accenture NHS

NHSmail Intune Service

Session 3: Intune Portal Demo

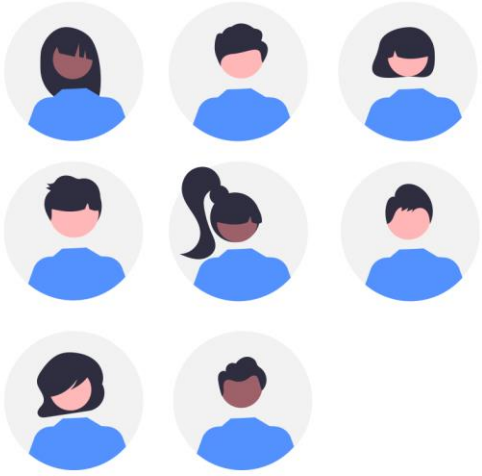
9th June 2022

Upskilling Series | Housekeeping

Event name:	Session 3: Intune Demo
Date:	09 June 2022
Location:	Online Webinar
Start / end time:	13:30–14:30
Attendees:	NHSmail Intune Team and LAs from June onboarding organisations.
Objectives & purpose:	To provide an overview of the key areas of the Intune Portal, discuss how LAs using NHSmail Intune can complete Group Management tasks and address common early access issues.
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

- As this is a webinar, all attendees, other than the presenters will be on mute during the event.
- There will be a question and answer section at the end of the session, time permitting. If you wish to ask a question during this section, please raise your hand. Alternatively, please ask your question via the chat.
- Any questions submitted in the chat which we don't have time to answer in the session or are unable to answer in the session, will be answered via follow-up email after the session where appropriate.
- Information outlined in red indicates key information.



Agenda

Session 3: Intune Demo

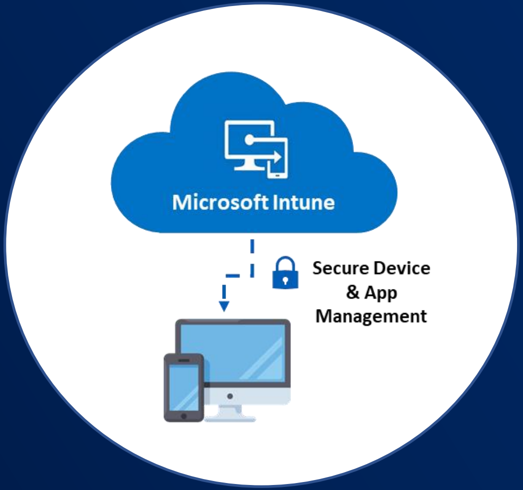
01 Intune Portal Overview

02 Intune Demo

- Portal Overview
- Dashboard
- Device Overview
- Enrolment
- Compliance Policies
- Configuration Profiles
- Applications
- RBAC Roles
- Monitoring
- Wiping and Removing Devices

03 Questions and Close

Session 3



Intune Portal 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 3 will provide a demonstration of the Intune Portal to support LAs who may be new or relatively new to using Intune to familiarise themselves with the Portal.

Objectives of this session

- Demonstrate key areas of the Intune Portal and outline how Group Management tasks can be completed.
- 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

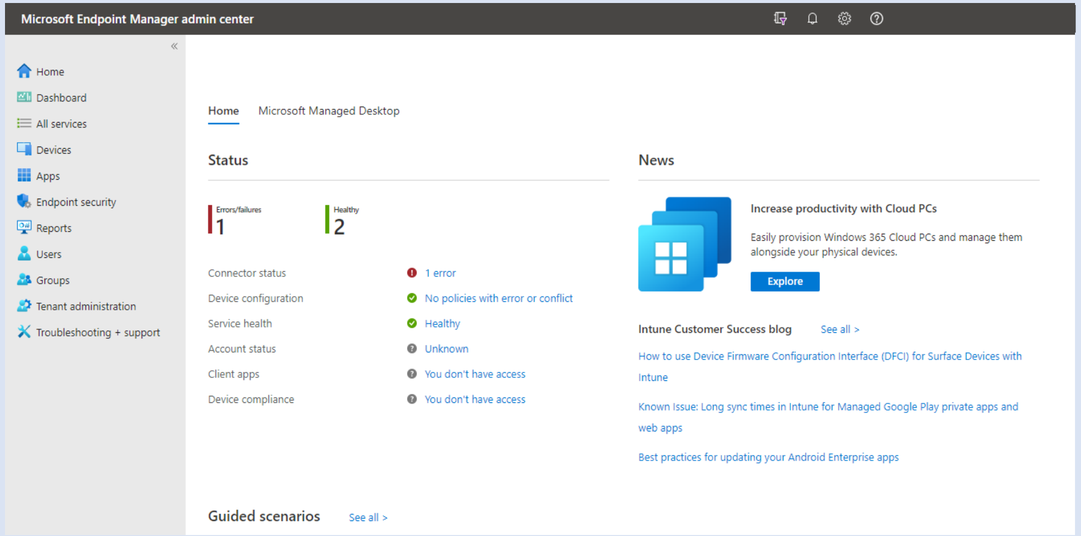
NHSmail Intune runs from the standard Intune Portal but there are some differences to using the Intune Portal when enrolled onto NHSmail Intune

1. INTUNE PORTAL

NHSmail 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 at your organisation should have the following URL bookmarked: https://endpoint.microsoft.com

Organisations can request for additional LAs to be provided with RBAC permissions at any time. This can be done by raising a **service request** and providing us with the name and nhs.net account of the individual/s.



Status

Errors/failures 1

Healthy 2

Connector status 1 error

Device configuration No policies with error or conflict

Service health Healthy

Account status Unknown

Client apps You don't have access

Device compliance You don't have access

News

Increase productivity with Cloud PCs

Easily provision Windows 365 Cloud PCs and manage them alongside your physical devices.

Intune Customer Success blog

How to use Device Firmware Configuration Interface (DFCI) for Surface Devices with Intune

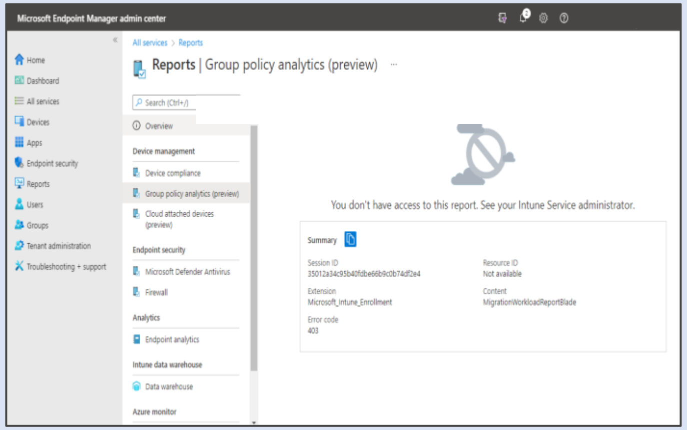
Known Issue: Long sync times in Intune for Managed Google Play private apps and web apps

Best practices for updating your Android Enterprise apps

Guided scenarios

2. EMS E3 & AADP2 LICENCE ASSIGNMENT

To be able to use all the functionality of the Intune Portal (which is available to NHSmail 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 when trying to use the functionality available via the Intune Portal.



You don't have access to this report. See your Intune Service administrator.

Summary

Session ID
35012a34c95b40fdbe66b9c0b74df2e4

Resource ID
Not available

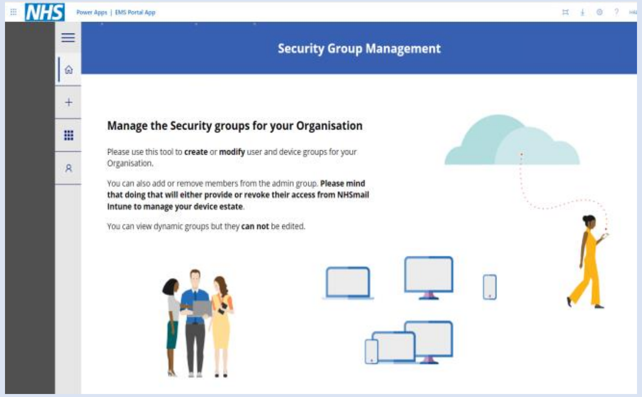
Extension
Microsoft_Intune_Enrollment

Content
MigrationWorkloadReportBlade

Error code
403

3. SECURITY GROUP MANAGEMENT APP

Organisations onboarded to NHSmail 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**.



Manage the Security groups for your Organisation

Please use this tool to **create** or **modify** user and device groups for your Organisation.

You can also add or remove members from the admin group. **Please mind that doing that will either provide or revoke their access from NHSmail Intune to manage your device estate**.

You can view dynamic groups but they **can not** be edited.

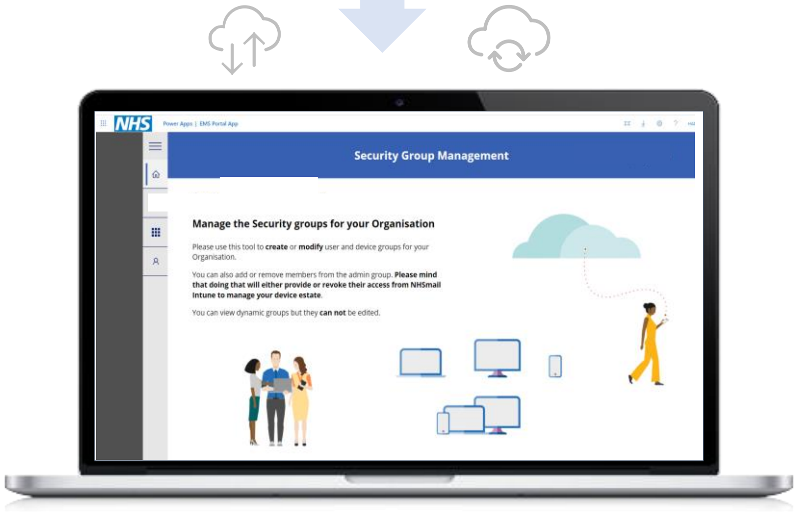
Attempting to complete Group Management tasks natively via the Intune Portal and not correctly assigning licences are the most common causes of early tickets among onboarded organisations.

Intune Demo | Security Group Management App

The NHSmail Intune solution supports LAs to manage Groups within Intune without requiring write access to Azure AD

NHSmail Intune will allow LAs (with RBAC permissions) at onboarded organisations to manage Groups without requiring native access to Azure AD. This will allow LAs granular control over the creation, editing and deletion of their organisation's Groups within Intune and permit LAs to closely and independently manage Groups scoped to their organisation. The below details all Group Management tasks LAs at onboarded organisations will be able to do:

LAs will be able to sign into the Security Group Management App with SSO if they are logged into their NHSmail account.



Security Group Management

Manage the Security groups for your Organisation

Please use this tool to **create** or **modify** user and device groups for your Organisation.

You can also add or remove members from the admin group. **Please mind that doing that will either provide or revoke their access from NHSmail Intune to manage your device estate**.

You can view dynamic groups but they **can not** be edited.

- ✓ A link to the Security Group Management App will be included in the Operations Guide for Local Admins and Onboarding Managers.
- ✓ All RBAC permission LAs will have access to this app and will be able to manage access to this app at their organisation by adding more LA's if required.

LAs at onboarded organisations will be able to complete the following Group management tasks via the NHSmail Intune Security Group Management Application:

VIEW AND SEARCH GROUPS

LAs will be able to view and search all Groups assigned to their organisation's ODS scope tag.

CREATE GROUPS

LAs will be able to create groups for users and Windows 10/11 devices (excluding dynamic groups).

EDIT AND DELETE EXISTING GROUPS

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

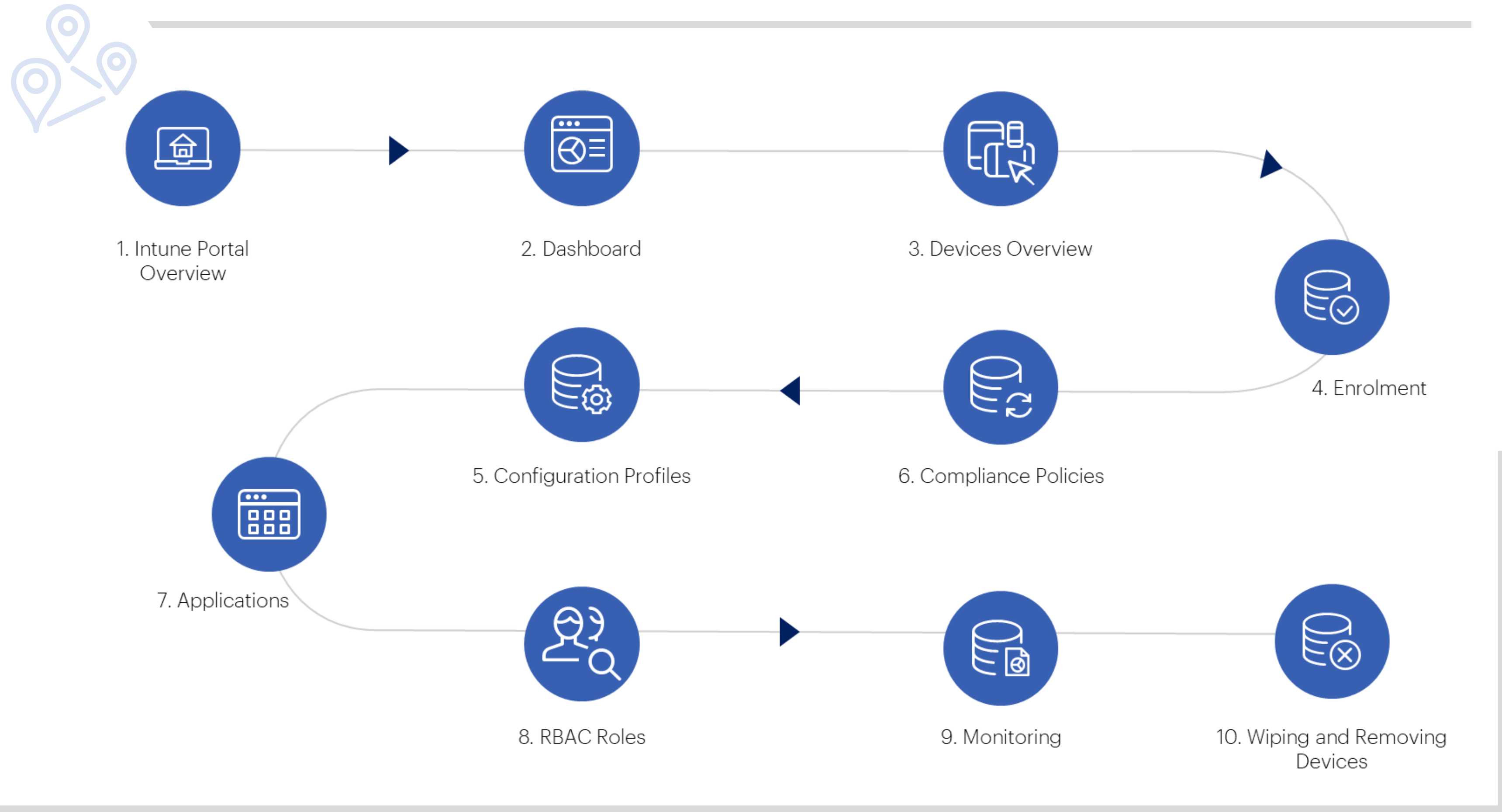
LAs will be able to add and remove Group members for user groups and Windows 10/11 device groups (including with a .csv file) and add and remove members to the organisation's Intune Administration group.

Important: LAs are unable to add dynamic groups using the Security Group Management App. If an LA needs to create a dynamic group, this will need to be raised as a service request.

Intune Demo | Demo Roadmap

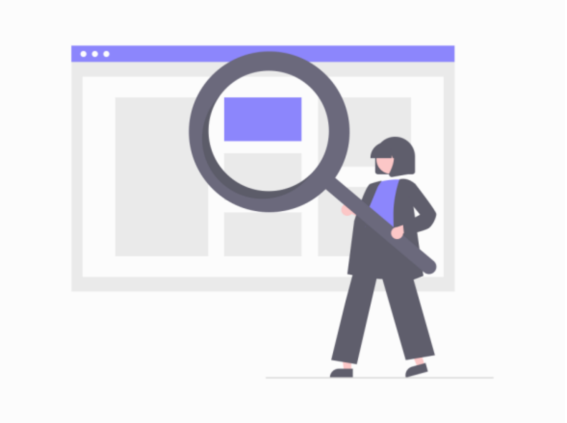
Intune Demo journey including key requirements which should be in place to allow LAs to explore the Intune Portal fully

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**.



DEMO

Intune Portal

Intune Demo | Overview

Overview of the Intune Portal when you first login

TOM

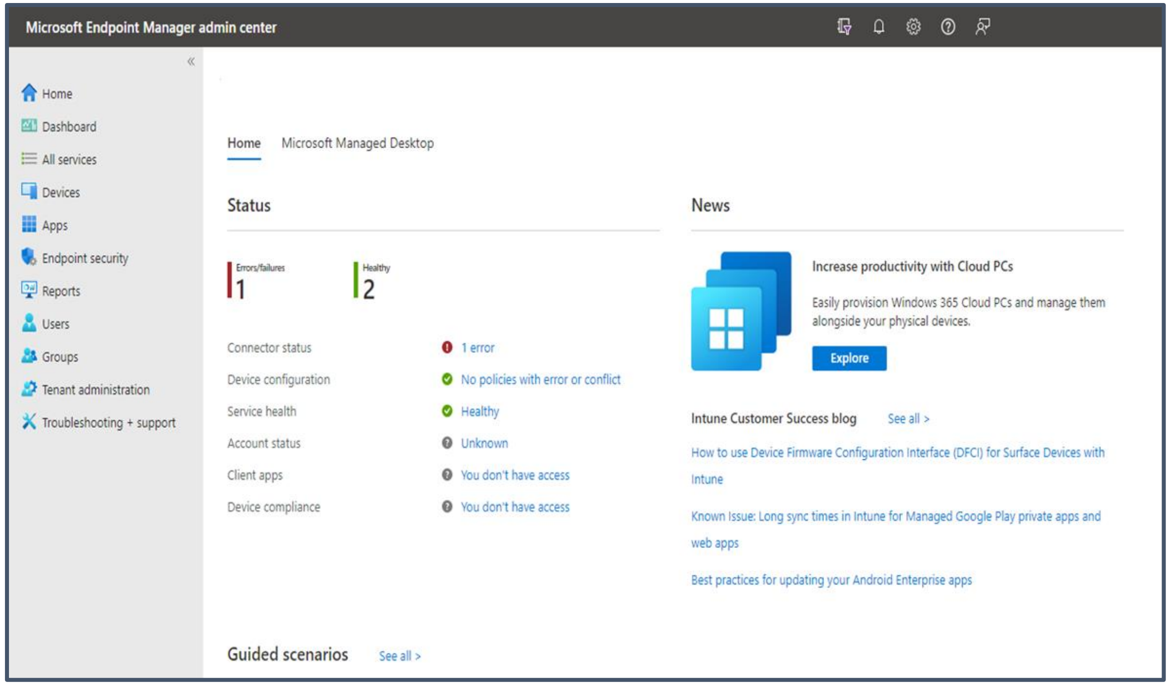
Tom is an LA at a newly onboarded organisation.

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; he can begin exploring the Portal.

2. Tom has a look at what he can access from the main pane in the Intune Portal before he navigates to the dashboard.



Connector status: 1 error
Device configuration: No policies with error or conflict
Service health: Healthy
Account status: Unknown
Client apps: You don't have access
Device compliance: You don't have access

Increase productivity with Cloud PCs

Easily provision Windows 365 Cloud PCs and manage them alongside your physical devices.

Intune Customer Success blog

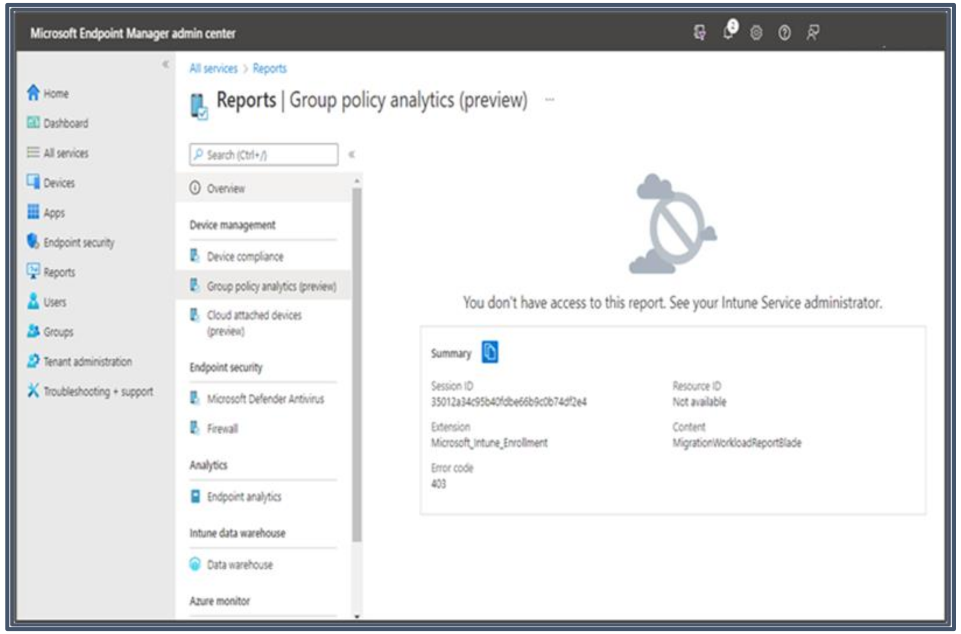
How to use Device Firmware Configuration Interface (DFCI) for Surface Devices with Intune

Known Issue: Long sync times in Intune for Managed Google Play private apps and web apps

Best practices for updating your Android Enterprise apps

3. A colleague has moved to Tom's team and has logged into the Intune Portal. This colleague receives the error message below.

4. This error message is most likely due to licences so Tom needs to ensure the EMS E3 licence is assigned to this LA through the NHSmail Portal.



You don't have access to this report. See your Intune Service administrator.

Summary

Session ID
35012a34c95b40fdbe66b9c0b74df2e4

Resource ID
Not available

Extension
Microsoft_Intune_Enrollment

Content
MigrationWorkloadReportBlade

Error code
403

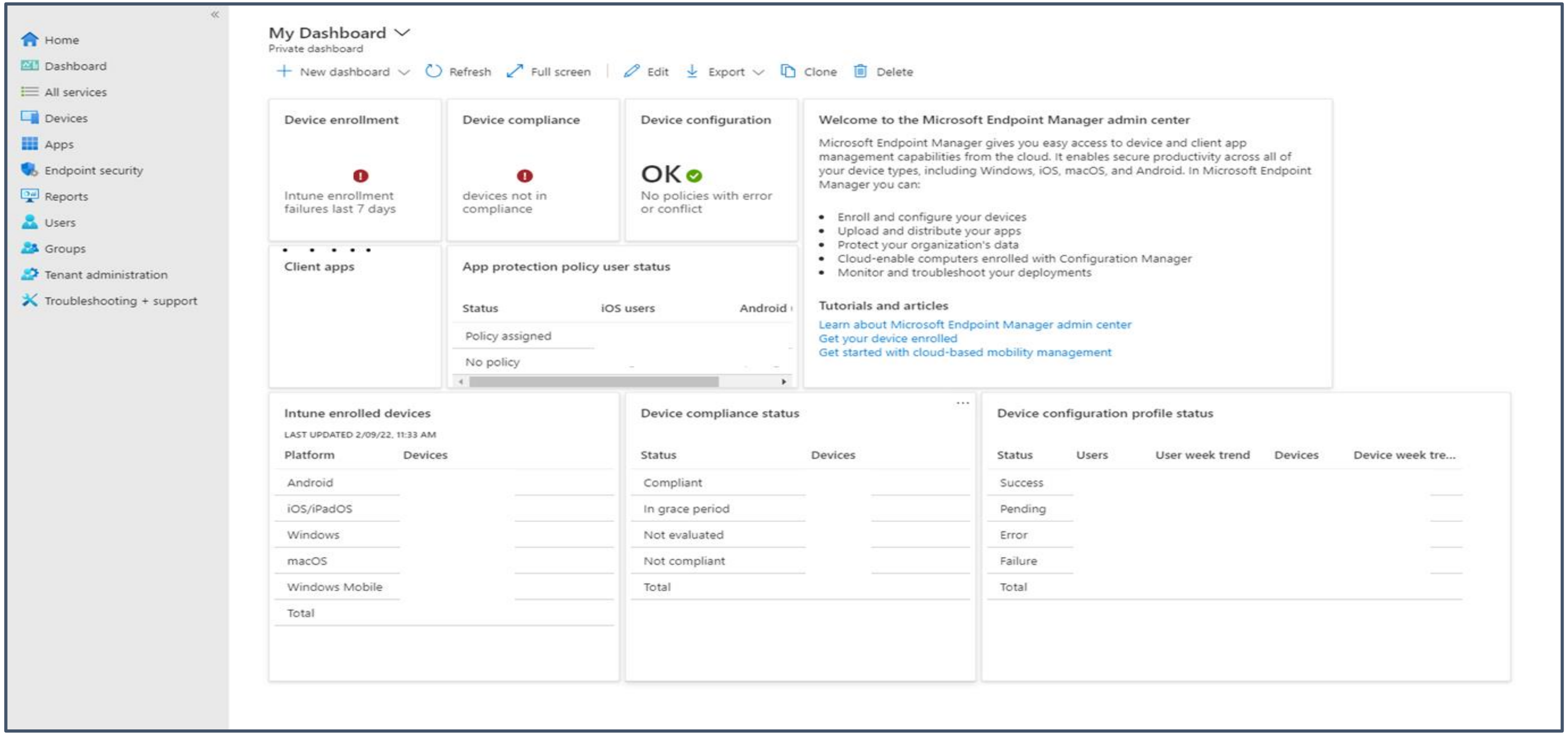
EMS E3 licences need to be assigned to all LAs who will be using and managing Intune. This licence allows access to the Intune portal.

Intune Demo | Dashboard

How to access an overview of the dashboard on the platform

TOM

5. Tom would now like to take a look at the Dashboard tab in the main pane. He sees an overview of the number of devices on the tenant, configuration profiles and compliance policies on the platform. Tom has the ability to customise the dashboard to display information specific to his organisation.



Device enrollment

Intune enrollment failures last 7 days

Device compliance

devices not in compliance

Device configuration

OK ✓

No policies with error or conflict

Welcome to the Microsoft Endpoint Manager admin center

Microsoft Endpoint Manager gives you easy access to device and client app management capabilities from the cloud. It enables secure productivity across all of your device types, including Windows, iOS, macOS, and Android. In Microsoft Endpoint Manager you can:

- Enroll and configure your devices
- Upload and distribute your apps
- Protect your organization's data
- Cloud-enable computers enrolled with Configuration Manager
- Monitor and troubleshoot your deployments

Tutorials and articles

Learn about Microsoft Endpoint Manager admin center
Get your device enrolled
Get started with cloud-based mobility management

Client apps

App protection policy user status

Status	iOS users	Android
Policy assigned		
No policy		

Intune enrolled devices

LAST UPDATED 2/09/22, 11:33 AM

Platform	Devices
Android	
iOS/iPadOS	
Windows	
macOS	
Windows Mobile	
Total	

Device compliance status

Status	Devices
Compliant	
In grace period	
Not evaluated	
Not compliant	
Total	

Device configuration profile status

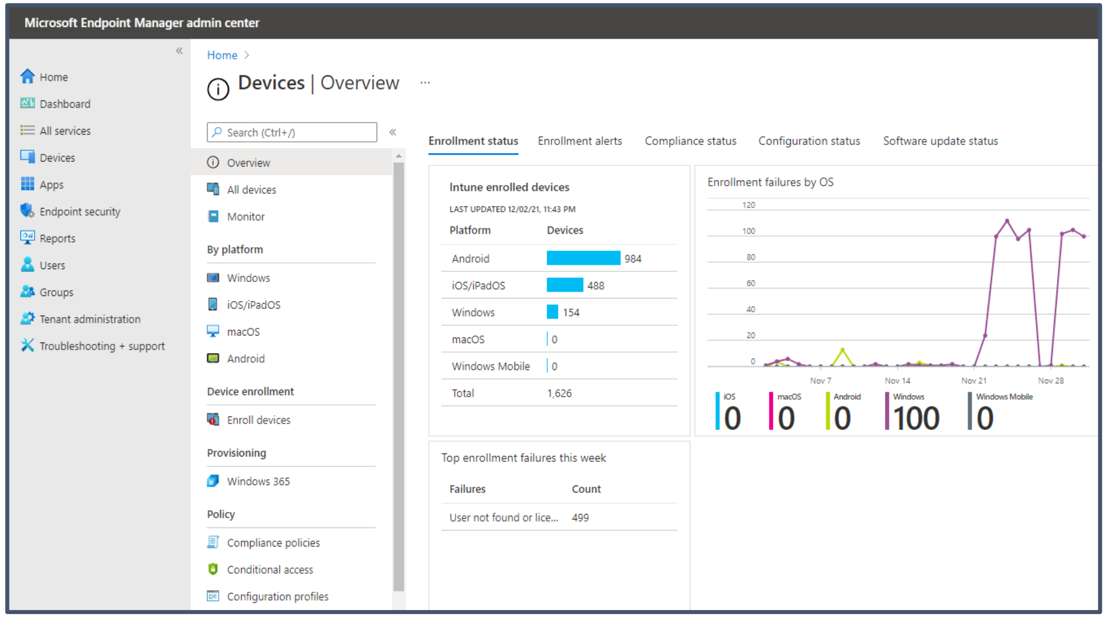
Status	Users	User week trend	Devices	Device week tre...
Success				
Pending				
Error				
Failure				
Total				

Intune Demo | Devices

How to access an overview of devices on the platform

TOM

6. 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.



Intune enrolled devices

LAST UPDATED 12/02/21, 11:43 PM

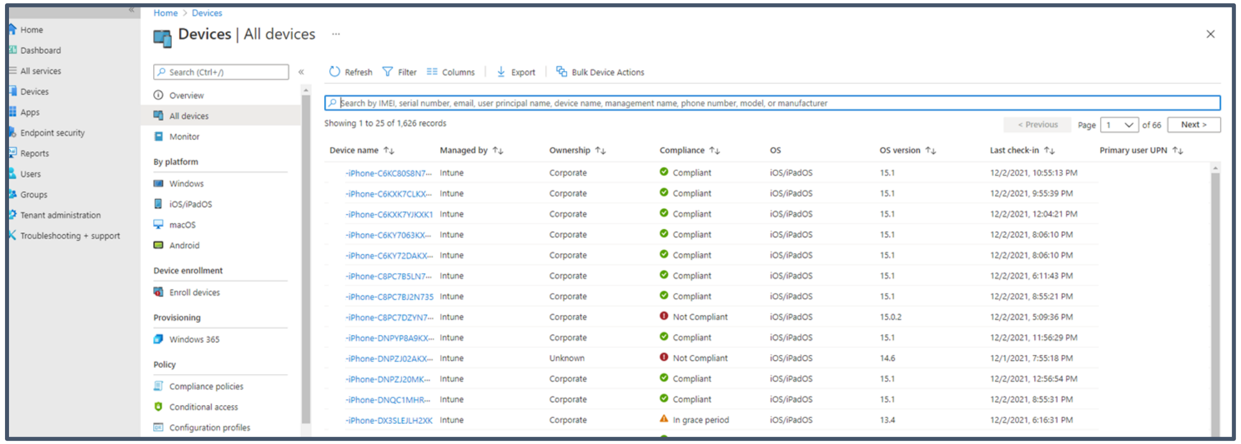
Platform	Devices
Android	984
iOS/iPadOS	488
Windows	154
macOS	0
Windows Mobile	0
Total	1,626

Top enrollment failures this week

Failures	Count
User not found or lice...	499

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.

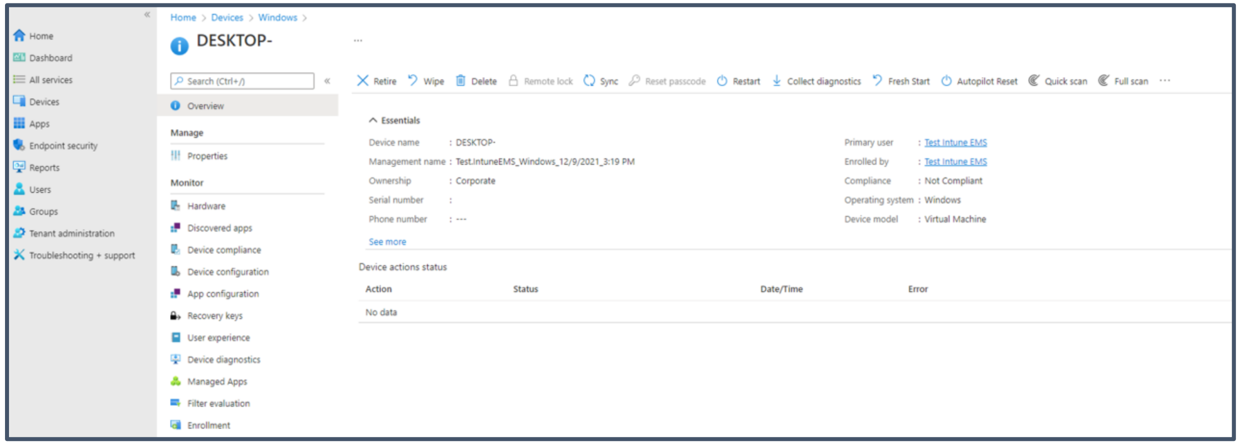
7. Tom navigates to the All devices tab to view a more detailed list of the devices enrolled at his organisation. Again, Tom is able to filter by platform type. This page only shows devices from Tom's own organisation.



Showing 1 to 25 of 1,626 records

Device name	Managed by	Ownership	Compliance	OS	OS version	Last check-in	Primary user UPN
-iPhone-C6KC80S8N7...	Intune	Corporate	✓ Compliant	iOS/iPadOS	15.1	12/2/2021, 10:55:13 PM	
-iPhone-C6KXK7CLKX...	Intune	Corporate	✓ Compliant	iOS/iPadOS	15.1	12/2/2021, 9:55:39 PM	
-iPhone-C6KXK7YJKXK1	Intune	Corporate	✓ Compliant	iOS/iPadOS	15.1	12/2/2021, 12:04:21 PM	
-iPhone-C6KY7063KX...	Intune	Corporate	✓ Compliant	iOS/iPadOS	15.1	12/2/2021, 8:06:10 PM	
-iPhone-C6KY72DAKX...	Intune	Corporate	✓ Compliant	iOS/iPadOS	15.1	12/2/2021, 8:06:10 PM	
-iPhone-C8PC7B5LN7...	Intune	Corporate	✓ Compliant	iOS/iPadOS	15.1	12/2/2021, 6:11:43 PM	
-iPhone-C8PC7BJ2N735	Intune	Corporate	✓ Compliant	iOS/iPadOS	15.1	12/2/2021, 8:55:21 PM	
-iPhone-C8PC7DZYN7...	Intune	Corporate	! Not Compliant	iOS/iPadOS	15.0.2	12/2/2021, 5:09:36 PM	
-iPhone-DNPYP8A9KX...	Intune	Corporate	✓ Compliant	iOS/iPadOS	15.1	12/2/2021, 11:56:29 PM	
-iPhone-DNPZJ02AKX...	Intune	Unknown	! Not Compliant	iOS/iPadOS	14.6	12/1/2021, 7:55:18 PM	
-iPhone-DNPZJ20MK...	Intune	Corporate	✓ Compliant	iOS/iPadOS	15.1	12/2/2021, 12:56:54 PM	
-iPhone-DNQC1MHR...	Intune	Corporate	✓ Compliant	iOS/iPadOS	15.1	12/2/2021, 8:55:31 PM	
-iPhone-DX3SLEJLH2XK	Intune	Corporate	⚠ In grace period	iOS/iPadOS	13.4	12/2/2021, 6:16:31 PM	

8. Tom selects a device to have a further look at its properties.



Essentials

Device name : DESKTOP-
Management name : Test.IntuneEMS_Windows_12/9/2021_3:19 PM
Ownership : Corporate
Serial number :
Phone number : ---

Primary user : Test Intune EMS
Enrolled by : Test Intune EMS
Compliance : Not Compliant
Operating system : Windows
Device model : Virtual Machine

Device actions status

Action	Status	Date/Time	Error
No data			

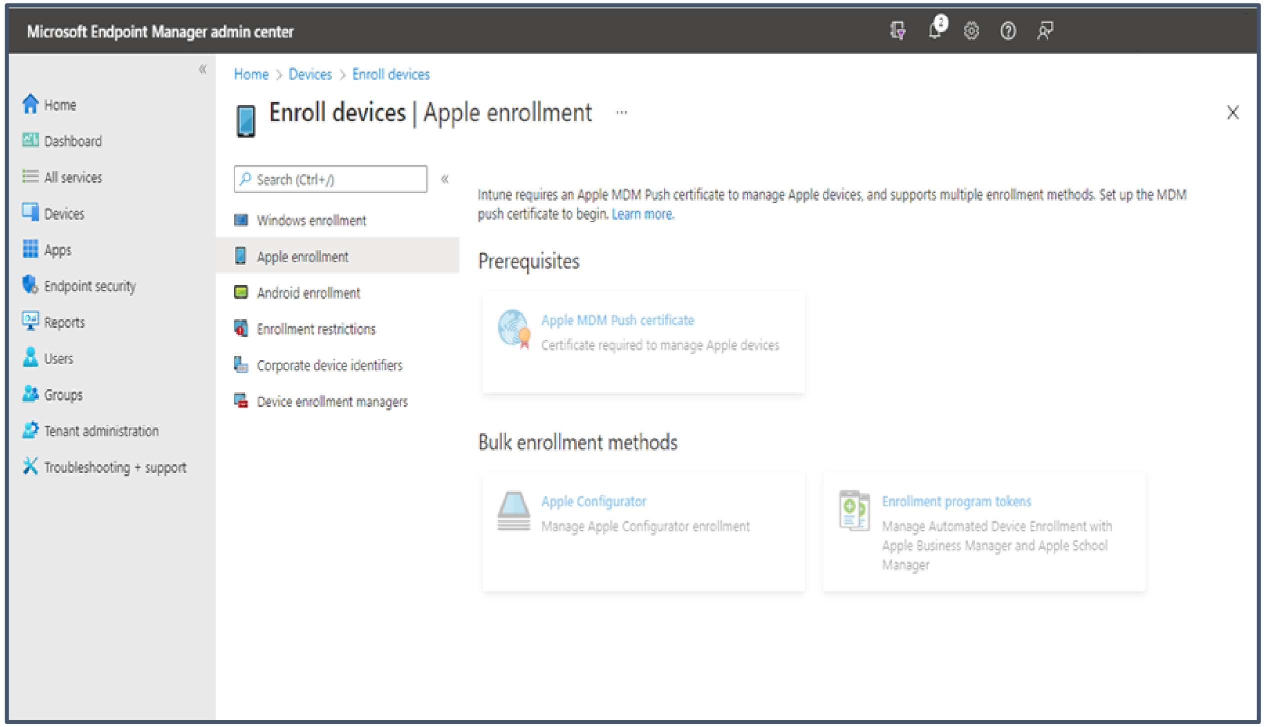
Intune Demo | Enrolment

Overview of where to find the enrolment screens which LAs will need to access prior to enrolling any devices

TOM

9. Tom is now interested in the device enrolment and takes a look at the enrolment page. To do this, Tom will need to navigate to Devices > Device Enrollment > Enroll devices and then select the target platform.

10. 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 platforms.



Enroll devices | Apple enrollment

Intune requires an Apple MDM Push certificate to manage Apple devices, and supports multiple enrollment methods. Set up the MDM push certificate to begin. Learn more.

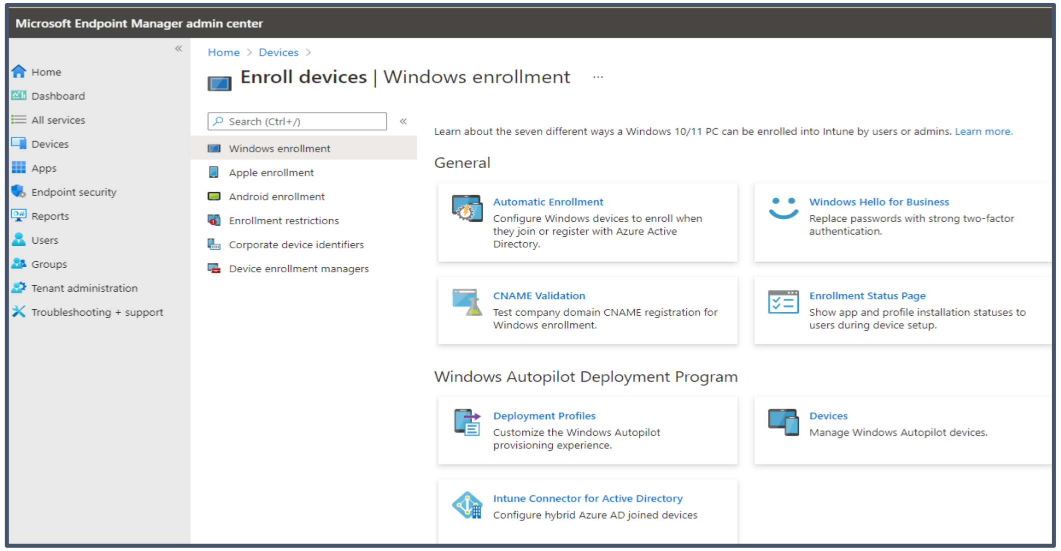
Prerequisites

Apple MDM Push certificate
Certificate required to manage Apple devices

Bulk enrollment methods

Apple Configurator
Manage Apple Configurator enrollment

Enrollment program tokens
Manage Automated Device Enrollment with Apple Business Manager and Apple School Manager



Enroll devices | Windows enrollment

Learn about the seven different ways a Windows 10/11 PC can be enrolled into Intune by users or admins. Learn more.

General

Automatic Enrollment
Configure Windows devices to enroll when they join or register with Azure Active Directory.

Windows Hello for Business
Replace passwords with strong two-factor authentication.

CNAME Validation
Test company domain CNAME registration for Windows enrollment.

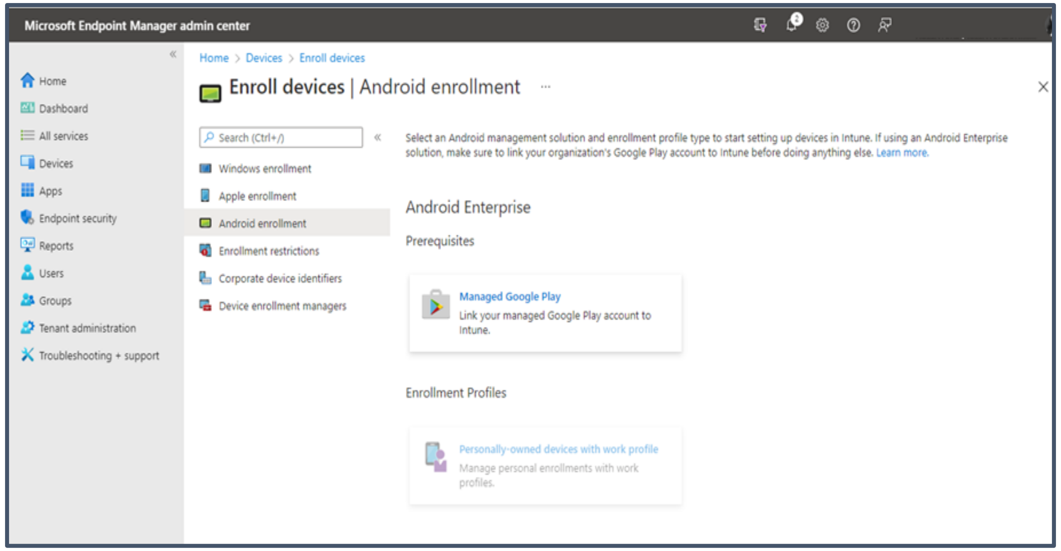
Enrollment Status Page
Show app and profile installation statuses to users during device setup.

Windows Autopilot Deployment Program

Deployment Profiles
Customize the Windows Autopilot provisioning experience.

Devices
Manage Windows Autopilot devices.

Intune Connector for Active Directory
Configure hybrid Azure AD joined devices



Enroll devices | Android enrollment

Select an Android management solution and enrollment profile type to start setting up devices in Intune. If using an Android Enterprise solution, make sure to link your organization's Google Play account to Intune before doing anything else. Learn more.

Android Enterprise

Prerequisites

Managed Google Play
Link your managed Google Play account to Intune.

Enrollment Profiles

Personally-owned devices with work profile
Manage personal enrollments with work profiles.

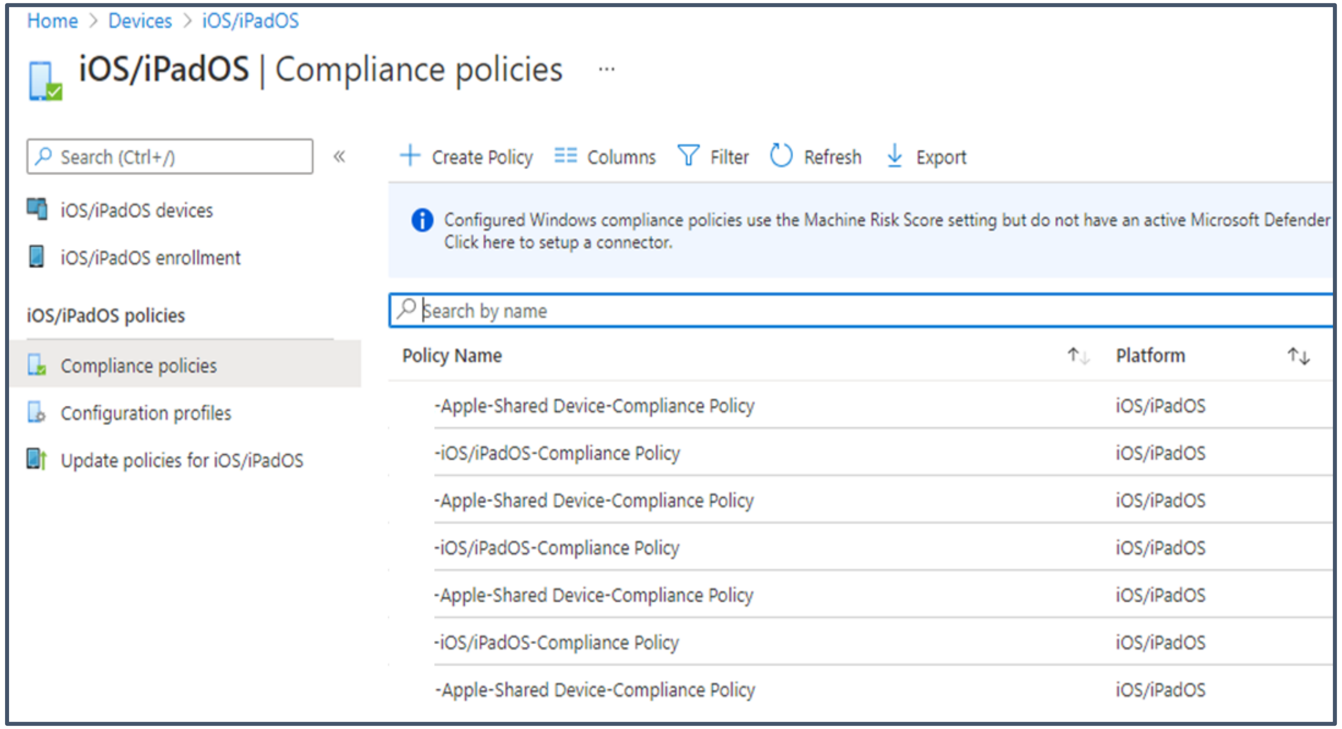
Intune Demo | Compliance Policies

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

TOM

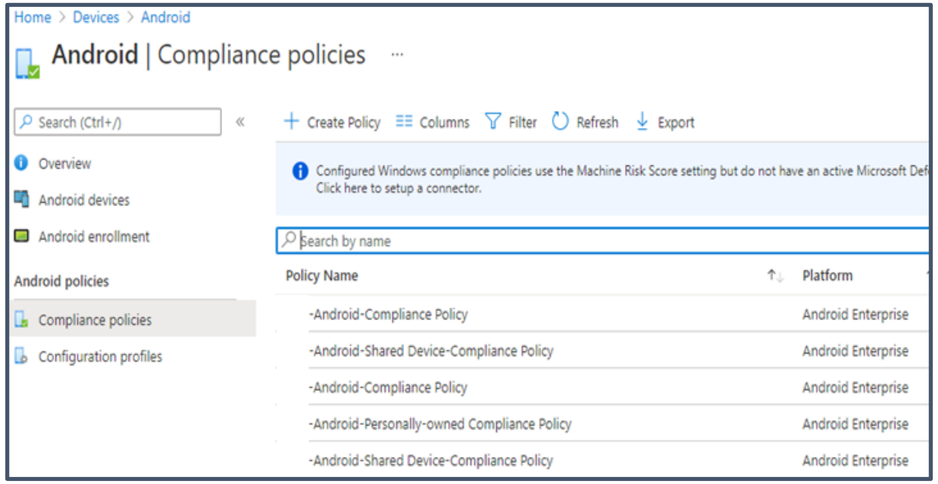
11. Tom would now like to see how he can use the Intune Portal to help him to set and manage compliance policies for devices enrolled onto the platform. Local Administrators can use compliance policies (rules and settings) to help protect organisational resources. There are a broad range of settings which can be used to tailor protection to specific needs.

12. He navigates to Devices > iOS/iPadOS/Android/Windows 10/11 > Compliance Policies and is able to create compliance policies for devices. The correct naming standard should be used when creating compliance policies.



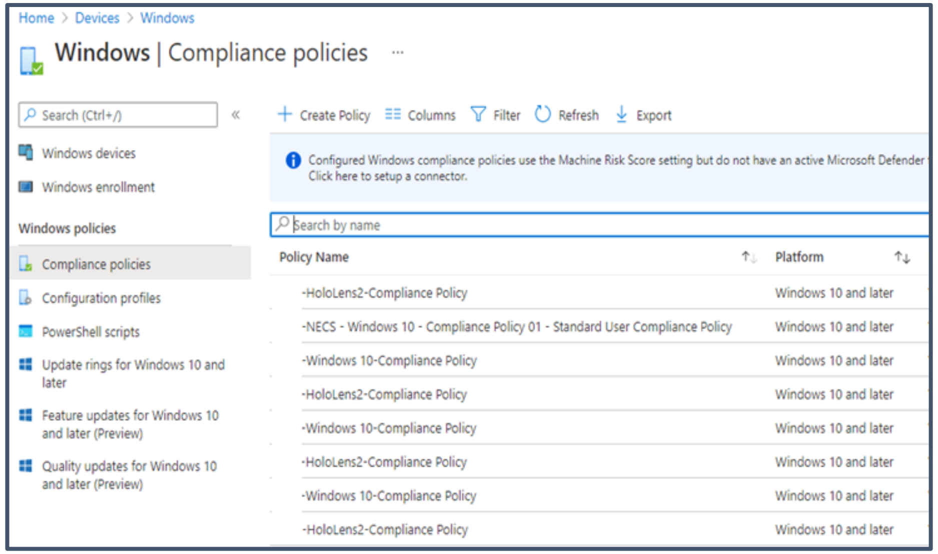
Configured Windows compliance policies use the Machine Risk Score setting but do not have an active Microsoft Defender
Click here to setup a connector.

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



Configured Windows compliance policies use the Machine Risk Score setting but do not have an active Microsoft Def
Click here to setup a connector.

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



Configured Windows compliance policies use the Machine Risk Score setting but do not have an active Microsoft Defender
Click here to setup a connector.

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

The Windows 10/11 view also includes any HoloLens 2 devices.

Intune Demo | Configuration Profiles

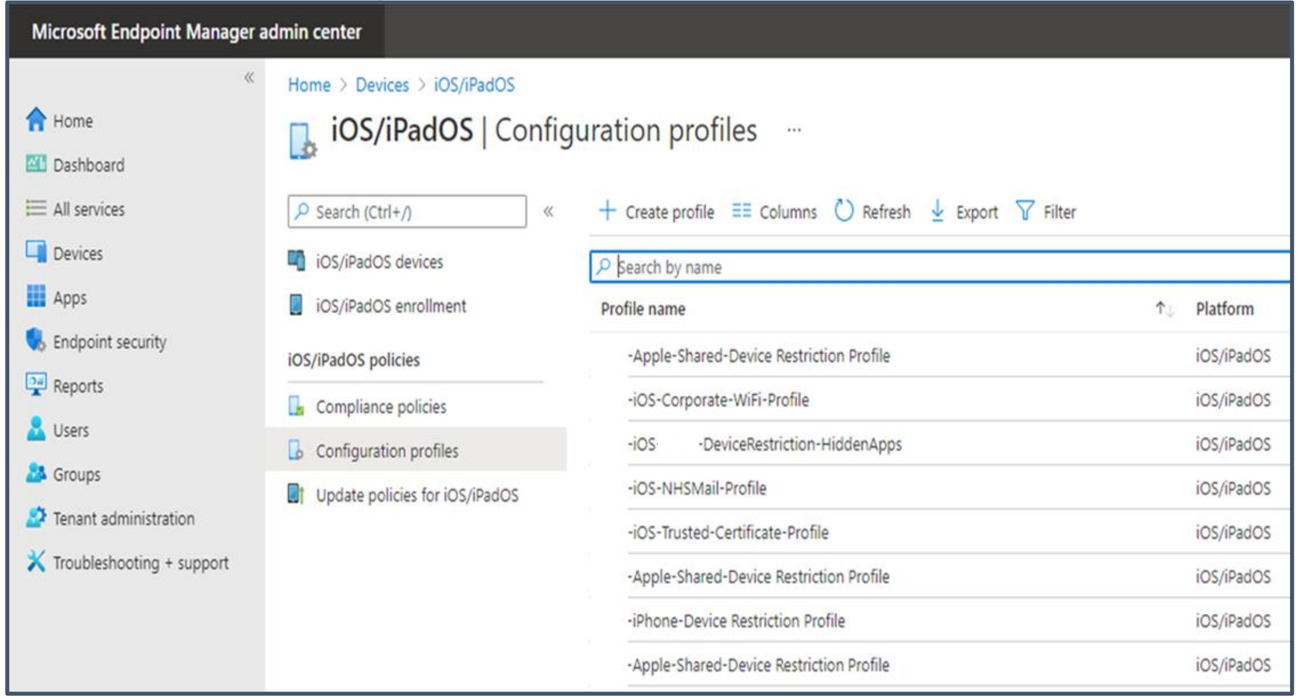
How to access and set-up configuration profiles across the full range of supported device types on NHSmail Intune

TOM

13. 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 devices estate.

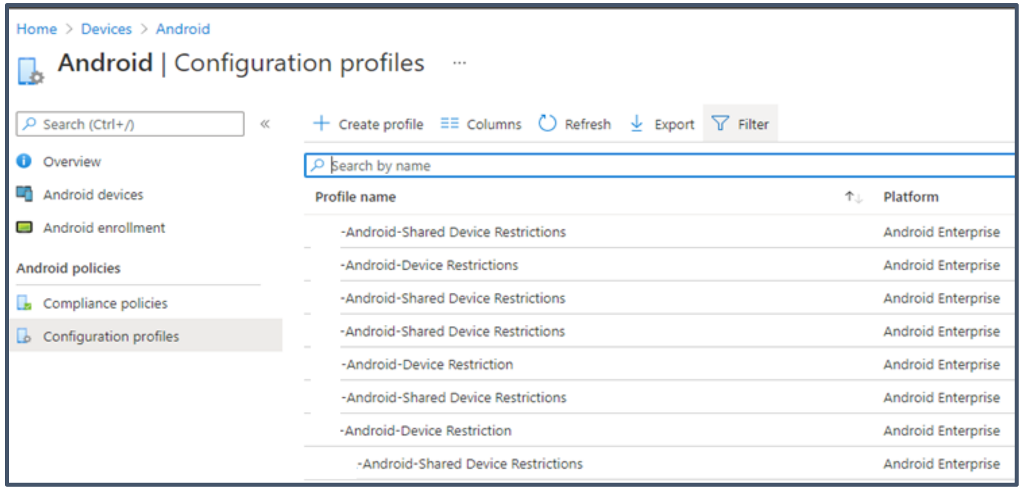
14. He navigates to Devices > iOS/iPadOS/Android/Windows 10/11 > Configuration Profiles.

15. He can select a profile to view details of the profile and the settings which have been configured.



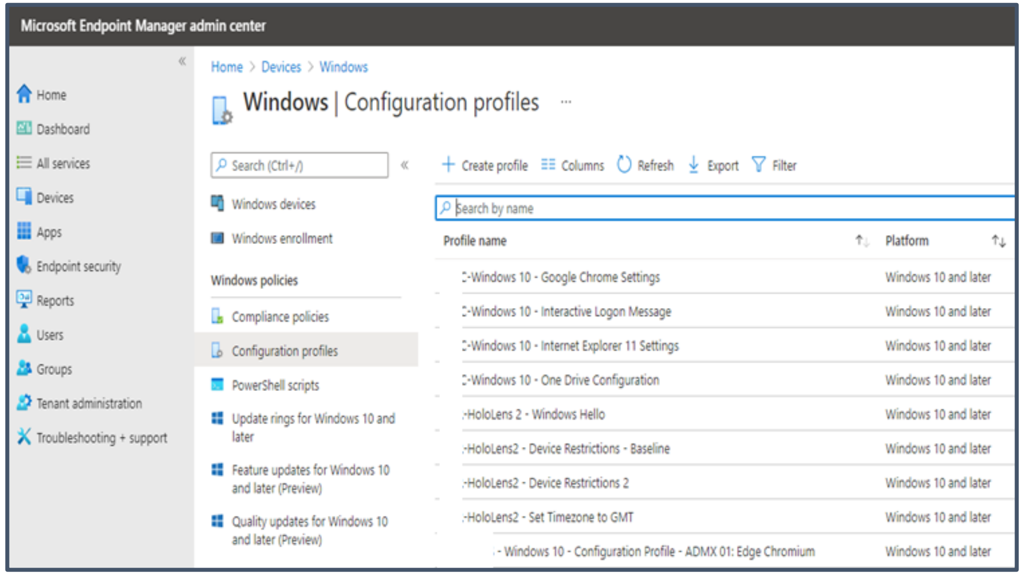
iOS/iPadOS | Configuration profiles

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



Android | Configuration profiles

Profile name	Platform
-Android-Shared Device Restrictions	Android Enterprise
-Android-Device Restrictions	Android Enterprise
-Android-Shared Device Restrictions	Android Enterprise
-Android-Shared Device Restrictions	Android Enterprise
-Android-Device Restriction	Android Enterprise
-Android-Shared Device Restrictions	Android Enterprise
-Android-Device Restriction	Android Enterprise
-Android-Shared Device Restrictions	Android Enterprise



Windows | Configuration profiles

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 10/11 view also includes any HoloLens 2 devices.

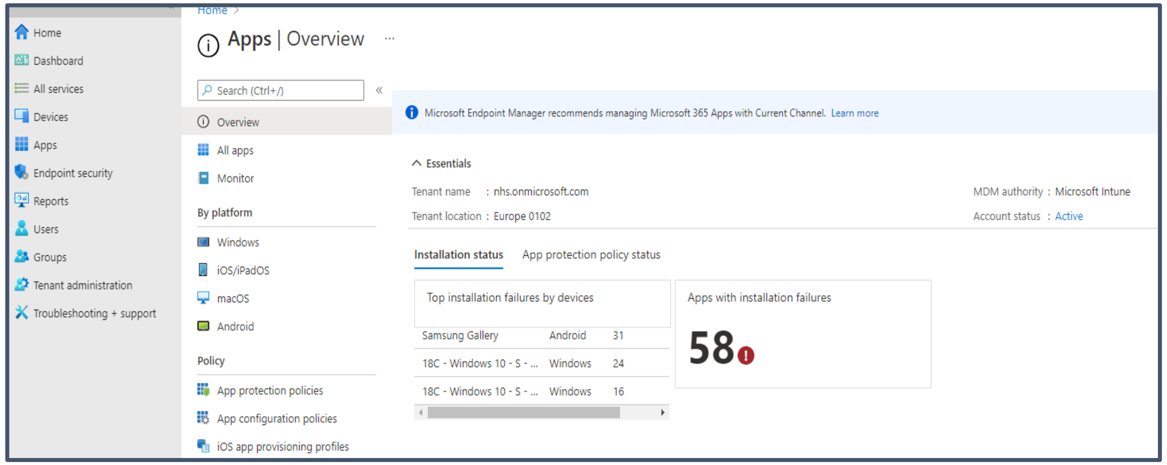
Intune Demo | Applications

How to access an overview of applications on the platform and view applications for each device type

TOM

16. Tom would now like to take a look at applications from the main pane.
He navigates to Applications > Overview.

The overview page shows him all applications on the platform and allows him to filter by device type to push specific apps.



Apps | Overview

Microsoft Endpoint Manager recommends managing Microsoft 365 Apps with Current Channel. Learn more

Essentials

Tenant name : nhs.onmicrosoft.com

Tenant location : Europe 0102

MDM authority : Microsoft Intune

Account status : Active

Installation status | App protection policy status

Top installation failures by devices

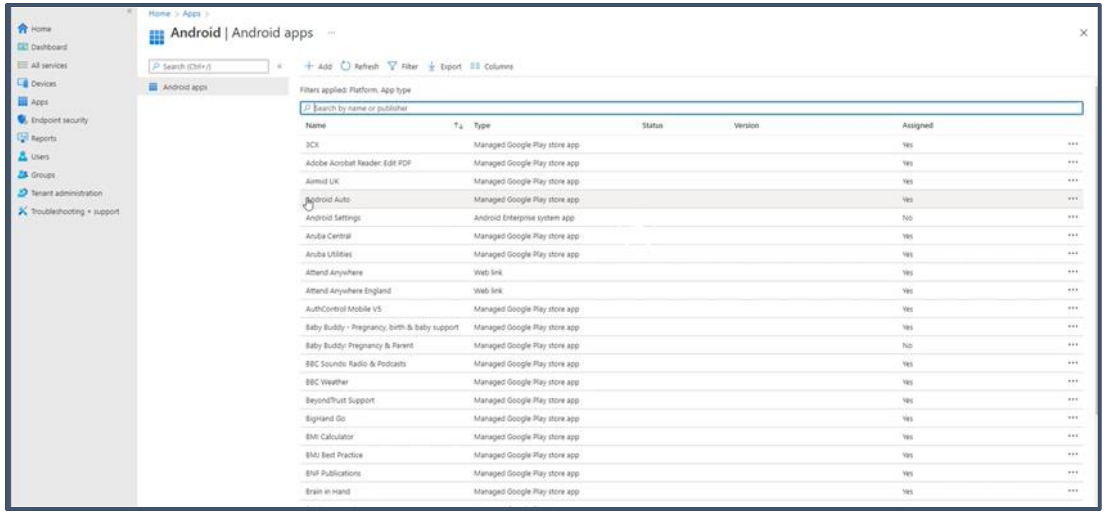
Samsung Gallery	Android	31
18C - Windows 10 - S - ...	Windows	24
18C - Windows 10 - S - ...	Windows	16

Apps with installation failures

58

17. He then reviews the list of applications pushed to Android devices through the Google Play Store.

Tom can select one application, view it's properties and assign it to a Group.



Android | Android apps

Filters applied: Platform, App type

Name	Type	Status	Version	Assigned
3CX	Managed Google Play store app			Yes
Adobe Acrobat Reader: Edit PDF	Managed Google Play store app			Yes
Airmid UK	Managed Google Play store app			Yes
Android Auto	Managed Google Play store app			Yes
Android Settings	Android Enterprise system app			No
Aruba Central	Managed Google Play store app			Yes
Aruba Utilities	Managed Google Play store app			Yes
Attend Anywhere	Web link			Yes
Attend Anywhere England	Web link			Yes
AuthControl Mobile V5	Managed Google Play store app			Yes
Baby Buddy - Pregnancy, birth & baby support	Managed Google Play store app			Yes
Baby Buddy: Pregnancy & Parent	Managed Google Play store app			No
BBC Sounds: Radio & Podcasts	Managed Google Play store app			Yes
BBC Weather	Managed Google Play store app			Yes
BeyondTrust Support	Managed Google Play store app			Yes
BigHand Go	Managed Google Play store app			Yes
BMI Calculator	Managed Google Play store app			Yes
BMJ Best Practice	Managed Google Play store app			Yes
BNF Publications	Managed Google Play store app			Yes
Brain in Hand	Managed Google Play store app			Yes

The Applications 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.

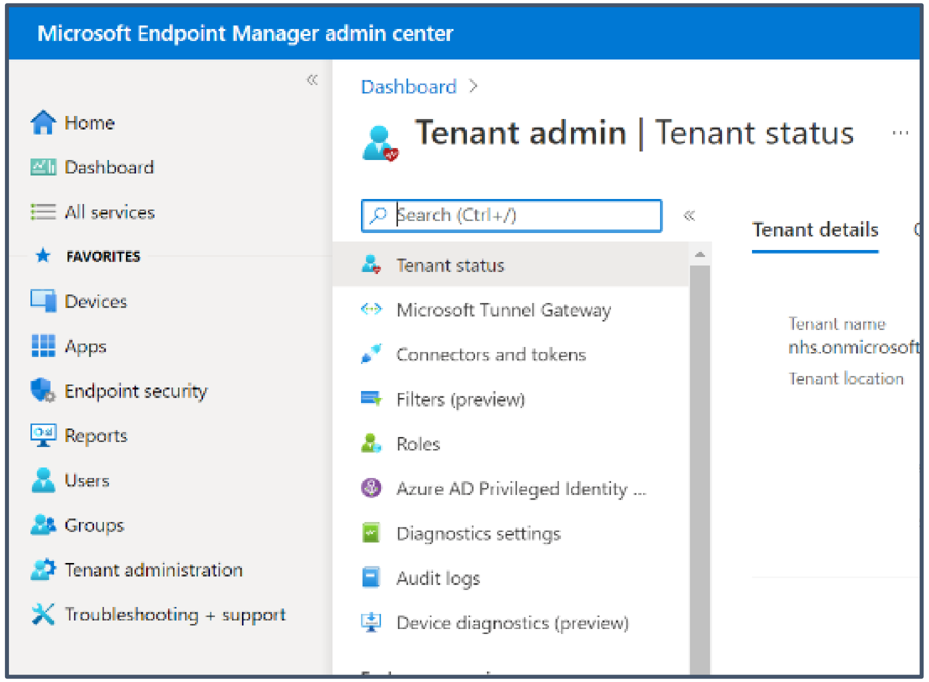
Intune Demo | RBAC Roles

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

TOM

18. 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.

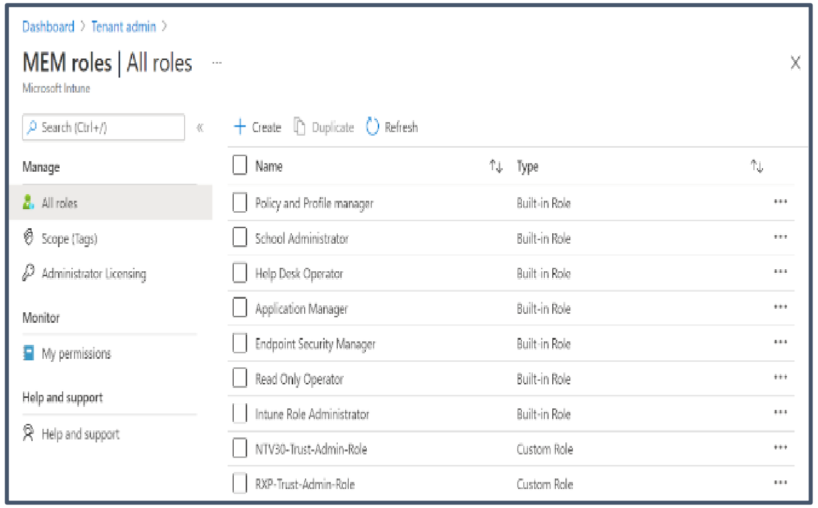
19. He navigates to Tenant Administration > Roles > All roles.



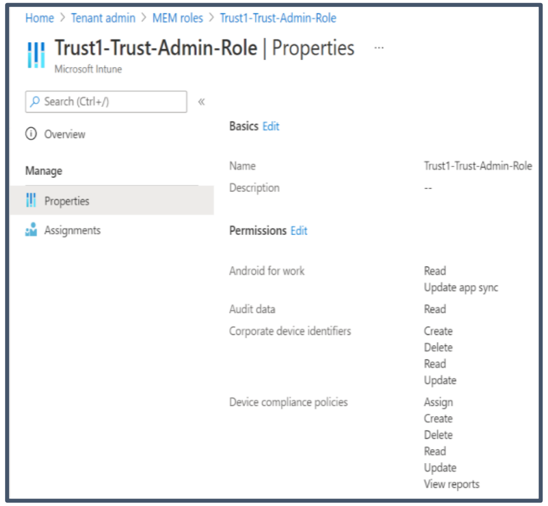
Tenant name
nhs.onmicrosoft

Tenant location

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



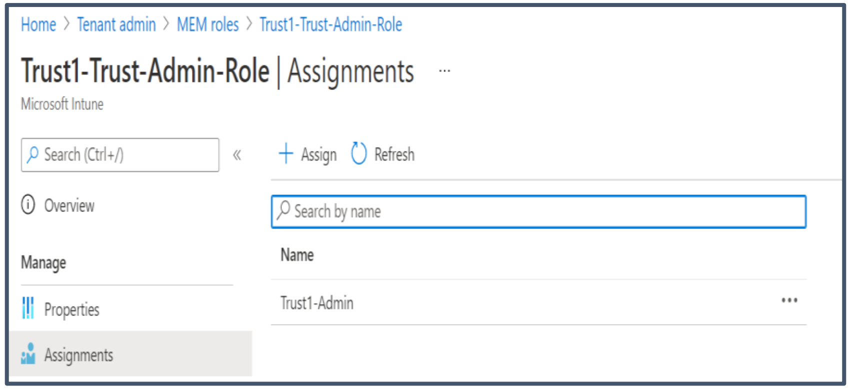
Name	Type
Policy and Profile manager	Built-in Role
School Administrator	Built-in Role
Help Desk Operator	Built in Role
Application Manager	Built-in Role
Endpoint Security Manager	Built-in Role
Read Only Operator	Built-in Role
Intune Role Administrator	Built-in Role
NTV30-Trust-Admin-Role	Custom Role
RXP-Trust-Admin-Role	Custom Role


Home > Tenant admin > MEM roles > Trust1-Trust-Admin-Role
Trust1-Trust-Admin-Role | Properties
Microsoft Intune
Search (Ctrl+/)
Overview
Manage
Properties
Assignments
Basics Edit
Permissions Edit

Name	Trust1-Trust-Admin-Role
Description	--

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

20. 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
Trust1-Admin

Intune Demo | Monitoring

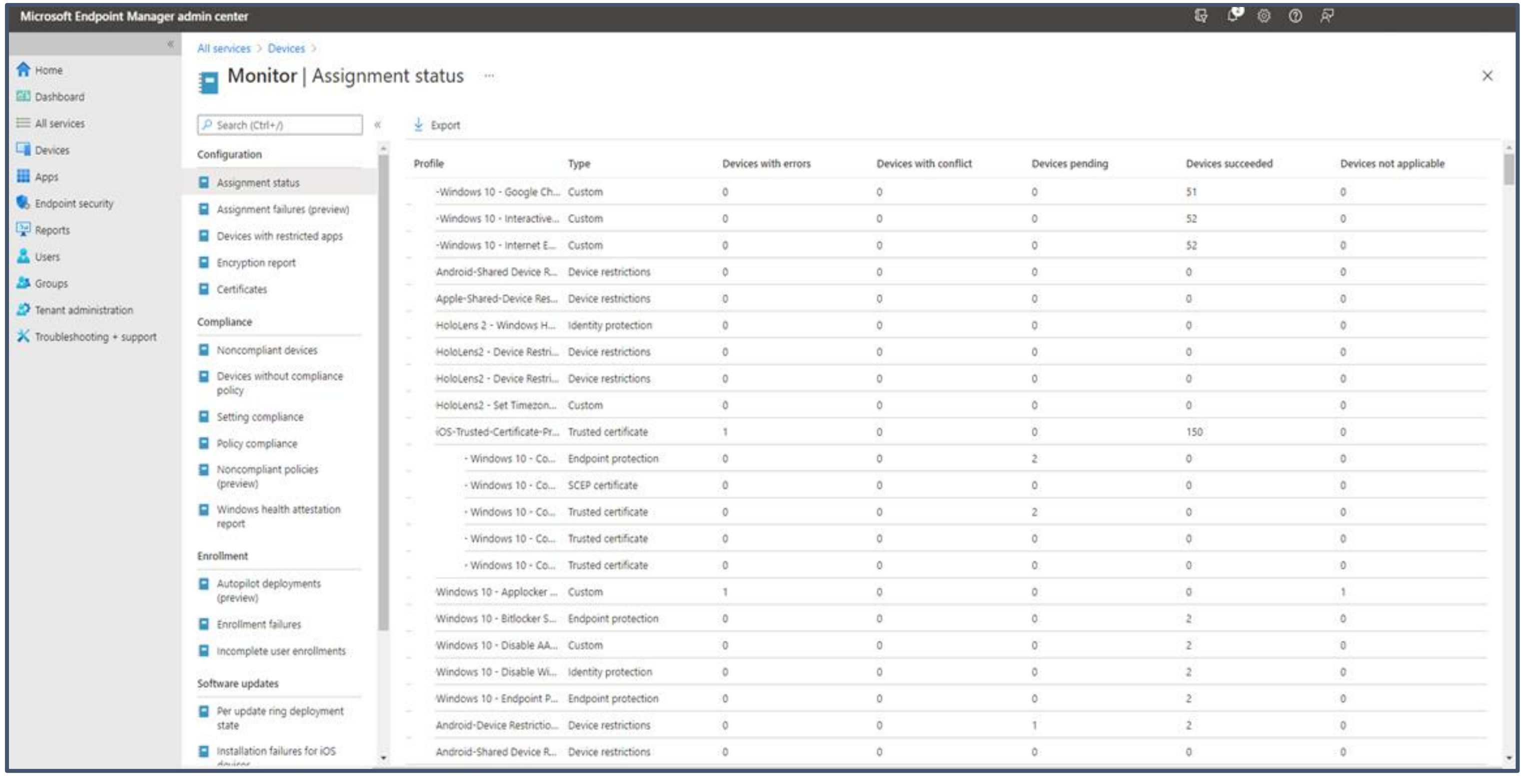
How to access and use the monitoring feature available to support LAs to manage devices on the Intune Portal

TOM

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

He wants to understand how the Intune Portal can help him to produce reports on his devices so he can monitor them for compliance etc.

22. He navigates to Devices > Monitor and then Assignment Status. Tom is also able to view additional monitoring views depending on what he would like to monitor on the left-hand pane.


Microsoft Endpoint Manager admin center
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
All services > Devices >
Monitor | Assignment status
Search (Ctrl+/)
Configuration
Assignment status
Assignment failures (preview)
Devices with restricted apps
Encryption report
Certificates
Compliance
Noncompliant devices
Devices without compliance policy
Setting compliance
Policy compliance
Noncompliant policies (preview)
Windows health attestation report
Enrollment
Autopilot deployments (preview)
Enrollment failures
Incomplete user enrollments
Software updates
Per update ring deployment state
Installation failures for iOS devices
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
HoloLens 2 - 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.

Intune Demo | Wiping / Removing Devices

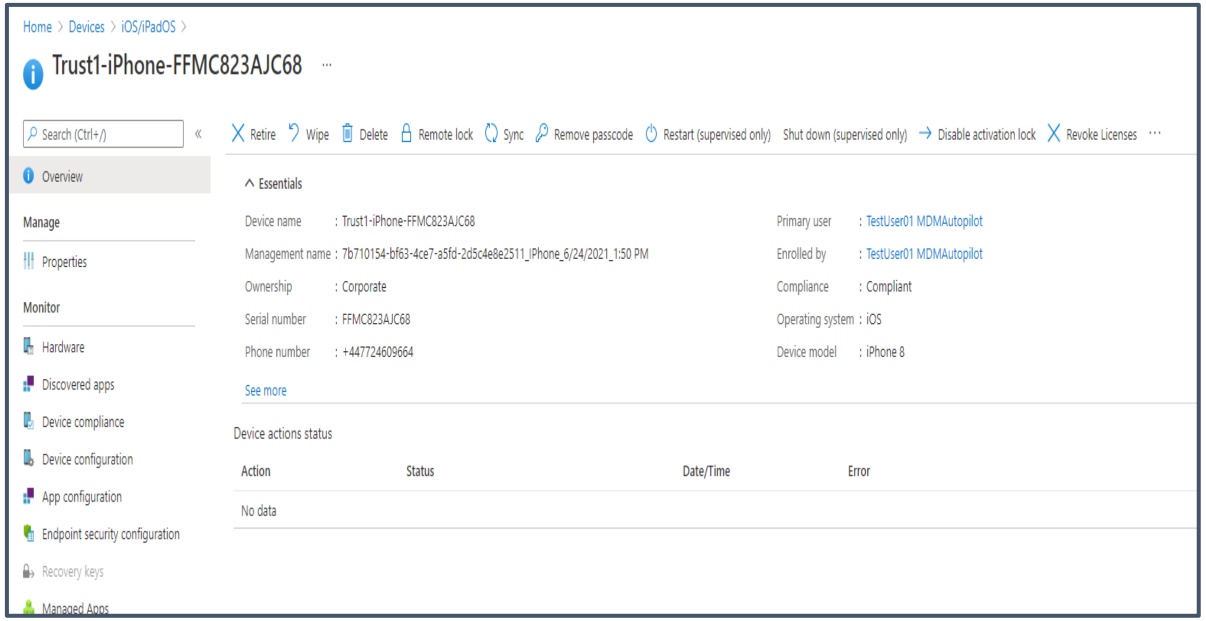
How to access and use the remote wipe, retire and delete features to manage devices on the Intune Portal

TOM

23. Before Tom concludes his review of the Intune Portal, 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.

24. He navigates to Devices and selects a device.

25. 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 portal. This is the view Tom will see for mobile devices.

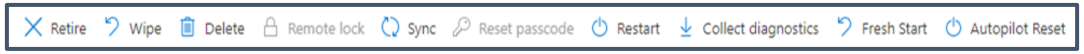


Device name : Trust1-iPhone-FFMC823AJC68
Management name : 7b710154-bf63-4ce7-a5fd-2d5c4e8e2511_IPhone_6/24/2021_1:50 PM
Ownership : Corporate
Serial number : FFMC823AJC68
Phone number : +447724609664
Primary user : TestUser01 MDMAutopilot
Enrolled by : TestUser01 MDMAutopilot
Compliance : Compliant
Operating system : iOS
Device model : iPhone 8

Device actions status

Action	Status	Date/Time	Error
No data			

26. For Windows 10/11 devices and HoloLens 2, Tom will some additional options for wiping and resetting devices. Each option (and it's implications/recommended usage) is explained in the Operations Guide for Local Administrators and Onboarding Managers.



THANK YOU