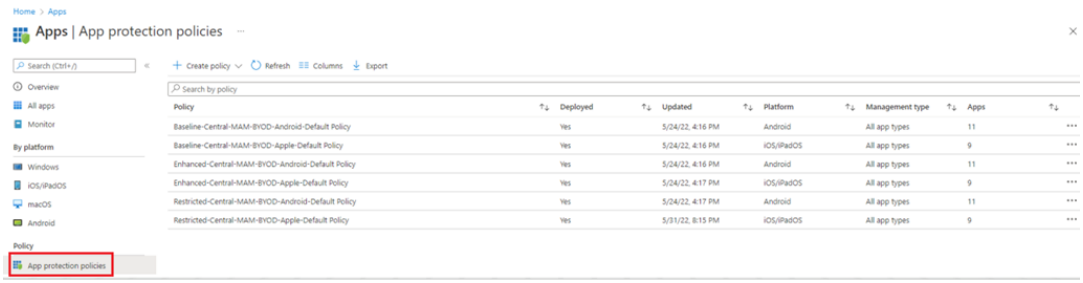
Important Note

There are different delivery window timings for app protection policies. For further details on the delivery timing summary, please review the following Microsoft documentation:

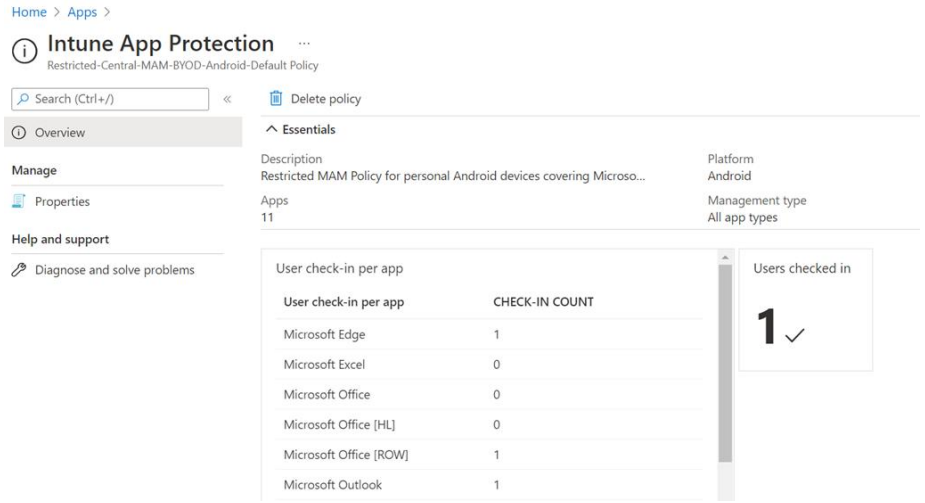
https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policy-delivery#delivery-timing-summary

To assign a policy, please complete the following steps:

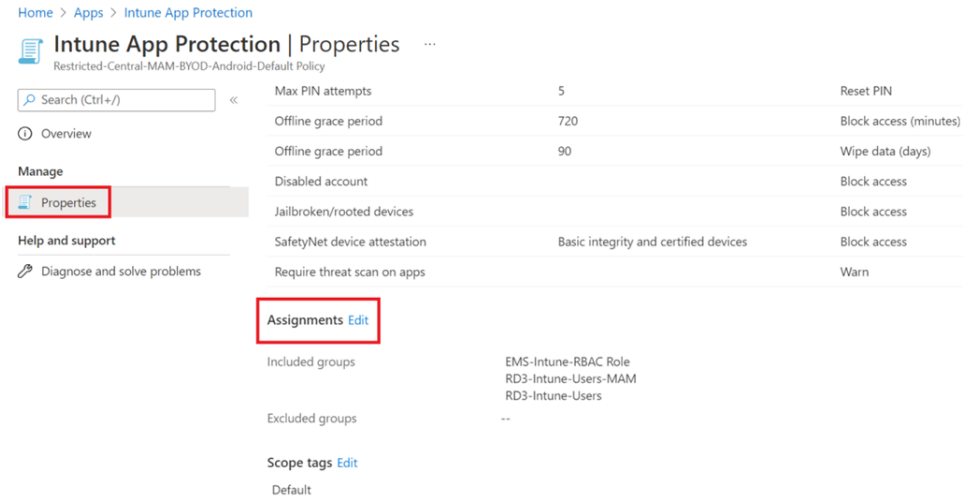
1. Sign into the **Microsoft Intune Admin center > Apps > App Protection Polices**.



2. Select one of the policies e.g., Restricted-Central-MAM-BYOD-Android-Default Policy



3. Select **Properties > Assignments > Add groups**. Search for the Azure AD group to apply the policy. There is a group created during the onboarding process with this name: ODS-Intune-Users-MAM



4. Click on **Review + save > Save**

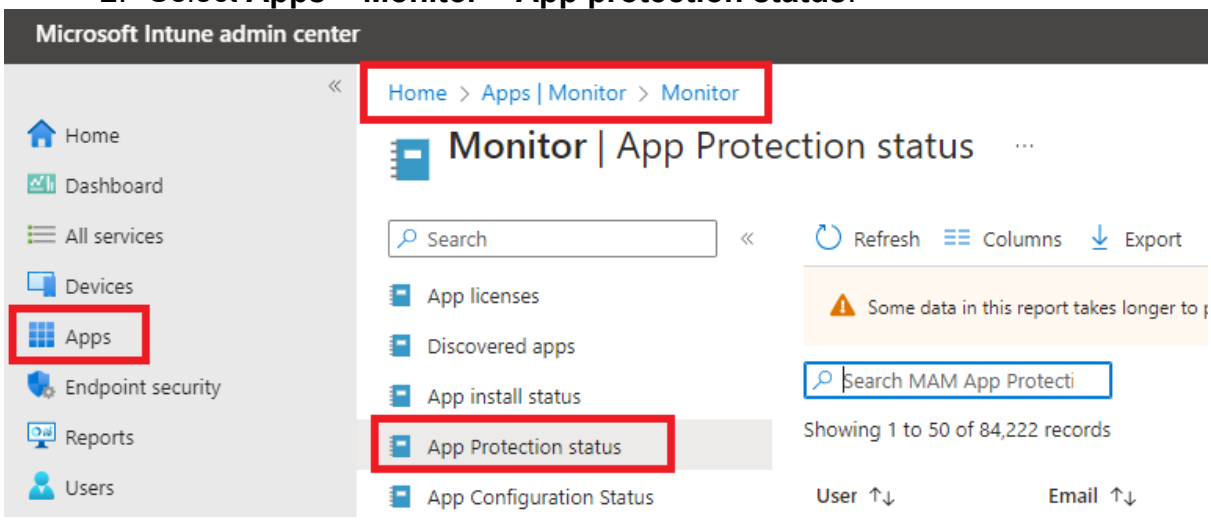
!	**Important Note** Centralised App Protection Policies cannot be modified by Intune LAs. Organisations can assign or unassign Azure AD groups scope for their organisations only.

7.3 Monitoring App Protection Policies

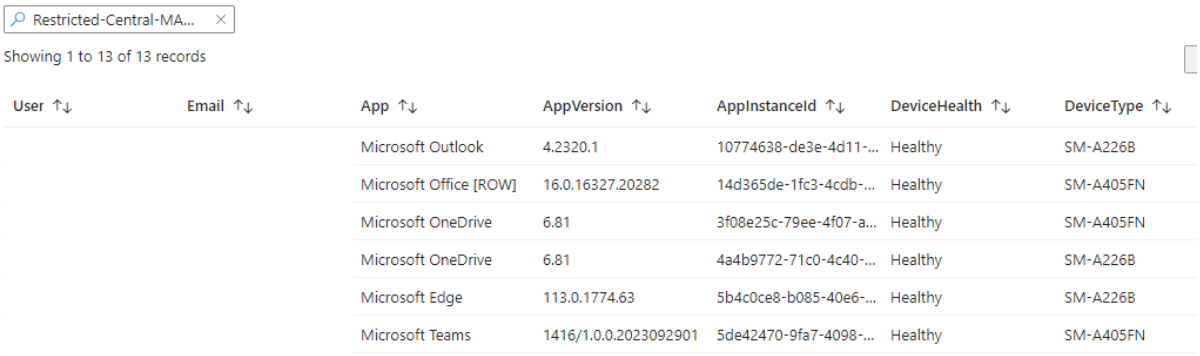
Intune LAs can monitor the status of app protection policies applied to users from the App protection section in Intune. Below are instructions detailing how Intune LAs can monitor app protection policies:

Important Note
The data in the “monitor” section is not delegated. Admins will be able to see App Protection data for all users on the tenant.

1. Sign into the **Microsoft Intune admin centre**.
2. Select **Apps > Monitor > App protection status**.



3. In the search box, type in the name of the user you wish to get the report on.
4.



Recommendation / Recommended Use

We recommend checking the following Microsoft documentation which provides support with troubleshooting app protection policy deployment in Intune if you are experiencing any issues:

	https://docs.microsoft.com/en-us/troubleshoot/mem/intune/troubleshoot-app-protection-policy-deployment

7.4 App Selective Wipe

Corporate data can be deleted from Intune-enrolled devices and Personal devices. App wide device can be used on devices that have been lost or stolen, or if a device needs to be reassigned to another end user.

If end users are using a personal device, their personal data will be preserved.

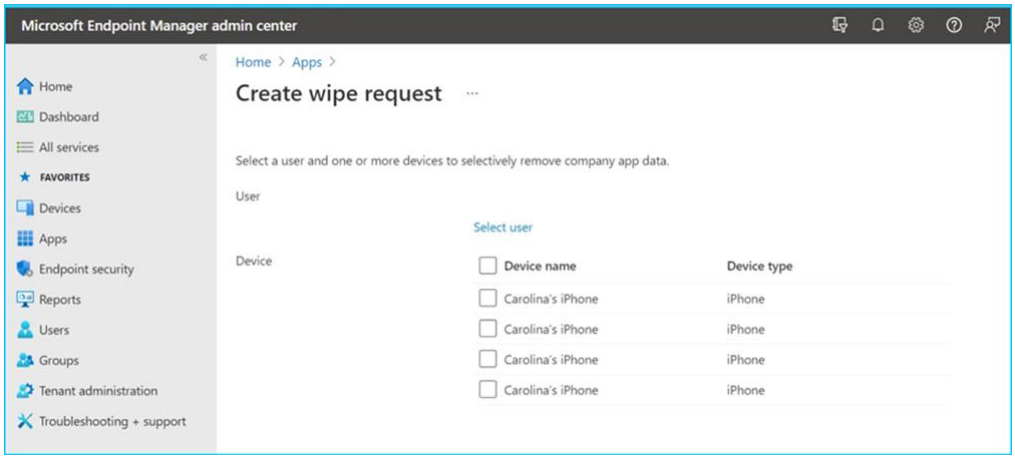
!	**Important Note** iOS/iPadOS, Android and Windows 10/11 are the only platforms currently supported for wiping corporate data from Intune managed apps.

There are two types of Selective Wipe:

- **Device based wipe request**: This will action a device wipe for one or all devices for a particular user.
- **User based wipe request**: This will action a data wipe for the user. The account is forced to sign out from all the protected Apps.

7.5 Creating a Device Wipe Request

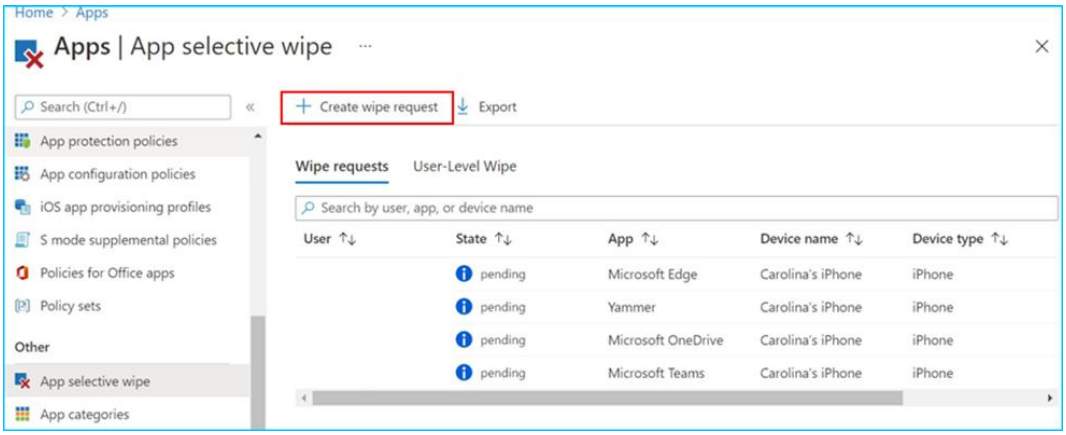
1. Sign into the Microsoft Intune admin centre.
2. Select **Apps > App selective wipe > Create wipe** request. The **Create wipe request** pane is displayed.
3. Click **Select user**, choose the user whose app corporate data you would like to wipe, and click **Select** at the bottom of the **Select user** pane.
4. Click **Select the device**, choose the device, and click **Select** at the bottom of the **Select Device** pane.



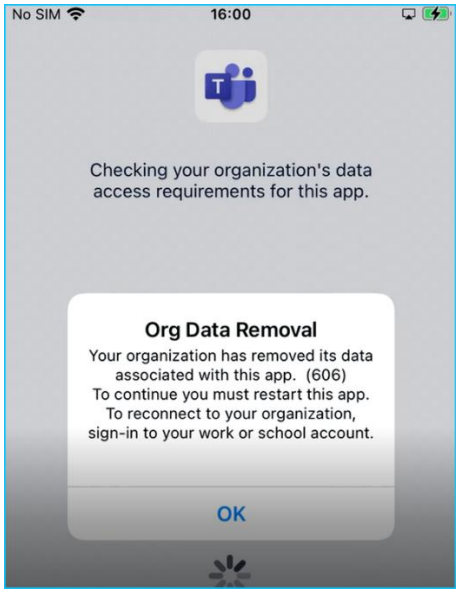
Important Note

Select all the devices listed if they have the same name. In effect, this will be only one device.

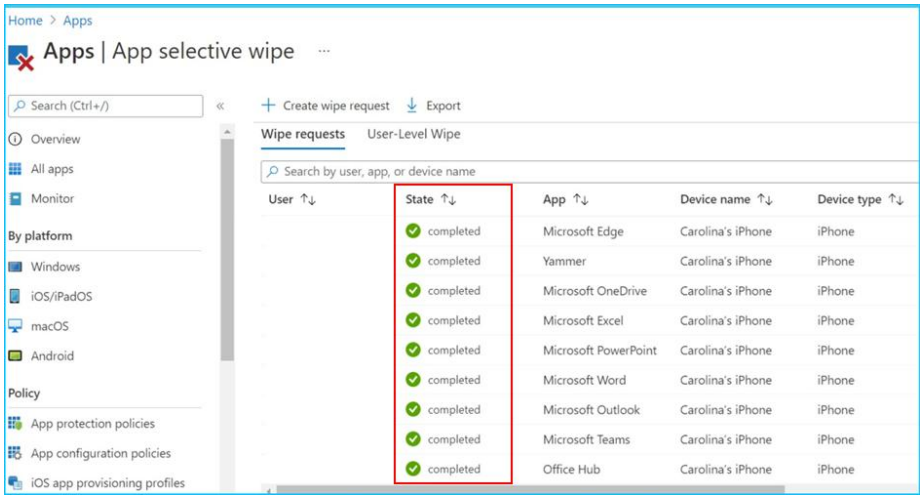
5. Click **Create** to make a wipe request
6. You will see a **Pending** Status.



7. If the end user accesses the Managed Apps from their device, they will see a similar message as per below screenshot:

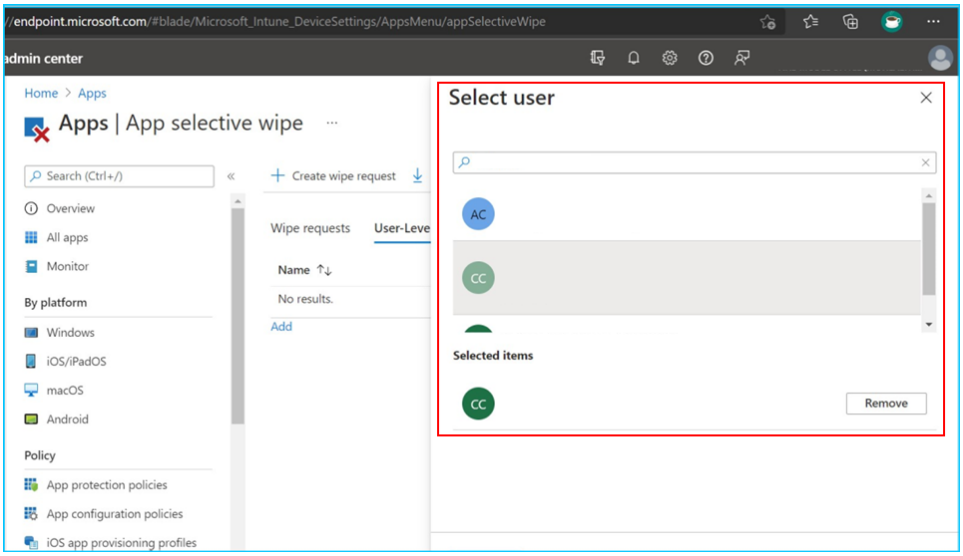


8. Once the Wipe is fully complete, the status will change to **Completed**.



7.6 Creating a User Wipe Request

1. Sign into the Microsoft Intune admin centre.
2. Select **Apps > App selective wipe > User-Level Wipe**.
3. Click **Add** and **Select user pane** is displayed.
4. Chose whose app data you would like to wipe and click **Select**.


endpoint.microsoft.com/#blade/Microsoft_Intune_DeviceSettings/AppsMenu/appSelectiveWipe
admin center
Home > Apps
Apps | App selective wipe
Search (Ctrl+/)
Overview
All apps
Monitor
By platform
Windows
iOS/iPadOS
macOS
Android
Policy
App protection policies
App configuration policies
iOS app provisioning profiles
Create wipe request
Wipe requests
User-Leve
Name
No results.
Add
Select user
AC
CC
Selected items
CC
Remove

8 Windows 10/11 Device Enrolment and Management

This section will outline the process you will need to follow and complete to successfully enrol a Windows 10/11 device via Autopilot.

Specifically, this section will cover:

- The Windows 10/11 security baseline
- Gathering hardware IDs, adding group tags and uploading to Intune
- What you will need to do to maintain the Windows 10/11 environment
- Naming standards and deployment profiles for Windows 10/11 devices

!	**Important Note** The following steps are for Windows 10/11 device enrolment directly onto the Intune platform (cloud-only). Should you wish enrol a Hybrid device, please refer to the Cloud + SSO and Hybrid Tracks Support Site Pages and Operations Guide.

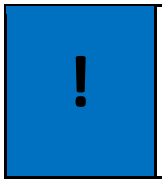
8.2 Hardware and Software Requirements

Prior to enrolling any Windows 10/11 devices onto Intune, the following minimum device and software specifications should be validated.

Device and software requirements:

- Windows 10 Pro/Enterprise version 20H2 or higher with relevant OS licence will be supported (includes Windows 10 Team editions for Surface Hub).
- For Windows 10, Intune LAs should ensure that TPM 2.0 is enabled in the BIOS / UEFI settings
- For Windows 11 devices, the following requirements must be met in order to enrol:
    - Your device must be running Windows 10, version 2004 or later, to upgrade.
    - Processor: 1 gigahertz (GHz) or faster with 2 or more cores on a compatible 64-bit processor or System on a Chip (SoC).
    - RAM: 4 gigabyte (GB).
    - Storage: 64 GB or larger storage device
    - TPM: Trusted Platform Module (TPM) version 2.0.

If your device does not meet these requirements, you may not be able to install Windows 11 on your device. If you are unsure whether your PC meets these requirements, you can check with your PC Original Equipment Manufacturer (OEM) or, if your device is already running Windows 10, you can use the PC Health Check app to assess compatibility. Note that this app does not check for graphics card or display.



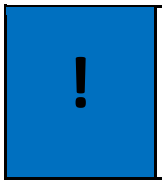
Important Note

Windows end of life release information – for further details on end of life information for Windows

8.2.1 Windows 10/11 Security Baseline

The Windows Security Baseline is a global baseline which has been centrally configured.

Organisations should consider whether the Windows security baseline settings and RBAC settings may conflict with any local settings or policies and should adjust any conflicting local policies and / or settings accordingly to minimise enrolment delays.



Important Note

The Windows 10/11 Security Baseline settings will take precedence over any other locally configured security policies.

Managed Centrally

The Windows 10/11 Security Baseline settings are set and managed centrally. Intune LAs are not able to edit these security settings.

If Organisations can raise a ticket if there are issues with the Security Baselines. To do this Intune LAs will need to raise a service request via Helpdesk Self-Service (option: Request an update to the Windows 10 baseline (centrally managed)).

For a full list of the Windows 10/11 Security Baseline settings, please see the Appendix.

8.2.2 Global-Defender for Endpoint Baselines

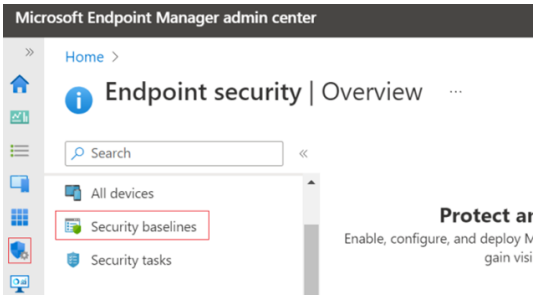
The Defender for Endpoint security baseline sets Defender for Endpoint security controls to provide optimal protection to devices in Intune. This is an in-built set of configurations recommended by Microsoft. The MDE baseline is applied to All Windows devices.

This baseline is optimized for physical devices and is not recommended for use on virtual machines (VMs) or VDI endpoints.

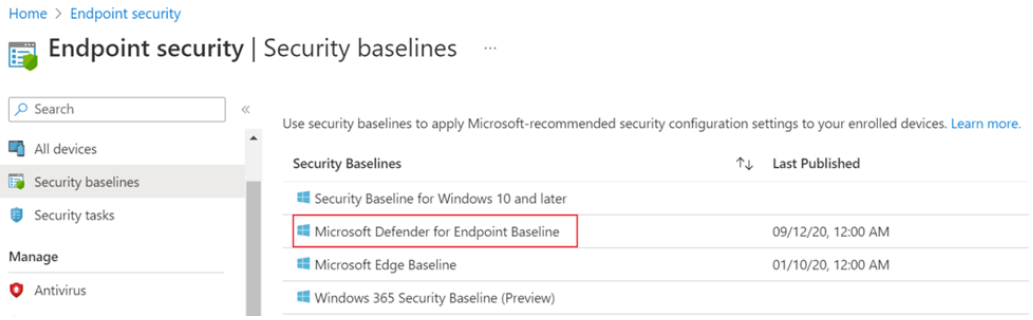
You can see a summary of the configuration settings in the Appendix of this document.

To see the settings for the Global-Defender for Endpoint from Intune, follow the below steps:

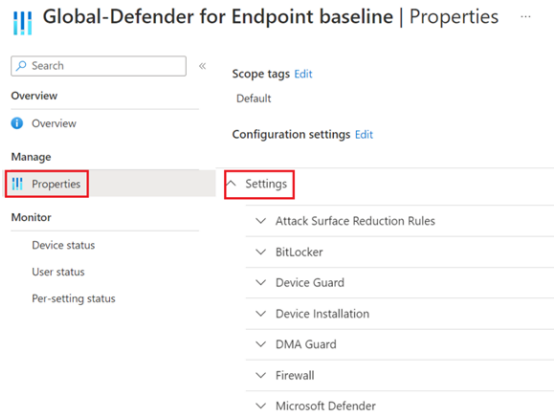
1. Login to Intune admin console > https://endpoint.microsoft.com
2. Navigate to Endpoint Security
3. Select Security baselines



4. Select Microsoft Defender for Endpoint Baseline



5. Select Properties > Configuration Settings > Expand Settings



!	**Important Note** Intune Local admins don't have right to modify the security baseline.

!	**Important Note** Some settings might conflict if you already have a separate device configuration enabled for your organization. You might need to review it.

8.2.3 Global-Edge-Baseline

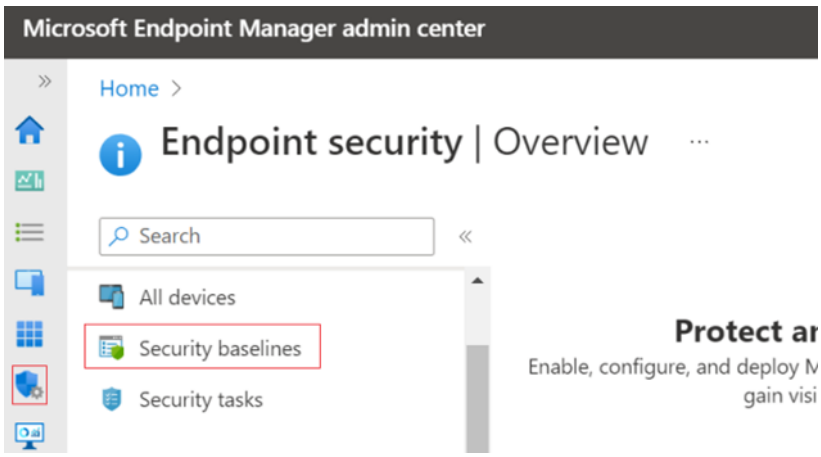
The Microsoft Edge Baselines are an extension/addition to the Existing Windows 10/11 Security baseline settings and are designed to provide additional security measures on the Microsoft Edge browser.

For each setting you'll find the baselines default configuration, which is also the recommended configuration for that setting provided by the Microsoft security team.

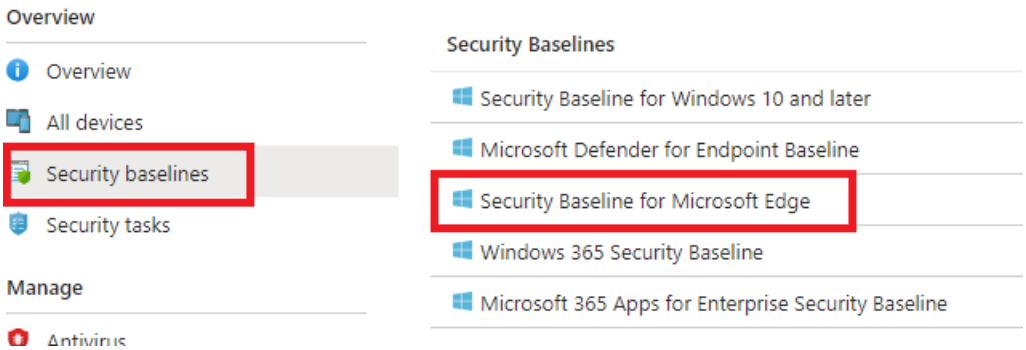
You can see a summary of the configuration settings in the Appendix of this document.

To see the settings for the Global-Defender for Endpoint from Intune, follow the below steps:

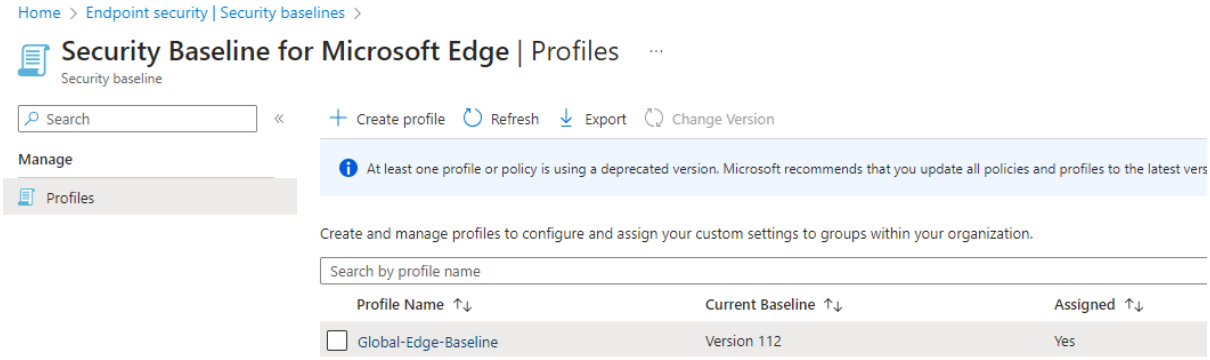
1. Login to Intune admin console > https://endpoint.microsoft.com
2. Navigate to Endpoint Security
3. Select Security baselines



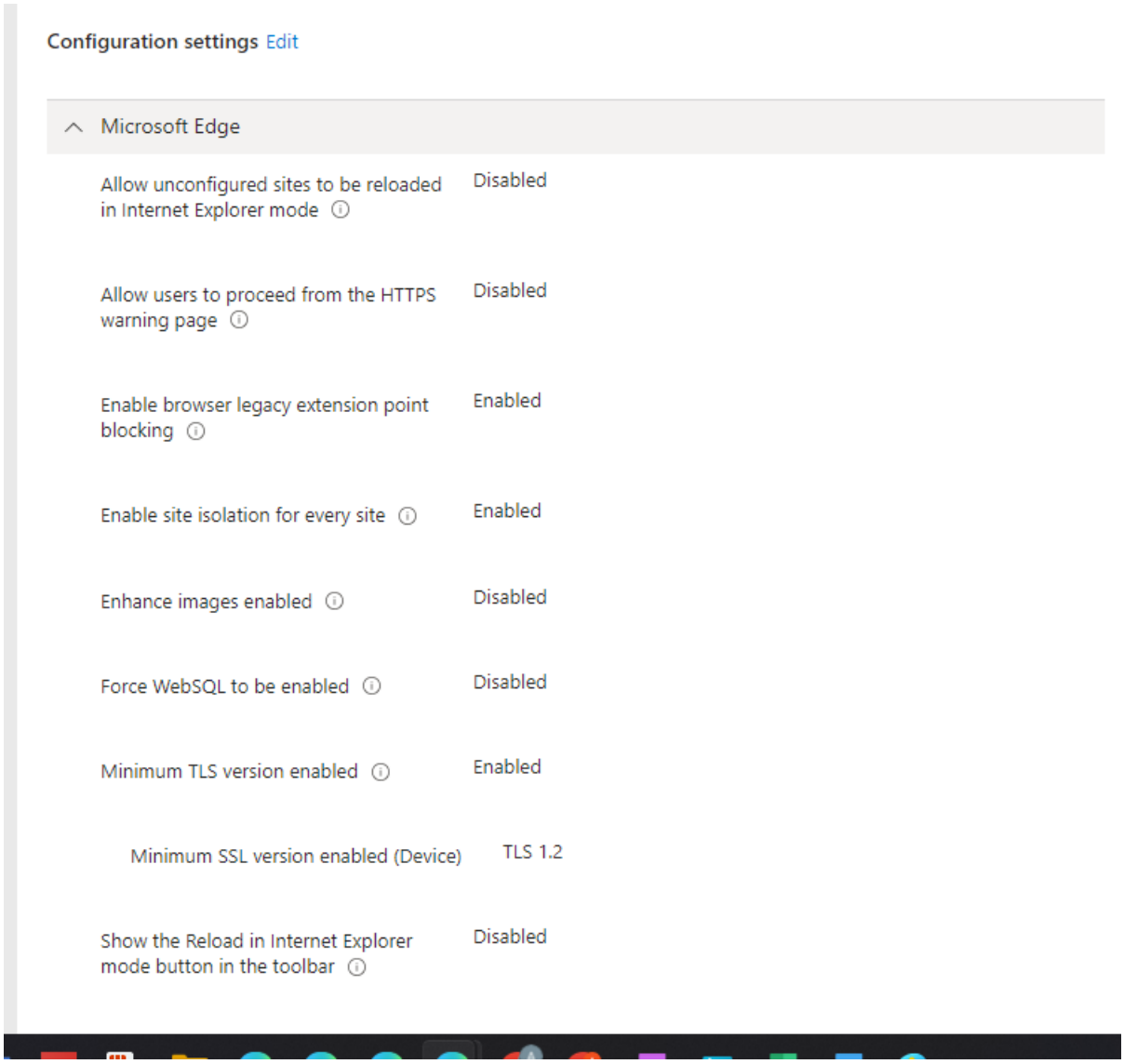
4. Select Security Baseline for Microsoft Edge



5. Select Global-Edge-Baseline



6. Scroll to Configuration Settings > Expand Settings



8.3 Gathering Hardware IDs (Autopilot Enrolment)

There are several ways to gather hardware IDs from your Windows 10/11. The following section is focus on Windows 10/11 Autopilot on the cloud only.

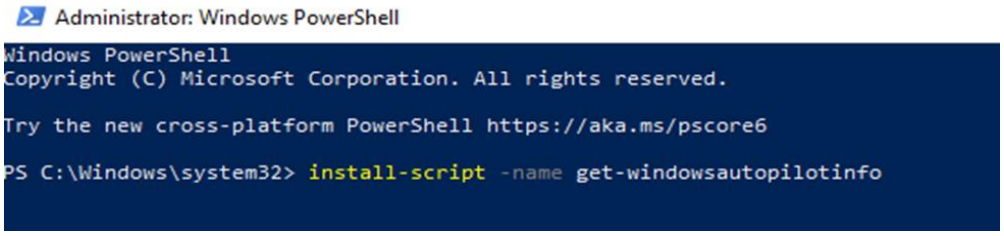
If your organisation is using SCCM, please refer to information on the SCCM Windows Autopilot Hardware Hash Methods in the Appendix of this document for more detailed information.

8.3.1 PowerShell Script

You can use **Get-WindowsAutoPilotInfo.ps1 script** to gather the hardware ID of a Windows 10/11 device.

1. Open a PowerShell window as an administrator and type in the following command:

Install-Script -name Get-WindowsAutoPilotInfo



2. If prompted, type **Y <Enter>** to accept the PATH Environment Variable Change.

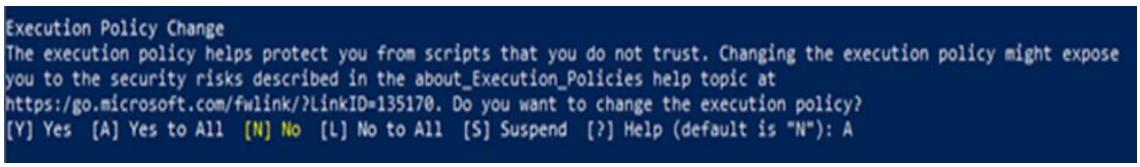
3. If prompted, type **A <Enter>** to accept Untrusted Repository.

4. Type the following command to change the directory to the Script Route:

5. Type the following command to set the Execution Policy to Unrestricted:

   Set-ExecutionPolicy –ExecutionPolicy Unrestricted

6. Accept the Execution Policy change by typing **A <Enter>**.



7. Type the following command to run the Get-WindowsAutoPilotInfo script:

   .\Get-WindowsAutoPilotInfo.ps1 -Output C:\Temp\HardwareID.CSV

8. The hardware ID should be exported to the .CSV file location that you specify in the output parameter.

8.3.1.1 Adding Group Tags

Critical Notes that will require action

Before uploading the hardware hash data into Intune, you must add the Trust's Group Tag to the .CSV file. If this step is missed**, the Windows 10/11 device will not be assigned to an AutoPilot enrolment policy and the device will fail to enrol**.

It is possible to assign the Group Tag manually after the import of the hardware IDs. However, this will have to be performed one device at a time and will not be easy to identify devices amongst other organisations', especially if importing large numbers of hardware IDs. For this reason, it is not a recommended practice.

To add the Group Tag, a new column needs to be added to the .CSV file populated with the

Group ID of the Trust. To do this please follow these steps:

1. Open the .CSV file containing the exported hardware IDs in Excel. There should be three columns containing the exported data.

Device Serial Number	Windows Product ID	Hardware Hash

2. Row 1 should show the header information. Delete any rows above the header row.
3. Delete any extra columns on the left side that do not contain device information.
4. If the Column headings do not match the above, edit them so they are an exact match.
5. There should now be three columns A, B, C with the above headings in row 1, the rest of the rows should be populated with the number of data rows that were exported.
6. To add the Group Tag for your organisation, add the Group Tag column header in cell D1.
7. Populate the remaining data rows in column D with the Trust's Group ID – (in the below example VN105 is the Group ID).

Important Note

For HoloLens 2 Group Tag information, please review the HoloLens 2 Device Enrolment Section.

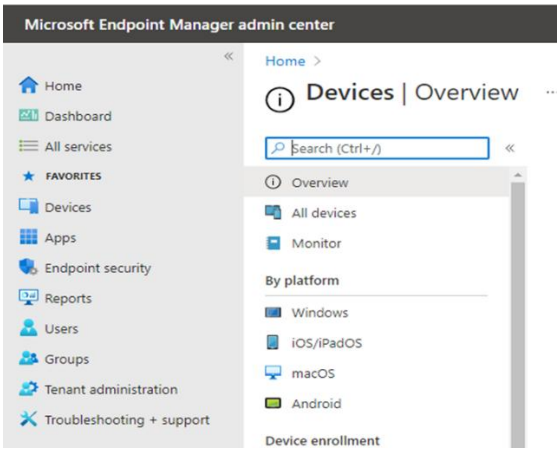
```
Untrusted repository
You are installing the scripts from an untrusted repository. If you trust this repository, change its
InstallationPolicy value by running the Set-PSRepository cmdlet. Are you sure you want to install the scripts from
'PSGallery'?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "N"): A
```

8. The AutoPilot device data should now be ready to be imported into Intune.

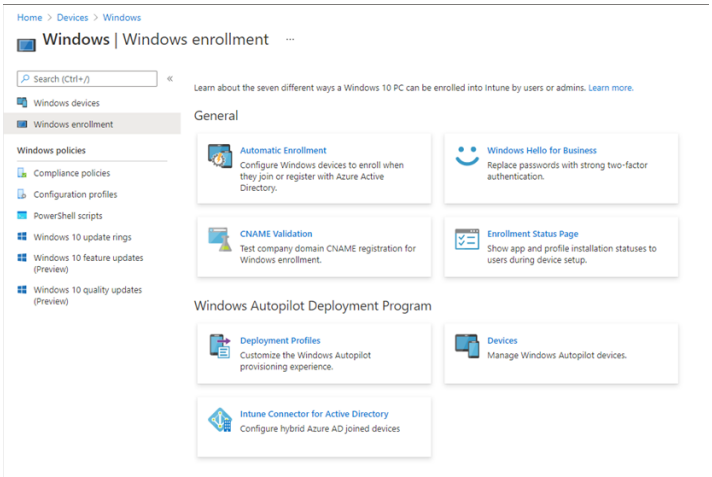
8.3.1.2 Uploading Hardware IDs into Intune

Please follow the below steps to upload hardware IDs into Intune:

1. Sign into **Microsoft Intune** (https://endpoint.microsoft.com) on a web browser using an admin account with an active Intune Administrator role and select **Devices**.



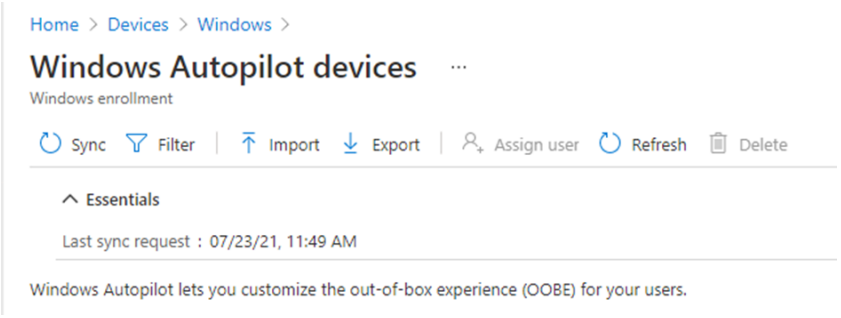
2. Select **Windows > Windows Enrolment** and then select "**Devices**" (Manage Windows AutoPilot Devices).



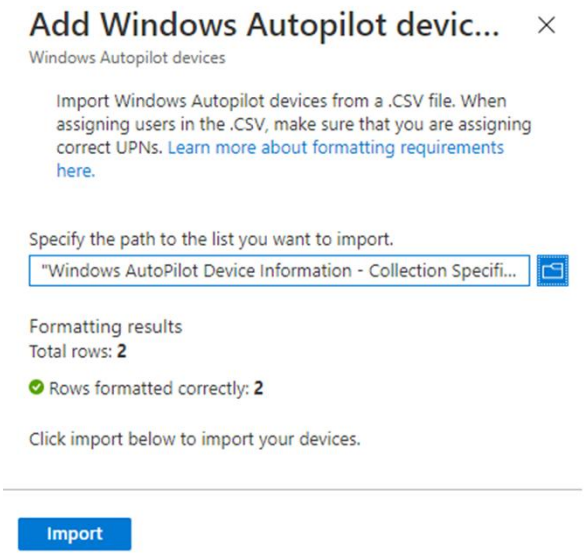
!	**Important Note** As imported Autopilot devices cannot have scope tags attached to them, Intune LAs can delete any Autopilot device which does not

	have a profile assigned, including those belonging to other organisations. **Intune LAs should take sufficient care to:** **1. Assign a profile to a device as soon as it is added** **2. Avoid deleting any devices when accessing the Devices blade under Windows Autopilot Deployment Program.** Any deleted device information can be imported again and this does not affect any active enrolled devices.

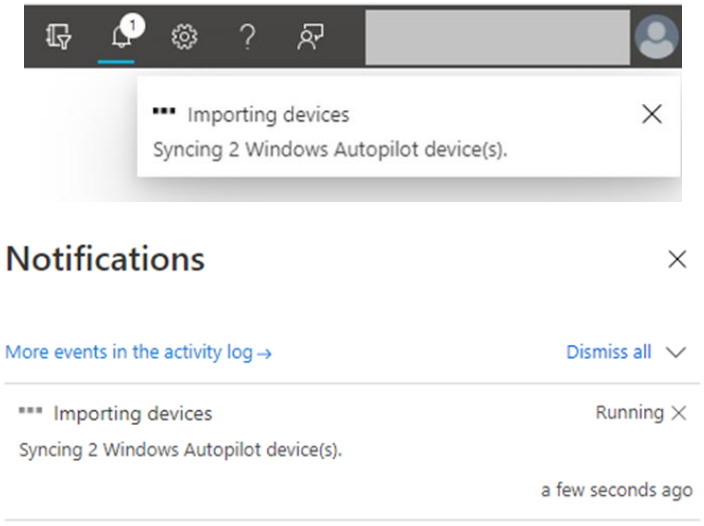
3. In the **Windows Autopilot devices** window, select **Import**.



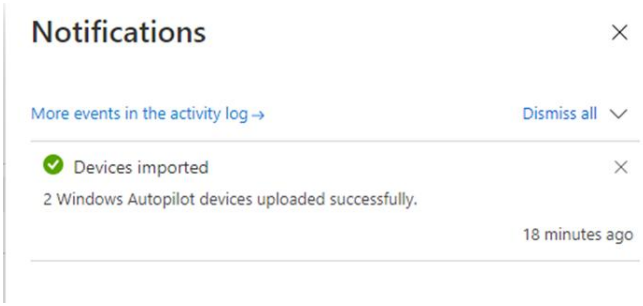
4. Browse to the .CSV file that contains the data that you want to import. If the data is formatted correctly a tick will show in the **Formatting results** information pane. Verify the number of rows match the number of devices to import and then click **Import**.



5. The notification (Bell Icon) will show the progress of the data import. You can click on the notification icon to see the status.



6. It will take a while to upload the data. A success message will appear once the data has been successfully uploaded.



8.3.2 Obtaining Device Hardware IDs from vendors

Some hardware vendors will provide the hardware IDs of devices you have purchased in .CSV format.

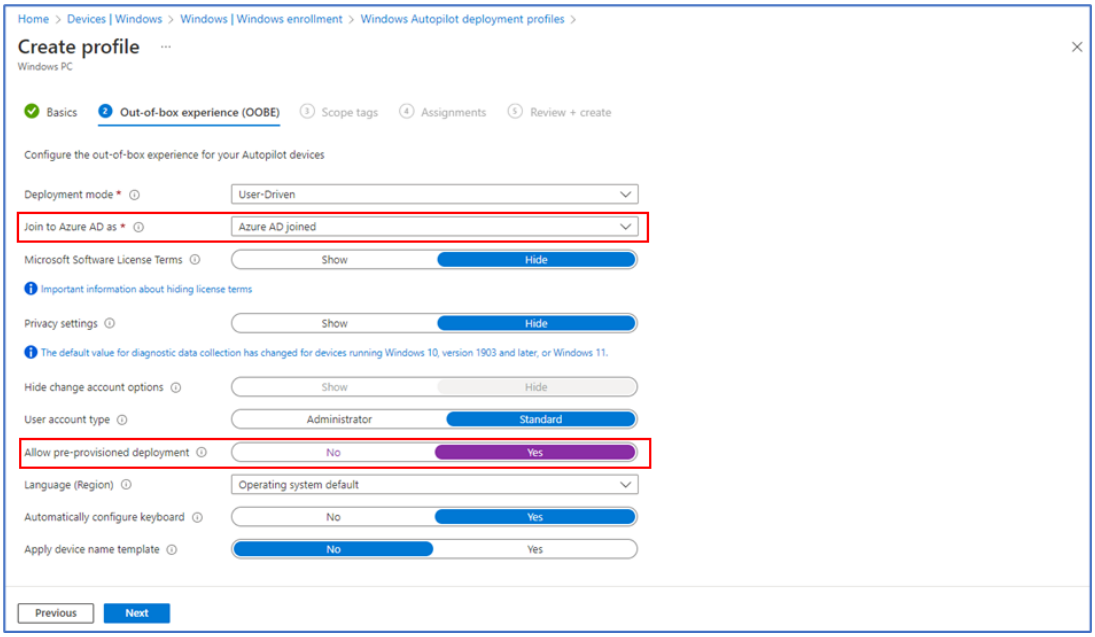
Speak to your hardware vendor to see if they can provide this service.

8.3.3 Autopilot Manufacturer Provisioning

8.3.3.1 Configuring Autopilot Pre-provisioning

Once the requisite OEM / VAR is supported in NHSMail Intune, LAs can proceed to use Autopilot Deployment profiles with 'pre-provisioning' enabled. The following steps outline the key configuration items to deploy a pre-provisioning profile:

1. Create an Autopilot Profile in the typical fashion and select **Azure AD Joined** and allow **pre-provisioned deployment** from the options as below

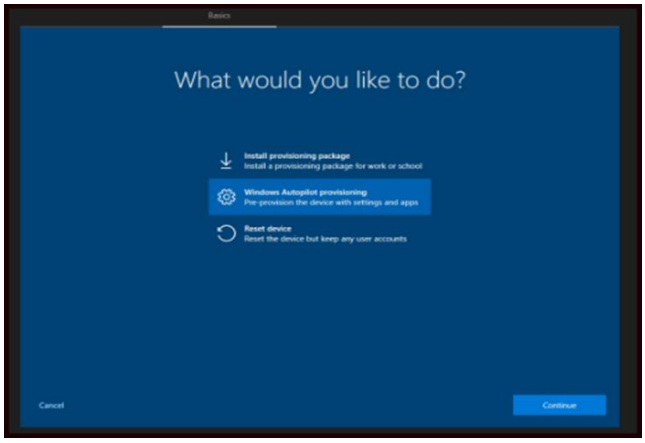


2. Complete the Scope Tags and Assignments to the groups targeted for pre-provisioned devices and create the profile.

> **!** **Important Note**
>
> The users and devices targeted by the profile need to be registered in the NHSMail Intune tenant prior to the device being shipped to them.

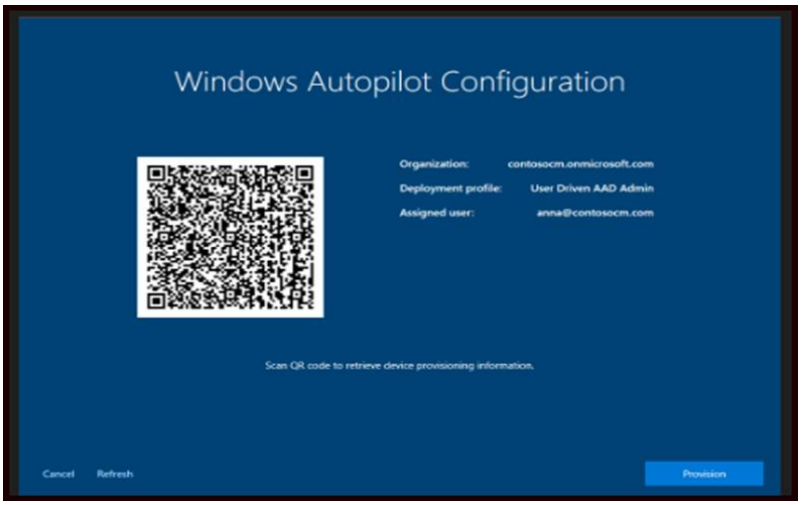
8.3.3.2 Pre-ship Experience for Pre-provisioning (at VAR or OEM location):

- **Power-on the device**.
- From the first **OOBE screen** (which could be a language selection or locale selection screen), **don't click Next**. Instead, press the Windows key five times to view an additional options dialogue. Choose the **Windows Autopilot provisioning** option from that screen and click **Continue**.



On the **Windows Autopilot Configuration** screen, information will be displayed about the device:

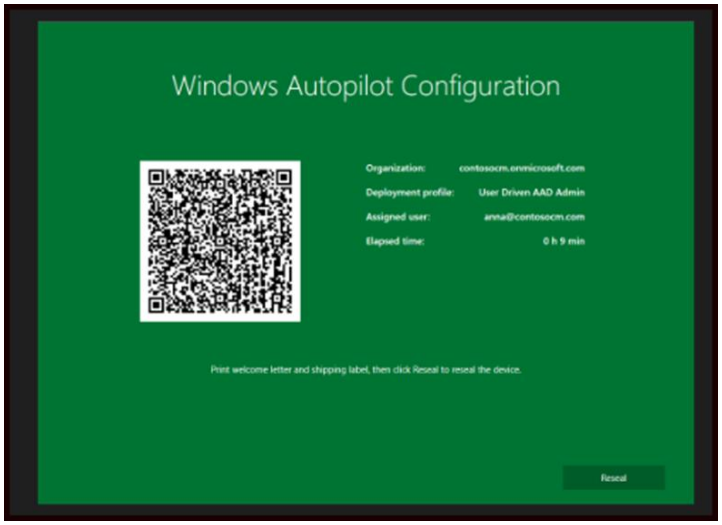
- The Autopilot profile assigned to the device.
- The organization name for the device.
- The user assigned to the device (if there is one).
- A QR code containing a unique identifier for the device. You can use this code to look up the device in Intune. You might want to do this to make configuration changes, like assigning a user or adding the device to groups needed for app or policy targeting.
    - Validate the information displayed. If any changes are needed, make the changes and then click Refresh to re-download the updated Autopilot profile details.



- Select Provision to begin the provisioning process.

If the pre-provisioning process completes successfully:

A green status screen appears with information about the device, including the same details presented previously. For example, Autopilot profile, organization name, assigned user, and QR code. The elapsed time for the pre-provisioning steps is also provided.



- Select Reseal to shut down the device. At that point, the device can be shipped to the end user.

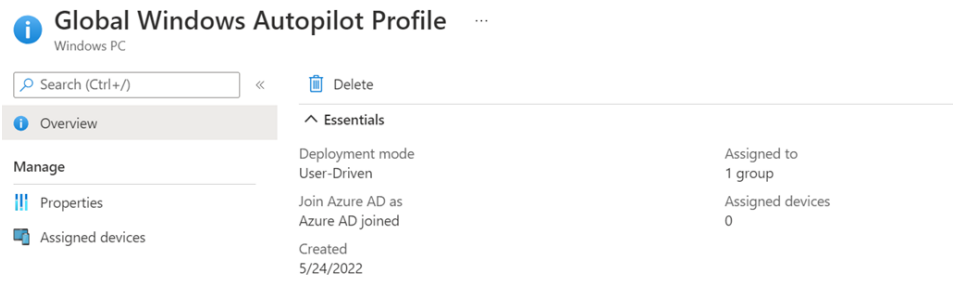
8.3.3.4 Step 2: – End-User Experience – after pre-provisioning

When the device is shipped from the OEM/VAR, the end user will complete the normal Windows Autopilot user-driven process following these steps:

- Power on the device.
- Select the appropriate language, locale, and keyboard layout.
- Connect to a network (if using Wi-Fi). Internet access is always required.
- On the branded sign-on screen, enter the user's Azure Active Directory credentials.
- Additional policies and apps will be delivered to the device, as tracked by the Enrolment Status Page (ESP). Once complete, the user can access the desktop.

8.4 Windows 10 Enrolment Process

There is a Global Autopilot profile setup for Windows devices in Intune. Once the hardware hash has been imported, the device will be added automatically to the Dynamic group that contain all the Windows 10 devices for your Organisation (ODS-Intune-Windows10-Devices).

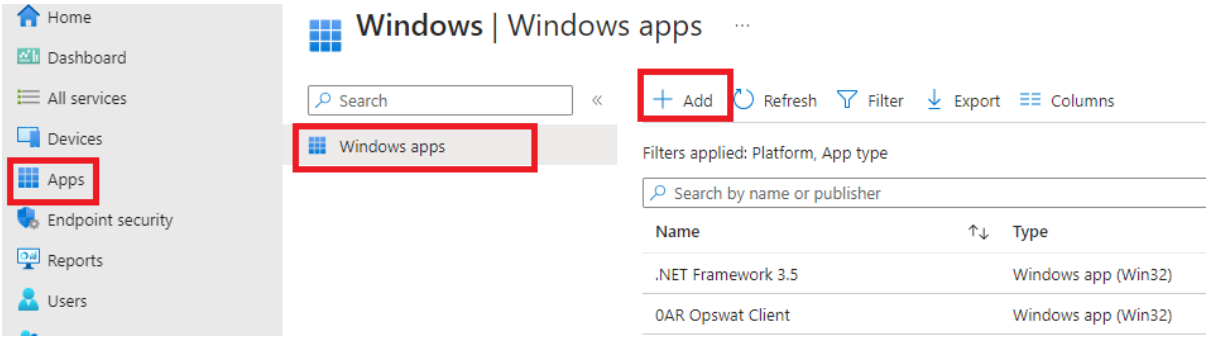


!	**Important Note** Global Windows Autopilot Profile is not editable by Intune LAs.

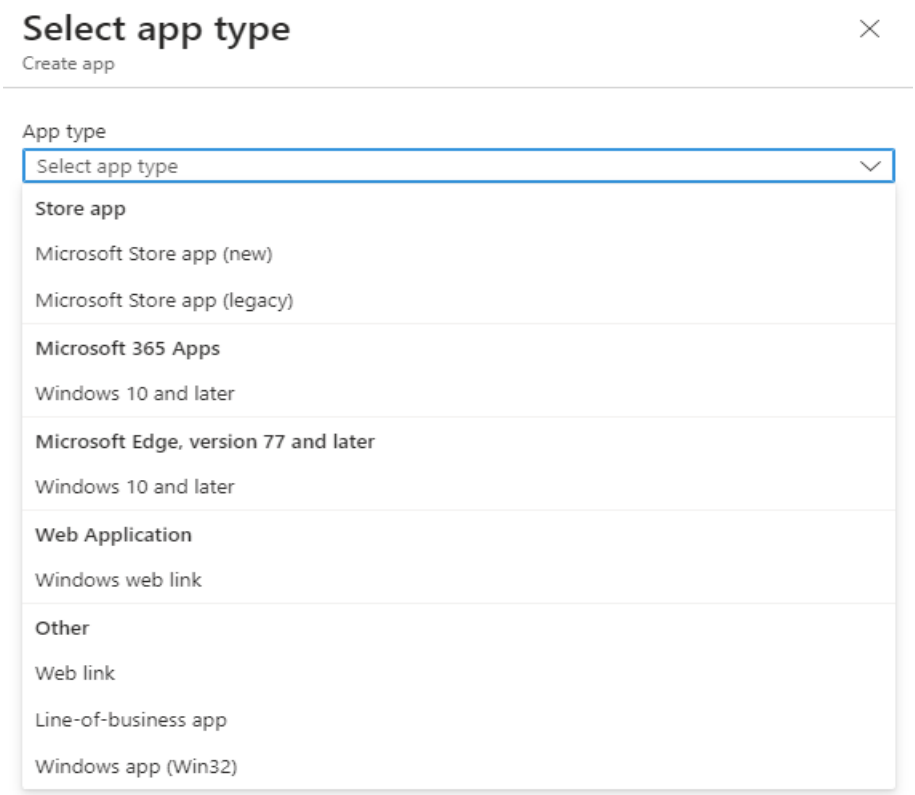
8.5 Windows 10/11 Application Management

Intune LAs can manage and push applications to Windows 10/11 and later devices via NHSmail Intune.

Intune LAs can add an app in Microsoft Intune by selecting **Apps > All apps > Add**.



Then Select app type pane is displayed and allows you to select the App type. The next sections will describe in detail how to deploy Apps in Intune.



Important Note

MSI installers are relatively straightforward to deploy via Intune with transforms and options preserved in the deployment package.

Compound installers that reference external packages and require a script wrapper may require transforms, embedded logic, or further scripting to deploy. More info via Win32 app management in Microsoft Intune

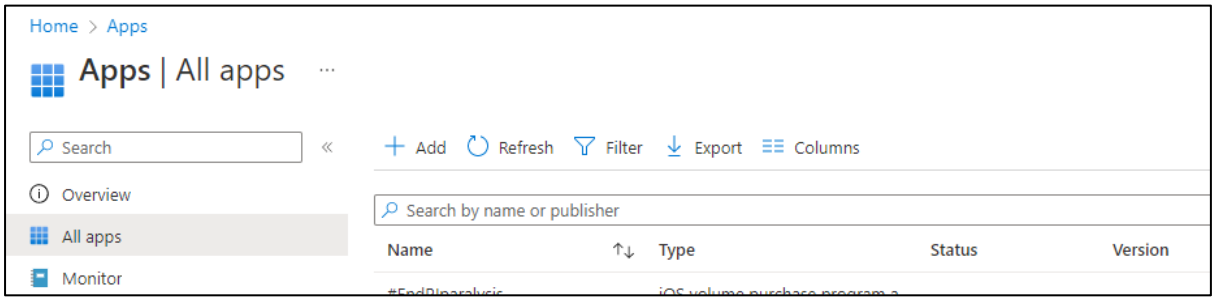
8.5.1 Microsoft Store Repository

In early 2023 the legacy Microsoft Store for Business was retired and replaced with the “New” Microsoft Store.

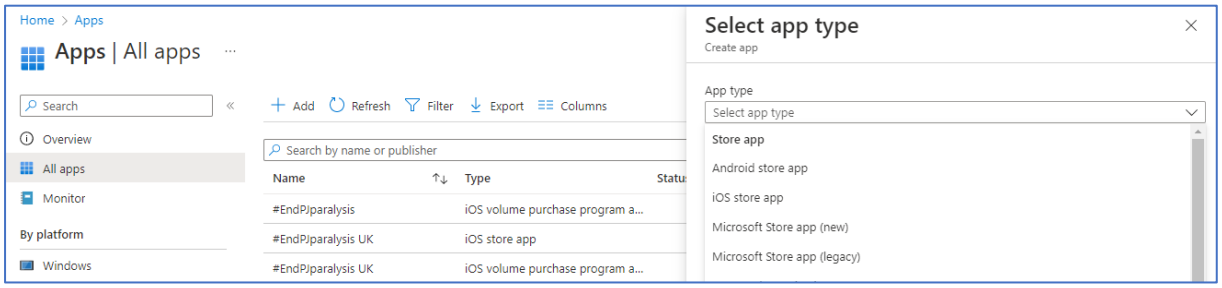
The following steps are used to create and deploy apps from Microsoft Store Repository.

8.5.1.1 Step 1: Create an app from the New Microsoft Store

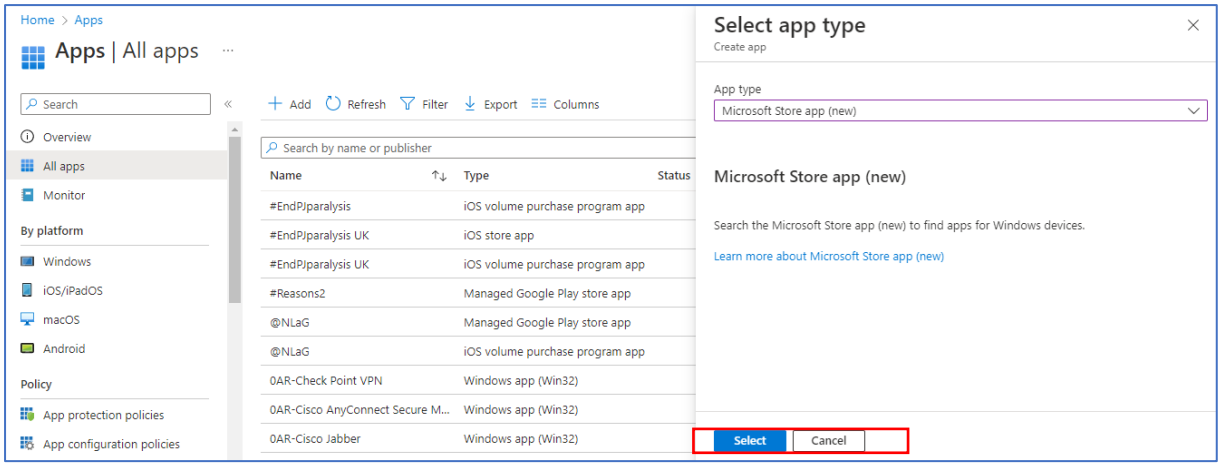
1. In the admin portal, navigate to the Apps section and click All apps.



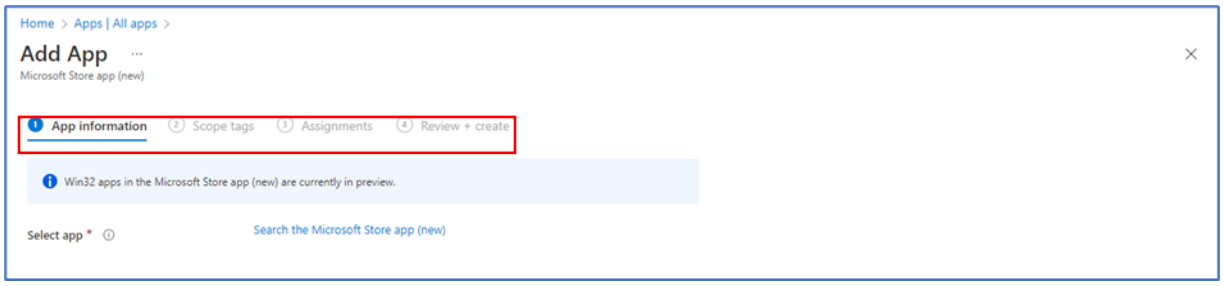
2. In the All-apps pane, click Add to add an app and select **Microsoft Store App (new)** type the App type.



3. Choose Select at the bottom of the page to create an app from the Microsoft Store repository.

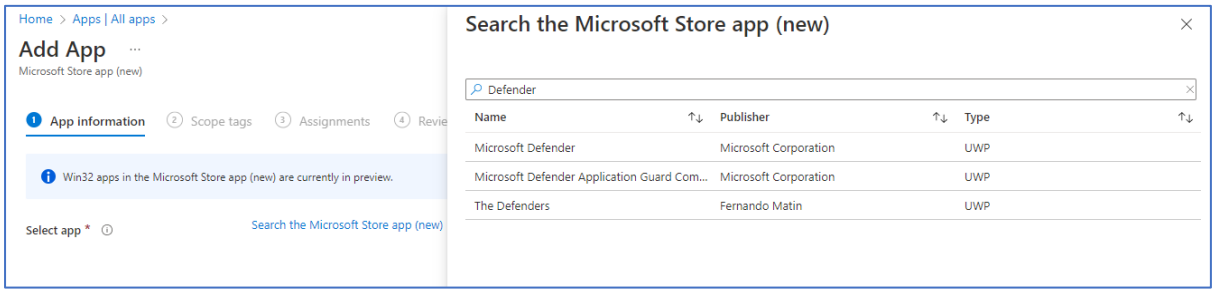


4. The app creation experience will have four steps: **App information**, **Scope tags, Assignments** and **Review + create**

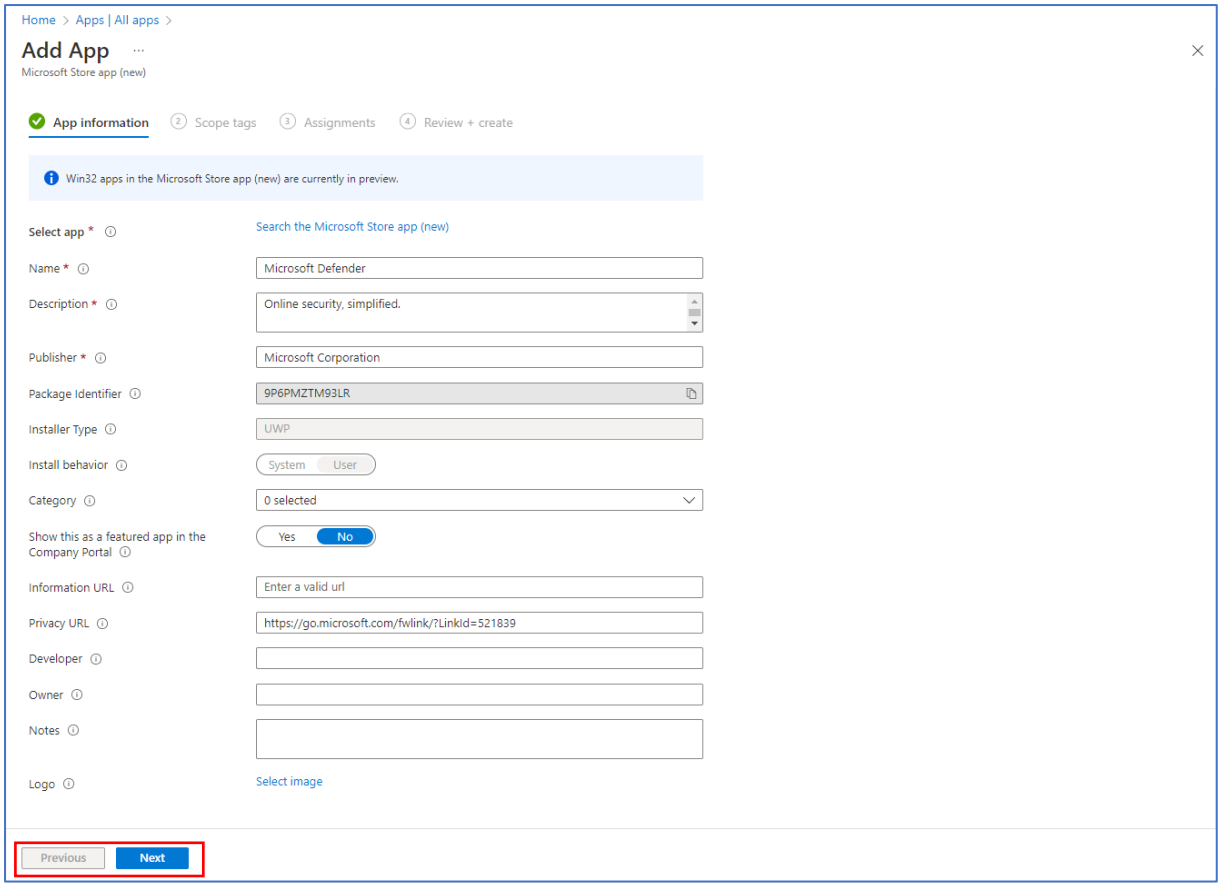


8.5.1.2 Step 2: Search the store repository

5. Select Search the Microsoft Store Repository to display the search panel, which will feature search bar and include the Name and Publisher columns



6. In the search bar, type the name of the app that you want to find. Then, choose the app you want to deploy from the returned list and click Select. The App Information will be presented with the selected app's metadata and specific fields will be pre-populated.



8.5.1.3 App information reference

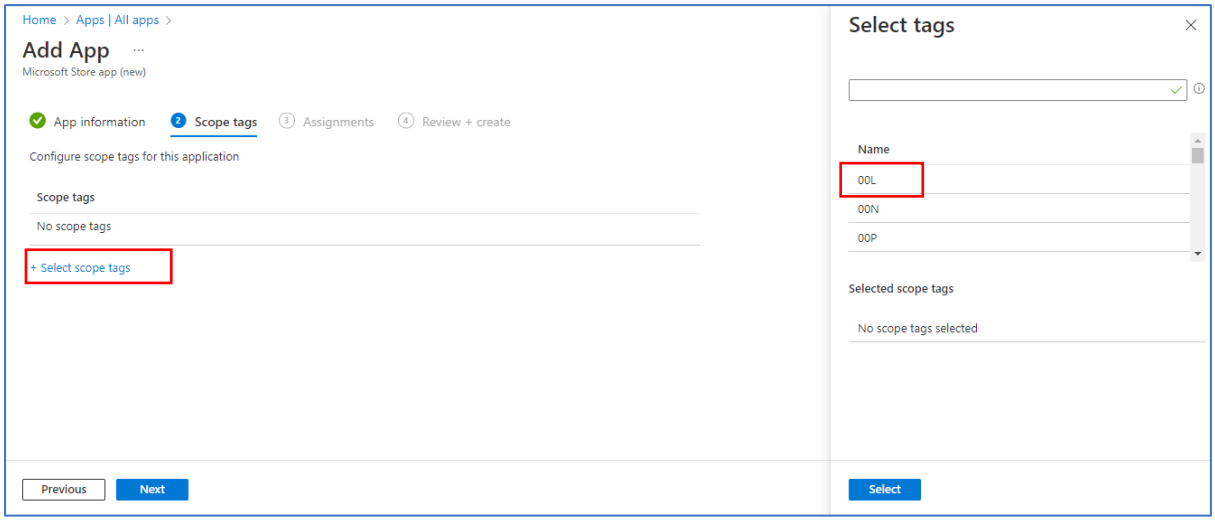
- **Name**: Enter the app's name as it appears in the Company Portal. Make sure all app names that you use are unique. If the same app name exists twice, only one of the apps appears in the company portal.
- **Description**: The app's description will be pre-populated from the Store's metadata, and you can edit the field. The description appears in the Company Portal.
- **Publisher:** The app's publisher will be pre-populated from the Store's metadata, and you can edit the field.
- **Package Identifier:** The app's unique ID in the Microsoft Store Repository.
- **Install behaviour:** The install behaviour of the app; for preview, the admin should only
- **Category:** Optionally, select one or more of the built-in app categories, or select a category you created. Categories make it easier for users to find the app by browsing through the Company Portal.
- **Show this as a featured app in the Company Portal**: Display the app prominently on the main page of the company portal when users browse for apps.
- **Information URL:** Optionally, enter the URL of a website that contains information about this app. The URL appears in the company portal.
- **Privacy URL**: Optionally, enter the URL of a website that contains privacy information for this app. The URL appears in the company portal.
- **Developer**: Optionally, enter the name of the app developer.
- **Owner**: Optionally, enter a name for the owner of this app. An example is the HR department.
- **Notes:** Enter any notes that you want to associate with this app. Optional

- **Logo:** Upload an icon that is associated with the app. This icon is displayed with the app when users browse the company portal.

7. Once the admin finishes populating the fields, select **Next**

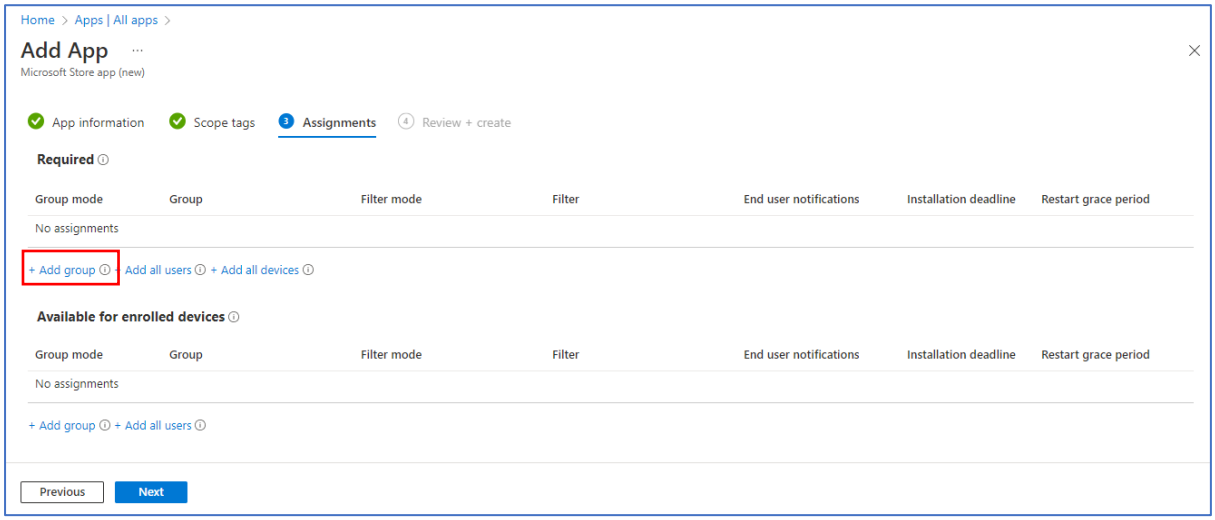
!	**Note:** Currently, apps can only be searched by app name. Win32 Apps are not supported in this experience and will not be searchable or deployable.

8.5.1.4 Step 3: Search and select your organisation's Scope tag

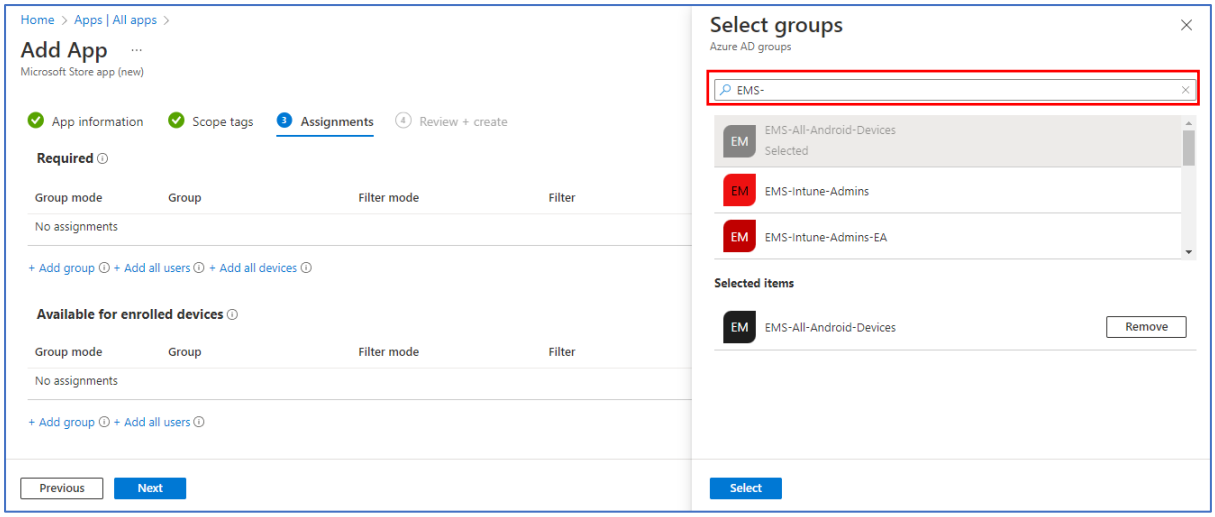


8.5.1.5 Step 4: Creating assignments

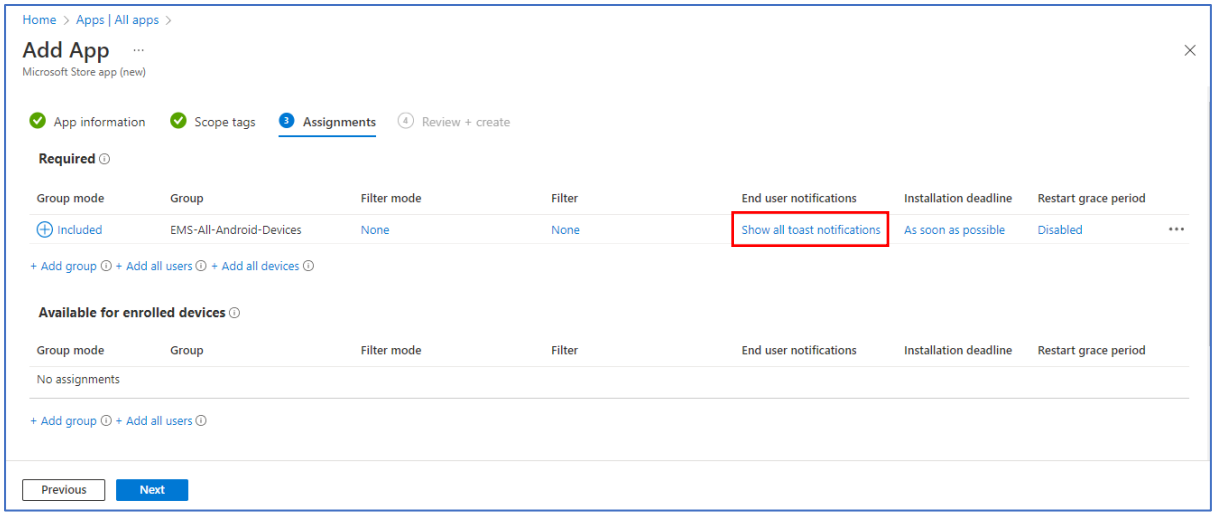
8. Select Add group and assign the groups that will use this app.



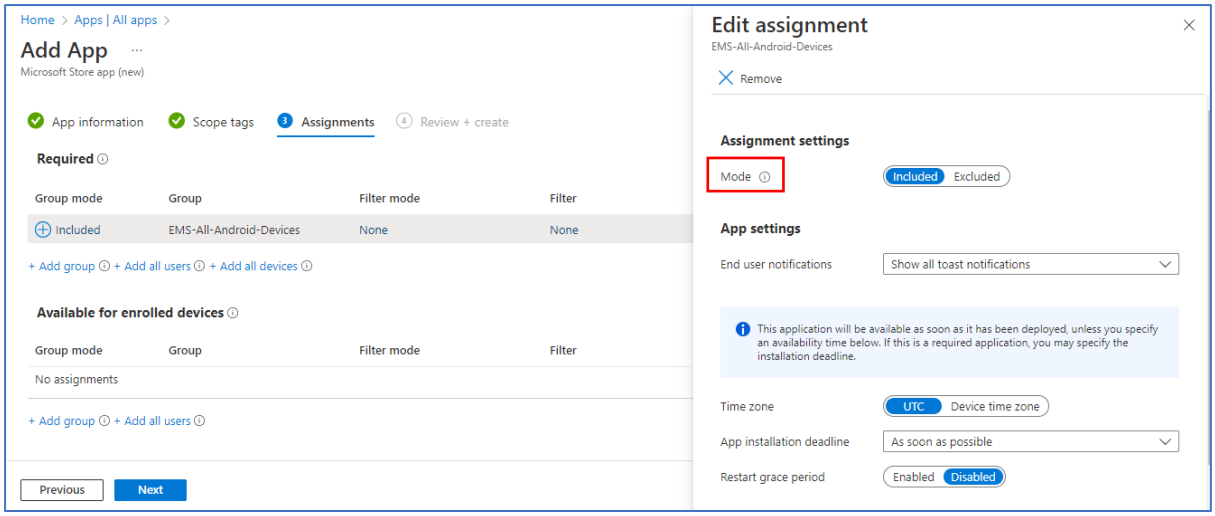
9. Select groups to assign based on users or devices on the Select group pane.



10. After you select your groups, you can also set End user notifications, Availability, and Installation deadline.



11. If you don't want this app assignment to affect groups of users, select Included under the MODE column. In the Edit assignment pane, change the mode value from Included to Excluded.

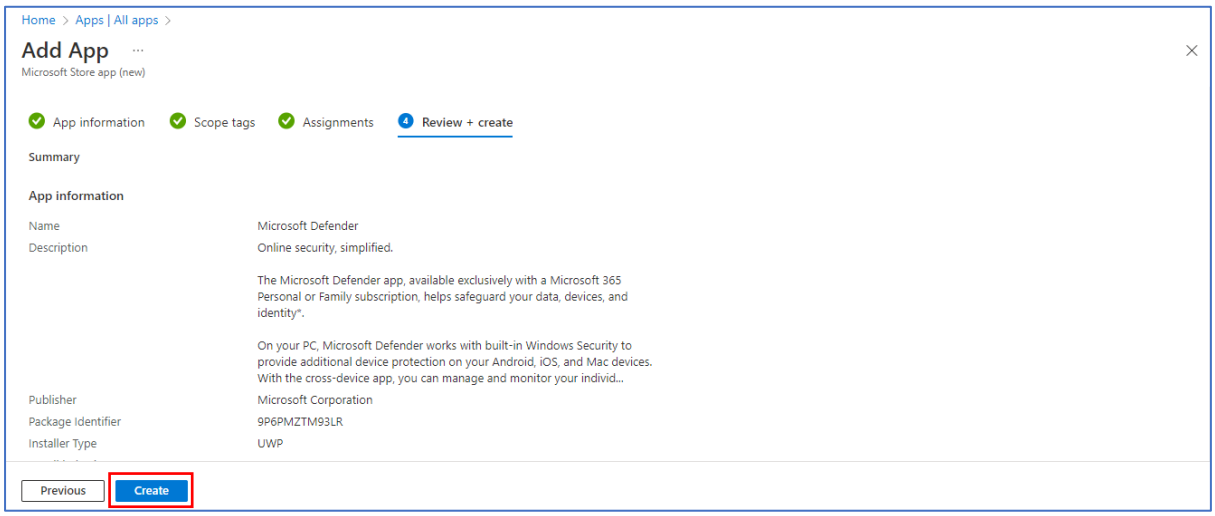


12. Select OK to close the Edit assignment pane.

8.5.1.6 Step 5: Review and create

13. Review the values and settings that you entered for the app. Verify that you configured the app information correctly.

14. Select Create to add the app to Intune



8.5.1.7 App Updates

Deployed apps will be auto-updated by the Store. Note that the group policy for store auto-update should not be disabled for this feature to work properly.

8.5.1.8 Microsoft Store Win32 apps

!	**Note:** Win32 apps that are in the Microsoft Store are currently in preview. Not all Win32 apps will be available or searchable. The Win32 apps that are in preview will be identifiable with Win32 and a banner. Third party vendors or publishers that add Win32 apps to the Microsoft Store are responsible for hosting their own content in their respective infrastructure. If your devices are behind a firewall, please reach out to application owner to understand and confirm network requirements.

8.5.1.9 Intune management of Microsoft Store Win32 apps

When a Microsoft Store Win32 app is published to a device as **Required**, but it is already installed (either manually or via the Microsoft Store for Business), Intune will take over the management of the application.

For available Microsoft Store Win32 apps, as well as UWP apps, the end user must click install in the Company Portal before Intune takes over the management of the application. Intune will not attempt to re-install the app.

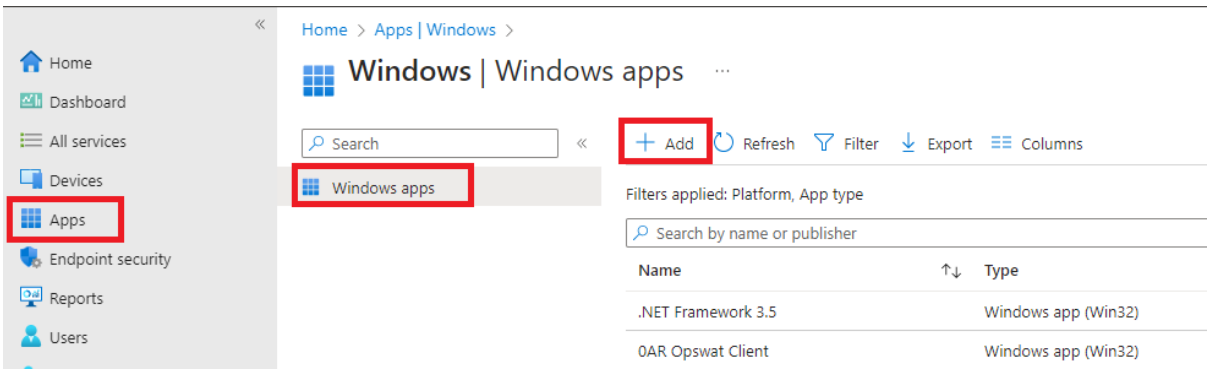
The Microsoft Store supports Win32 app types including **.exe** and **.msi** installers. These apps have external content sourcing hosted by the app publisher. Based on their installer definition in the store, each Win32 app supports either **User** or **System** context installation. For related information, see Traditional desktop apps in the Microsoft Store on Windows.

8.5.2 Windows Line of Business (LOB) Apps

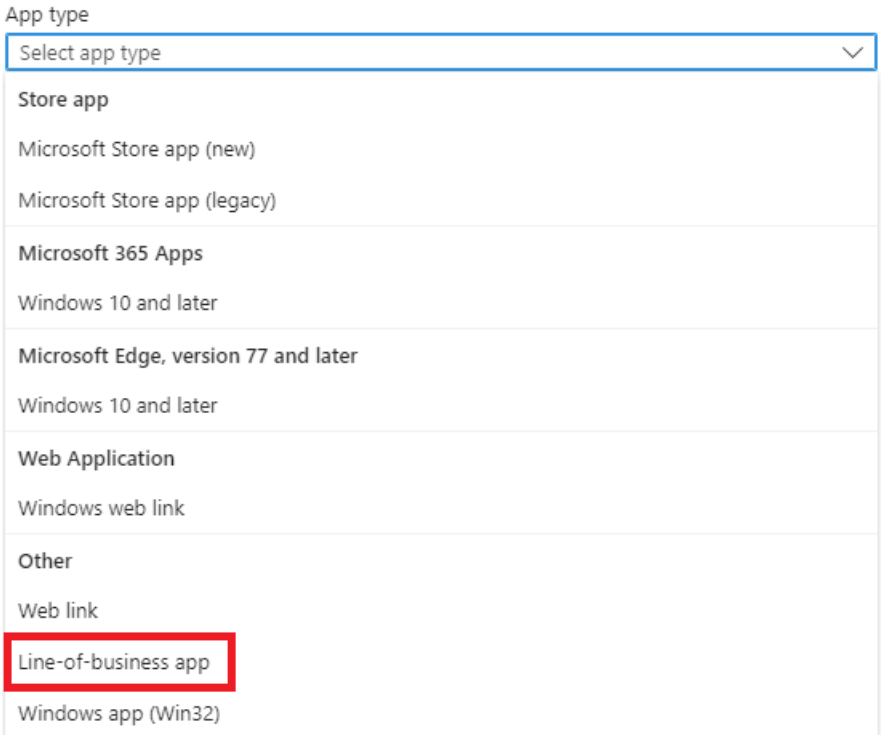
A line-of-business app is added from a traditional app installation file. The following steps provide guidance to help you add a Windows LOB app to Microsoft Intune.

Please see the steps to deploy LOB apps below:

1. Sign into the Microsoft Intune admin center.
2. Select Apps > Windows under “By Platform” category > Add.



3. In the Select app type pane, under the “Other” app types, select Line-of-business app.

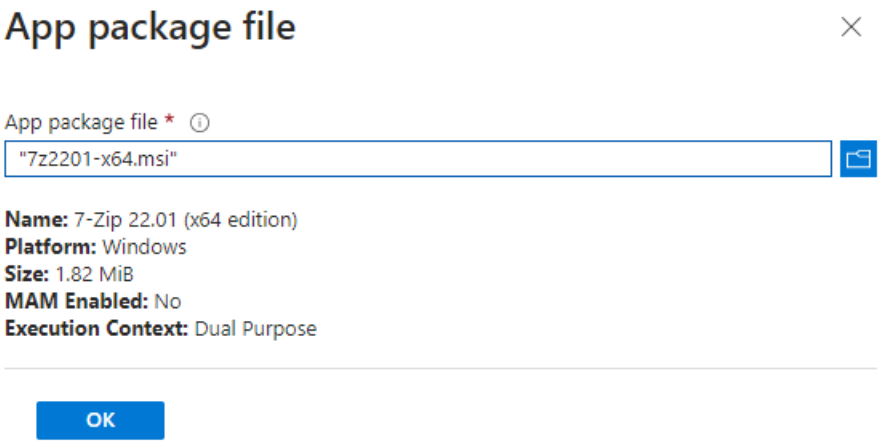


4. Click Select.
5. Click on Select app package file
6. In the App package file pane, select the browse button. Then, select a Windows installation file with the extension .msi, .appx, or .appxbundle.

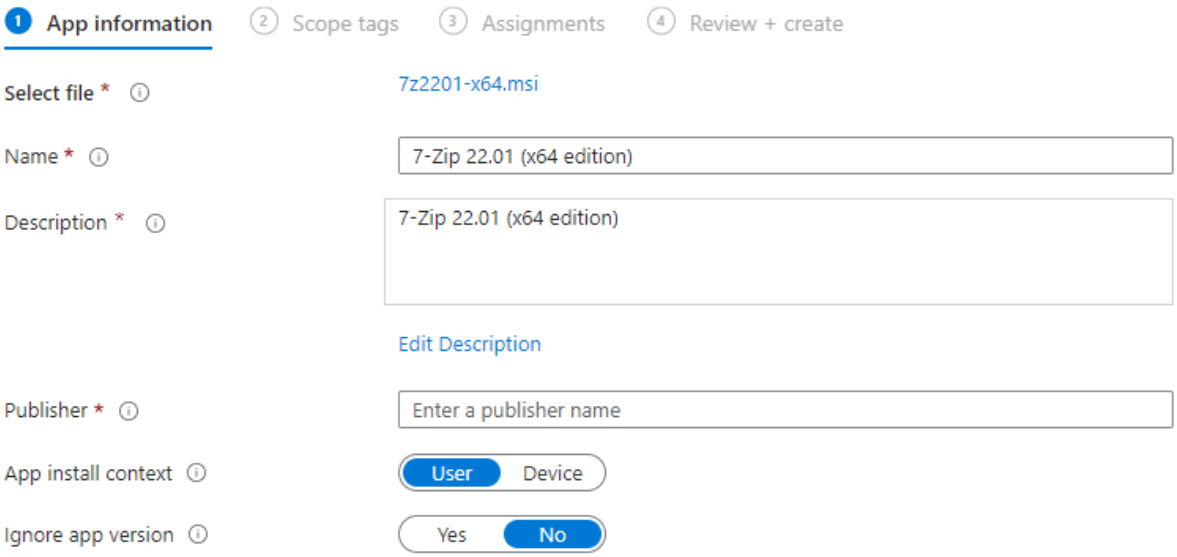
Recommendation / Recommended Use

Please refer to MSIX App Distribution Documentation for more detailed information.

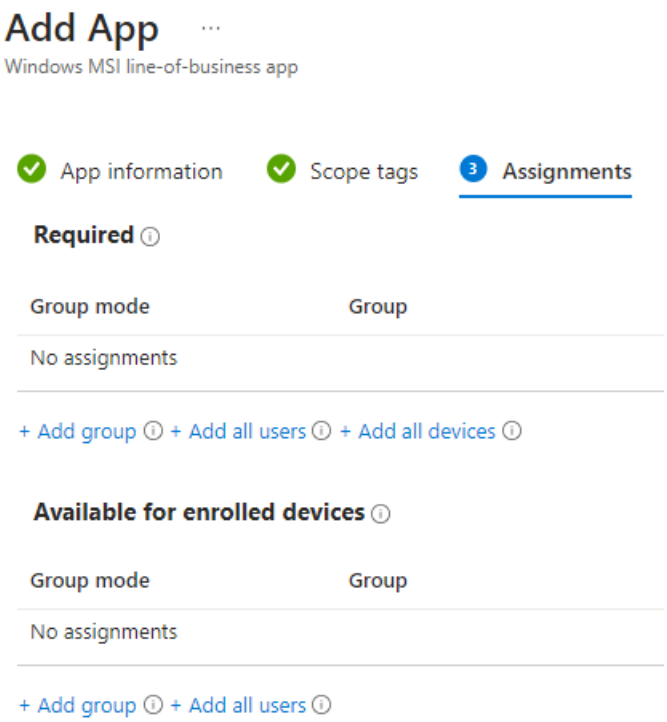
7. Select OK on the App package file pane to add the app



8. Set App information. Depending on the app, some values might be automatically filled in. More details be can here.



9. Click Next to display the Scope tags page. Your Organisation Scope Tag is automatically pre-populated.
10. Select the Required, Available for enrolled devices, or Uninstall group assignments for the app.



11. Click Next to display the Review + create page.

8.5.3 Win32 App Management

This app management capability supports both 32-bit and 64-bit operating system architecture for Windows applications.

!	**Important Note** When deploying Win32 apps, consider using the Intune Management Extension approach exclusively, particularly when having multiple-file Win32 app installer. If you mix the installation of Win32 apps and line-of-business apps during Autopilot enrolment, the app installation might fail. **The Intune management extension is installed automatically when a PowerShell script or Win32 app is assigned to the user or device.**

To use Win32 app management, the following criteria should be met:

1. Use Windows 10 version 1607 or later (Enterprise or Pro).
2. Devices must be enrolled in Intune and either:
    a. Azure AD joined
    b. Hybrid Azure AD joined
3. Windows application size must not be greater than 8 GB per app.

4. Prepare the app by using the Microsoft Win32 Content Prep Tool. The tool converts application installation files into the '.intunewin' format. For more information and steps, Prepare Win32 app content for upload.

Once the app has been prepared by using the Microsoft Win32 Content Prep Tool, the app can be added into Intune and tested for deployment.

8.5.3.1 Adding a Win32 App to Intune

The following steps help you add a Windows app to Intune:

1. Sign into the Microsoft Intune admin center.
2. Select Apps > All apps > Add.
3. On the Select app type pane, under the other app types, select Windows app (Win32).

!	**Important Note** Be sure to use the latest version of the Microsoft Win32 Content Prep Tool. If you don't use the latest version, you'll see a warning that says the app was packaged using an older version of the tool.

4. Click Select. The Add app steps appear.
5. On the Add app pane, click Select app package file.
6. On the App package file pane, select the browse button. Then, select a Windows installation file with the extension .intunewin. The app details appear.
7. When you're finished, select OK on the App package file pane.
8. On the App information page, add the details for your app. Depending on the app that you chose, some of the values on this page might be automatically filled in.
9. On the Program page, configure the app installation and removal commands for the app:
    a. Install command: Add the complete installation command line to install the app.
    b. For example, if your app's file name is MyApp123, add the following: msiexec /p "MyApp123.msp"
    c. If the application is ApplicationName.exe, the command would be the application name followed by the command arguments (switches) that the package supports. For example: ApplicationName.exe /quiet
    d. For the specific arguments that the application package supports, contact your application vendor.

Important Note

Admins must be careful when they use the command tools. Unexpected or harmful commands might be passed via the Install command and Uninstall command fields.

e. Uninstall command: Add the complete command line to uninstall the app based on the app's GUID. For example: msiexec /x "{12345A67-89B0-1234-5678-000001000000}"

f. Install behaviour: Set the install behaviour to either System or User.

Important Note

- You can configure a Win32 app to be installed in **User** or **System** context. **User** context refers to only a particular user. System context refers to all users of a Windows 10 device.
- Users are not required to be logged in on the device to install Win32 apps.
- The Win32 app installation and uninstallation will happen under admin privilege (by default) when the app is set to install in user context and the user on the device has admin privileges.

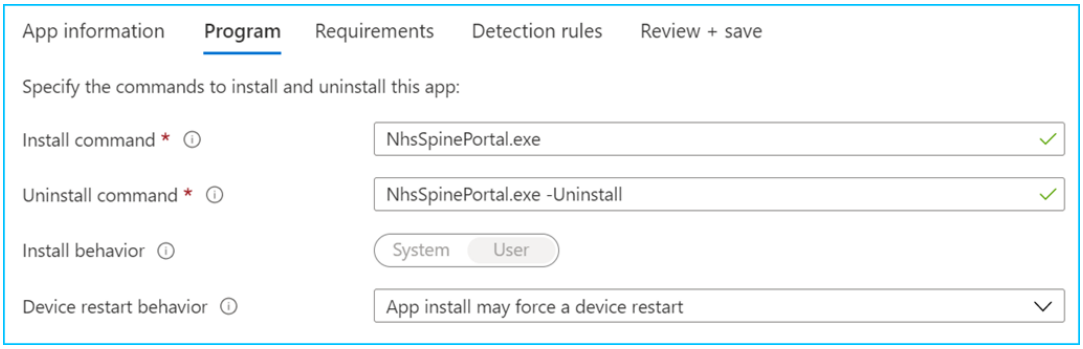
g. Device restart behaviour: Select one of the following options:

i. Determine behaviour based on return codes: Choose this option to restart the device based on the return codes.

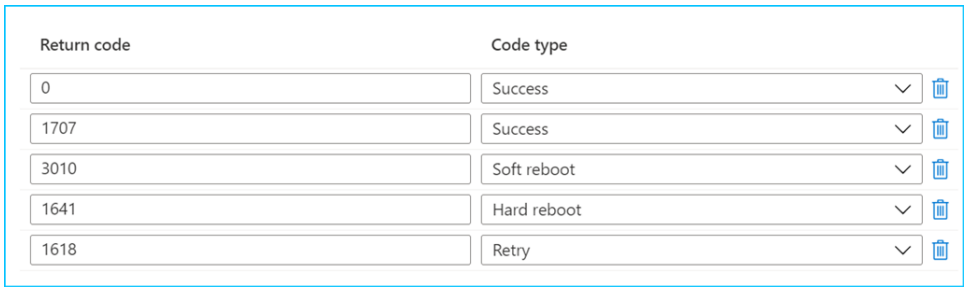
ii. No specific action: Choose this option to suppress device restarts during the app installation of MSI-based apps.

iii. App install may force a device restart: Choose this option to allow the app installation to finish without suppressing restarts.

iv. Intune will force a mandatory device restart: Choose this option to always restart the device after a successful app installation.



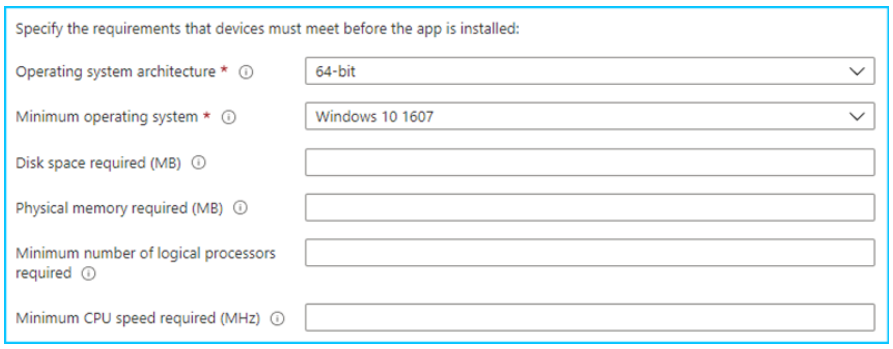
h. **Specify return codes to indicate post-installation behaviour**: Add the return codes that are used to specify either app installation retry behaviour or post-installation behaviour. Return code entries are added by default during app creation. However, you can add more return codes or change existing return codes.



i. Select **Next** to display the **Requirements** page.

10. On the Requirements page, specify the requirements that devices must meet before the app is installed:

- Operating system architecture: Choose the architectures needed to install the app.
- Minimum operating system: Select the minimum operating system needed to install the app.
- Disk space required (MB): Optionally, add the free disk space needed on the system drive to install the app.
- Physical memory required (MB): Optionally, add the physical memory (RAM) required to install the app.
- Minimum number of logical processors required: Optionally, add the minimum number of logical processors required to install the app.
- Minimum CPU speed required (MHz): Optionally, add the minimum CPU speed required to install the app.



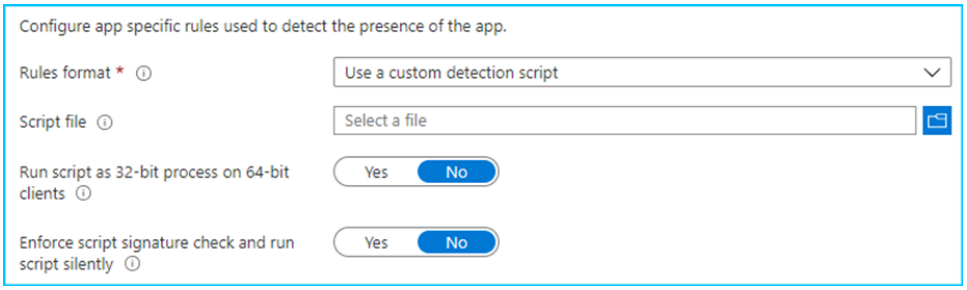
- Configure additional requirement rules: Please find more details on the rules here.

11. On the **Detection rules** pane, configure the rules to detect the presence of the app

a. **Rules format**: Select how the presence of the app will be detected. You can choose to either manually configure the detection rules or use a custom script to detect the presence of the app. There are 2 options:

   i. **Manually configure detection rules**

   ii. **Use a custom detection script**



For more details, please refer to the detection rules in the Microsoft Documentation.

12. Configuring Dependencies for the App. App dependencies are applications that must be installed before your Win32 app can be installed. You can add Win32 app dependencies only after your Win32 app has been added and uploaded to Intune. After your Win32 app has been added, you'll see the **Dependencies** option on the pane for your Win32 app. Please refer to Dependencies in the Microsoft Documentation.

13. Configuring Supersedence for the App. When you supersede an application, you can specify which app will be updated or replaced. To add apps that the current app will supersede:

    a. In the **Supersedence** step, click **Add** to choose apps that should be superseded.

!	**Important Note** There can be a maximum of 10 nodes in a supersedence relationship in Intune.

    b. Find and click the apps to apply the supersedence relationship in the **Add Apps** pane. Click **Select** to add the apps to your supersedence list.

    c. In the list of superseded apps, modify the **Uninstall previous version** option for each selected app to specify whether an uninstall command will be sent by Intune to each selected app.

    d. Once this step is finalized, click **Next**.

    For additional information see Add Win32 app supersedence.

14. Enter the group assignment for the app.

> **Important Note**
>
> For the scenario when a Win32 app is deployed and assigned based on user targeting, if the Win32 app requires device admin privileges or any other permissions that the standard user of the device does not have, the app will fail to install.

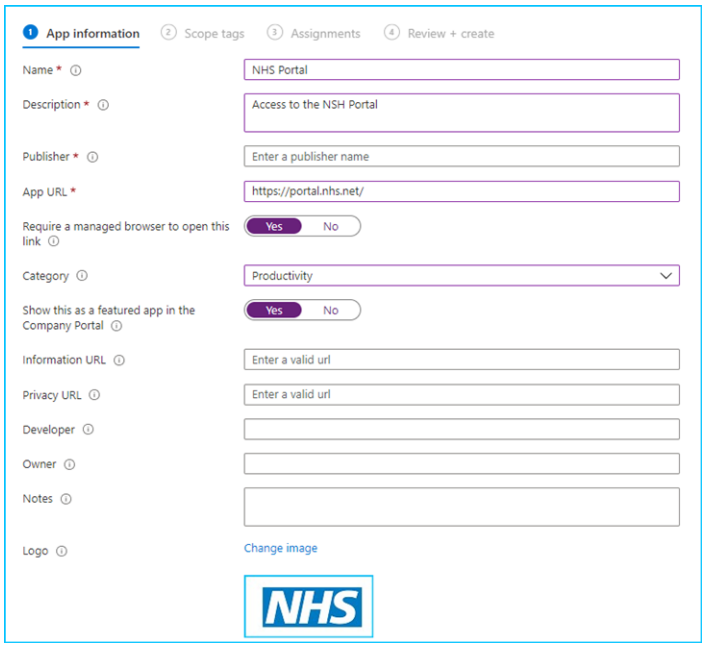
15. Review and Create

8.5.4 Web Links Apps

Intune supports Web Apps where a URL is published to provide access via a Browser. Before managing and assigning the App to the users, Intune LAs must add the app to Intune. A shortcut to the web app is place on the start menu.

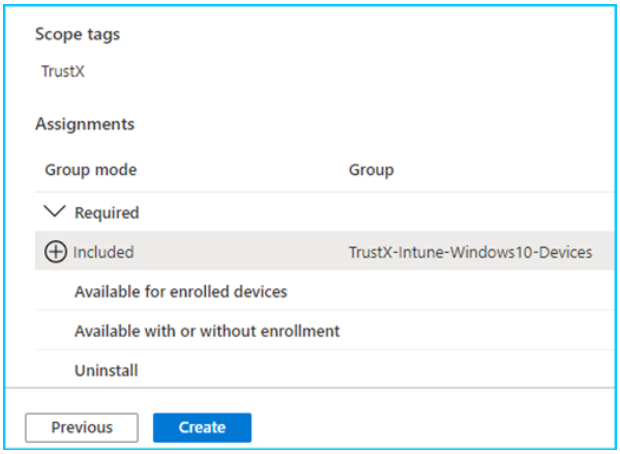
To add a web app to Intune, follow the steps below:

1. Sign into the Microsoft Intune admin center.
2. Select **Apps > All apps > Add**.
3. In the **Select app type** pane, under the available **other** types, select **Web link**.
4. Click **Select**. The **Add app** steps are displayed.
5. On the **App information** page, add the relevant information as example below:



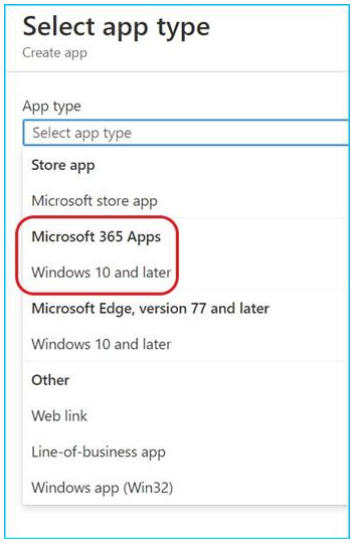
> **Important Note**
>
> Changing the name of the App from Intune after being deployed and installed will caused the app no to be target using commands.

6. Click **Next** to display the **Scope tags** page. Select Scope Tags
7. Click **Next** to display the **Assignments** page. Select the group assignments for the app.
8. Click Next to display the **Review + create** page.



8.5.5 Deploying Microsoft 365 Apps for Enterprise

Microsoft 365 apps for Windows 10/11 devices is one of options available from Intune. By selecting this option, Intune LAs can deploy Microsoft 365 apps to devices that run Windows 10/11. The available Microsoft 365 apps are displayed as a single entry in the list of apps in the Intune console within Azure.

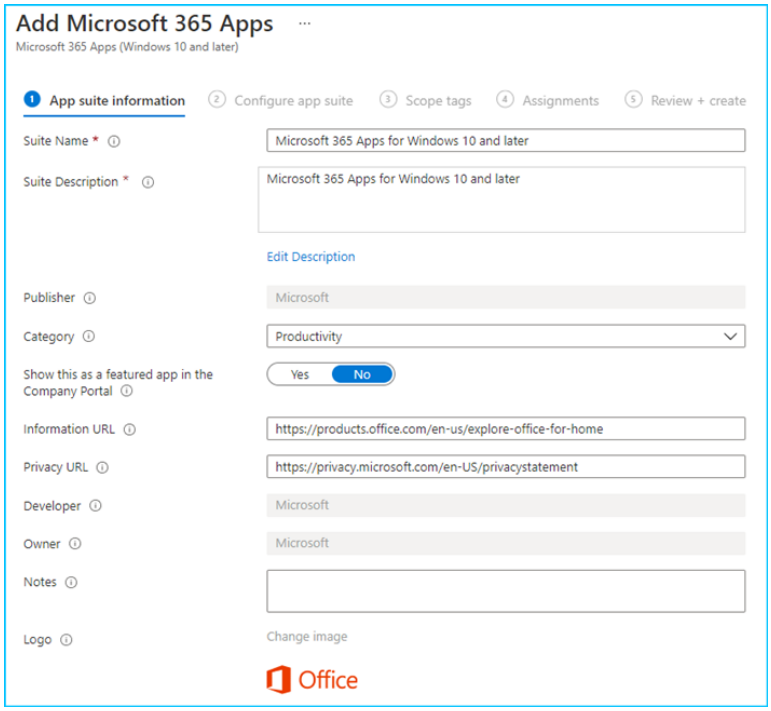


!	**Important Note** Microsoft Office 365 ProPlus has been renamed to Microsoft 365 Apps for enterprise.

> **Important Note**
>
> You must use Microsoft 365 Apps licenses to activate Microsoft 365 Apps deployed through Microsoft Intune. Microsoft 365 Apps for business edition is supported by Intune, however you must configure the app suite of the Microsoft 365 Apps for business edition using XML data. For more information, see Configure app suite using XML data.

8.5.5.1 Adding Microsoft 365 Apps

1. Sign in to the Microsoft Intune admin center.
2. Select **Apps > Windows > Add**.
3. Under **Microsoft 365 App**, select "**Windows 10 and later**"
4. Click **Select**. The **Add Microsoft 365 Apps** steps are displayed.



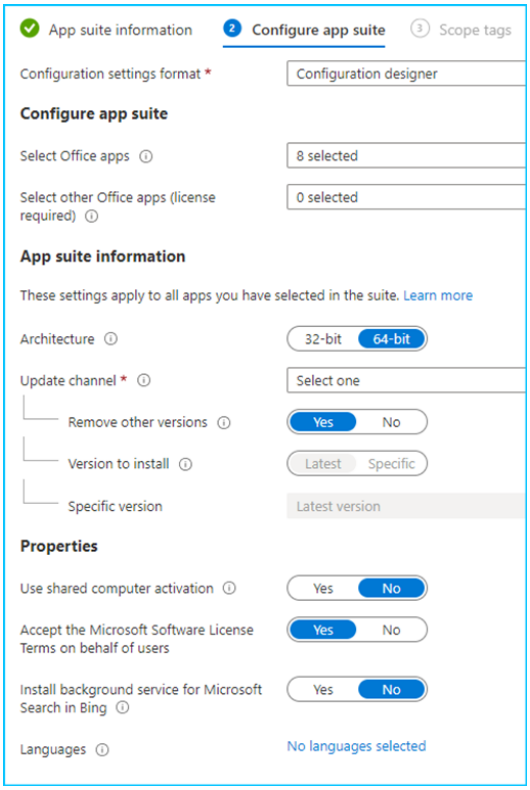
5. Configure App Suite information. There are two options for configuration settings:
    a. Configuration designer
    b. XML data

8.5.5.2 Using the Configuration Designer

When you choose Configuration designer the Add app pane will change to offer three additional settings areas:

a. Configure app suite
b. App suite information

c. Properties



The options presented on this page are the following:

- **Select Office apps**: Select the standard Office apps that you want to assign to devices by choosing the apps in the dropdown list.
- **Select other Office apps**: If you own licenses for these additional Office apps you can also assign them with Intune.
- **Architecture**: Choose whether you want to assign the 32-bit or 64-bit version of Microsoft 365 Apps.
- **Update Channel**: Choose how Office is updated on devices. Choose from:
    - Monthly
    - Monthly (Targeted)
    - Semi-Annual
    - Semi-Annual (Targeted)

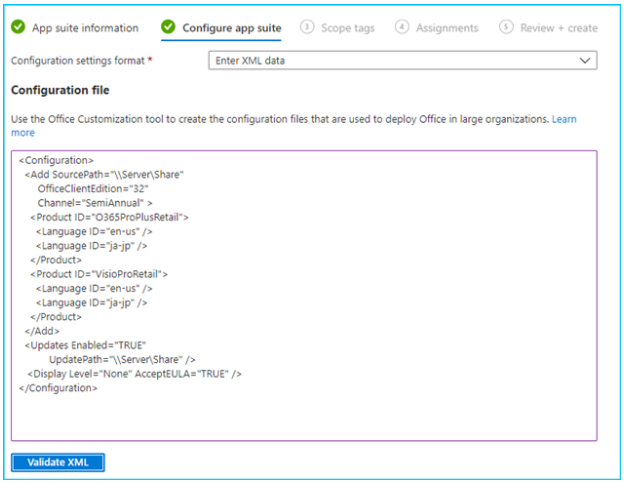
Please refer to Overview of update channels for Microsoft 365 Apps - Deploy Office | Microsoft Docs for more details.

- **Remove other versions**: Select Yes to remove other versions of Office (MSI) from user devices. The installation won't succeed if there are pre-existing .MSI apps on end-user devices.
- **Version to install**: Select the version of Office that should be installed.

- **Specific version**: If you have chosen **Specific** as the Version to install in the above setting, you can select to install a specific version of Office for the selected channel on end user devices.
- **Use shared computer activation**: Shared computer activation lets you deploy Microsoft 365 Apps to computers that are used by multiple users.
- **Accept the Microsoft Software License Terms on behalf of users**: Select this option if you don't require end users to accept the license agreement. Intune then automatically accepts the agreement.
- **Install background service for Microsoft Search in Bing**: Installs a background service that helps determine whether a Microsoft Search in Bing extension for Google Chrome is installed on the device.
- **Languages**: By default, Intune will install Office with the default language of the operating system. Choose any additional languages that you want to install.

8.5.5.3 Using XML Data

If you select the **Enter XML data** option under the setting format dropdown box on the Configure app suite page, you can configure the Office app suite using a custom configuration file.



Please refer to the Office deployment tool for detailed information.

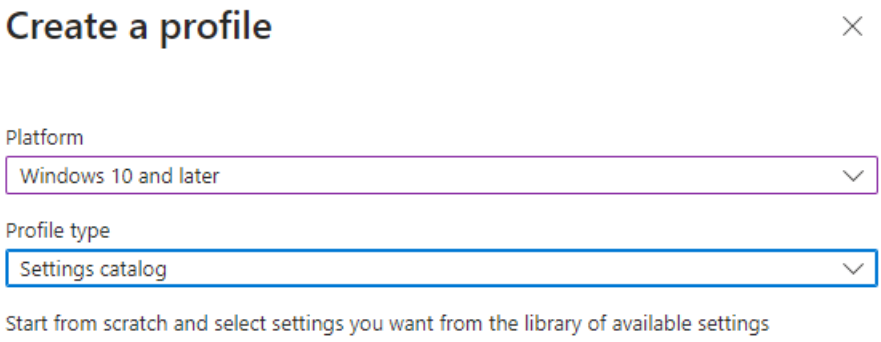
6. Click **Next** to get to **Scope Tags**. Select **Scope Tags** for the Office suite.
7. Click **Next** to go to **Assignment's page**. Select the **Required, Available for enrolled devices**, or **Uninstall** group assignments for the app suite.

!	**Important Note** The installation will be in silent mode if the assignment of Microsoft 365 is configured as required. If the assignment is configured as **Available**, the Office applications will appear in the Company Portal application so that end-users can trigger the installation manually.

8. Click **Next** to get the **Review + create** page. Select **Create** to add the app in Intune.

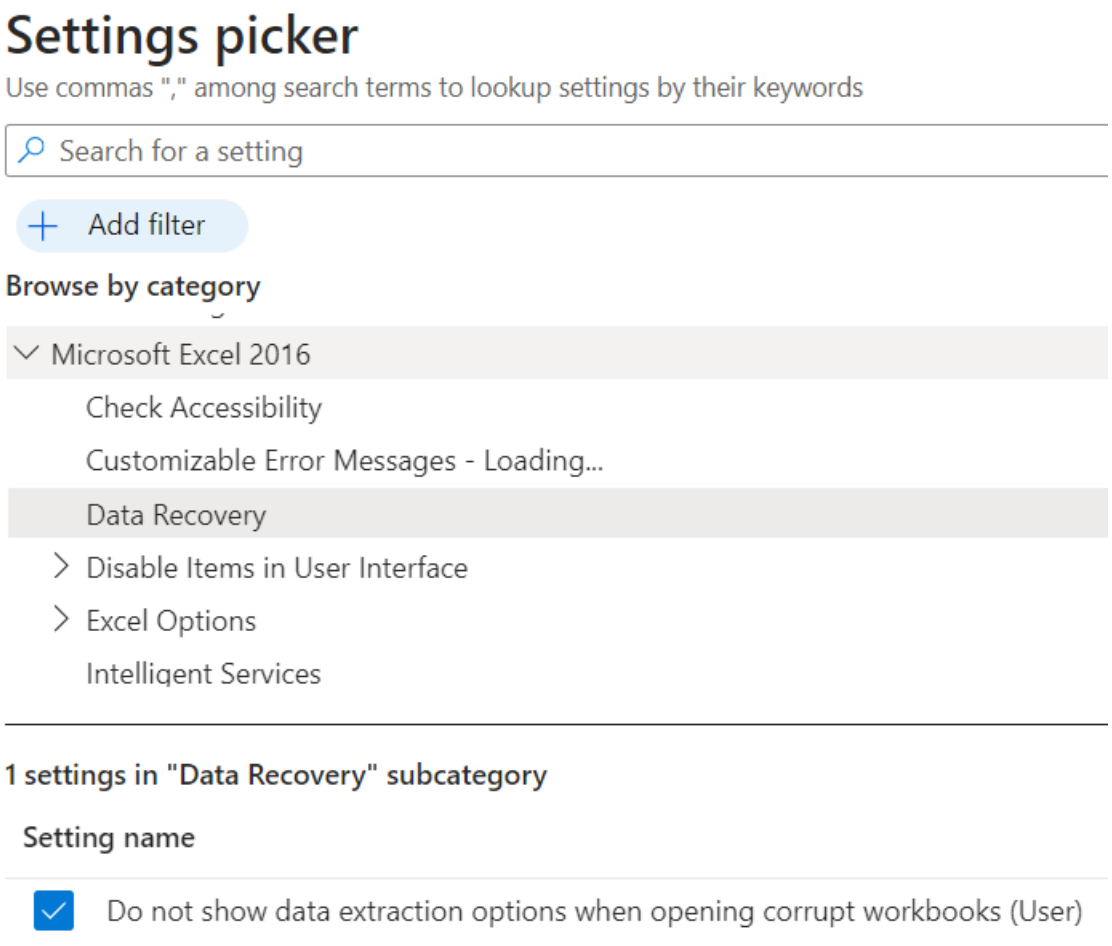
8.5.6 Policies for Office Apps

1. To create a policy for Office Apps LAs should direct to Configuration Profiles, Windows 10 and Later, Settings catalog.



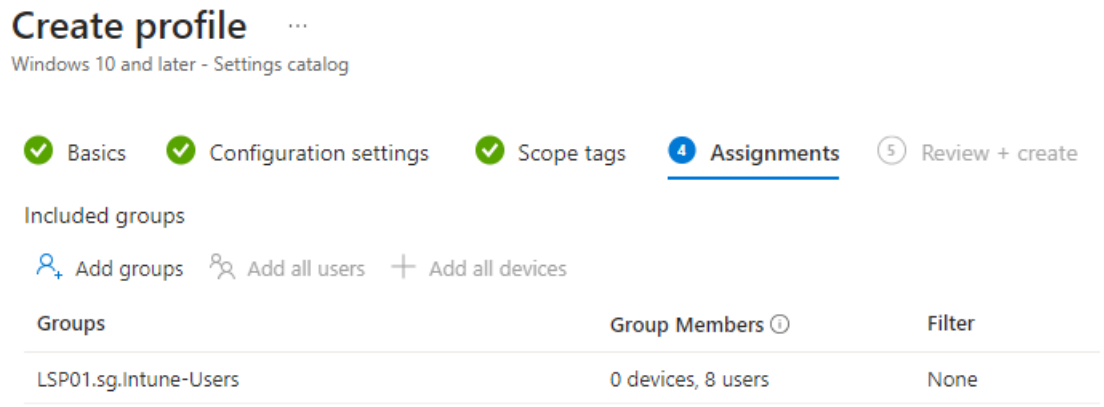
2. Follow the naming standard when creating the profile (<ODS>-Intune-<Platform>-<policy name>)

3. Select the desired Office app and chose the relevant setting.



4. Chose the correct scope tag.

5. Assign the relevant groups



6. Review and Save

> **Important Note**
>
> Intune LAs are not able to access Policies for Office Apps in the Apps section, due to an additional role assignment needed. Instead LAs will be able to access the same settings though the above steps in Configuration Profiles

8.6 Windows Feature Update Compatibility Risk Report

The Windows feature update compatibility risks report provides a summary view of the compatibility risks across your organisation associated with an upgrade or update to a chosen version of Windows.

8.6.1 Prerequisites

The NHSMail Intune service has carried out the required configuration to enable Windows diagnostic data processor configuration at a tenant level.

Licensing
The Windows feature update compatibility risks report requires users of enrolled devices to have one of the following licenses:

- Windows 10/11 Enterprise E3 or E5
- EMS E3 license

Devices
To be eligible for the Windows feature update compatibility risk reports, devices must:

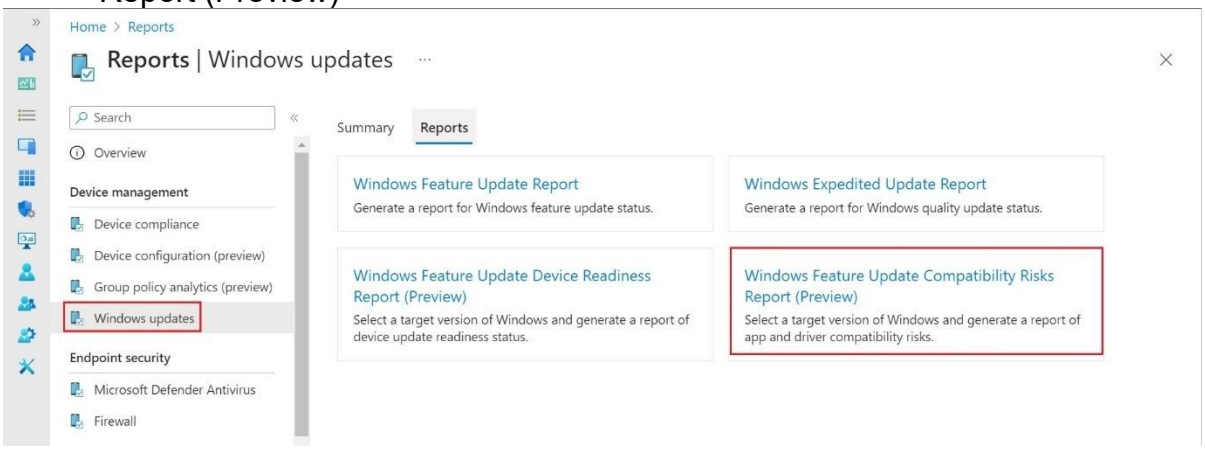
- Run a supported version of Windows 10 or later with the latest cumulative update.
- Be Azure AD joined or hybrid Azure AD joined.
- Managed by Intune (including co-managed devices)

- Have Windows diagnostic data enabled at the Required level or higher.

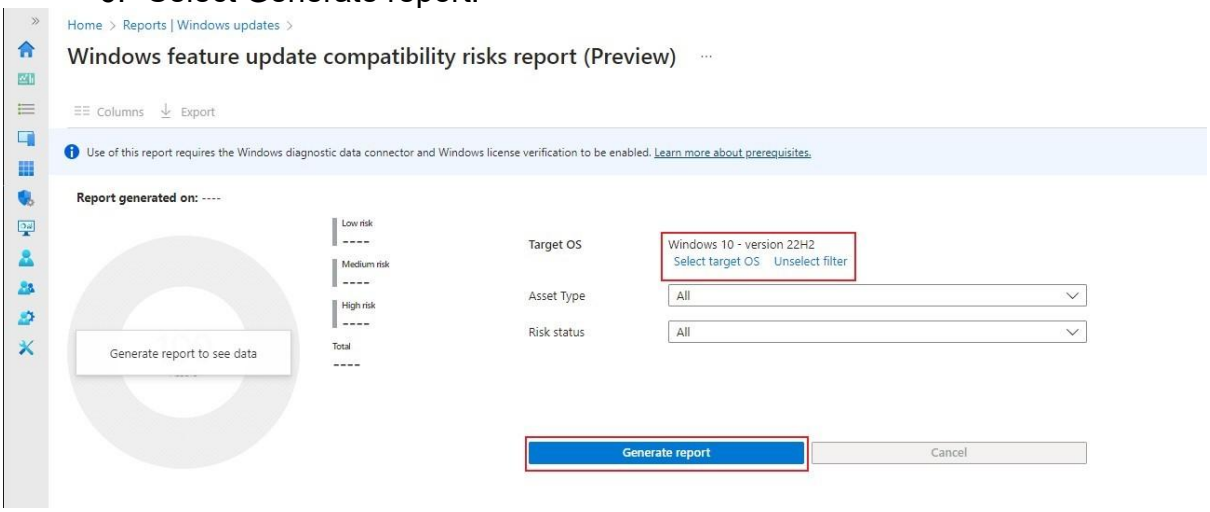
8.6.1.1 How to generate a compatibility risk report

To generate a report:

1. Login to the Intune portal https://intune.microsoft.com/
2. Navigate to Reports > Windows updates.
3. A summary with the Windows Updates Reports is observed.
4. Select the **Reports** tab > Windows Feature Update Compatibility Risks Report (Preview)

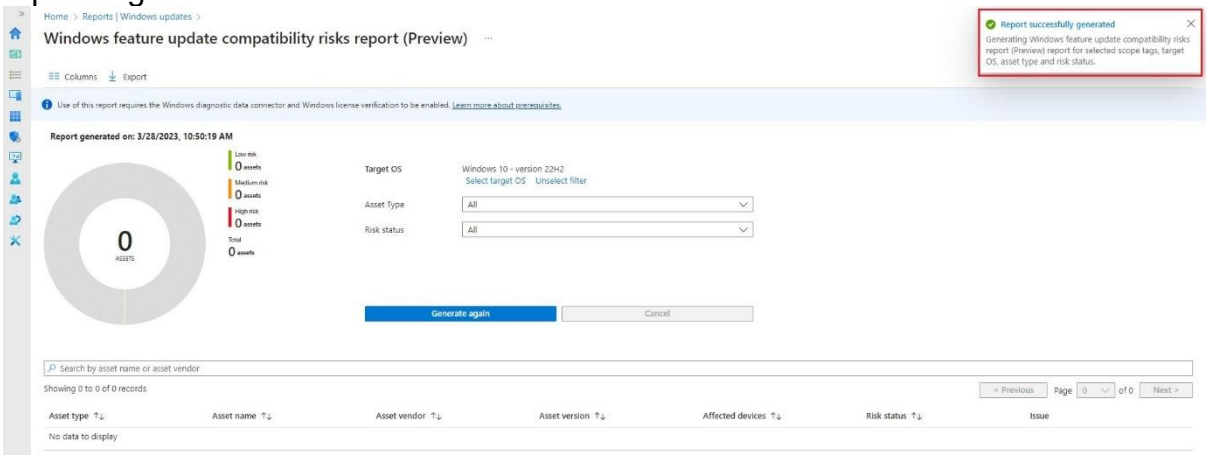


5. Enter the following information:
    a. **Target OS** e.g., Windows 10 – version 22H2 > select OK.
    b. **Asset Type:** this is optional. “All” is the default option.
    c. **Risk status:** this is optional. “All” is the default option.
6. Select Generate report.



!	**Note:** The insights in this report are specific to the target version of Windows you select when generating the report. To ensure the accuracy of insights, confirm that your selected OS version matches the version of Windows you intend to deploy.

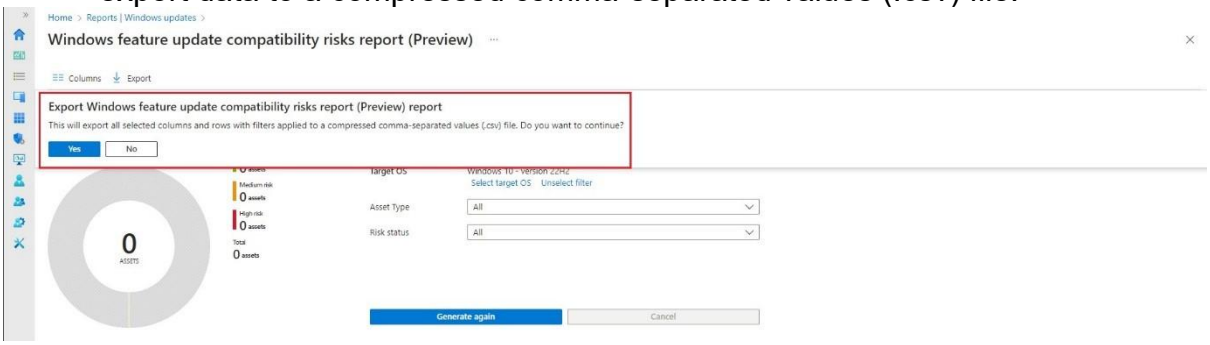
7. A notification will appear automatically in the top right-hand once the report is generated.



8.6.1.2 Exporting the Windows Update Compatibility Risks Intune Report

To export a report, please following the below steps:

1. From the Windows feature update compatibility risks report (Preview) > Click on **Export**.
2. A popup will appear confirming the export action. Click **Yes**. This will export data to a compressed comma-separated values (.csv) file.



3. Once the report is generated, it will appear in the download option of the browser used to access this Intune feature.

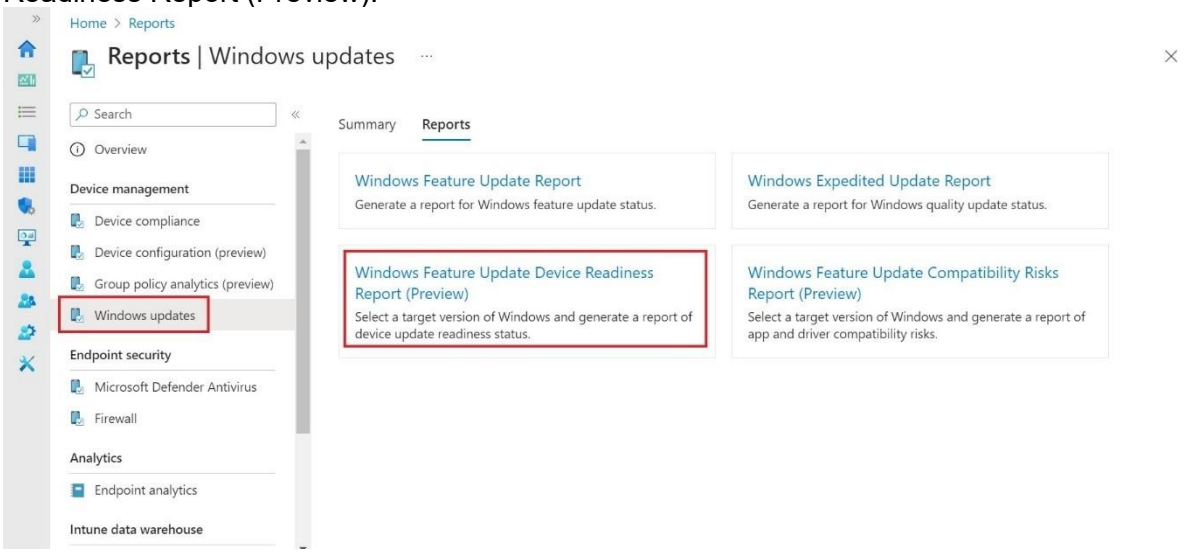
8.6.2 Windows Feature Readiness Reporting

The following steps are used to configure and generate the reports.

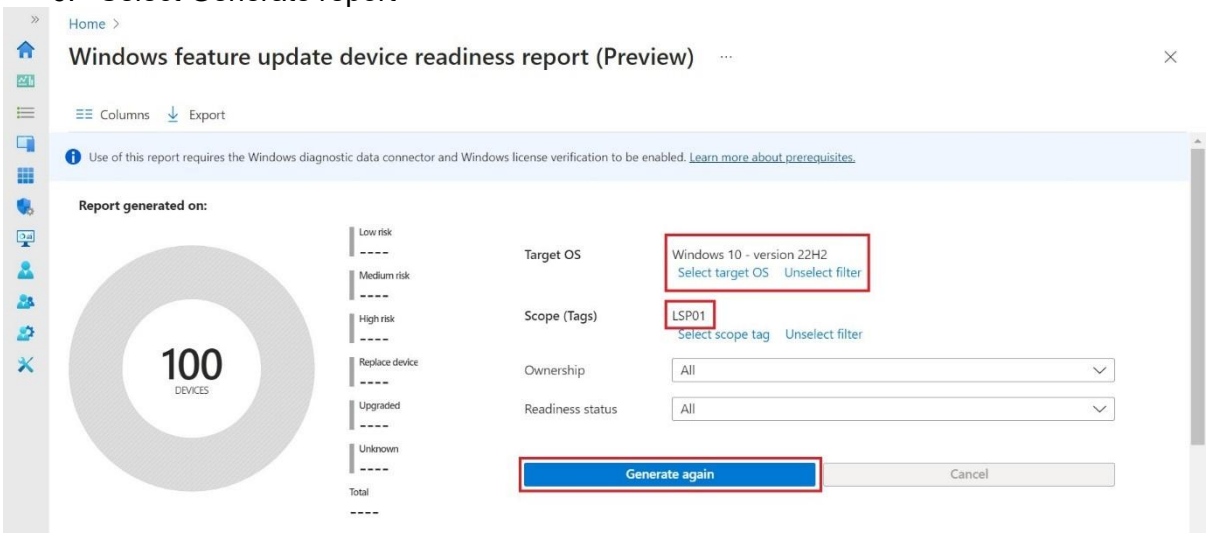
8.6.2.1 How to generate a readiness report

To view a report across windows devices for feature update device readiness:

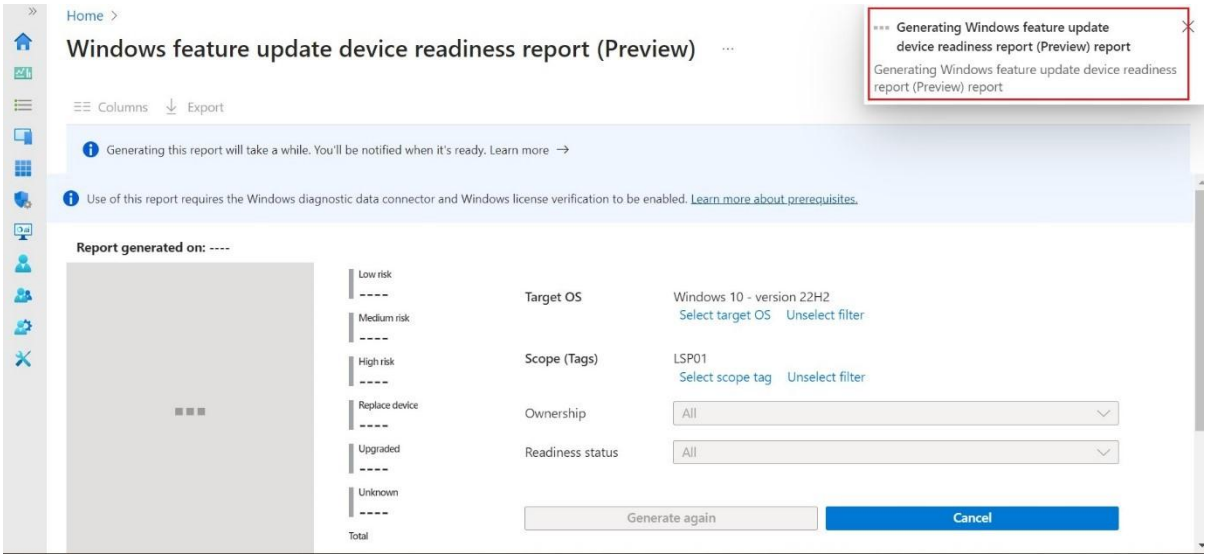
1. Login to the Intune portal https://intune.microsoft.com/
2. Navigate to Reports > Windows updates.
3. A summary with the Windows Updates Reports is observed.
4. To generate a Report, select Reports > Windows Feature Update Device Readiness Report (Preview).



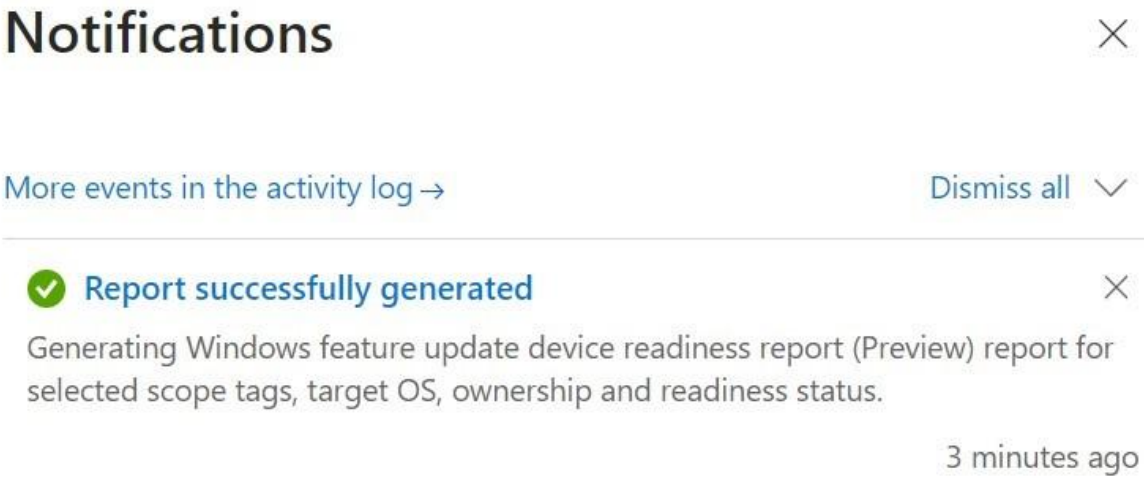
5. Enter the following information:
    a. **Target OS** e.g., Windows 10 – version 22H2 > select OK
    b. **Scope Tag:** select your Organization ODS code e.g., LSP01
    c. **Ownership:** this is optional. “All” is the default option
    d. **Readiness status:** this is optional. “All” is the default option
6. Select Generate report



7. A notification will appear automatically in the top right-hand corner with the message “Generating Windows feature update device readiness report”. This process can take several minutes.



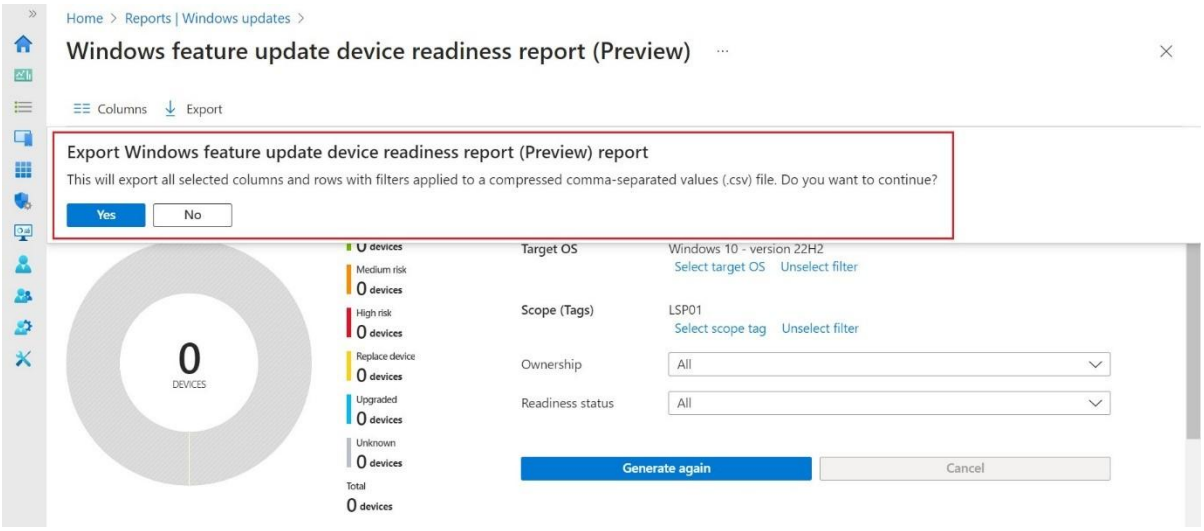
8. You'll be notified when report generation is complete



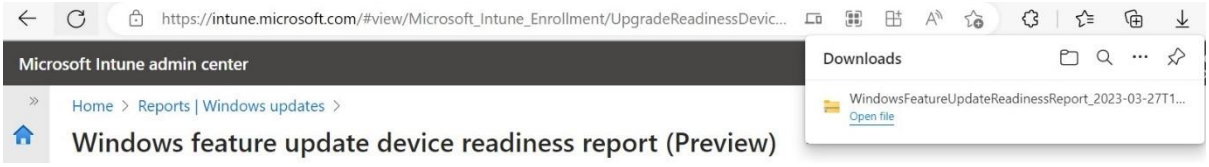
8.6.2.2 To export a report

Follow the below steps:

1. From the Windows feature update device readiness report (Preview) > Click on **Export**.
2. A popup will appear confirming the export action. Click **Yes**. This will export data to a compressed comma-separated values (.csv) file.



3. Once the report is generated, it will appear in the download option of the browser used to access this Intune feature.



8.7 Windows 10/11 Update Rings

Update rings can be used to upgrade your eligible Windows 10/11 devices in Intune. Intune LAs have the option to use a Centralised Channels to apply feature and quality update however they are unable to modify the settings.

The Centralised channels are the following:

- **Preview Channel**: Allow to gain visibility into feature updates early, before they are available to the General Availability channel. This is part of the Windows Insiders Program.
- **Early Adopter Channel**: this is intended to target a small set the devices to gather feedback and compatibility with Applications before rolling out to the whole organisation. This is part of the Windows General Availability Ring.
- **General Availability Channel**: This channel is intended to target a wide broad set of users/devices. This is part of the Windows General Availability Ring.

If the channels don't offer what Organisations want to use, they are able to create their own channels.

The table below specified the settings for each channel:

Update Ring Settings	Description	Preview Channel	Early Adopters Channel	General Channel
Update settings				
Microsoft product updates	Control whether to scan for updates from Microsoft Update	Allow	allow	allow
Windows drivers	Allow or block driver updates via Windows Update	Allow	allow	allow
Quality update deferral period (days)	Defer quality updates for the specified number of days	0	15	30
Feature update deferral period (days)	Specify the number of days for which Feature Updates are deferred. This period is in addition to any deferral period that is part of the service channel you select. The deferral period begins when Microsoft releases the update	0	30	90
Upgrade Windows 10 devices to Latest Windows 11 release	Set to upgrade eligible Windows 10 devices to latest Windows 11 release	No	No	No
Set feature update uninstall period (2 - 60 days)	Set feature update uninstall period	2	20	60
Enable pre-release builds	Devices that receive this setting as Enabled will move to the pre-release build you specify and will also reboot.	Enabled	Not configured	Not configured
Select pre-release channel	When enabled, specify one of the following prerelease builds: Windows Insider - Release Preview (default) Beta Channel Dev Chanel	Windows Insider - Release Version	Not configured	Not configured
User experience settings				

Update Ring Settings	Description	Preview Channel	Early Adopters Channel	General Channel
Automatic update behavior	Manage automatic update behavior to scan, download, and install updates			
Auto install at maintenance time	Default: Auto install at maintenance time. Updates download automatically and then install during Automatic Maintenance when the device isn't in use or running on battery power. When restart is required, users are prompted to restart for up to seven days, and then restart is forced.	Auto install	Auto install	Auto install
Active hours start		6:00 AM	6:00 AM	6:00 AM
Active hours end		7:00 PM	7:00 PM	7:00 PM
Notify download	Notify the user before downloading the update. Users choose to download and install updates. If the user takes no action, the update will not install until the deadline you have configured is reached.			
Auto install and restart at maintenance time	Updates download automatically and then install during Automatic Maintenance when the device isn't in use or running on battery power. When restart is required, the device restarts when not being used, which is the default for unmanaged devices.			
Active hours start				
Active hours end				

Update Ring Settings	Description	Preview Channel	Early Adopters Channel	General Channel
Auto install and restart at scheduled time	Specify an installation day and time. If unspecified, installation runs at 3 AM daily, followed by a 15-minute countdown to a restart. Logged on users can delay countdown and restart.			
Automatic behavior frequency	Use this setting to schedule when updates are installed, including the week, the day, and the time. Default: every week			
Scheduled install day	Default: Any day			
Scheduled install time	Default: 3 AM			
Auto install and reboot without end-user control	Updates download automatically and then install during Automatic Maintenance when the device isn't in use or running on battery power. When restart is required, the device restarts when not being used. This option sets the end-users control pane to read-only.			
Reset to default	Restore the original auto update settings on machines that run the Windows 10 October 2018 Update or later, and that run Windows 11.			
Restart checks	Set to skip all check before restart: Battery level = 40%, User presence, Display Needed, Presentation mode, Full screen mode, phone call state, game mode etc.	Allow	Allow	Allow
Option to pause	An option in Windows Update that, when enabled, lets device	Enable	Enable	Enable

Update Ring Settings	Description	Preview Channel	Early Adopters Channel	General Channel
Windows updates	users pause updates for a certain number of days.			
Option to check for Windows updates	A button in Windows Update that, when enabled, lets device users check the update service for updates.	Enable	Enable	Enable
Change notification update level	Specifies what Windows Update notifications users see Supported options: Not configured Use the default Windows Update notifications Turn off all notifications, excluding restart warnings Turn off all notifications, including restart warnings	Use the default	Use the default	Use the default
Use deadline settings	Allows user to use deadline settings	Not configured	Not configured	Not configured
When Allow, the following settings are available:				
Deadline for feature updates	Specifies the number of days a user has before feature updates are installed on their devices automatically (2-30)			
Deadline for quality updates	Specifies the number of days a user has before quality updates are installed on their devices automatically (2-30)			
Grace period	Specifies a minimum number of days after deadline until restarts occur automatically (0-7)			
Auto reboot before deadline	Specifies whether the device should auto reboot before deadline	Not configured	Not configured	Not configured

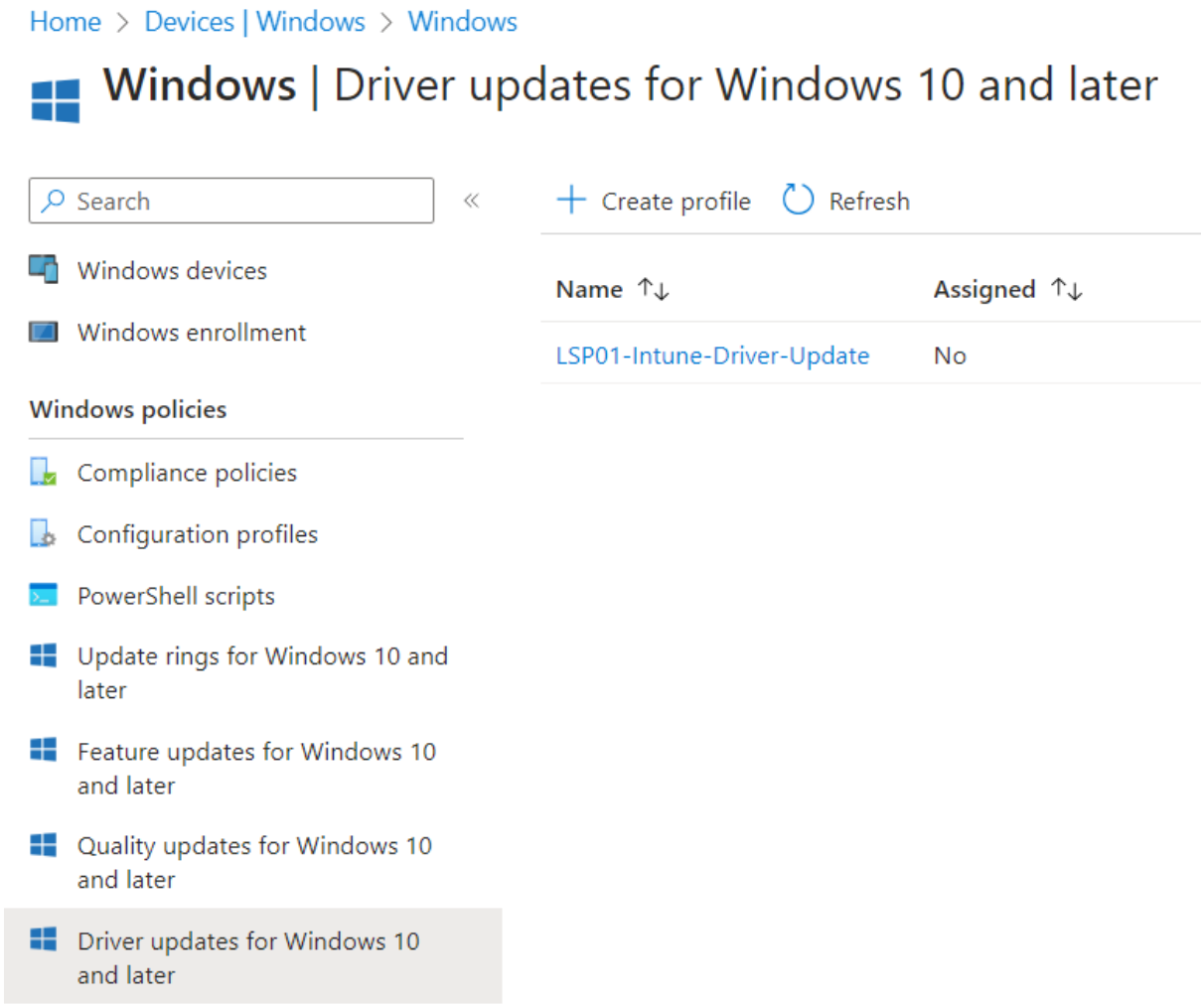
8.8 Driver Updates for Windows 10 and later

Driver updates allow you to manage driver and firmware updates for Windows devices. The functionality makes it easier to keep drivers on you Windows devices up to date in two ways.

- No longer need to do the manual work of downloading, repackaging and deploying drivers using generic tools
- Instead use the driver update management policies

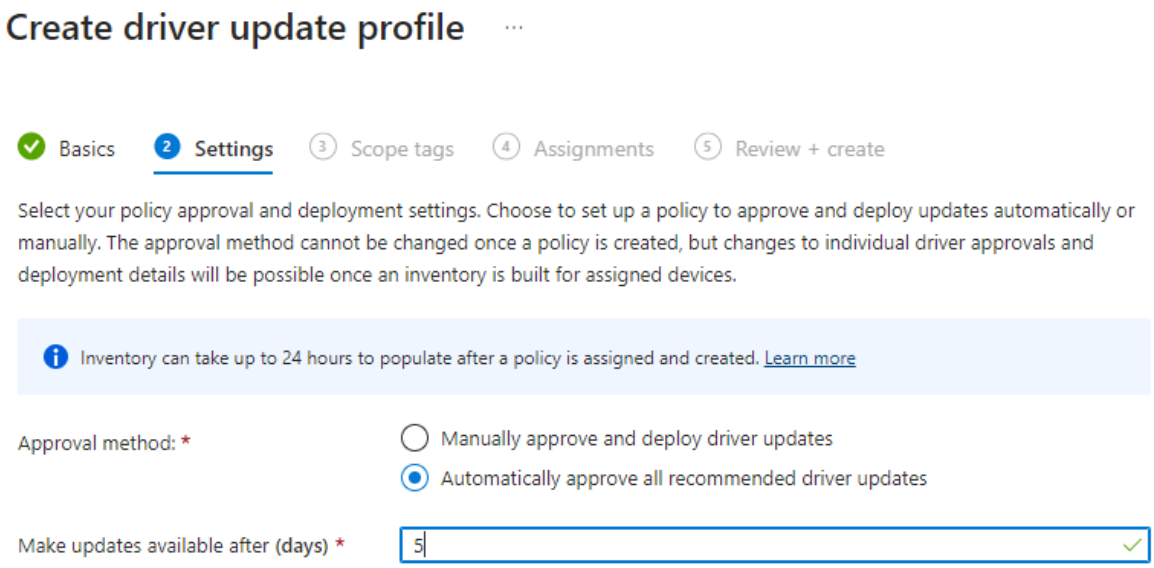
8.8.1 Create and manage drive update policies

1. Go to Devices > Windows > Driver Updates for Windows 10 and later > +Create Policy



2. Decide on a name, keeping in line with the naming convention of ODS-Intune-Driver-Updates <LSP01-Intune-Default-Driver-Update>
3. Choose between two options:

- Manually approve drivers and select the day to start offering the update when you approve them. With this option, no drivers are offered until manually approved.
- Automatically approve all recommended drivers and set how long after discovery to start offering them
    - With this option there is an additional setting to chose the number of days to make updates available after.

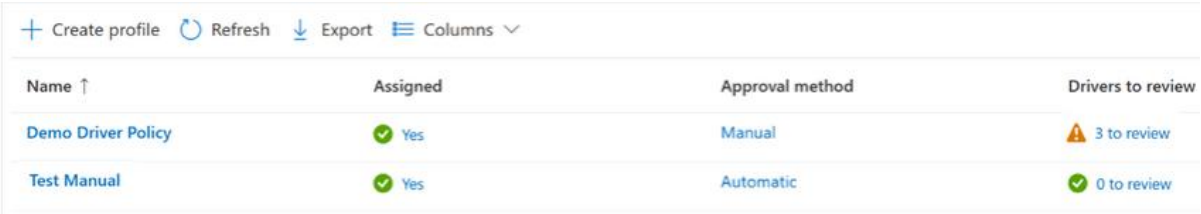


4. Chose your organisations scope tag
5. Select the groups to assign the policy to
6. Review and Create

8.8.2 Review available Drivers

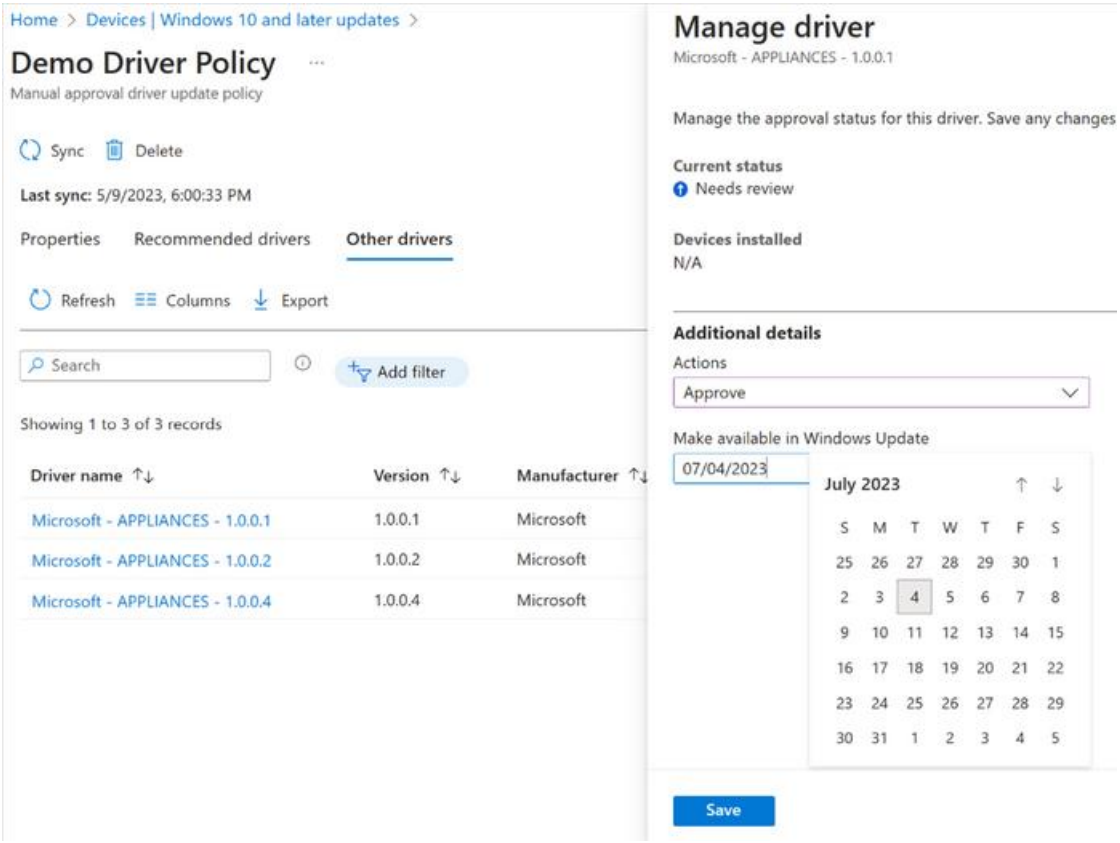
After the policies have been created, the device will need a suggested 24 hours to scan for updates. Once complete, you will be able to open the policy and review all available updates

In an automatic update scenario, drivers to review will remain at 0, since they are automatically approved, but for manual review approval method, this will require LAs to review and approve each update.



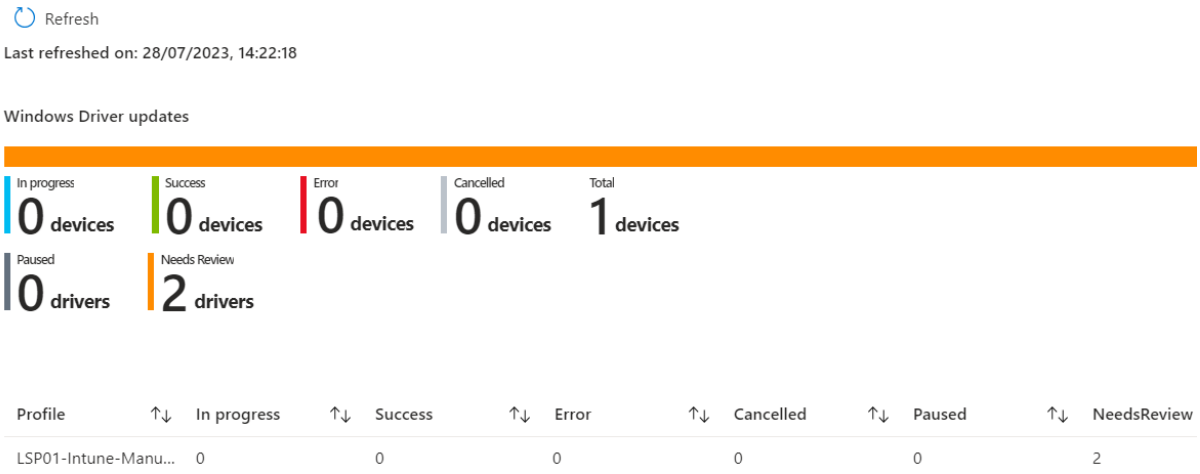
To review the updates:

1. Under **Drivers to Review**, select the link in correspondence with your policy.
2. Updates can appear in both **Recommended Drivers** and **Other Drivers** tabs.
3. Select the **Approve** option under **Actions**.
4. Specify the date to make the driver available to devices with they scan for Windows updates.



8.8.3 Driver Update Reports

1. Select the Reports tab
2. Select the Windows update tab
3. Scroll down to the Windows Driver Updates report.

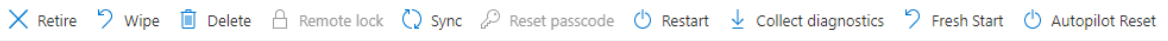


8.9 Managing Windows 10/11 Devices

With delegated RBAC controls, Intune LAs also have permissions to remotely wipe and remove Windows 10/11 and HoloLens 2 devices from the NHSmail Intune platform. This action should be performed only as a last resort for devices experiencing issues and Intune LAs are not required to seek support from the Intune Live Service Team to complete this action.

!	**Important Note** The device unenroll process detailed below is separate from the NHSmail user Joiners, Movers and Leavers (JML) process.

The device unenroll process detailed below is separate from the NHSmail user Joiners, Movers and Leavers (JML) process.



Please read through the details of each option and decide which option will allow you to manage your devices best, then follow the step-by-step process to complete the action.

8.9.1 Retire/Delete

The **Retire** action removes app data, settings, and Intune managed email profiles from the device. The device will still show in Intune until the device ultimately checks in. If you want to remove stale devices immediately, use the **Delete** action instead. **Delete** will also issue the **Retire** command but it will remove the device from the All devices list immediately.

!	**Important Note** Retire/Delete leaves users' personal data on devices.

Recommendation / Recommended Use

Retire/Delete is the best option for devices that are no longer needed. It removes all access to the device completely, as it also deletes the Azure AD record. Please note however that device will not be deleted from Azure AD.

If you want to delete the AAD device, you will need to first remove the AutoPilot Device record in **Intune Admin Centre**, and then navigate to **Devices > Windows > Windows Enrolment > Devices**. Once you have deleted the AutoPilot device record, the device can be removed from AAD.

Action	Data type	Windows 10/11
Retire/Delete	Company apps and associated data installed by Intune	Apps are uninstalled. Sideloading keys are removed. Microsoft 365 Apps are not removed. Intune management extension installed Win32 apps will not be uninstalled on unenrolled devices.
Retire/Delete	Settings	Configurations that were set by Intune policy are no longer enforced. Users can change the settings.
Retire/Delete	Wi-Fi and VPN profile settings	Removed
Retire/Delete	Certificate profile settings	Certificates are removed and revoked.
Retire/Delete	Email	Removes email that's EFS-enabled. This includes emails and attachments in the Mail app for Windows. Removes mail accounts that were provisioned by Intune. (PST or OST files are not removed!)
Retire/Delete	User accounts	Only if a local account exists (non AAD accounts) a sign-in is possible after Retire/Delete Action.
Retire/Delete	Personal Data	Users' personal data is not removed.
Retire/Delete	Remove from Intune	Yes, wait until device ultimately checks in.
Delete	Remove from Intune	No, remove from Intune immediately.
Retire/Delete	Azure AD unjoin	The Azure AD record is removed.

Without a local administrator account provisioned, you will not be able to access the device after a **Retire/Delete**. **Retire/Delete** will remove all management Intune settings like Wi-fi, VPN profile, certificates, e-mail accounts, the Azure AD join record and apps. However, it will not remove Microsoft 365 Apps for Enterprise (Office ProPlus) and other Win32 apps or any user's personal data.

8.9.2 Wipe

The **Wipe** action is a destructive action with potential data loss. It will restore a device to its default settings (OOBE, out-of-box experience). The **Wipe** action has an option to keep the enrolment state and associated user account. **If this option is not set, all data, apps, and settings will be removed**.

Recommendation / Recommended Use

The **Wipe** action is useful for resetting a device before it will be given to a new user, or when the device has been lost or stolen.

The option "**Wipe the device and continue to wipe even if device loses power**" is an additional option to avoid the circumvention of a wipe by simply power cycling the device. This option will keep trying to reset the device until it succeeds.

Action	Keep enrolment state and user account	Removed from Intune management?	Description
Wipe	Checked	No	✓ Wipes all MDM Policies. ✓ Keeps user accounts and data (Profile). ✓ Resets user settings back to default, removes user-installed apps, ✓ Resets the operating system to its default state and settings. ✓ Keeps AAD join, MDM policies will be reapplied the next time device connects to Intune.
Wipe	Not checked	Yes	✓ Wipes all user accounts, ✓ Wipes all user data and user-installed apps, ✓ Removes MDM policies, and non-default settings. ✓ Resets the operating system to its default state and settings (OOBE).

8.9.3 Fresh Start

The **Fresh Start** device action removes any apps that are installed on a device running Windows 10/11. **Fresh Start** helps remove pre-installed (OEM) apps that are typically installed with a new PC. It is almost identical to a **Wipe** action. The only advantage of **Fresh Start** is it removes OEM-preloaded applications.

Fresh Start comes with one option: If you do not retain user data, the device will be restored to the default OOBE completed state retaining the built-in administrator account.

Azure AD joined devices will be enrolled into mobile device management again when an Azure Active Directory enabled user signs into the device.

Recommendation / Recommended Use

Fresh Start is ideal for devices that do not come with a non-OEM Windows (Signature Edition) installed. With **Fresh Start**, you reset the device to the only built-in applications included with the default Microsoft Windows 10 ISO image.

Action	Retain user data on this device	Removed from Intune management?	Description
Fresh Start	Not checked	Yes	✓ Wipes all user accounts, all user data and installed Win32 apps, MDM policies, and non-default settings. ✓ Keep Windows Store Apps, ✓ Updates Windows to latest version and its default state and settings. ✓ Keeps AAD join.
Fresh Start	Checked	No	✓ Keeps all user accounts and data, ✓ Wipes all MDM Policies and Win32 apps. ✓ Keeps Store Apps. ✓ Resets user settings back to default. ✓ Removes user-installed apps. ✓ Updates Windows to latest version. ✓ Keeps AAD join.

8.9.4 Autopilot Reset

Autopilot Reset removes all the files, apps, and settings on a device (including the user profile) but retains the connection to Azure AD and Intune. It wipes a device maintaining the enrolment state but not the user data.

Autopilot Reset also maintains the region/language/keyboard, any machine provisioning packages applied, and Wi-Fi connections. There is no OOBE or Autopilot ability **after Autopilot Reset**, as this data is retained. The user will be presented directly with the Windows 10/11 login screen and can sign-in directly.

Recommendation / Recommended Use

Autopilot Reset is the best option for re-using a working device within your organisation. The last user is removed from a device and it can be handed over to the next user.

Action	Removed from Intune management?	Description
Autopilot reset	No	✓ Wipes all MDM Policies and User data. ✓ Resets user settings back to default. ✓ Removes user-installed apps. ✓ Keeps user accounts. ✓ Resets the operating system to its default state and management settings. ✓ Keeps AAD join

8.9.5 Summary

The following table summarises all the scenarios detailed above, when they should be used and how these actions each affect Intune management and Azure AD enrolment.

Method	Usage	Intune management	Azure AD enrolment
Retire/Delete	Remove outdated devices	Removed	Removed
Wipe (keep enrolment)	Reset device to default, remove Apps, keep user's data/files	Keep, Re-apply policies	Keep
Wipe	Lost stolen device, device handover, Return to OOBE	Removed	Removed
Fresh Start (keep enrolment)	Reset device to Signature Edition, remove Apps, keep user's data/files update to latest Windows version	Keep	Keep
Fresh Start	Reset device to latest Windows Signature Edition	Removed	Keep
Autopilot Reset	Reuse a device and remove previous user's profile/data	Keep	Keep

8.10 Surface Hub Enrolment

!	**Important Note** Enrolment of a Surface hub device will require a Resource account with a Teams Rooms licence. The Resource account will also need to be a part of the <ODS>.sg.Intune-Users group.

It is not possible to extract a hardware hash from a Surface Hub device, so the following method is recommended by Microsoft.

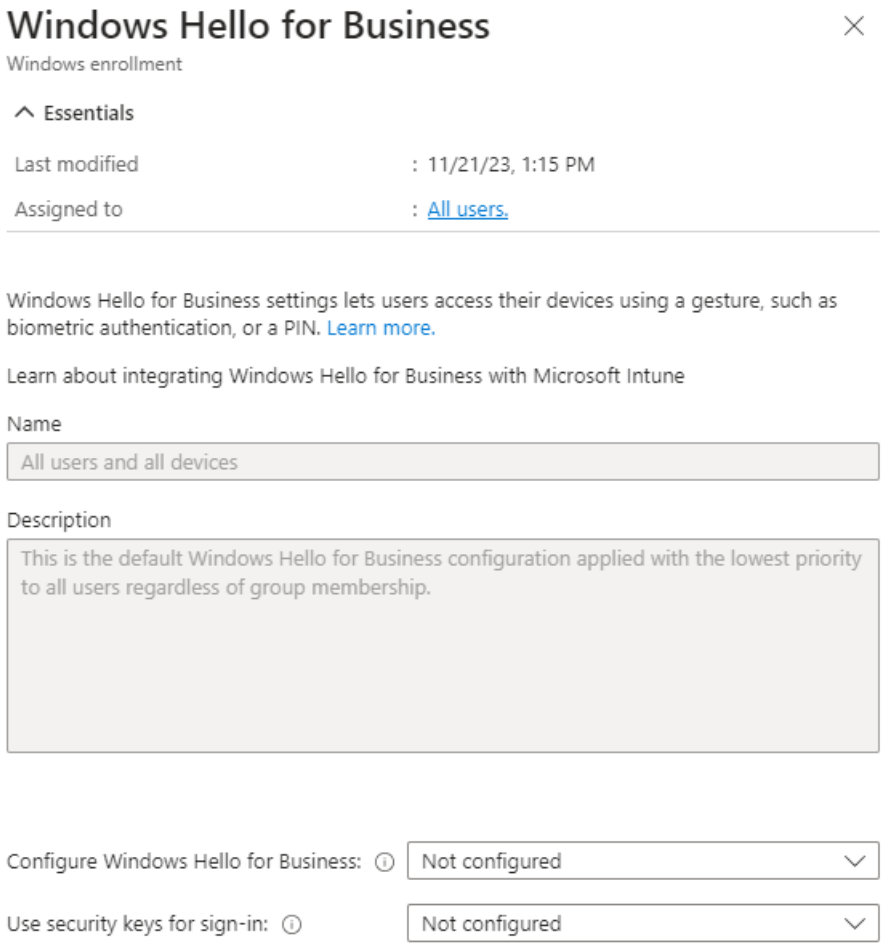
1. Open the **Settings** app and sign in as a local administrator.
   Select **Surface Hub** > **Device management** and then select **+Device management**.

2. You will be prompted to sign in with the account to use for your MDM provider. After authenticating, the device automatically enrols with your MDM provider. If the server address is not detected, enter **manage.microsoft.com**

> **Important Note**
>
> After the Surface Hub has been enrolled, LAs will need to notify Live Service via a service request, detailing the serial number and UPN of the resource account in order to make the device visible.

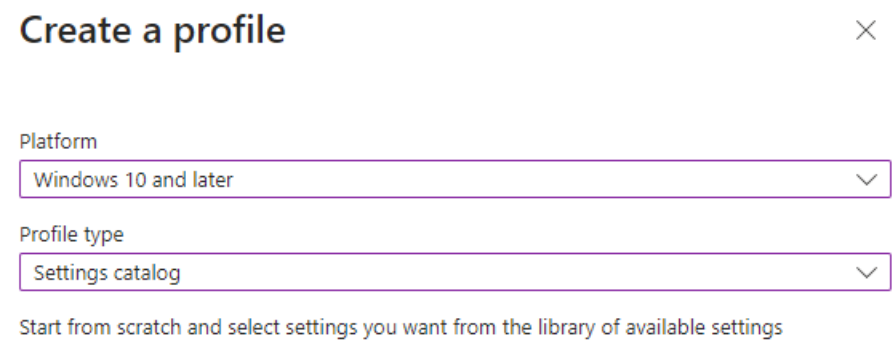
8.11 Windows Hello For Business

Tenant wide, the Windows Hello for Business feature is turned off, however it can be enabled on an individual organization basis with the use of Configuration profiles.

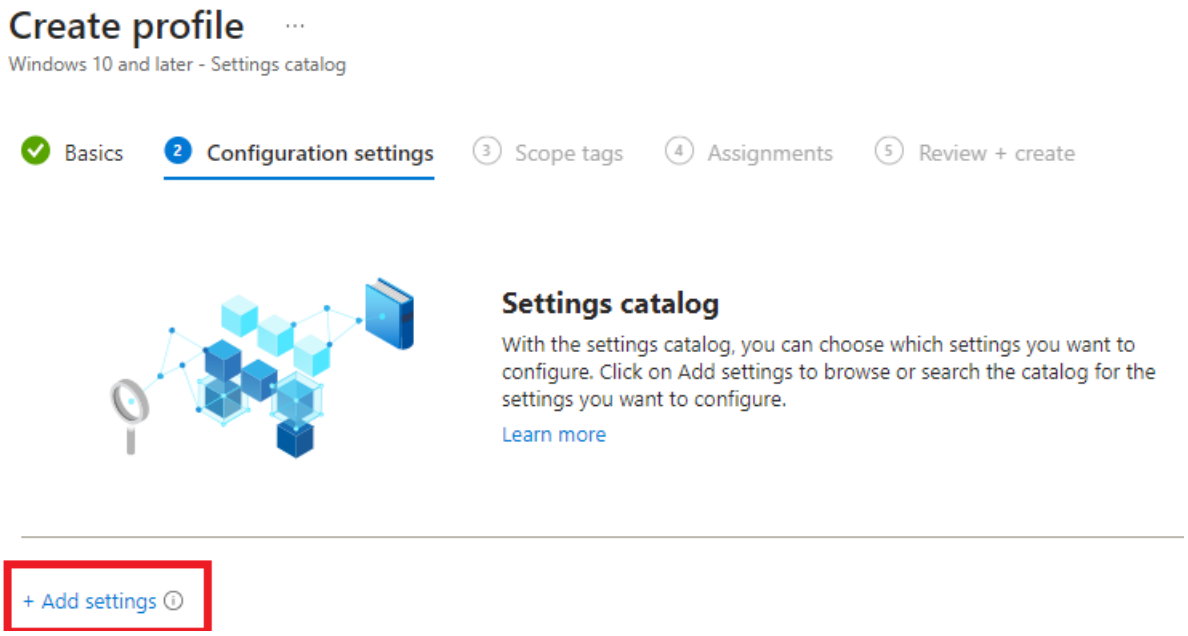


8.11.1 Enable Windows Hello For Business

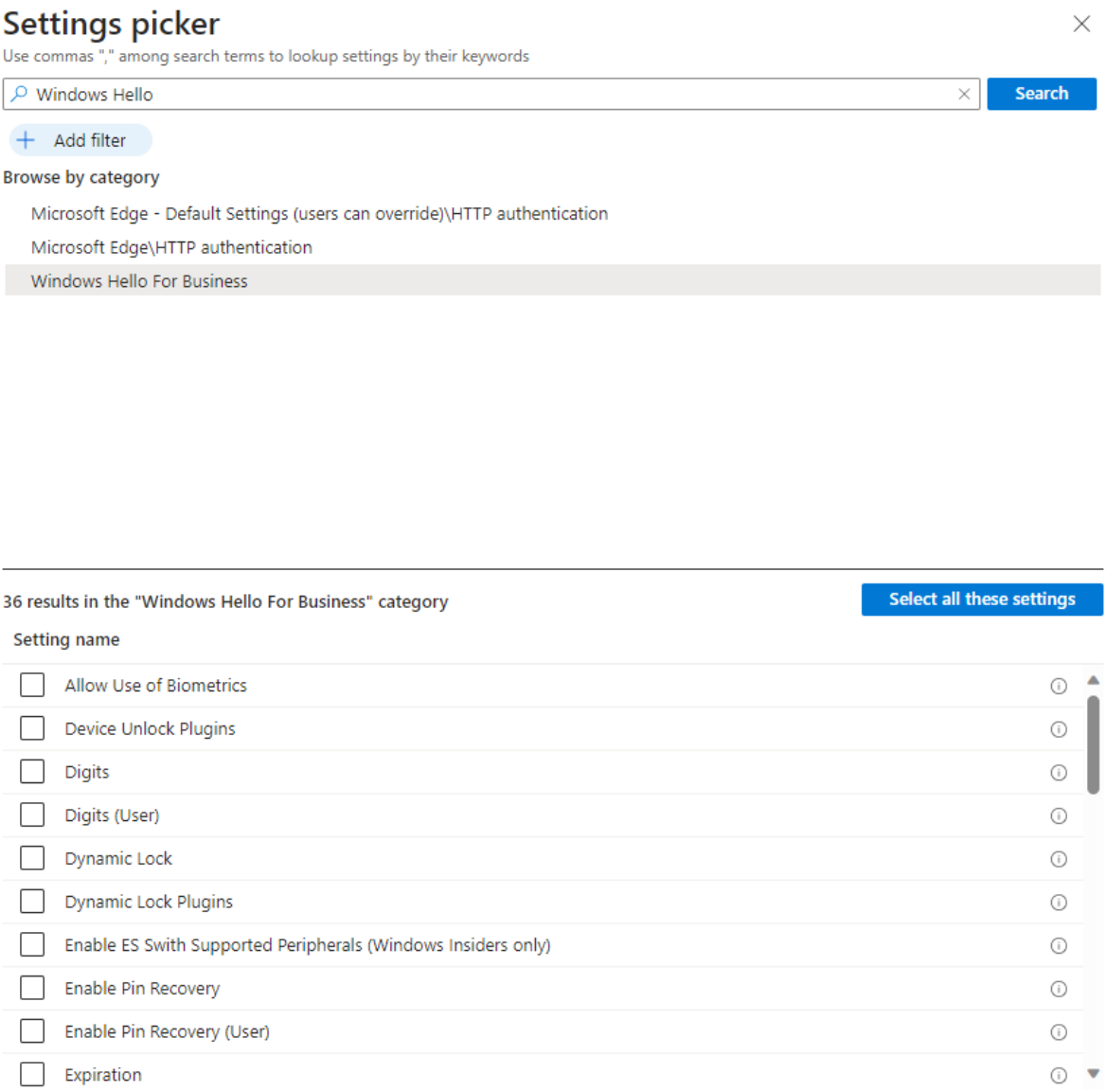
1. To configure Windows Hello for Business, direct to: **Devices, Configuration Profiles, Create, Windows 10 and Later,** under *Profile type,* select **Settings Catalog**



2. Select **Add Settings**



3. Search for Windows Hello for Business – A further explanation of settings can be reviewed from the linked Microsoft document



4. Review and save your profile, ensuring you have selected the group of users or devices you wish to target

8.12 Windows 365

Windows 365 Cloud PCs are now available on the tenant and can be requested though a Service Request after the correct licences have been acquired and uploaded to the NHS Portal.

Windows 365 Cloud PCs are administered in the same format as a regular Windows device.

8.12.1 Windows 365 Frontline Cloud PCs

W365 Frontline Cloud PCs can now be requested through a Service Now request once the licenses have been procured. The W365 Frontline License is used to create both Dedicated, Shared and Cloud Apps scenarios of W365 Frontline Cloud PCs so the same license is used regardless of whether the organizations is looking to deploy Shared, Dedicated or Cloud Apps Cloud PCs.

There are some differences of what can be achieved with Frontline Dedicated, Shared and Cloud Apps Cloud PC scenarios;

- One W365 Frontline License configured to Dedicated will create Cloud PCs for each user in the specified group (multiples of Three) with One user being able to access their Cloud PC at a time. Other users will not be able to access their Cloud PC until a session has ended, and a license becomes available.

- Two W365 Frontline Licenses enables Two users to connect to their Cloud PCs concurrently. The more licenses, the more concurrent users can use their Cloud PC.

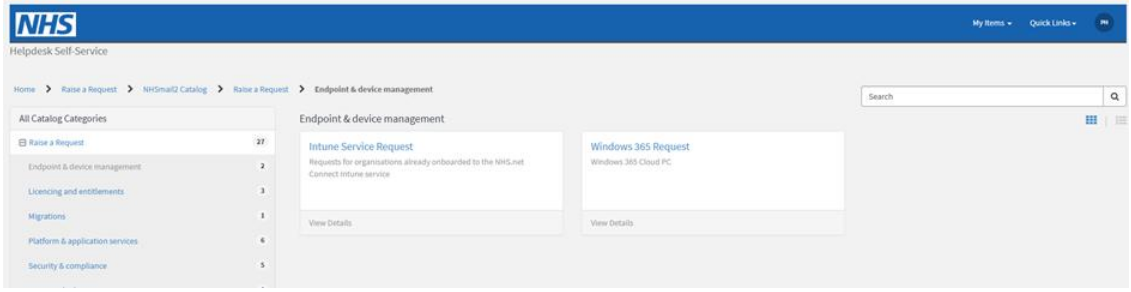
- One W365 Frontline License configured to Shared will create One Cloud PC that can be accessed by all users in the specified group, however only One concurrent user at any time. All other users will have to wait until a user disconnects from the session to connect to the Shared Cloud PC.

- One W365 Frontline License configured to Cloud Apps will allow 1 user to be able to open the published apps via their Windows App without starting a full Cloud PC session. Great for convenience and quicker productivity.

The following outlines the steps required to request W365 Frontline Cloud PCs for an organization;

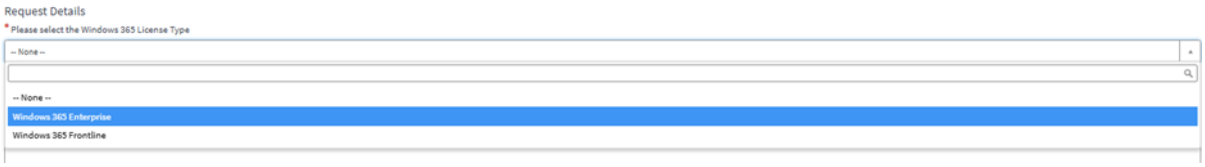
- W365 Frontline Licenses should be procured through the bring your own license procedure. NHSmail Intune Operations Guide – NHSmail Support

- Once W365 Frontline licenses have been procured, navigate to Service Now and click Windows 365 Request.



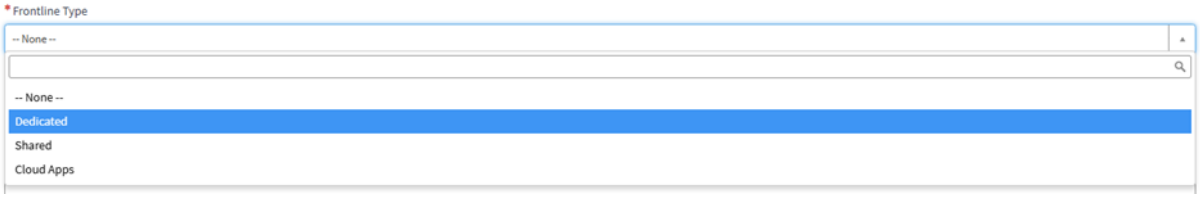
To successfully complete this request and deploy Cloud PCs or Cloud Apps to the desired users in your organisation, the Live Service team needs some specific information;

- Under “Request Details” select “Windows 365 Frontline” from the drop down box.

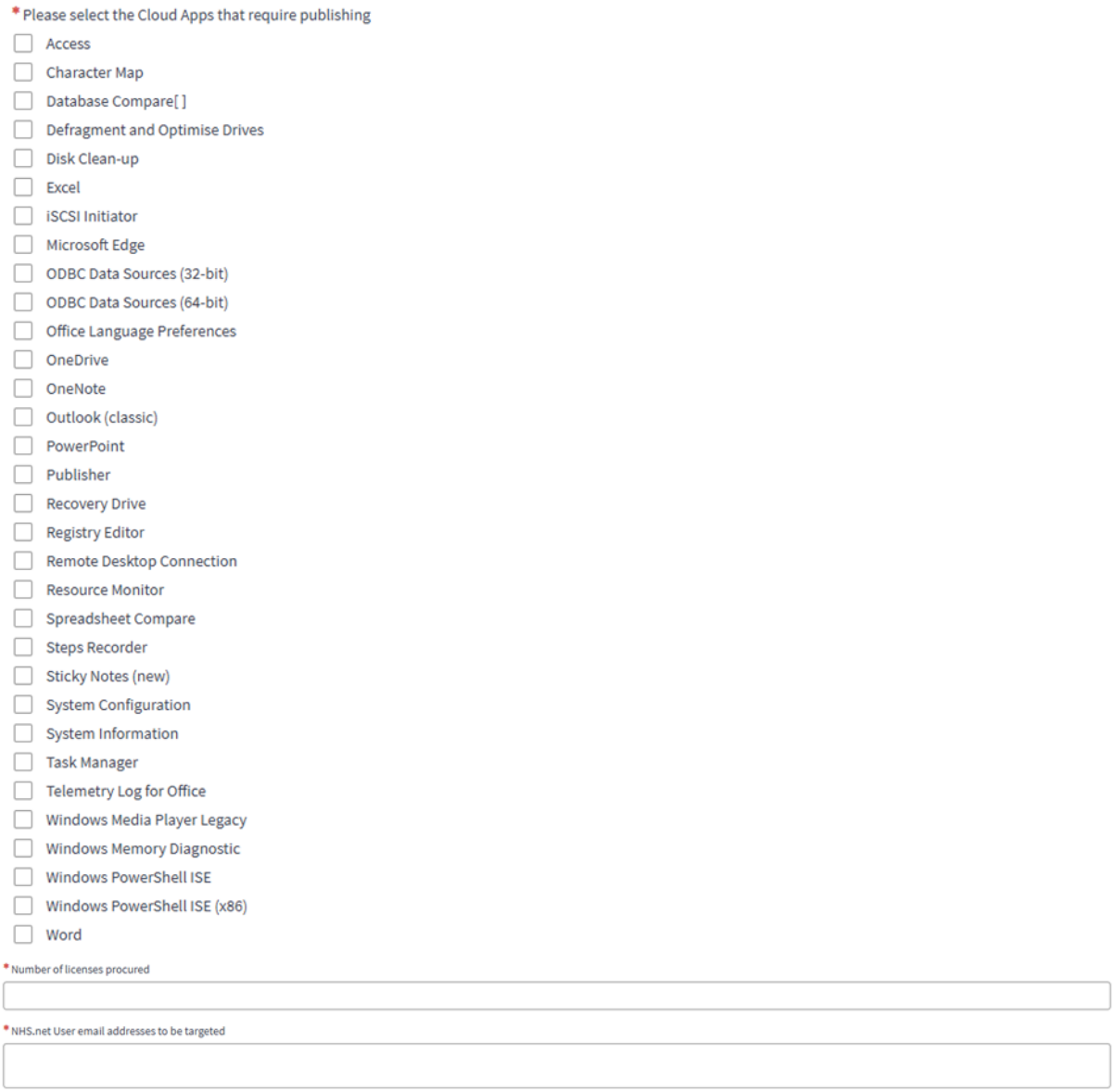


- Enter the ODS code of your organisation.

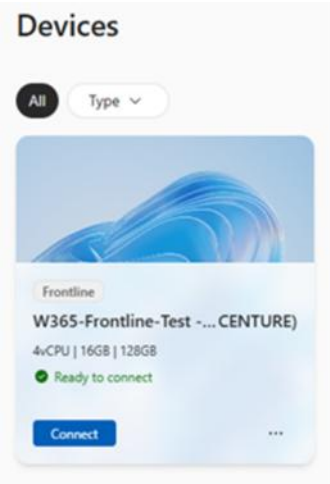
- Under “Frontline Type” select either “Shared”, “Dedicated” or “Cloud Apps”, depending on the Frontline type you require.



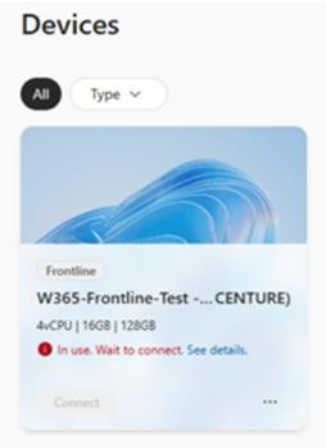
- For Cloud Apps, select the apps that are required to be accessible vis the Windows App.
- For all scenarios, under “number of licenses procured” enter the number of licenses you have procured.
- For all scenarios, under “NHS.net User email addresses to be targeted” enter the email addresses of the users you wish to target with Frontline / Cloud Apps Cloud PCs. After entering each email address, hit enter and enter the next email address on a new line.



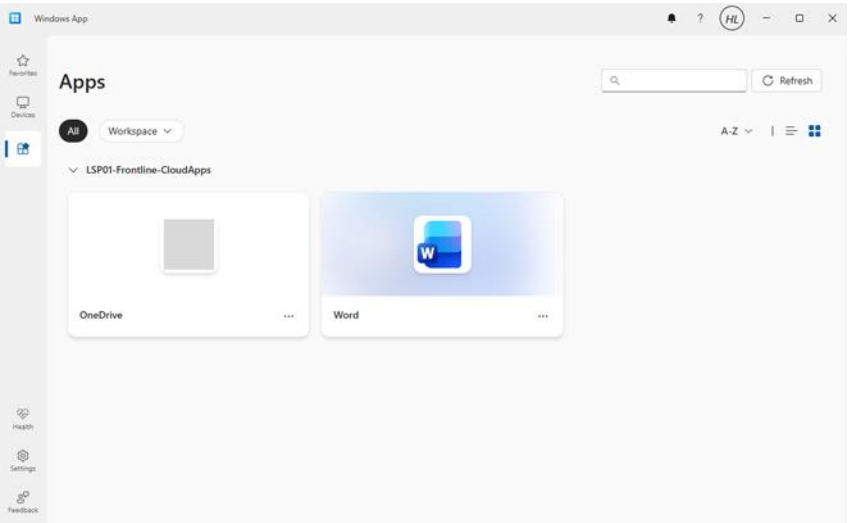
Complete the rest of the form with the relevant information. Once the Cloud PCs have been provisioned, users will see the Frontline Cloud PC, or a new tab called Apps if Cloud Apps Scenario is provisioned, in the Windows App once logged in with their NHS credentials. This can be done on any device where the Windows App is available for download.



If all Frontline Dedicated licenses are being consumed, or users are using all the Frontline Shared Cloud PCs, all other users will see a prompt on the Cloud PC that they will need to wait for a session to become available before they can connect to the Cloud PC.



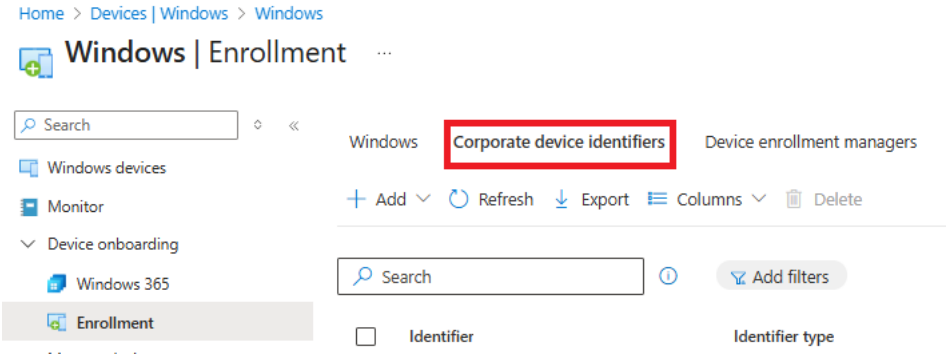
Cloud Apps scenario will display a new Apps tab in the Windows App. Select this to see the published apps and select one to launch the app.



8.12.2 Windows 365 Link devices

To enroll a Windows 365 Link device for Cloud PCs, the device will need to be added as a “deivce corporate identifier”.

1. To do this go to Devices, Windows, Enrollment.
2. Across the top of the screen select Corporate Device Identifiers



3. Select Add and Enter Manually
4. In the first drop down, select “Serial Number” as identifier type
5. In the identifier text box, enter the **serial number**.
6. In the details box, type use the format <ODS>-W365-Link-Device (for example, if the orgs ODS code is LSP01, the format would be LSP01-W365-Link-Device

The Link devices require an Intune licence and Windows enterprise licence, both of which can be enabled as part of the M365 E3 national licencing and finally a Cloud PC licence

!	**Important Note** When connecting to a Link device, the Cloud PC must be fully setup and connected within the last 30 days.

9 SCCM Windows Autopilot Hardware Hash Methods

9.1.1 Windows Autopilot for existing devices using SCCM Task sequence

NHSMail Intune tenant supports JSON file for Windows Autopilot for existing devices. If the NHS Trust wants to adopt JSON file deployment, LA have to log a Service request with Intune Live service teams, so that Intune Live service Engineer could attached Global windows deployment JSON file with Service request and Create respective Dynamic group associated with the enrolment profile.

Windows Autopilot for existing devices lets you reimage and provision a Windows device for Autopilot user-driven mode using a single, native Configuration Manager

task sequence. The existing device can be on-premises domain-joined as end result is a Windows 10 or Windows 11 device joined to Azure Active Directory (Azure AD)

!	**Important Note** *The JSON file for Windows Autopilot for existing devices only supports user-driven Azure AD . Self-deploying and pre-provisioning Autopilot profiles aren't supported with JSON files due to these scenarios requiring TPM attestation.* *However, during the Windows Autopilot for existing devices deployment, if the following conditions are true:* • *Device is already a Windows Autopilot device before the deployment begins* • *Device has an Autopilot profile assigned to it* *then the assigned Autopilot profile takes precedence over the JSON file installed by the task sequence. In this scenario, if the assigned Autopilot profile is either a self-deploying or pre-provisioning Autopilot profile, then the self-deploying and pre-provisioning scenarios are supported.*

There are five steps involved in Windows autopiloting for existing devices .

1. Create a package containing the JSON file
2. Create a target collection
3. Create a task sequence
4. Distribute content to distribution points
5. Deploy the Autopilot task sequence to target collection

9.1.2 Create a package containing the JSON file

1. In the Configuration Manager console, go to the **Software Library** workspace, expand **Application Management**, and select the **Packages** node.
2. On the ribbon, select **Create Package**.
3. In the Create Package and Program Wizard, enter the following details for the package:
   - *Name*: **Autopilot for existing devices config**
   - Select **This package contains source files**
   - *Source folder*: Specify the UNC network path that contains the AutopilotConfigurationFile.json file
   - For the program, select the *Program Type*: **Don't create a program**
4. Complete the wizard.

9.1.3 Create a target collection

1. In the Configuration Manager console, go to the **Assets and Compliance** workspace, and select the **Device Collections** node.
2. On the ribbon, select **Create**, and then choose **Create Device Collection**.
3. In the Create Device Collection Wizard, enter the following **General** details:
   Name: Autopilot for existing devices collection
   ***Comment*:** Add an optional comment to further describe the collection
   Limiting collection: All Systems
4. On the **Membership Rules** page, select **Add Rule**. Specify either a direct or query-based collection rule to add the target Windows devices to the new collection.
5. Complete the wizard with the default settings.

9.1.4 Create a task sequence

1. In the Configuration Manager console, go to the **Software Library** workspace, expand **Operating Systems** and select the **Task Sequences** node.
2. On the **Home** ribbon, select **Create Task Sequence**.
3. On the **Create new task sequence** page, select the option to **Deploy Windows Autopilot for existing devices**.
4. On the **Task sequence information** page, specify the following information:
5. A name for the task sequence. For example, **Autopilot for existing devices**.
6. Optionally add a description to better describe the task sequence.
7. Select a boot image.
8. On the **Install Windows** page, select the Windows **Image package**. Then configure the following settings:
   - ***Image index:*** *Select either Enterprise, Education, or Professional, as required by your organization.*
   - *Enable the option to* ***Partition and format the target computer before installing the operating system****.*
   - ***Configure task sequence for use with Bitlocker:*** *If you enable this option, the task sequence includes the steps necessary to enable BitLocker.*
   - *Product key: If you need to specify a product key for Windows activation, enter it here.*
   - *Select one of the following options to configure the local administrator account in Windows depends upoio the organization requirement.*
9. On the **Configure Network** page, select the option to **Join a workgroup**.
10. On the **Install Configuration manager** page, add any necessary installation properties for your environment.
11. The **Include updates** page selects by default the option to **Do not install any software updates**.
12. On the **Install applications** page, you can select applications to install during the task sequence. However, Microsoft recommends that you mirror the signature image approach with this scenario. After the device provisions with Autopilot, apply all applications and configurations from Microsoft Intune or Configuration Manager co-management. This process provides a consistent

experience between users receiving new devices and those using Windows Autopilot for existing devices.

13. On the **System Preparation** page, select the package that includes the Autopilot configuration file. By default, the task sequence restarts the computer after it runs Windows Sysprep. You can also select the option to **Shutdown computer after this task sequence completes**. This option lets you prepare a device and then deliver it to a user for a consistent Autopilot experience.
14. Complete the wizard.

!	**Important Note** You see screens that you've disabled in your Windows Autopilot profile, such as the Windows 10 License Agreement screen. This issue happens because Windows 10, version 1903 and 1909 deletes the AutopilotConfigurationFile.json file. To fix this issue: • Edit the Configuration Manager task sequence and disable the **Prepare Windows for Capture** step. • Add a new **Run command-line** step that runs c:\windows\system32\sysprep\sysprep.exe /oobe /reboot

9.1.5 Distribute content to distribution points

Next distribute all content required for the task sequence to distribution points.

1. Select the **Autopilot for existing devices** task sequence, and in the ribbon select **Distribute Content**.
2. On the **Specify the content destination** page, select **Add** to specify either a **Distribution Point** or **Distribution Point Group**.
3. Specify content destinations that let the devices get the content.
4. When you're finished specifying content distribution, complete the wizard.

9.1.6 Deploy the Autopilot task sequence

1. Select the **Autopilot for existing devices** task sequence, and in the ribbon select **Deploy**.
2. In the Deploy Software Wizard, specify the following details:
   General :
   Task Sequence: **Autopilot for existing devices**
   Collection: Autopilot for existing devices collection.
3. Deployment Settings select Availble or required depends upon org requirement. *Make available to the following*: **Only Configuration Manager Clients.** *Note : Choose the option here that is relevant for the context of your test. If the target client doesn't have the Configuration Manager agent or Windows installed, you must select an option that includes PXE or Boot Media.*
4. **Scheduling :** Set a time for when this deployment becomes available
5. **User Experience :** Select Show Task Sequence progress

6. **Distribution Points :** *Deployment options*: Download content locally when needed by the running task sequence
7. Complete the wizard.
8. To check the autopilot deployment task sequence, reboot to the device and initiate the deployment process

9.2 System Centre Configuration Manager Report Method

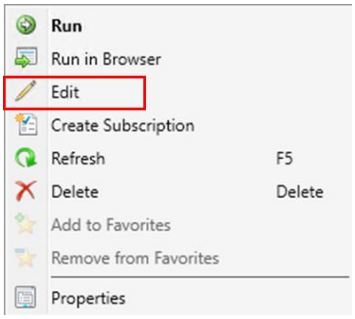
You can use Configuration Manager to collect and report the device information required by Intune. This information includes the device serial number, Windows product identifier, and a hardware identifier. It is used to register the device in Intune to support Windows Autopilot.

Please follow the steps outlined below to do this:

1. In the **Configuration Manager Console**, navigate to the **Monitoring Workspace**.

2. **Select Reporting > Reports.**

3. Browse to the report named **Windows AutoPilot Device Information**. **Right click the report name** and select **Edit** from the drop-down menu.

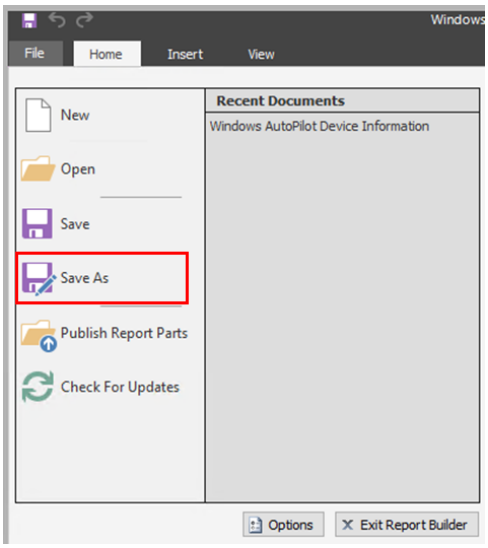


4. This default report will output the hardware hash of every device in Config. Manager that has a client installed. To convert it to a collection-based report to enable only a collection of devices to be targeted, this will need to be edited.

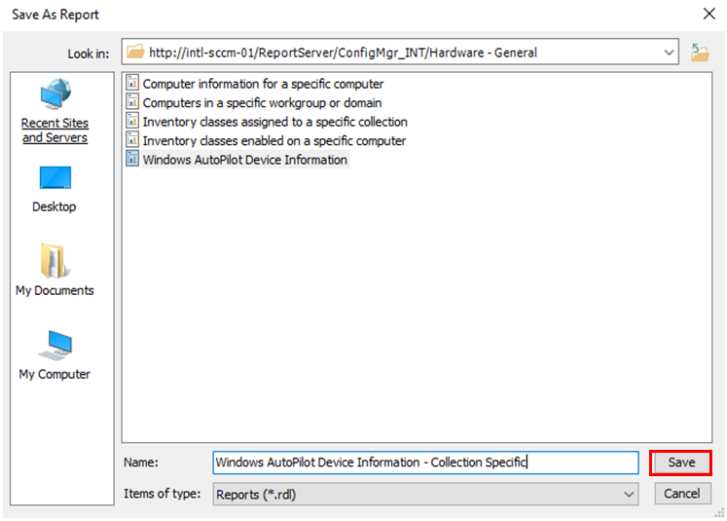
9.3 Editing the Configuration Manager Report

You can edit the Configuration Manager Report to allow collection of a specific query. Please follow the steps detailed below to do this:

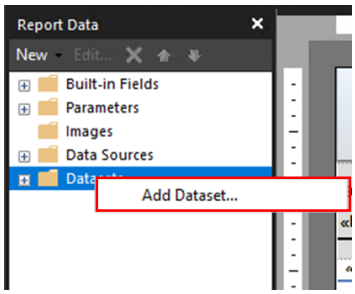
1. From the Home menu, select **Save as**.



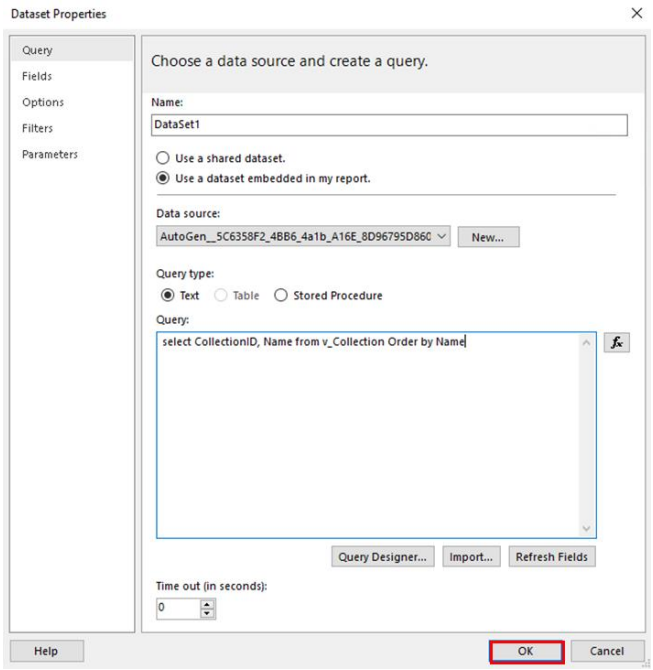
2. **Save** the report as another name, e.g., "**Windows Autopilot Device Information – Collection Specific**".



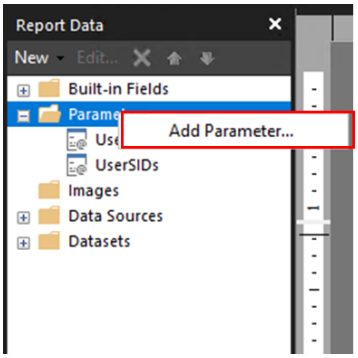
3. In the **Report Data** window, right click **Datasets** and select **Add Dataset**.



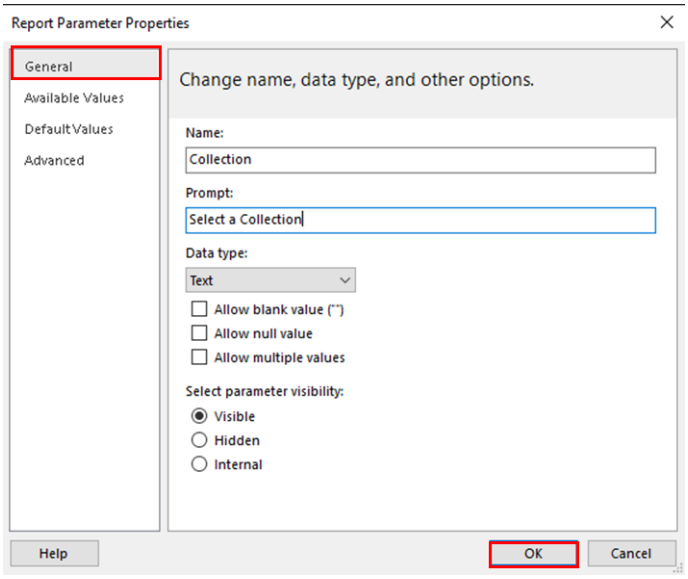
4. Edit the dataset properties to reflect the settings in the figure below and click **OK**.



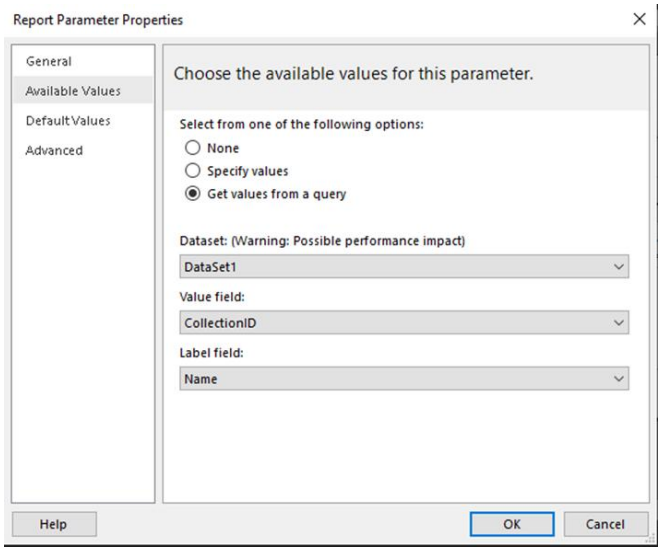
5. In the Report Data window, right click on **Parameters** and select **Add Parameter**.



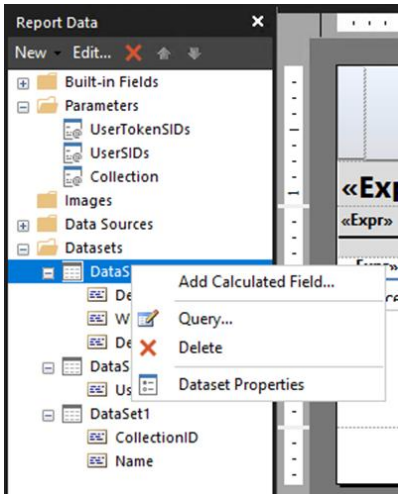
6. Edit the Parameter properties in the **General** tab to reflect the settings in the figure below and click **OK**.



7. Select the **Available Values** tab. Edit to reflect the settings in the figure below and click **OK**.



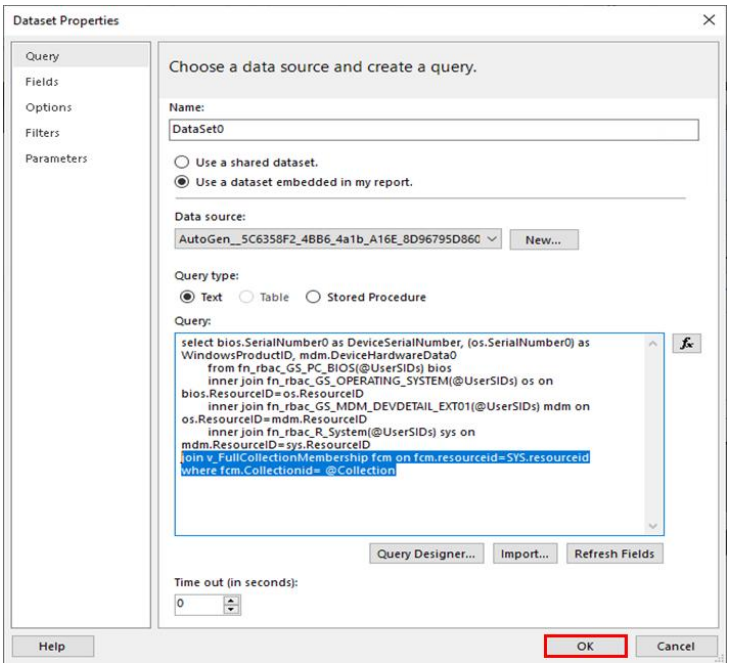
8. In the Report Data window, right click **DataSet0** and select **Query** from the drop-down menu.



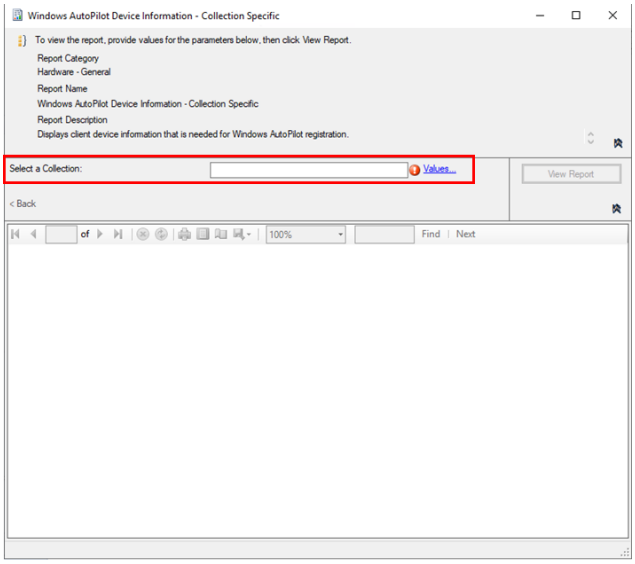
9. Edit the query with this data: **Join V_FullCollectionMembership fcm on fcm.resourceid=SYS. Resourceid**

   Where fcm.Collectionid=@Collection

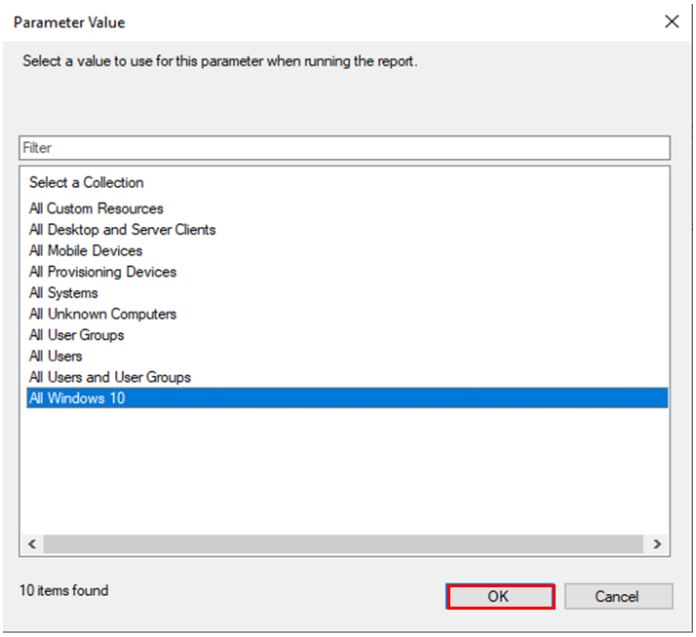
This data is also highlighted in the screenshot below. Once you have edited the query, please click **OK**.



10. When the report is run, the **Select a Collection** field is showing. To select a collection to run the report against, click **Values**.



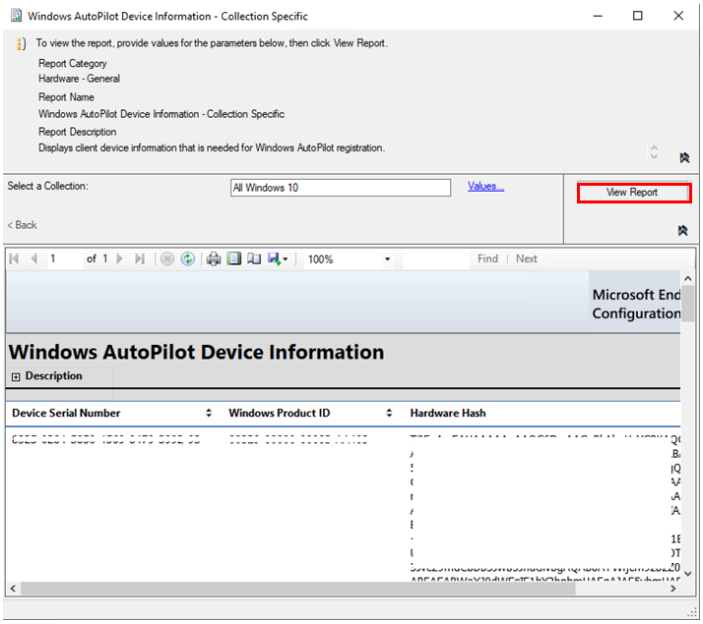
11. **Select the name of the device collection** to import the hardware IDs from. In this example the collection is called “All Windows 10”.



9.4 Exporting the Hardware ID into a .CSV file

Follow the steps below to export the hardware ID into a .CSV file:

1. Run the report and select the **View Report** button.



2. Export the report data by clicking the disk icon and select **CVS (comma delimited)**.
3. Save the report as a .CSV file.

10.Windows Autopatch

10.1 What is Autopatch?

Windows Autopatch is a Microsoft-Managed service that automates the deployment and management of updates for select Microsoft Products, including:

1. Windows Feature and quality updates
2. Microsoft 365 Apps for Enterprise updates
3. Microsoft Edge updates
4. Microsoft Teams client updates

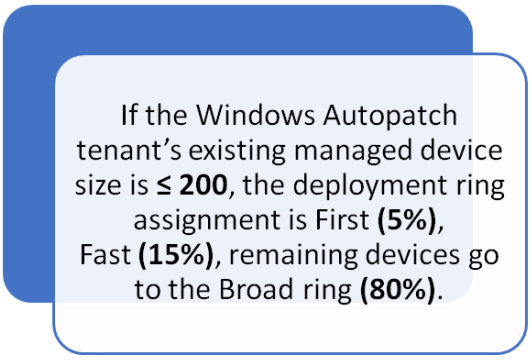
Devices are marked healthy / unhealthy to indicate update status and can be monitored in the Intune UI blades to examine the coverage of updates in your organisation's estate.

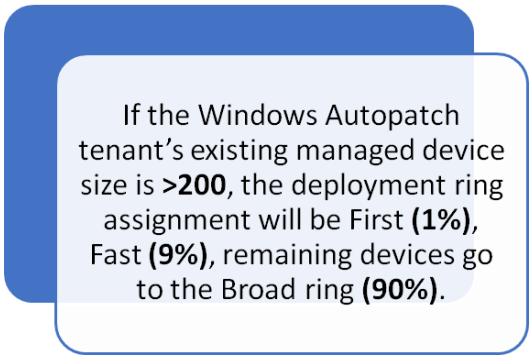
Windows Autopatch creates an update framework similar to Windows Update rings and devices can be aligned to 'fast' and 'slower' update cadence in a similar way.

To read a detailed description of the capabilities and operation of this framework, refer to the Microsoft Windows Autopatch Documentation reference

10.1.1 How Autopatch Works

Calculation Process





10.2 Pre-requisites for adopting Autopatch

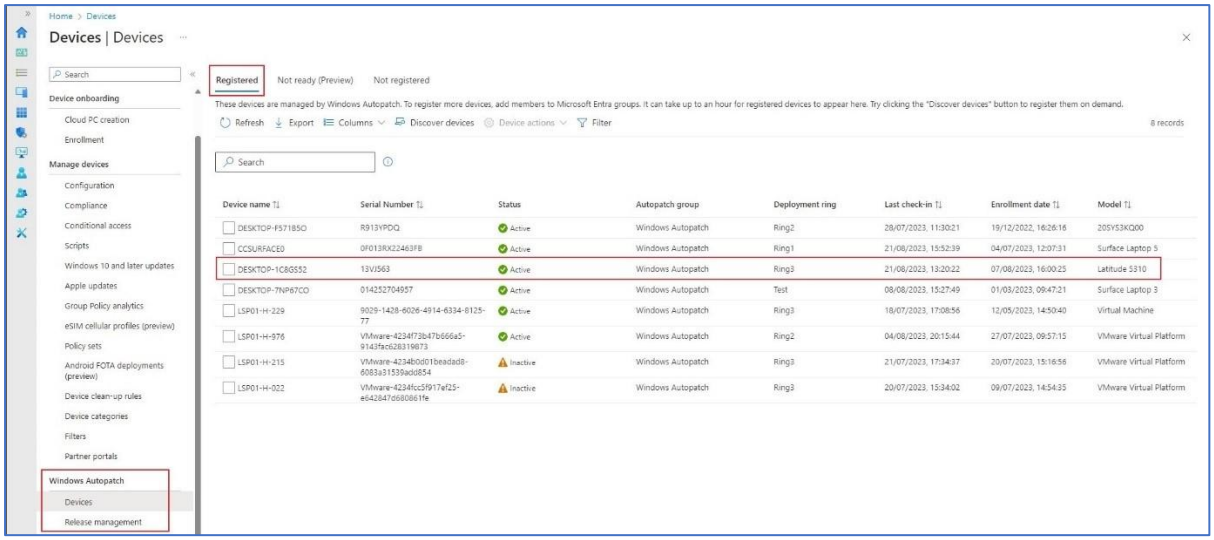
Prior to adoption and deployment of this NHSmail implementation of Autopatch, consider the following key points before committing to a full production deployment.

1. Before committing devices into windows autopatch configuration, consider windows device use settings (e.g. front line) when allocating devices to the service. Carry out initial pilot testing before incorporating a general population of devices.
2. Organisations choosing to use Windows Autopatch service should ensure the following checks are completed beforehand:

Check	Description
Windows OS build, architecture, and edition	Checks to see if devices support Windows 1809+ build (10.0.17763), 64-bit architecture and either Pro or Enterprise SKUs.
Windows update policies managed via Microsoft Intune	Checks to see if devices have Windows Updates policies managed via Microsoft Intune (MDM). If this the case, they should remove the devices the Windows update policy.
Windows update policies managed via Group Policy Object (GPO)	Checks to see if devices have Windows update policies managed via GPO and if so, remove the policy. **Windows Autopatch doesn't support Windows update policies managed via GPOs.**

	Windows update should be managed via Microsoft Intune.
Microsoft Office update policy managed via Group Policy Object (GPO)	Checks to see if devices have Microsoft Office updates policies managed via GPO and if so, remove the policy. **Windows Autopatch doesn't support Microsoft Office update policies managed via GPOs. Office updates must be managed via Microsoft Intune** or another Microsoft Office policy management method where Office update bits are downloaded directly from the Office Content Delivery Network (CDN).
Windows Autopatch network endpoints	There's a set of network endpoints that Windows Autopatch services should be able to reach for the various aspects of the Windows Autopatch service.
Microsoft Teams network endpoints	There's a set of network endpoints that devices with Microsoft Teams should be able to reach for software updates management.
Microsoft Edge network endpoints	There's a set of network endpoints that devices with Microsoft Edge should be able to reach for software updates management.
Internet connectivity	Checks to see if a device has internet connectivity to communicate with Microsoft cloud services. Windows Autopatch uses the PingReply class. Windows Autopatch tries to ping at least three different Microsoft's public URLs two times each, to confirm that ping results aren't coming from the device's cache.

2) The devices will be assigned to a Deployment Ring group, based on the calculation process described above. Device is listed as Registered in the Windows Autopatch devices list:

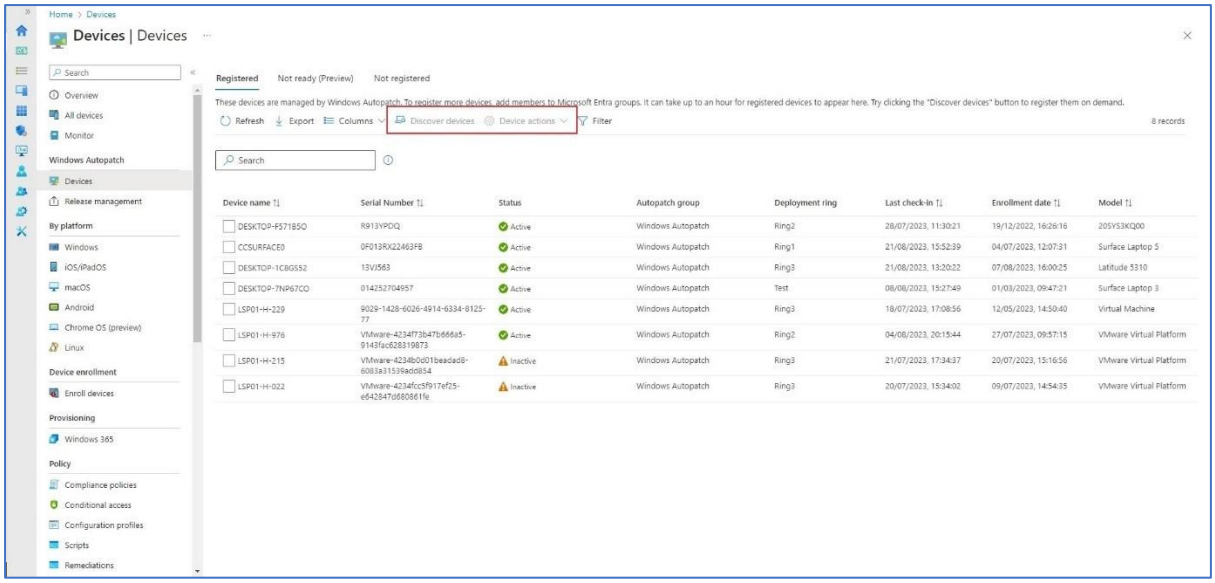


10.3 How to adopt Autopilot for NHSmail

Windows Autopatch is offered as an opt-in basis. Please raise a Service Request with the Intune Live Support team if you would like to use the functionality or if you have any questions.

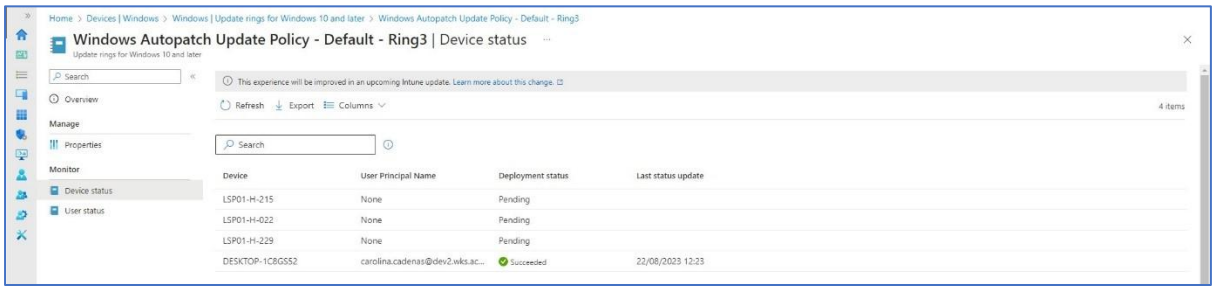
Once you have raised a Service Request, the Intune Live Support team will carry out the following steps to enable Autopatch:

1) Intune Live Support will add an organisation's Intune Admins who wants to use the service to the Azure AD group **Modern Workplace Roles – Service Reader**. Please note, LAs are unable to discover devices or do any device actions from the Autopatch section. Currently, this feature does not support scoped tags hence they will see all the Windows devices using the service.

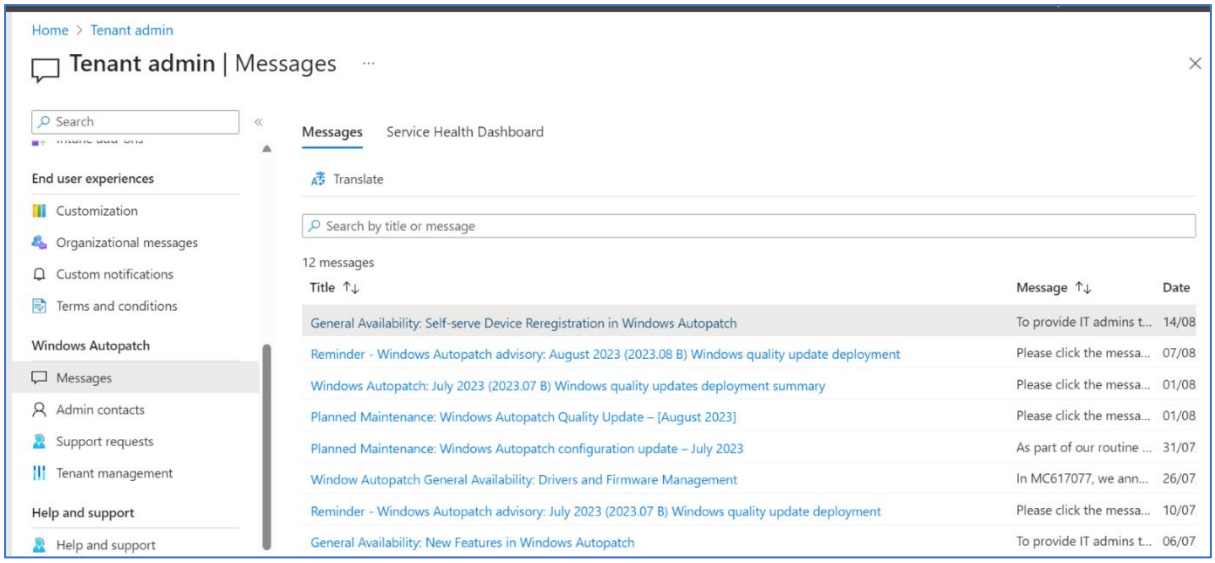


2) Intune Live Support will add the group that contains the organisation Windows devices to the **Windows Autopatch registration** group.

3) Intune Local Admins will see the updates assigned to a particular Deployment ring from Autopatch blade however, they can get more details on the current status by navigating to Window 10 updates and select the profile linked to the deployment Ring.



4) Under Windows Autopatch view from Tenant Admin, they can see the Messages board to monitor any changes on the service.



!	**Note:** Each Deployment ring has a different set of update deployment policies to control the update rollout.

10.4 Autopatch guidance for Microsoft Products

Windows Autopatch software update management scope includes the following software update workloads discussed in this section:

- Windows quality updates
- Windows feature updates.
- Microsoft 365 Apps for enterprise updates
- Microsoft Edge updates
- Microsoft Teams updates
- Anti-virus definition (refers to the Defender agent updates managed via Windows Updates)

10.4.1 Windows Autopatch Deployment Rings

The following default deployment rings are automatically created during Autopatch Deployment Enrollment:

1. **Service-based deployment ring**: exclusively used to keep Windows Autopatch updated with both service and device-level configuration policies, apps, and APIs.

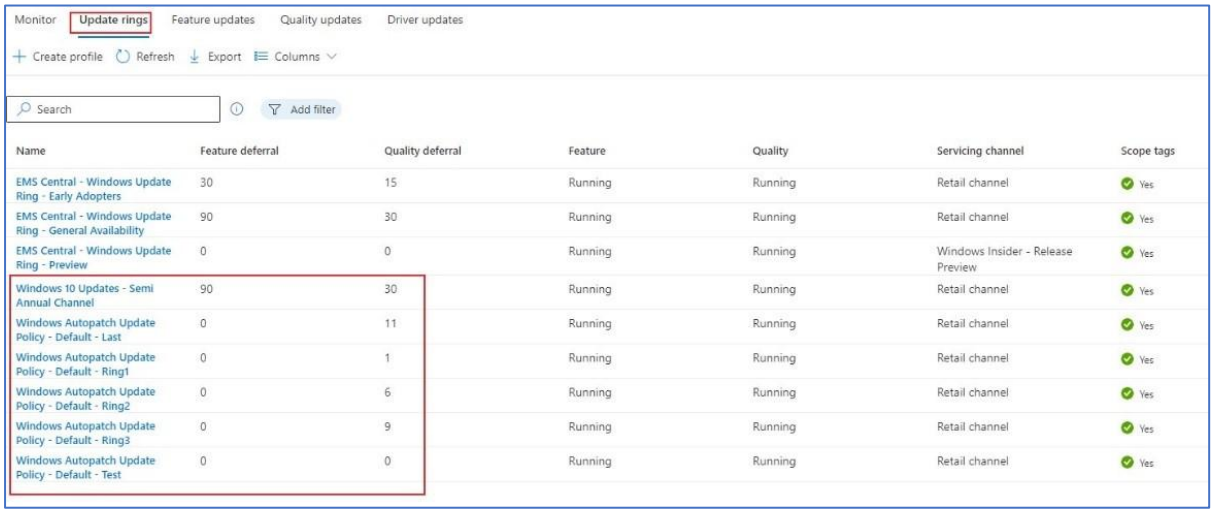
Name	Description

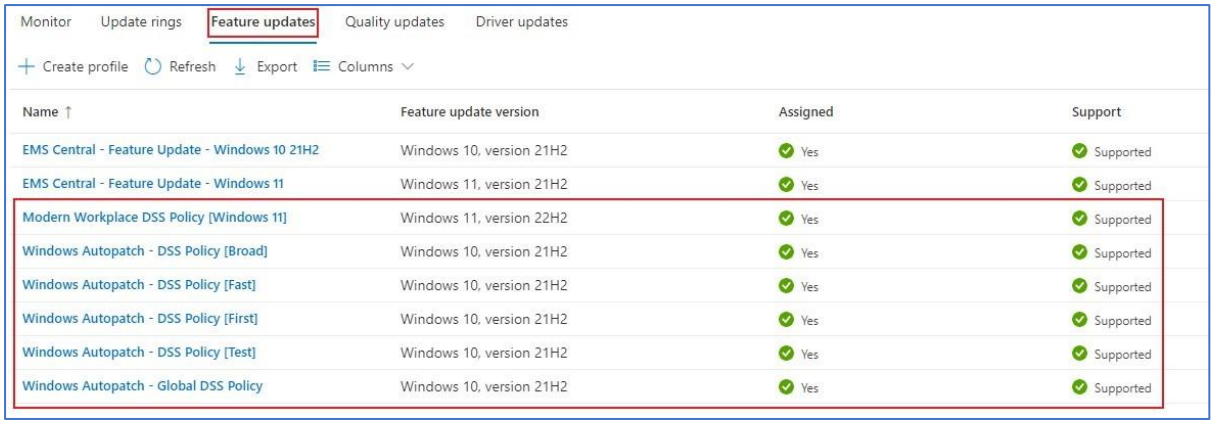
Modern Workplace Devices-Windows Autopatch-Test	Deployment ring for testing service-based configuration, app deployments prior production rollout
Modern Workplace Devices-Windows Autopatch-First	First production deployment ring for early adopters.
Modern Workplace Devices-Windows Autopatch-Fast	Fast deployment ring for quick rollout and adoption
Modern Workplace Devices-Windows Autopatch-Broad	Final deployment ring for broad rollout into the organization

2. **Software updates-based deployment ring** [(1)]: exclusively used with software update management policies, such as the Windows update ring and feature update policies.

Name	Description
Windows Autopatch - Test	Deployment ring for testing software updates-based deployments prior production rollout.
Windows Autopatch - Ring1	First production deployment ring for early adopters.
Windows Autopatch - Ring2	Fast deployment ring for quick rollout and adoption.
Windows Autopatch - Ring3	Final deployment ring for broad rollout into the organization.
Windows Autopatch - Last	Optional deployment ring for specialized devices or VIP/executives that must receive software update deployments after it's well tested with early and general populations in an organization.

(1) each deployment ring has a different set of update deployment policies to control the updates rollout.





10.4.2 Microsoft 365 Apps for Enterprise

Pre-requisites

For a device to be eligible for Microsoft 365 Apps for enterprise updates (both 32-bit and 64-bit versions), they must meet the following criteria:

- The device must be turned on and have an internet connection.
- The device must be able to access the required network endpoints to reach the Office Content Delivery Network (CDN).
- **There are no policy conflicts between** Microsoft Autopatch policies and customer policies.
- The device must have checked into the Intune service in the last five days.
- If Microsoft 365 Apps are running, the apps must close for the update process to complete. This is an expected behaviour for Microsoft 365 Apps update.

Update Release Schedule

- Updates are released on the second Tuesday of the month.
- Updates can include feature, security, and quality updates.
- These updates occur automatically and pulled directly from the Office Content Delivery Network (CDN).
- Windows Autopatch doesn't control the order in which updates are offered to devices across the estate. After the update downloads, there's a seven-day update deadline that specifies how long the user has until the user must apply the update.
- To ensure that users are receiving automatic updates, Windows Autopatch prevents the user from opting out of automatic updates.

!	**Note:** Windows Autopatch doesn’t allow pausing or rolling back an update in the Microsoft Intune Portal.

!	**Note:** Microsoft Teams uses a different channel from the rest of Microsoft 365 Apps.

10.4.3 Microsoft Edge

Pre-requisites

For a device to be eligible for Microsoft Edge updates as a part of Windows Autopatch, they must meet the following criteria:

- The device must be powered on and have an internet connection.
- **There are no policy conflicts between Windows Autopatch policies and customer policies.**
- The device must be able to access the required network endpoints to reach the Microsoft Edge update service.
- If Microsoft Edge is open, it must restart for the update process to complete.

Update Release Schedule

- Microsoft Edge will check for **updates every 10 hours.** Quality updates occur weekly by default. **Feature updates occur automatically every four weeks** and are rolled out progressively by the Microsoft Edge product group.
- All users will see the update within a few days of the initial release.
- Browser updates with critical security fixes will have a faster rollout cadence than updates that don't have critical security fixes to ensure prompt protection from vulnerabilities.
- **Devices in the Test device group receive feature updates from the Beta Channel**. This channel is fully supported and automatically updated with new features approximately every four weeks.

!	**Note:** Windows Autopatch can’t pause or resume Microsoft Edge updates.

10.4.4 Microsoft Teams

Pre-requisites

For a device to be eligible for automated Teams updates as a part of Windows Autopatch they must meet the following criteria:

- Microsoft Teams must be installed on the device.
- The user must be signed into both the device and Teams.

- The device must be able to access the Teams update service network endpoints.
- Once the update is downloaded, the user must be logged in with the device in an idle state for at least 40 minutes to ensure that Teams can automatically update.

Update Release Schedule

- The Teams desktop client updates are released **once a month for all users**.
- The update **usually takes place on a Monday.** If a critical update is needed, Teams will bypass this schedule and release the update as soon as it's available.

!	**Note:** Windows Autopatch can't pause or resume Teams updates.

10.4.5 Important considerations after deploying Windows Autopatch

- It is possible to exclude a device from Windows Autopatch however the device is not deleted/remove from Microsoft Intune. The device is flagged as **excluded** so Windows Autopatch doesn't try to restore the device into the service again.
- The exclusion command doesn't trigger device membership removal from the **Windows Autopatch Device Registration** group, or any other Azure AD group, used with Autopatch groups. Intune LAs should create a SR to get a device fully removed from Autopatch Service.

!	**Note:** Excluding devices from the **Windows Autopatch Device Registration group**, or any other Azure AD group, used with Autopatch groups doesn't exclude devices from the Windows Autopatch service.

- Intune Local Admins can’t create additional deployment rings or use their own rings for devices managed by the Windows Autopatch service.
- **Windows Autopatch – Test** and **Last** can be only used as **Assigned** device distributions.
- Make sure that all device-based Azure AD groups intended to use with Autopatch groups are created prior to using the feature.
- A device-based Azure AD group can only be used with one deployment ring in an Autopatch group at a time. This applies to deployment rings within the same Autopatch group and across different deployment rings across different Autopatch groups.
- Autopatch groups uses the following logic to solve device conflicts on your behalf within an Autopatch group:

- **Checks for the deployment ring distribution type (Assigned or Dynamic) that the device belongs to:** the deployment ring with Assigned distribution takes precedence over the one with the Dynamic distribution type.
- Checks for deployment ring ordering when device belongs to one or more deployment ring with the same distribution type (Assigned or Dynamic): For example, if a device is part of one deployment ring with Assigned distribution (Test), and in another deployment ring with Assigned distribution (Ring3) within the same Autopatch group, the deployment ring that comes later (Ring3) takes precedence over the deployment ring that comes earlier (Test) in the deployment ring order.
- For more information, please visit Manage Windows Autopatch groups
-

11. HoloLens 2 Device Enrolment

This section covers the steps Intune LAs should follow to enrol any HoloLens 2 device onto Intune via Autopilot.

Specifically, this section will cover:

- Hardware and software requirements.
- How to obtain a HoloLens 2 hardware hash.
- How to register HoloLens 2 devices in Intune.
- How to manage a HoloLens 2 device in Intune.
- How to access support with the HoloLens 2 Remote Assist app.

11.1 Hardware and Software Requirements

Prior to enrolling any HoloLens 2 devices onto Intune, the following minimum device and software specifications should be validated.

Device and software requirements:

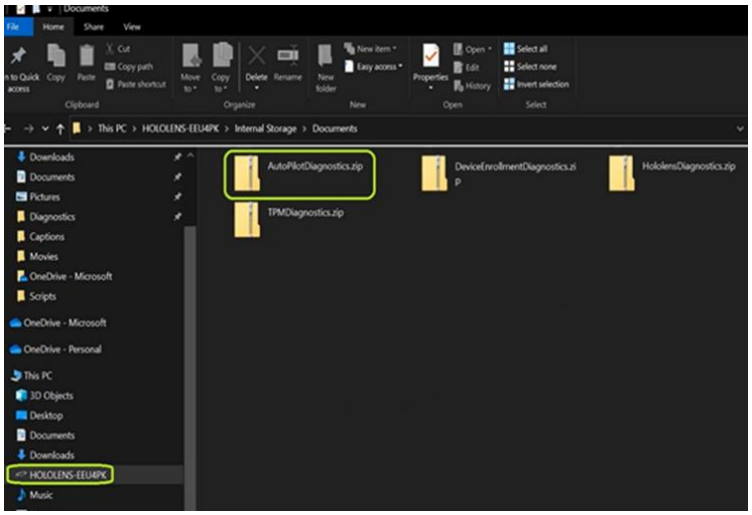
- HoloLens 2 device running the Windows Holographic build version 20H2.
- An internet connection of at least of 1.5 mbps bandwidth is recommended.

11.2 Obtaining HoloLens 2 Hardware Hashes

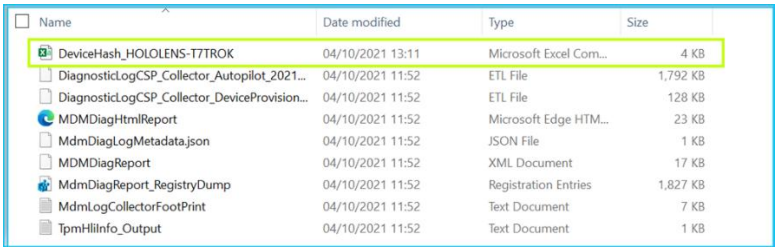
Please follow the steps below to manual obtain the hardware hash of your HoloLens 2 device:

1. Start the HoloLens 2 device and press **Power and Volume Down** at the same time and then release them. The device collects diagnostic logs and the hardware hash and store them in a .zip files.

2. Connect the device to a computer using a USB-C cable. On the computer, open **File Explorer**. Open, This **PC\<HoloLens device name>\Internal Storage\Documents** and locate the **AutopilotDiagnostics**.zip file.



3. Next, extract the contents of the AutopilotDiagnostics.zip file.
4. In the extracted files, locate the .CSV file that has a file name prefix of **DeviceHash**. Copy that file to a drive on the computer where you will be able to access it later.



5. If the Internal Storage folder does not show up, the device is waiting for a user to sign in. Either **sign-in** (AAD account) or **power cycle** the device by holding the **Power** button down for 10 seconds.
6. Press and immediately release the **Power + Volume Down** buttons together.
7. Wait a minute for the device to prepare the zip archives.

8. Refresh file explorer and navigate to the '**\Documents**' folder.

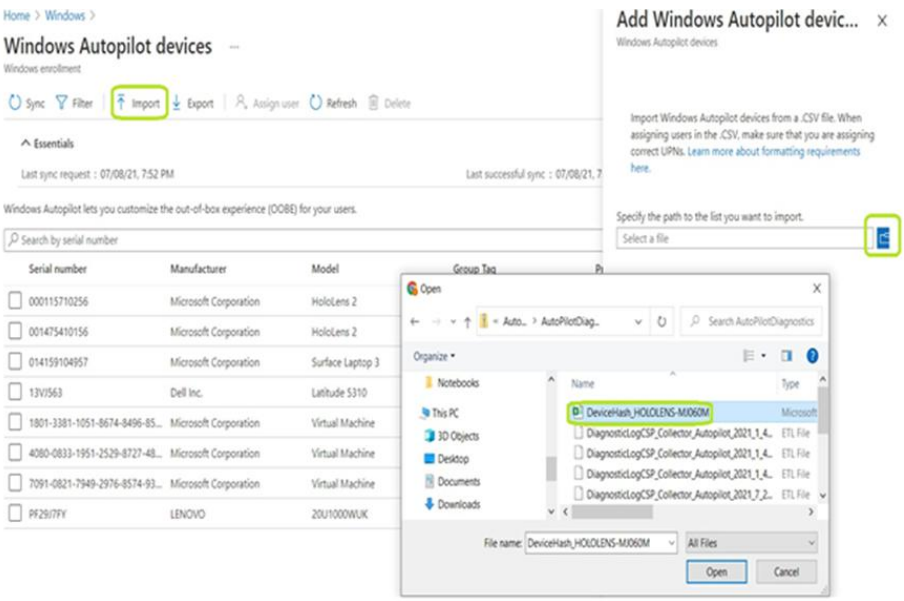
11.3 Register HoloLens 2 Device Through Intune

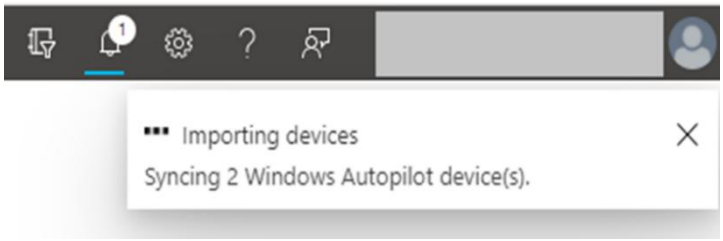
Once you have obtained the HoloLens 2 device hash, you will then need to register the device through Intune. Please follow the steps outlined below to complete this.

You will be adding Autopilot devices to this group – **ODS-Intune-Hololens2-**Devices. Autopilot devices that aren't yet enrolled are listed by using the device serial number as the device name.

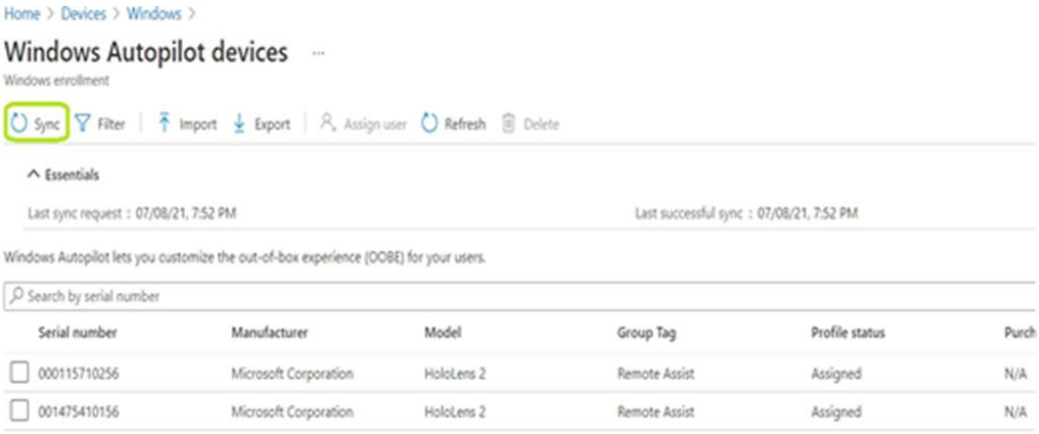
!	**Important Note** You can add a Group Tag to the DeviceHash CSV file. To do this: **Edit the file > In column D enter Group Tag as a header**. The format of the Group Tag is ODS_HoloLens2 e.g., RXL_HoloLens2. The device will be added automatically to the correspondent **ODS-Intune-Hololens2-Devices** group. See file example in the Appendix for further details.

1. In the Intune, select **Devices > Windows > Windows Enrolment**, and then select **Devices > Import** under **Windows Autopilot Deployment Program**.
2. Under **Add Windows Autopilot devices**, select **the DeviceHash CSV file**, select **Open**, and then select **Import**.



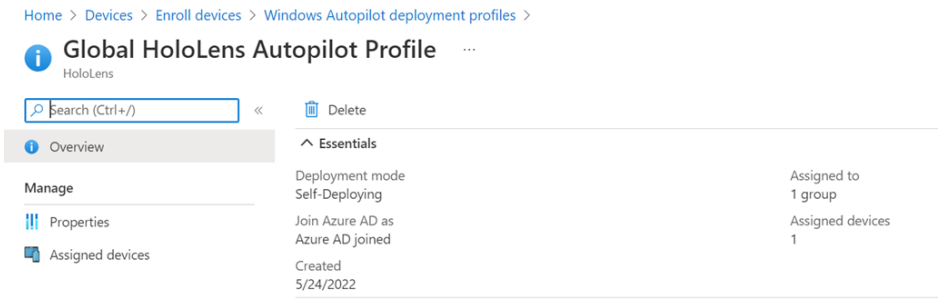


3. After the import finishes, select **Devices > Windows > Windows enrolment > Devices > Sync**. The process might take a few minutes to complete, depending on how many devices are being synchronized. To see the registered device, select **Refresh**.



11.4 HoloLens 2 Enrolment Process

There is a Global Autopilot profile setup for HoloLens 2 devices in Intune. Once the hardware hash has been imported, the device will be added automatically to the Dynamic group that contain all the HoloLens 2 devices to be enrolled in Intune.



!	**Important Note** Global HoloLens Autopilot Profile is not editable by Intune LAs.

15 minutes after importing the device into Intune and adding to a device group, Autopilot can be initiated on the device.

The HoloLens 2 Autopilot experience requires internet access. Please use one of following options to provide internet access:

1. Connect your device to a Wi-Fi network in the out-of-box experience (OOBE) and then let it detect Autopilot experience automatically. This is the only time the user needs to interact with OOBE until Autopilot experience completes on its own. Please note that by default, HoloLens 2 waits for 10 seconds to detect Autopilot after detecting an internet connection. If no Autopilot profile is detected within 10 seconds, OOBE will present the End-User licence agreement (EULA). As a work around, please reboot your device so another attempt can be made to detect Autopilot.

!	**Important Note** If Autopilot is not detected after several attempts, delete the hardware hash from Intune, then import it again without the Group Tag information. Once uploaded, you can add the Group Tag manually from Windows Autopilot device's view.

2. Connect your device with Ethernet using "USB-C to Ethernet" adapters for wired internet connectivity and allow HoloLens 2 to complete the Autopilot experience automatically.
3. Connect your device with "USB-C to Wi-Fi" adapters for wireless internet connectivity and let HoloLens 2 complete the Autopilot experience automatically.

!	**Important Note** Please note that by default, HoloLens 2 waits for 10 seconds to detect Autopilot after detecting an internet connection. If no Autopilot profile is detected within 10 seconds, OOBE will present the End-User licence agreement (EULA). As a work around, please reboot your device so another attempt can be made to detect Autopilot. Devices attempting to use Wi-Fi networks in OOBE for Autopilot must be on Windows Holographic, build version 20H2.

The device should automatically start the OOBE. Do not interact with OOBE. Let the HoloLens 2 device detect network connectivity and allow it to complete OOBE automatically. The device may restart during OOBE.

Please refer to the End User Guide, please refer to this link > NHSmail Intune Service | HoloLens 2 Quick Start End User Guide – NHSmail Support

!	**Important Note** If you experience issues connecting your HoloLens 2 device to your local network, please contact your Network team to confirm the configurations requirement in place. Please visit Connect HoloLens 2 to a network documentation.

11.5 HoloLens 2 Device Ownership

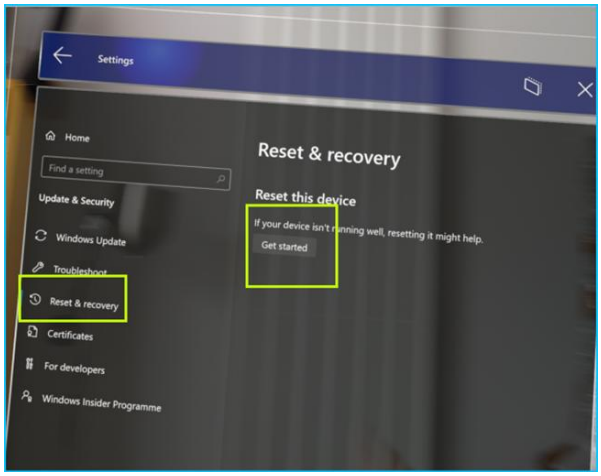
It is not possible to have multiple admins, and technically there is not a device admin. The first account that registers on the HoloLens during the Autopilot process becomes the device owner. The only difference between this user and other users if that the device owner can delete other accounts if needed.

11.6 HoloLens 2 Device Management

If a HoloLens 2 device was enrolled with an Azure AD account or Autopilot, it cannot be unenrolled from Intune. To unjoin HoloLens 2 from Azure AD or re-join it to a different to Azure AD tenant, the HoloLens 2 device must be **reset** or **reflashed**. Any HoloLens 2 devices joined to another tenant needs to be un-enrolled ahead of being enrolled again in the NHSmail central tenant. There are several ways to do this. If this applies to any devices in your organisation, please follow the steps below:

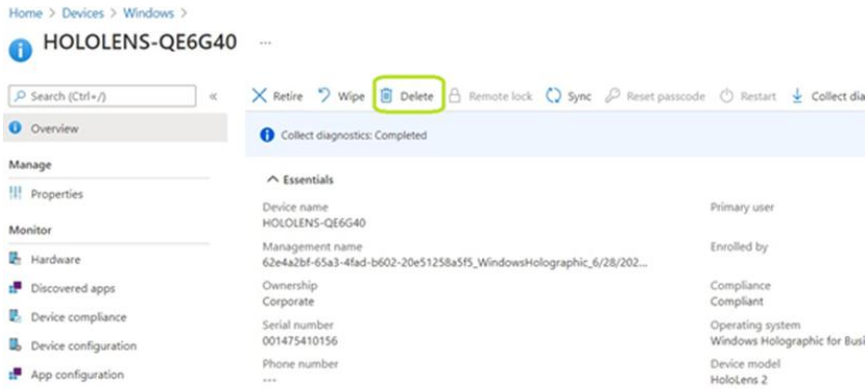
11.7 Resetting HoloLens 2 Manually

1. Reset the device manually from HoloLens 2 by turning on the device and navigating to **Start Menu > Settings > Update & Security > Troubleshoot > Reset device**.



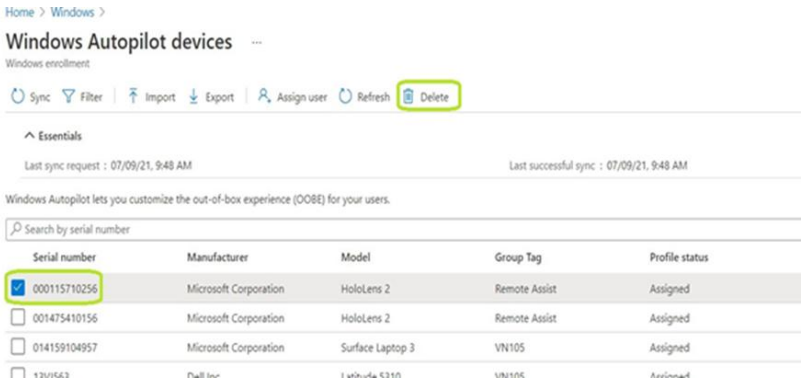
11.8 Deleting the Intune Device Object

1. From Admin Centre Tenant Administration navigate to **Devices> Windows devices > Select 'device name'** and then click on **Delete**.



11.9 Removing the Device from Autopilot Enrolment

1. From Admin Centre Tenant Administration navigate to **Devices > Windows devices > Windows enrolment > Devices > Select 'device'** and then click on **Delete**.



11.10 HoloLens 2 Remote Assist

Once you have successfully enrolled a HoloLens 2 device into Intune and providing you have the correct licensing in place, Intune LAs should be able to use the Remote Assist app.

For guidance documentation which provides more details on how to get started using this app please refer to these links:

- **Dynamics 365 Remote Assist and HoloLens 2**
  https://support.nhs.net/knowledge-base/dynamics-365-remote-assist-and-hololens2/
- **Dynamics 365 Remote Assist and HoloLens 2 scope and support**
  https://support.nhs.net/knowledge-base/dynamics-365-remote-assist-and-hololens-2-scope-and-support/
- **Dynamics 365 Remote Assist licencing**
  https://support.nhs.net/knowledge-base/dynamics-365-remote-assist-licencing/
- **Integration with M365 Core Products**
  https://support.nhs.net/knowledge-base/integration-with-m365-core-products/

- **NHSmail and Multi-Tenant Collaboration**
  https://support.nhs.net/knowledge-base/nhsmail-and-multi-tenant-collaboration/

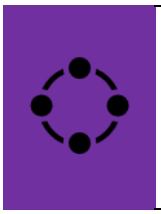
HoloLens 2 and Dynamics 365 Remote Assist Training and Key References
https://support.nhs.net/knowledge-base/hololens-2-and-dynamics-365-remote-assist-training-and-key-references/

12. NCSC – CIS NHSmail Intune Baselines

The NHSmail Intune Tenant offers a set of Configuration Profiles based on the Security Framework from the Center for Internet Security (CIS) and National Cyber Security Centre (NCSC). Intune LAs can utilize the Baselining policies to support accreditation efforts towards the UK Government Cyber or Cyber Essentials Plus certifications. These policies are focused on device security.

The policies represent an extended Centralised Baseline available to all onboarded organisations. Similar to the Centralised Configuration Profiles, onboarded organisations can make use of them as required by assignment.

Alternately, Intune LAs can use the device configuration profiles as a template and assign Azure AD group for testing purposes before rolling out to their own organisation or creating their own custom device configurations.



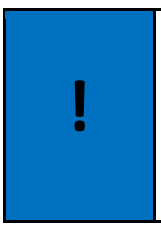
Managed Centrally

NCSC – CIS NHSmail Intune baselines are configured centrally. Intune LAs are able to assign/unassign to their scoped security groups only.

Windows 10/11 NCSC baseline complements the existing Intune Global Microsoft Security baselines. For Android and iOS devices, CIS provide alternatives baselines.

The policies available in the Intune NHSMail Tenant are the following:

- **NCSC - CIS Google Android device restriction**
- **NCSC - CIS iPhone/iPadOS device restriction**
- **NCSC - Windows 10/11 Baseline collection**: This is a set of policies that contain Configuration profiles created for Windows 10/11 devices based on the NSCS benchmarks.



Important Note

CIS baseline for Windows 10/11 devices is deemed too restrictive for most organisations and CyberEssentials assessment is formally supported by NCSC baselines.

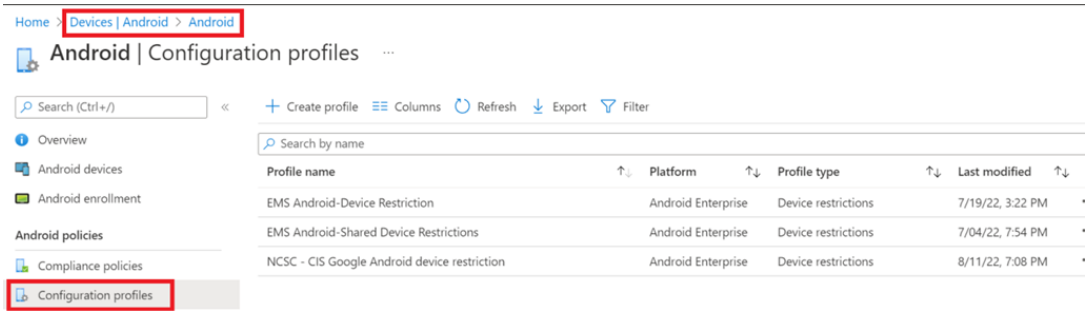
12.1 NCSC – CIS Google Android Device Restriction

This benchmark provides prescriptive guidance for establishing a secure configuration posture for the Google Android OS. This guide was tested against the Android 11.0.0 OS. This benchmark covers Android 11.0.x and all hardware devices on which this OS is supported.

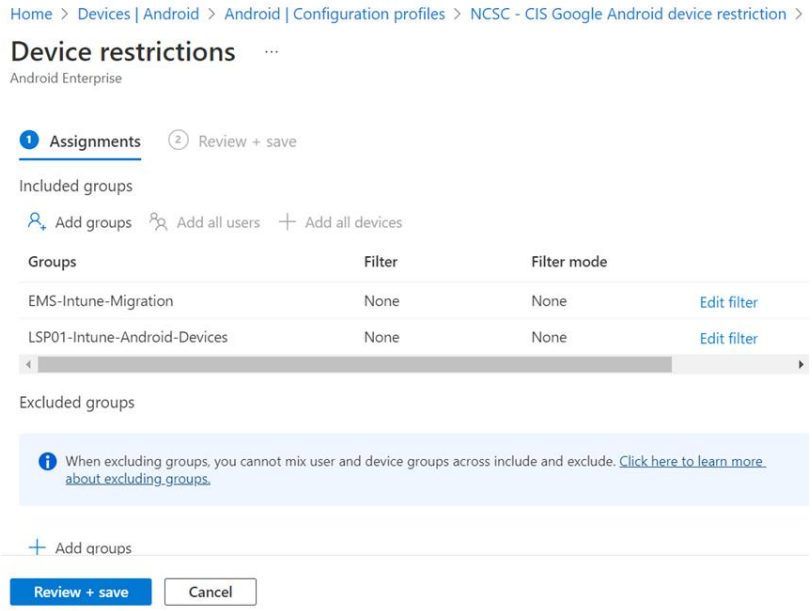
To see detailed settings for this policy, please refer to the Appendix in this document.

Intune LAs can assign this Configuration following these steps:

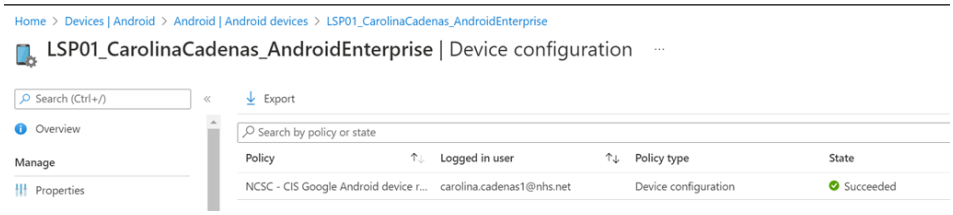
1. Sign in to https://endpoint.microsoft.com/
2. Navigate to Devices > Android > Configuration Profiles



3. Select NCSC - CIS Google Android device restriction
4. Navigate to Assignments and click on “Edit”
5. Select Add groups and search for a group to target this policy > Select
6. Select Review + Save > Save to accept the changes



7. Select an Android device targeted to the above device configuration profile and check if the policy has been applied successfully



Important Note

If there are conflicts with another device configurations, we recommend verifying if the device / user azure AD group is assigned to one or more policy.

12.2 NCSC – CIS iPhone/iPadOS Device Restrictions

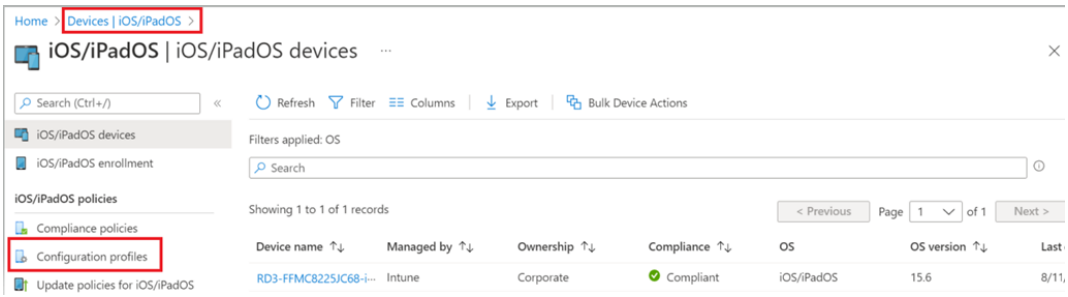
This benchmark is a guidance for corporate devices. This benchmark covers the Apple iOS 14 and iPadOS 14 on all supported devices. As of the publication of this guidance, devices supported by iOS 14 or iPadOS 14.

To see detailed settings for this policy, please refer to the Appendix in this document.

Intune LAs can assign this Configuration following these steps:

1 Sign in to https://endpoint.microsoft.com/

2 Navigate to Devices > iOS/iPadOS > Configuration Profiles

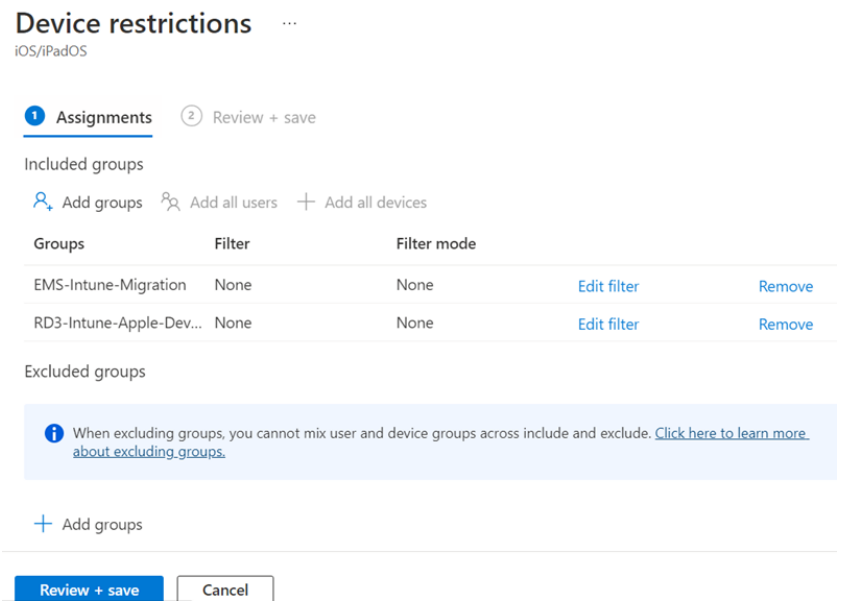


3 Select NCSC - CIS iPhone/iPadOS device restrictions

4 Navigate to Assignments and click on “Edit”

5 Select Add groups and search for a group to target this policy > Select

6 Select Review + Save > Save to accept the changes



7 Select an iPhone/iPadOS device targeted to the above device configuration profile and check if the policy has been applied successfully

!	**Important Note** If there are conflicts with another device configuration, we recommend verifying if the device / user azure AD group is assigned to one or more policy.

12.3 NCSC - Windows 10/11 Baseline Configurations

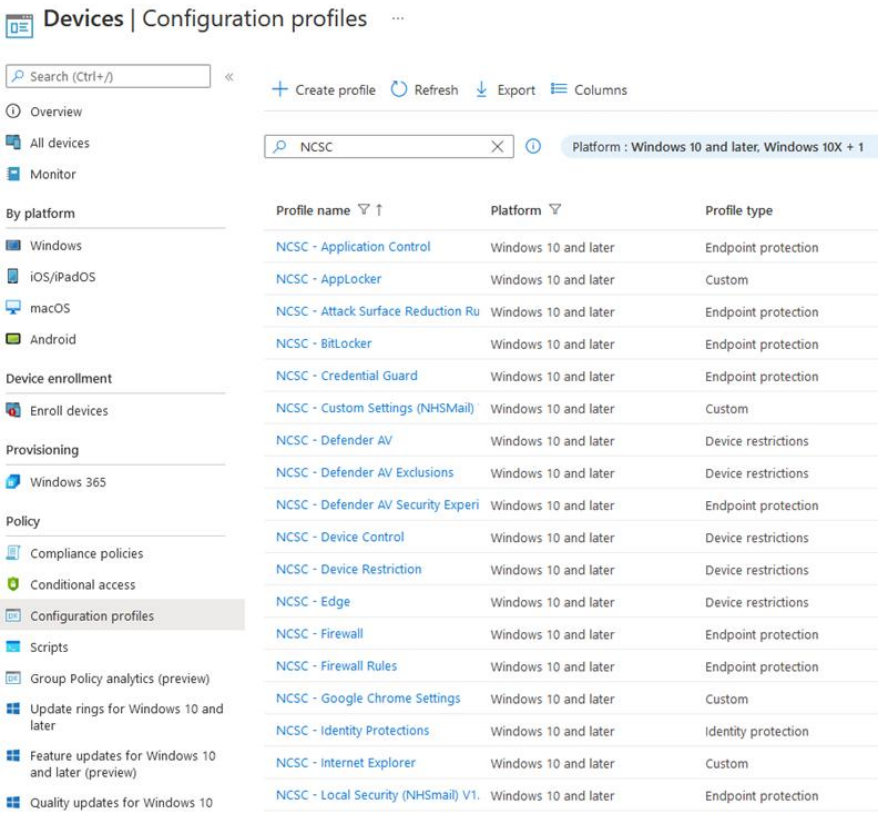
The Windows 10 (and later) NCSC policies are provided to be assigned by Local Administrators either in conjunction with existing central configuration baselines or individually as an NCSC 'baseline'.

The following configurations are available within the tenant for baselining / assignment:

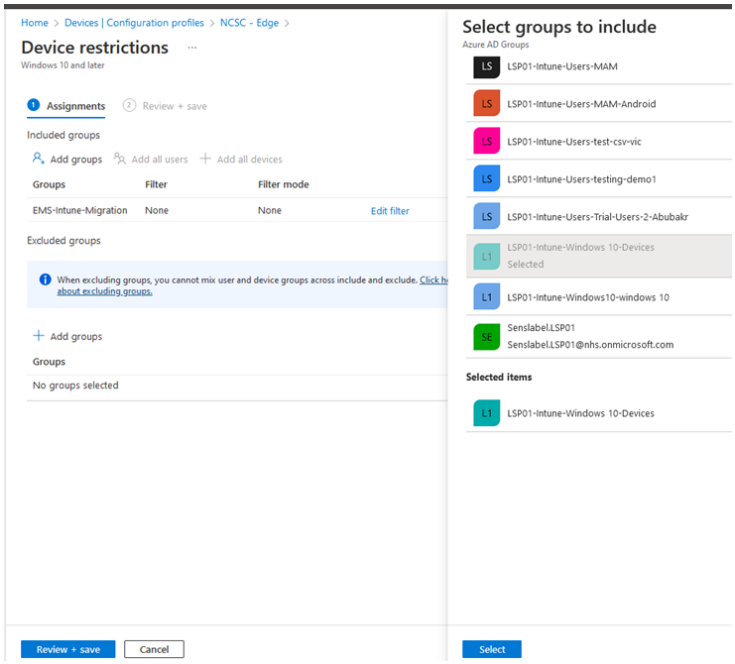
Profile name	Description	Profile type
NCSC - Application Control	Application Access control	Endpoint protection
NCSC - AppLocker	AppLocker helps defend against malware and ransomware attacks	Custom
NCSC - Attack Surface Reduction Rules	Applies configurations to improve attack surface area posture	Endpoint protection
NCSC - BitLocker	Provides configuration to apply NCSC settings for device encryption	Endpoint protection
NCSC - Credential Guard	Configuration settings for domain credentials protection	Endpoint protection

Profile name	Description	Profile type
NCSC - Custom Settings (NHSMail) V1.0	Custom settings for security configuration	Custom
NCSC - Defender AV	Configures settings and behaviours for Antivirus	Device restrictions
NCSC - Defender AV Exclusions	Defines some exclusions for AV	Device restrictions
NCSC - Defender AV Security Experience	Defines the icons available in the security centre for AV	Endpoint protection
NCSC - Device Control	Device control restrictions	Device restrictions
NCSC - Device Restriction	Device Restrictions	Device restrictions
NCSC - Edge	Configures Edge security settings	Device restrictions
NCSC - Firewall	Configures firewall behaviours	Endpoint protection
NCSC - Firewall Rules	Applies firewall rules	Endpoint protection
NCSC - Google Chrome Settings	Applies Chrome security settings	Custom
NCSC - Identity Protections	Configures IDP settings	Identity protection
NCSC - Internet Explorer	Configures IE security settings	Custom
NCSC - Local Security (NHSmail) V1.0	Configures local security behaviours including UAC	Endpoint protection
NCSC - Password	Provides password policy for devices	Device restrictions
NCSC - Web Protections (DR)	Web protection settings for Device	Device restrictions
NCSC - Web Protections (EP)	Web protection settings for Device Web endpoint protection	Endpoint protection
NCSC - Xbox Services	Secures configuration for Xbox gaming services	Endpoint protection

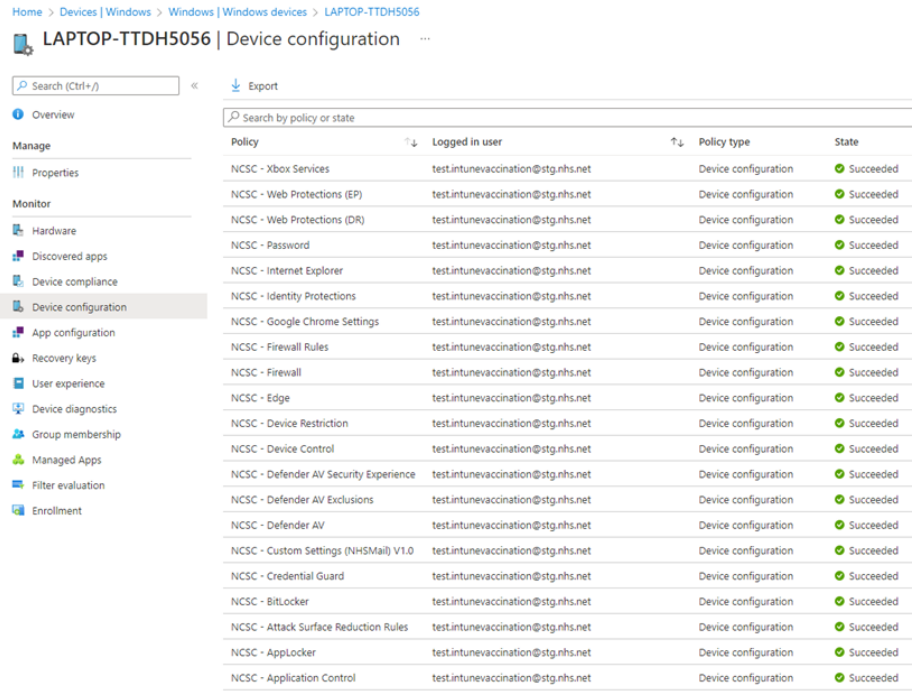
These policies can be assigned en-masse to devices to provide a security baseline to support Cyber Essentials accreditation requirements. To assign the policies, navigate to Configuration Profiles in Intune:



In assignments for the policies, add device groups that you would like to assign (some or all) of the configuration profiles to:



NCSC Configuration successfully applied can be viewed on the Windows Device blade for the resource:



13. Co-Management

Co-management enables NHSmail Intune organisations to concurrently manage Windows 10/11 using both Configuration Manager and Microsoft Intune. It allows organisations cloud-attach existing investment in Configuration Manager by adding new functionality.

For further information please refer to the Cloud + SSO and Hybrid Tracks Guidance Material (Intune LAs).

14. Certificate and Connector Services for Intune

Organisations can use Certificates with Intune to authenticate users into Applications and corporate resources in the organisation.

For further information please refer to the Cloud + SSO and Hybrid Tracks Guidance Material (Intune LAs).

14.1 Microsoft Tunnel

MS Tunnel is a VPN feature for Mobile Devices managed by Intune. It provides remote connection to on-premises resources from the Defender for Endpoint Client on Android and Apple devices.

The setup requirements for MS Tunnel are extensive and rely largely on Local Organisation's posture for Remote access infrastructure and Certificate Authorities.

As such, the LA guide for NHSMail cannot accommodate the full scenarios for administering and configuring the MS Tunnel feature, the Intune LA should follow the below Microsoft Documentation steps to setup Microsoft Tunnel in Intune:

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

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

Additional Live Service support may be required to add instances to the tenant from Local Organisation Linux Administration resources.

To complete the MS Tunnel configuration, Organizations should raise a Service Request with the Intune Live Support Team only when Linux On-premises Tunnel prerequisites have been met.

Local Administrators can view and manage Tunnel Sites and servers with the provided RBAC ‘Read’ and ‘Update’ permissions.

!	**Note:** Local Organisations would be entirely responsible for Tunnel Server configurations (Linux, on premises), including VPN and Certificate renewal processes.

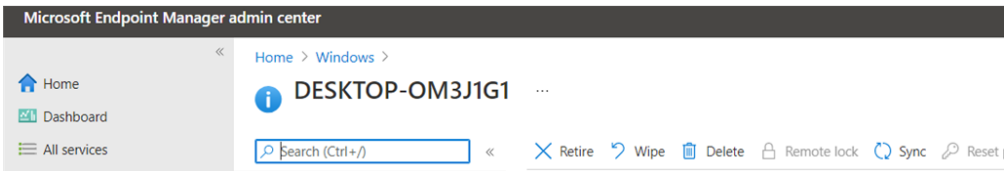
15. User Offboarding

In addition to the different methods of wiping and resetting devices, it is important that Intune LAs who will be managing devices via NHSmail Intune understand what is required when an end user leaves an organisation, and therefore leaves their Intune-enrolled device.

When end users leave an organisation, Intune LAs are required to complete the below actions to ensure that their device is available for further ruse by other end users:

Firstly, Intune LAs will need to wipe the device/devices associated with that user:

1. Log into Microsoft Intune admin center.
2. **Devices** > select the relevant platform (iOS, Android or Windows 10/11) > Search and select the relevant device > Select **Wipe**.



This will set the device back to its factory settings.

Once the device has been wiped, Intune LAs will need to unassign the licences from the end user. Please see this link for further details on unassigning licences from end users: https://support.nhs.net/knowledge-base/marking-an-nhsmail-office-365-hybrid-user-as-a-leaver/

16. Offboarding Process

Organisations have the option to offboard from the NHSmail Intune service.

Intune LAs will need to raise a service request via Helpdesk Self-Service (option: request to offboard an organisation) if they wish to offboard their organisation from the NHSmail Intune service.

Given the finality of the action, the service request to offboard an organisation does require evidence of secondary sign-off from a senior member of the IT Leadership Team within your organisation to be attached.

Once an Intune LA has submitted the service request to offboard their organisation, the Intune Live Service Team will contact Intune LAs at the organisation to support with completing the offboarding.

The time required to offboard an organisation from the NHSmail Intune Service will vary depending on several factors, including (but not limited to); the number of devices enrolled, and the types of devices enrolled.

Recommendation / Recommended Use

If an organisation wishes to offboard from the NHSmail Intune Service, it is strongly recommended that the organisation has plans in place to enrol all devices onto another MDM solution to ensure the continued security of devices.

17. Feedback and Comments

If you have any feedback on this guide, including but not limited to suggestions of topics, steps or notes that you believe should be added or if you think there is an error in this document or even if you would like to drop a note about the service you have received from the team, we'd be grateful if you could send your feedback to feedback@nhs.net.

18. Appendix

18.1 Device Configuration Profile for iOS/iPadOS and Android

For the list of policy settings for iOS/iPadOS and Android which are part of the Centralised Configuration profiles, please see the below document:

Please note: This document does not contain an exhaustive list of policies in Intune. Please refer to the Microsoft Documentation https://docs.microsoft.com/en-us/mem/intune/configuration/

NHSmail%20Intune _iOS%20and%20And

18.2 Windows 10/11 Security Baseline Settings

For the full list of Windows 10/11 Security Baseline settings, please see the below document:

NHSmail%20Intune %20Win10%20Secur

18.3 HoloLens 2 Hardware Hash

HoloLens 2 Hardware Hash example file:

DeviceHash_HOLOLE NS-T7TROK.csv