



# NHSmail Intune Service

## Session 2: Intune Demo

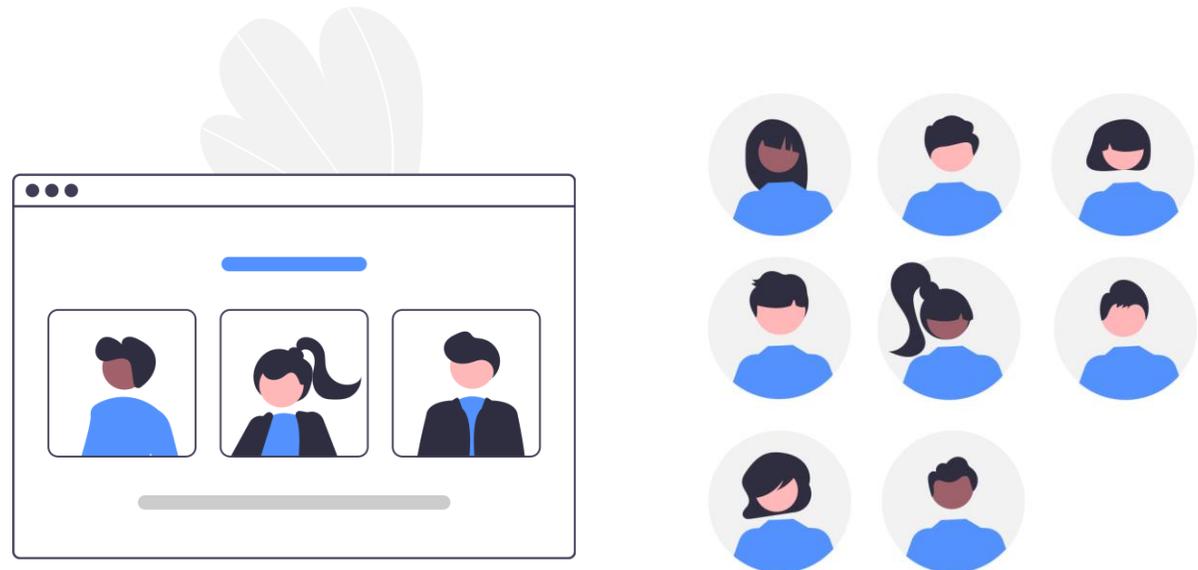
10<sup>th</sup> January 2022



# Upskilling Series | Housekeeping

Event name:	Session 2: Intune Demo
Date:	10 January 2021
Location:	Online Webinar
Start / end time:	14:30-15:15
Attendees:	NHSmal Intune Team and LAs from January onboarding organisations
Objectives & purpose:	To provide an overview of the key areas of the Intune Portal.
End goal:	Attendees understand more about how to access Intune and key tabs / areas of the Portal they will need to use when getting started.

Housekeeping
<ul style="list-style-type: none"><li>• As this is a webinar, all attendees, other than the presenters will be on mute during the event.</li><li>• There will be a question and answer section at the end of the session, time permitting. If you wish to ask a question during one of these, please raise your hand.</li><li>• Any questions submitted in the chat which we don't have time to answer in the session will be answered via follow-up email after the session where appropriate.</li><li>• Information outlined in <b>red</b> indicates key information.</li></ul>



# Upskilling Series | Sessions

An overview of the NHSmail Intune upskilling series, created to support organisations to onboard to NHSmail Intune



17 sessions over 4 weeks



All sessions are optional



Recordings and session materials available



Suggested further reading & resources



Supported upskilling

KEY		Intune Fundamentals	Onboarding + Support Basics	Mobile Devices	Windows 10	HoloLens 2	MAM	Intune Advanced
Week	Date	Focus	Session Title	Session Content	Duration	Session Audience	Preparations prior to session	Target Audience
1	10/01	Intune Fundamentals	Introductory Session	Pre-requisites, licencing, how to get started using NHSmail Intune	1 hour	All organisations	None required	All LAs
	10/01		Intune Demo	Demo of the key sections of the Intune portal	45 minutes	All organisations	None required	LAs who have never used Intune or are beginners
	11/01		RBAC and Security Baselines	Overview of the custom RBAC permissions and security baselines set up for the NHSmail Intune	45 minutes	All organisations	None required	All LAs
	11/01		Intune Features and Group Management App	Session exploring the specific features of NHSmail Intune and a demo of the Security Group Management App	1 hour	All organisations	None required	All LAs
1	12/01	Onboarding and Support Basics	Support Model / Raising a ticket	Overview of the NHSmail Intune Support Model and how to raise a ticket via Helpdesk Self-Service	1 hour	All organisations	None required	All LAs
	12/01		Documentation Walkthroughs	Orientation and walkthrough of the key supporting documentation available to all onboarded organisations	30 minutes	All organisations	None required	All LAs
	13/01	Mobile Devices	Android Deep Dive	Deep dive session focused on managing Android devices on NHSmail Intune	1 hour	Organisations with Android devices	None required	LAs who will be enrolling and managing Android devices on NHSmail Intune
	13/01		iOS Deep Dive	Deep dive session focused on managing iOS/iPadOS devices on NHSmail Intune	1 hour	Organisations with iOS devices	None required	LAs who will be enrolling and managing iOS devices on NHSmail Intune
2	17/01	Windows 10, HoloLens 2 & MAM	Windows 10 Deep Dive	Deep dive session focused on managing Windows 10 devices on NHSmail Intune and preparations required for the Hybrid-Join feature	1 hour	Organisations with Windows 10 devices	None required	LAs who will be enrolling and managing Windows 10 devices on NHSmail Intune
	18/01		HoloLens 2 Deep Dive	Deep dive session focused on managing HoloLens 2 devices on NHSmail Intune	30 minutes	Organisations with HoloLens 2 devices	None required	LAs who will be enrolling and managing HoloLens 2 devices on NHSmail Intune
	19/01		Mobile Application Management (MAM) Overview	Overview of MAM policies on NHSmail Intune and how to use them	1 hour	All organisations	None required	LAs wishing to deploy Mobile Application Management policies to devices
2	20/01	Intune Advanced	Co-Management and Certificate Services	Overview of the co-management and certs. connector feature on NHSmail Intune	1 hour	Organisations with co-management / SCCM requirements	None required	LAs from organisations requiring co-management and / or certificate connectors
3	24/01	Supported Enrolments	Supported Device Enrolment Session (Android)	Guided enrolment session with Q & A	1 hour	Organisations with Android devices	EMS licences assigned, organisation technically onboarded and access to the Intune portal	LAs who will be enrolling and managing Android devices on NHSmail Intune
	25/01		Supported Device Enrolment Session (iOS/iPadOS)	Guided enrolment session with Q & A	1 hour	Organisations with iOS devices	EMS licences assigned, technically onboarded, access to the Intune portal, ABM link complete and VPP token added	LAs who will be enrolling and managing iOS devices on NHSmail Intune
	26/01		Supported Device Enrolment Session (Windows 10 - Azure AD-joined only)	Guided enrolment session with Q & A	1 hour	Organisations with Windows 10 devices	EMS licences assigned, organisation technically onboarded and access to the Intune portal	LAs who will be enrolling and managing Windows 10 devices on NHSmail Intune
	27/01		Supported Device Enrolment Session (HoloLens 2)	Guided enrolment session with Q & A	1 hour	Organisations with HoloLens 2 devices	EMS licences assigned, organisation technically onboarded and access to the Intune portal	LAs who will be enrolling and managing HoloLens 2 devices on NHSmail Intune
4	31/01	Intune Advanced	Windows Hybrid-Join Overview	A look ahead to the upcoming Windows Hybrid-Join feature on NHSmail Intune	30 minutes	All organisations	None required	LAs from organisations interested in enrolling Win 10 devices with access to both cloud and on-premises resources

January organisations can register to attend any of these sessions by signing up on the [January 2022 NHSmail Intune Upskilling page](#).

# Agenda

Session 2: Intune Demo

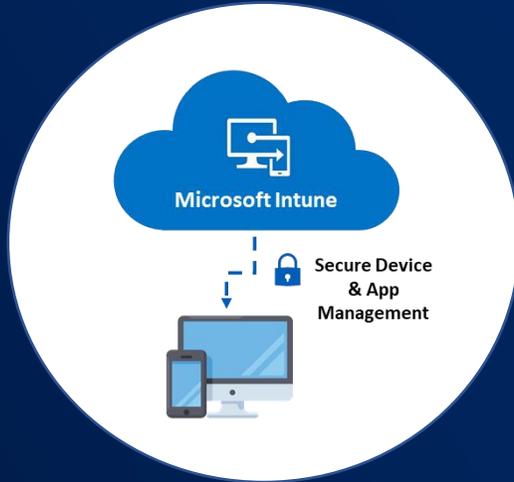
**01** Intune Portal Overview

**02** Intune Demo

- Enrolment
- Wiping and Removing Devices
- Device Overview and Apps
- Configuration Profiles
- Compliance Policies
- RBAC Roles
- Scope Tags
- Monitoring

**03** Questions and Close

# Session 2



## Intune Demo

### Overview & Objectives



#### Overview

- As a result of organisations having the opportunity to purchase EMS E3 and AADP2 licenses, Intune for Mobile Device Management (MDM) capabilities have been enabled, in a way that supports the shared NHSmail tenant multi-organisation model.
- The NHSmail Intune Service is a **supported live service** with the onboarding of organisations proceeding in a **phased manner**.
- An **upskilling series will be running each month** to provide onboarding organisations with the knowledge to be able to begin rolling out NHSmail Intune across their device estates.
- Session 2 will provide a **demonstration of the Intune Portal** to help those LAs who may be new or relatively new to using Intune to familiarise themselves with the Portal and the functionality available.



#### Objectives of this session

- Demonstrate key areas of the Intune Portal
- Discuss **common errors and issues** LAs tend to have when first using the Intune Portal and how to avoid these to save time
- Answer any questions on the Intune Portal and how to get started

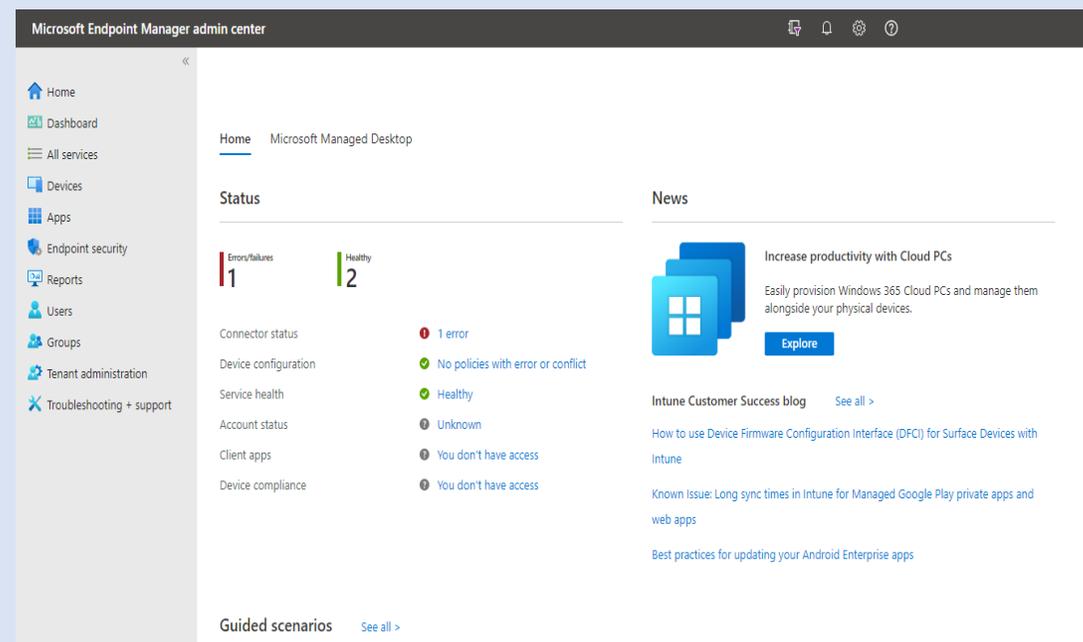
# Intune Demo | Intune Portal Overview

NHSmal Intune runs from the standard Intune Portal but there are some differences to using the Intune Portal when enrolled onto NHSmal Intune

## 1. INTUNE PORTAL

NHSmal Intune uses the standard Intune Portal - also referred to as Endpoint Manager - to allow LAs to complete most enrolment and management tasks associated with device management, **except for Group Management**.

All LAs with RBAC permissions should have the following URL bookmarked: <https://endpoint.microsoft.com>



## 2. SECURITY GROUP MANAGEMENT APP

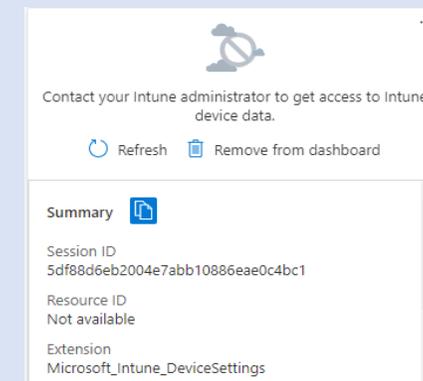
Organisations onboarded to NHSmal Intune are unable to complete Group Management tasks such as creating, viewing and editing Groups via the Intune Portal. Instead a **specific Security Group Management Application** has been created, which all LAs with RBAC permissions will be able to access and use.



## 3. EMS E3 & AADP2 LICENCE ASSIGNMENT

To be able to use all the functionality of the Intune Portal (which is available to NHSmal Intune organisations) **all LAs with RBAC permissions will need to have a EMS E3 licence assigned correctly**. Failure to do this will result in permissions errors.

For guidance on how assign licences correctly, please see [here](#).



Attempting to complete Group Management tasks natively via the Intune Portal and not correctly assigning licences are the most common causes of early tickets among onboarded organisations.

# DEMO

Intune Portal



# Intune Demo | Demo Roadmap

Intune Demo journey including key requirements which should be in place to allow LAs to explore the Intune Portal fully

To demonstrate what LAs can see, do and access when onboarded onto NHSmail Intune, this demo will cover the following key areas of the Intune Portal. All LAs who are enrolling and managing devices on NHSmail Intune will need to be able to access and use these areas of the Portal.



## Intune Portal Requirements



Ensure that you can access the Intune Portal by navigating to <https://endpoint.microsoft.com>



Ensure that an EMS E3 licence has been correctly assigned to you.



Ensure that you are logged into the Intune Portal on your **nhs.net** account.



This demo will not cover all tabs and functionality available to LAs with RBAC permissions within the Intune Portal.

# Intune Demo | Enrolment

Overview of where to find the enrolment screens which LAs will need to use to enrol devices

**TOM**



Tom is an LA at a newly onboarded organisation.

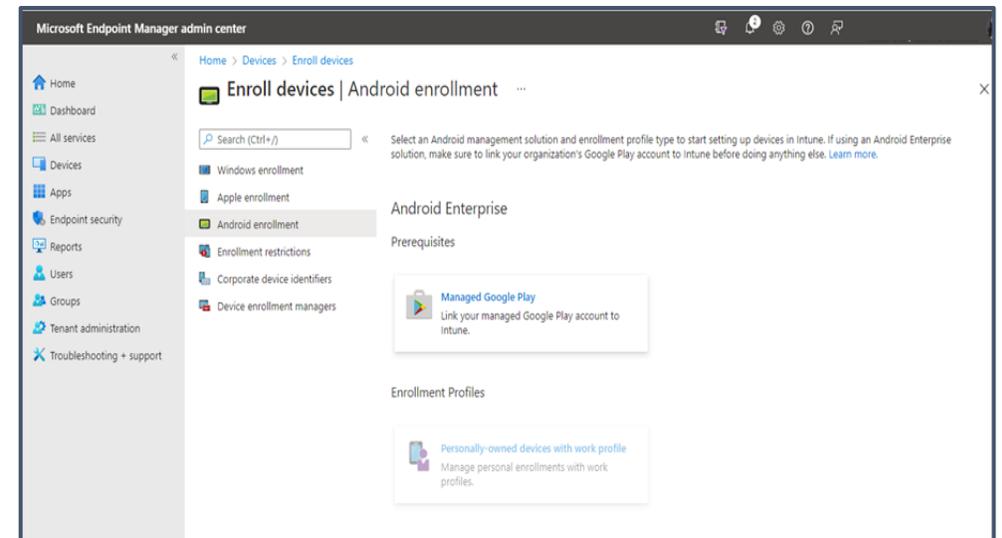
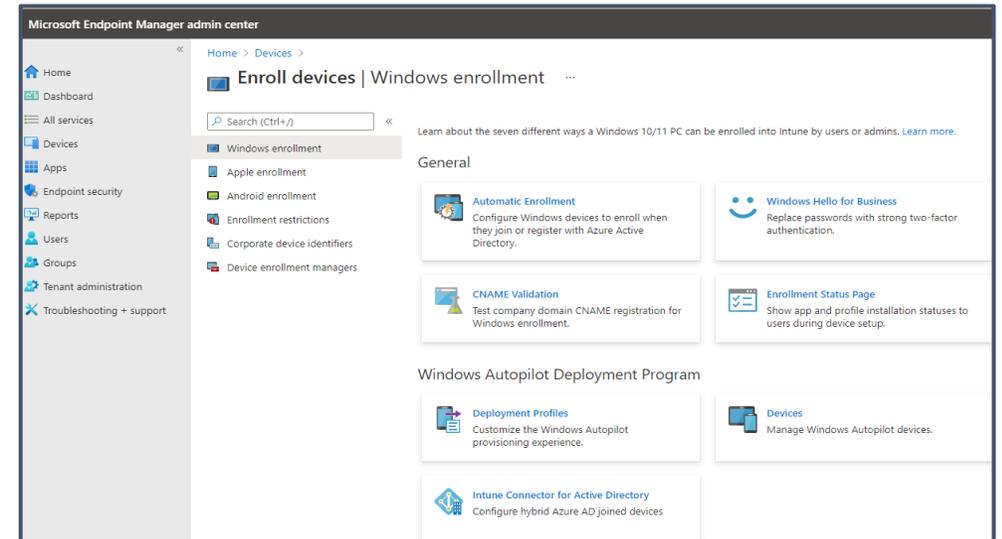
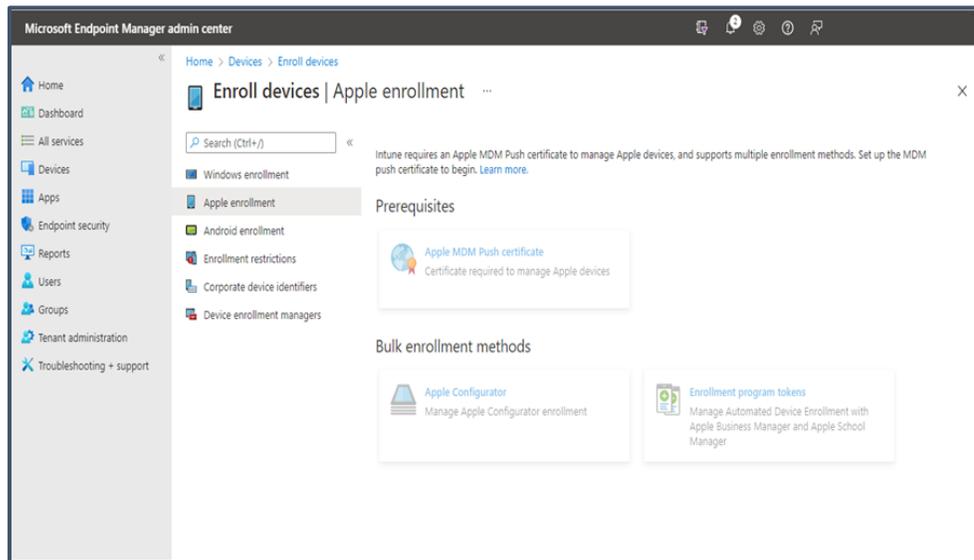
He has never accessed or used the Intune Portal before.

He will be going through some key areas of the Portal in order to familiarise himself with how to get started enrolling and managing the device estate for his organisation.

1. Tom has confirmed that he and his team have the correct EMS E3 licences assigned.

2. Tom starts by looking at the enrolment page. To do this, Tom will need to navigate to Devices > Device Enrollment > Enroll devices and then select the target platform.

3. Different enrolment options will be visible for each platform. [The Operations Guide for Local Administrators and Onboarding Mangers](#) details which enrolment method/s should be followed for each platform.



# Intune Demo | Wiping / Removing Devices

How to access and use the remote wipe, retire and delete features to manage devices on the Intune Portal

**TOM**



4. Having confirmed where he will need to start enrolling devices, Tom would now like to check what options are available on the Intune Portal for wiping and removing devices he has enrolled.

Tom's organisation's device estate changes quite often, so it will be important for him to be able to re-use devices among staff as well as wipe and remove any lost, stolen or old devices.

5. He navigates to Devices and selects a device.

6. Tom selects Wipe to factory reset the device and remove all data. After the wipe has been initiated the device will be removed from the Intune Portal.

Home > Devices > iOS/iPadOS >

## Trust1-iPhone-FFMC823AJC68 ...

Search (Ctrl+/) << X Retire ↶ Wipe 🗑️ Delete 🔒 Remote lock 🔄 Sync 🔗 Remove passcode ⏻ Restart (supervised only) 🛑 Shut down (supervised only) → Disable activation lock X Revoke Licenses ⋮

- Overview
- Manage
- Properties
- Monitor
  - Hardware
  - Discovered apps
  - Device compliance
  - Device configuration
  - App configuration
  - Endpoint security configuration
  - Recovery keys
  - Managed Apps

### Essentials

Device name	: Trust1-iPhone-FFMC823AJC68	Primary user	: TestUser01 MDMAutopilot
Management name	: 7b710154-bf63-4ce7-a5fd-2d5c4e8e2511_iPhone_6/24/2021_1:50 PM	Enrolled by	: TestUser01 MDMAutopilot
Ownership	: Corporate	Compliance	: Compliant
Serial number	: FFMC823AJC68	Operating system	: iOS
Phone number	: +447724609664	Device model	: iPhone 8

[See more](#)

### Device actions status

Action	Status	Date/Time	Error
No data			

7. For Windows 10 devices and HoloLens 2, Tom will see some additional options for wiping and resetting devices. Each option (and its implications/recommended usage) is explained in the Operations Guide for Local Administrators and Onboarding Managers.



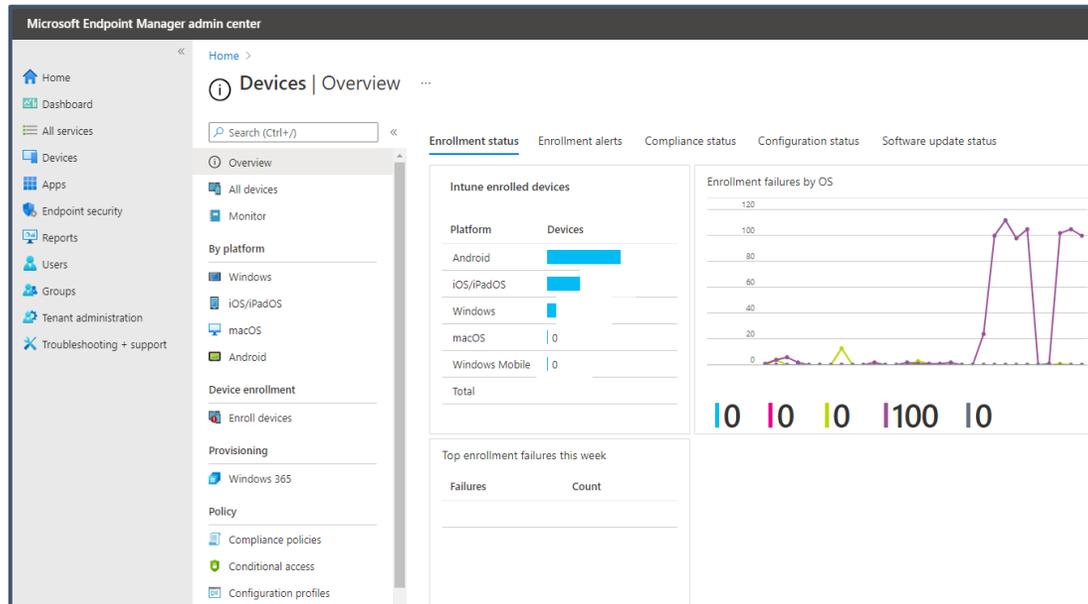
# Intune Demo | Devices and Apps

How to access an overview of devices on the platform and view applications

TOM



8. Tom would now like to take a look at the overview page which shows him how many devices are on the platform and allows him to filter for example, by device type. He navigates to Devices > Overview.

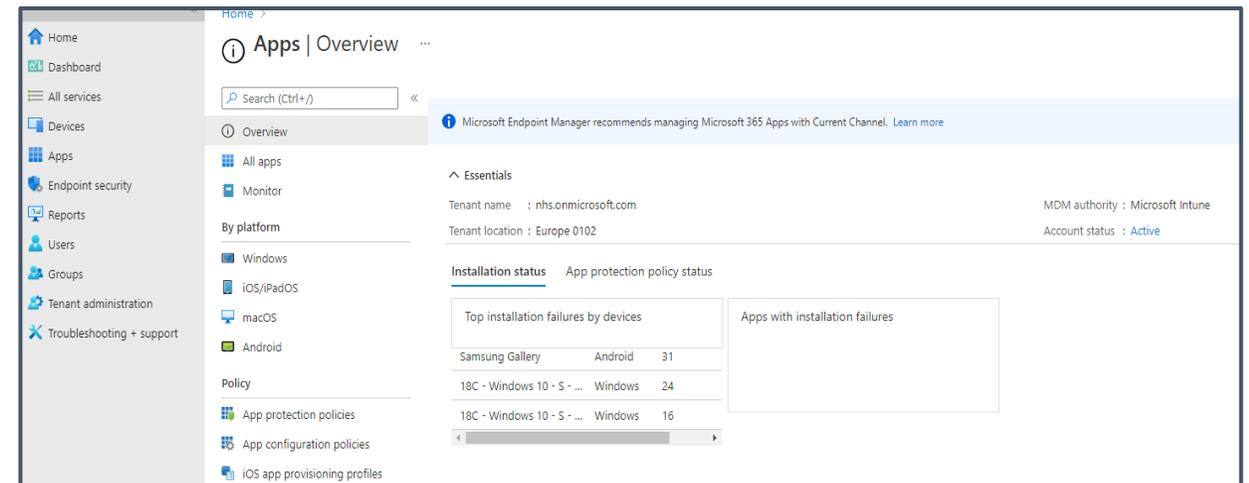


9. Tom navigates to the All devices tab to view a more detailed list of the devices enrolled at his organisation. Again, Tom is able to filter by platform type. This page only shows devices from Tom's own organisation.

The screenshot shows the 'Devices | All devices' page. It features a search bar, a refresh button, and filters for columns, export, and bulk device actions. A table lists 25 of 1,626 records. The table columns are: Device name, Managed by, Ownership, Compliance, OS, OS version, Last check-in, and Primary user UPN. The table contains various device entries with their respective details.

Device name	Managed by	Ownership	Compliance	OS	OS version	Last check-in	Primary user UPN
-iPhone-C6KX058N7...	Intune	Corporate	Compliant	iOS/iPadOS	15.1		
-iPhone-C6KX07CUXK...	Intune	Corporate	Compliant	iOS/iPadOS	15.1		
-iPhone-C6KX07VJ0XK1	Intune	Corporate	Compliant	iOS/iPadOS	15.1		
-iPhone-C6KY7063KX...	Intune	Corporate	Compliant	iOS/iPadOS	15.1		
-iPhone-C6KY72DAKX...	Intune	Corporate	Compliant	iOS/iPadOS	15.1		
-iPhone-C6PC785LN7...	Intune	Corporate	Compliant	iOS/iPadOS	15.1		
-iPhone-C6PC78J2N735	Intune	Corporate	Compliant	iOS/iPadOS	15.1		
-iPhone-C6PC7DZ2N7...	Intune	Corporate	Not Compliant	iOS/iPadOS	15.0.2		
-iPhone-DNYP98A9KX...	Intune	Corporate	Compliant	iOS/iPadOS	15.1		
-iPhone-DNPZJ22AIX...	Intune	Unknown	Not Compliant	iOS/iPadOS	14.6		
-iPhone-DNPZJ22MK...	Intune	Corporate	Compliant	iOS/iPadOS	15.1		
-iPhone-DNQC1MHR...	Intune	Corporate	Compliant	iOS/iPadOS	15.1		
-iPhone-DK35LEALH2XX	Intune	Corporate	In grace period	iOS/iPadOS	13.4		

10. He then reviews the list of applications pushed to these devices and can select one application, view its properties and assign it to a Group.



The Devices Overview is **not** customisable and all devices on the platform will be visible. For a more detailed statement on data visibility within NHSmail Intune, please refer either to Section 6 of the [NHSmail Intune Terms of Reference](#) or Section 3.1 of the [Operations Guide for Local Administrators and Onboarding Managers](#).

# Intune Demo | Configuration Profiles

How to access and set-up configuration profiles across the full range of supported device types on NHSmail Intune

**TOM**



11. Now that Tom has started to familiarise himself with the Intune Portal and tabs available, he'd like to see how he can set-up configuration profiles for all the devices which make up his organisation's device estate.
12. He navigates to Devices > iOS/iPadOS/Android/Windows 10 > Configuration Profiles.
13. He can select a profile to view details of the profile and the settings which have been configured and create new profiles.

The screenshot shows the Microsoft Endpoint Manager admin center interface. The breadcrumb navigation is 'Home > Devices > iOS/iPadOS'. The main heading is 'iOS/iPadOS | Configuration profiles'. Below the heading is a search bar and a toolbar with options: '+ Create profile', 'Columns', 'Refresh', 'Export', and 'Filter'. A table lists configuration profiles for iOS/iPadOS:

Profile name	Platform
-Apple-Shared-Device Restriction Profile	iOS/iPadOS
-iOS-Corporate-WiFi-Profile	iOS/iPadOS
-iOS-DeviceRestriction-HiddenApps	iOS/iPadOS
-iOS-NHSMail-Profile	iOS/iPadOS
-iOS-Trusted-Certificate-Profile	iOS/iPadOS
-Apple-Shared-Device Restriction Profile	iOS/iPadOS
-iPhone-Device Restriction Profile	iOS/iPadOS
-Apple-Shared-Device Restriction Profile	iOS/iPadOS

The screenshot shows the Microsoft Endpoint Manager admin center interface. The breadcrumb navigation is 'Home > Devices > Windows'. The main heading is 'Windows | Configuration profiles'. Below the heading is a search bar and a toolbar with options: '+ Create profile', 'Columns', 'Refresh', 'Export', and 'Filter'. A table lists configuration profiles for Windows:

Profile name	Platform
-Windows 10 - Google Chrome Settings	Windows 10 and later
-Windows 10 - Interactive Logon Message	Windows 10 and later
-Windows 10 - Internet Explorer 11 Settings	Windows 10 and later
-Windows 10 - One Drive Configuration	Windows 10 and later
-HoloLens 2 - Windows Hello	Windows 10 and later
-HoloLens2 - Device Restrictions - Baseline	Windows 10 and later
-HoloLens2 - Device Restrictions 2	Windows 10 and later
-HoloLens2 - Set Timezone to GMT	Windows 10 and later
- Windows 10 - Configuration Profile - ADMX 01: Edge Chromium	Windows 10 and later

The Windows 10 view also includes any HoloLens 2 devices which have been enrolled.

# Intune Demo | Compliance Policies

How to access and set-up compliance policies for devices enrolled onto NHSmail Intune

**TOM**



14. Tom would now like to see how he can use the Intune Portal to help him to set and manage compliance policies for devices enrolled onto the platform. Local Administrators can use compliance policies (rules and settings) to help protect organisational resources. There is an extensive range of settings which can be used to tailor protection to specific needs. For a full list of these, please refer to the [Operations Guide for Local Administrators and Onboarding Managers](#).

15. He navigates to Devices > iOS/iPadOS/Android/Windows 10 > Compliance Policies and is able to create compliance policies for devices.

Please note: The correct naming standard should be used when creating compliance policies in order to keep the environment tidy and make it easier to find items.

Policy Name	Platform
-Android-Compliance Policy	Android Enterprise
-Android-Shared Device-Compliance Policy	Android Enterprise
-Android-Compliance Policy	Android Enterprise
-Android-Personally-owned Compliance Policy	Android Enterprise
-Android-Shared Device-Compliance Policy	Android Enterprise

Policy Name	Platform
-Apple-Shared Device-Compliance Policy	iOS/iPadOS
-iOS/iPadOS-Compliance Policy	iOS/iPadOS
-Apple-Shared Device-Compliance Policy	iOS/iPadOS
-iOS/iPadOS-Compliance Policy	iOS/iPadOS
-Apple-Shared Device-Compliance Policy	iOS/iPadOS
-iOS/iPadOS-Compliance Policy	iOS/iPadOS
-Apple-Shared Device-Compliance Policy	iOS/iPadOS

Policy Name	Platform
-HoloLens2-Compliance Policy	Windows 10 and later
-NECS - Windows 10 - Compliance Policy 01 - Standard User Compliance Policy	Windows 10 and later
-Windows 10-Compliance Policy	Windows 10 and later
-HoloLens2-Compliance Policy	Windows 10 and later
-Windows 10-Compliance Policy	Windows 10 and later
-HoloLens2-Compliance Policy	Windows 10 and later
-Windows 10-Compliance Policy	Windows 10 and later
-HoloLens2-Compliance Policy	Windows 10 and later
-Windows 10-Compliance Policy	Windows 10 and later
-HoloLens2-Compliance Policy	Windows 10 and later

The Windows 10 view also includes any HoloLens 2 devices.

# Intune Demo | RBAC Roles

How to view RBAC roles, assignments and properties so LAs can manage devices on the Intune Portal

**TOM**



16. Tom understands RBAC permissions are given to LAs to manage devices on NHSmail Intune. Tom would like to know how to view the RBAC permissions which he and other members have been given as part of the technical onboarding process.

17. He navigates to Tenant Administration > Roles > All roles.

18. He selects a role > properties to view the RBAC role permissions.

Category	Item	Value/Action
Basics	Name	Trust1-Trust-Admin-Role
Basics	Description	--
Permissions	Android for work	Read, Update app sync
	Audit data	Read
	Corporate device identifiers	Create, Delete, Read, Update
	Device compliance policies	Assign, Create, Delete, Read, Update, View reports

19. Tom can view the assignment of the RBAC role by selecting Assignment. He can view the Groups assigned to the policy by selecting the assignment name.

Name	Actions
Trust1-Admin	...

# Intune Demo | Scope Tags

How to view scope tags for devices enrolled to the Intune portal and check the assignment of scope tags

**TOM**



20. Tom knows scope tags are used in the naming of Groups and help both LAs and the Intune Live Service Team to identify and manage their device and user Groups.

21. He navigates to Tenant Administration > Roles > Scope (Tags).

The screenshot shows the Microsoft Endpoint Manager admin center interface. On the left is a navigation pane with options like Home, Dashboard, All services, FAVORITES, Devices, Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main area displays the 'Tenant admin | Tenant status' page. A search bar is visible at the top of the main content area. Below it, the 'Tenant status' section is expanded, showing options like Microsoft Tunnel Gateway, Connectors and tokens, Filters (preview), Roles, Azure AD Privileged Identity..., Diagnostics settings, Audit logs, and Device diagnostics (preview). On the right side of the main content area, 'Tenant details' are visible, including 'Tenant name nhs.onmicrosoft' and 'Total Intune licenses 617153'.

22. He selects the ODS code for his organisation to view further details. For all onboarded NHSmail Intune organisations, an organisation's ODS code is the scope tag (identifier) which has already been created.

The screenshot shows the 'MEM roles | Scope (Tags)' page in Microsoft Intune. The breadcrumb navigation is 'Home > Tenant admin > MEM roles'. The page title is 'MEM roles | Scope (Tags)'. Below the title is a search bar with the text 'Search (Ctrl+ /)' and a '+ Create' button. The 'Manage' section is active, showing a list of scope tags. The list has columns for 'Name' and 'Description'. The first entry is 'Default' with the description 'By default, all Intune entities without scope tag are assign...'. The second entry is 'Trust1'. There is also a 'Search by name' input field above the list.

23. By selecting the scope tag, Tom can view the groups currently assigned to the scope tag.

The screenshot shows the 'Scope tag Trust1' page in the Microsoft Endpoint Manager admin center. The breadcrumb navigation is 'Home > Tenant admin > MEM roles >'. The page title is 'Scope tag Trust1'. The 'Basics' section shows the 'Name' as 'Trust1' and the 'Description' as '--'. The 'Assignments' section shows 'Included groups' with a list of group names: 'Trust1-Win10-Devices', 'Trust1-Apple-Devices-Dynamic-Group', 'Trust1-Android-Devices', 'Trust1-Win10-Devices-Test', and 'Trust1-Apple-Devices'.

# Intune Demo | Monitoring

How to access and use the monitoring feature available to support LAs to manage devices on the Intune Portal

**TOM**



Tom now has a much better idea of how to manage devices in the Intune Portal and how to apply policies.

Before Tom concludes his review of the Intune Portal, he wants to understand how the Intune Portal can help him to produce reports on his devices so he can monitor them for compliance, enrolment failures etc.

24. He navigates to Devices > Monitor and then Assignment Status to see an overview. Tom is able to view additional monitoring views depending on what he would like to monitor. All monitoring report options are listed on the left-hand pane.

Microsoft Endpoint Manager admin center

All services > Devices > Monitor | Assignment status

Search (Ctrl+/) Export

Profile	Type	Devices with errors	Devices with conflict	Devices pending	Devices succeeded	Devices not applicable
-Windows 10 - Google CH...	Custom	0	0	0	51	0
-Windows 10 - Interactive...	Custom	0	0	0	52	0
-Windows 10 - Internet E...	Custom	0	0	0	52	0
Android-Shared Device R...	Device restrictions	0	0	0	0	0
Apple-Shared-Device Res...	Device restrictions	0	0	0	0	0
HoloLens2 - Windows H...	Identity protection	0	0	0	0	0
HoloLens2 - Device Restri...	Device restrictions	0	0	0	0	0
HoloLens2 - Device Restri...	Device restrictions	0	0	0	0	0
HoloLens2 - Set Timezon...	Custom	0	0	0	0	0
iOS-Trusted-Certificate-Pr...	Trusted certificate	1	0	0	150	0
- Windows 10 - Co...	Endpoint protection	0	0	2	0	0
- Windows 10 - Co...	SCEP certificate	0	0	0	0	0
- Windows 10 - Co...	Trusted certificate	0	0	2	0	0
- Windows 10 - Co...	Trusted certificate	0	0	0	0	0
- Windows 10 - Co...	Trusted certificate	0	0	0	0	0
Windows 10 - Applocker ...	Custom	1	0	0	0	1
Windows 10 - Bitlocker S...	Endpoint protection	0	0	0	2	0
Windows 10 - Disable AA...	Custom	0	0	0	2	0
Windows 10 - Disable Wi...	Identity protection	0	0	0	2	0
Windows 10 - Endpoint P...	Endpoint protection	0	0	0	2	0
Android-Device Restrictio...	Device restrictions	0	0	1	2	0
Android-Shared Device R...	Device restrictions	0	0	0	0	0

The monitoring overviews available are not customisable, however monitoring reports can be filtered; meaning LAs can use the Intune Portal to produce more granular reports if required.

**THANK YOU**