

NHSmail Intune Service

Session 5: Intune Features & Group Management

17th February 2022



Upskilling Series | Sessions

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



11 sessions over 4 weeks



All sessions are optional



Recordings and session materials available



Suggested further reading & resources



Supported upskilling

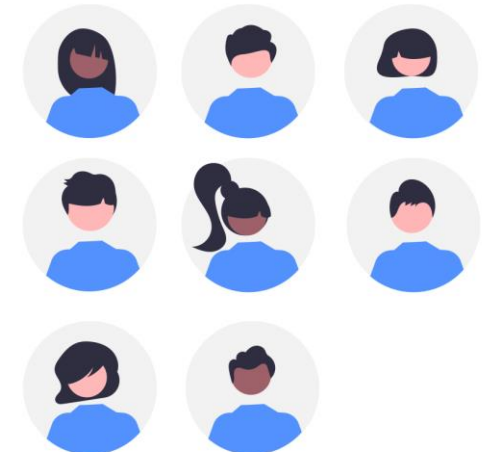
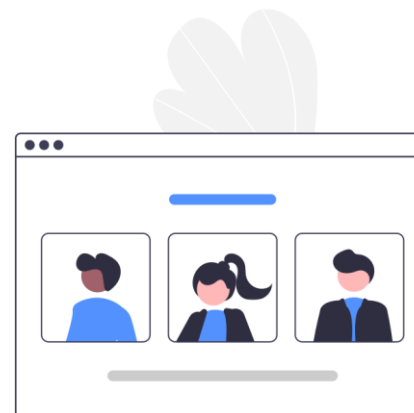
| KEY | | Intune Fundamentals | | Onboarding and Support Basics | Mobile Devices | Windows 10 | | HoloLens 2 | Intune Advanced |
|------------|-------|-------------------------------|--|--|----------------|--|--|---|-----------------|
| Week | Date | Focus | Session Title | Session Content | Duration | 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 | |
| 2 | 14/02 | 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 | |
| | 14/01 | | Documentation Walkthroughs | Orientation and walkthrough of the key supporting documentation available to all onboarded organisations | 30 minutes | All organisations | None required | All LAs | |
| | 16/02 | Intune Fundamentals | Intune Demo | Demo of the key sections of the Intune portal | 1 hour | All organisations | None required | LAs who have never used Intune or are beginners | |
| | 17/02 | | 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 | |
| Recordings | | 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 | |
| | | | iOS/iPadOS 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 | |
| 3 | 21/02 | Windows 10 | Windows 10 Deep Dive | Deep dive session focused on managing Windows 10 devices on NHSmail Intune and preparations required for the Hybrid-Join feature | 30 minutes | Organisations with Windows 10 devices | None required | LAs who will be enrolling and managing Windows 10 devices on NHSmail Intune | |
| Recordings | | HoloLens 2 | 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 | |
| | | 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 | 22/02 | 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 | |
| | 23/02 | | 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 | |
| | 24/02 | | 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 | |
| 4 | 28/02 | | 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 | |
| | 28/02 | Intune Advanced | Windows Hybrid-Join Overview | A look ahead to the upcoming Windows Hybrid-Join feature on NHSmail Intune | 30 minutes | Organisations interested in enrolling Win 10 devices with access to both cloud and on-premises resources | None required | LAs from organisations interested in enrolling Win 10 devices with access to both cloud and on-premises resources | |

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

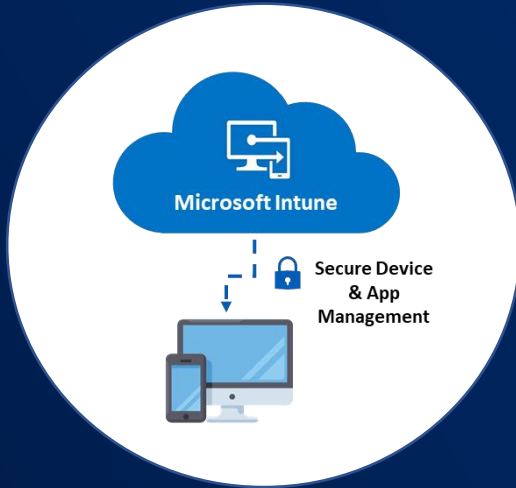
Upskilling Series | Housekeeping

| | |
|-----------------------|---|
| Event name: | Session 5: Intune Features & Grp. Mgmt. |
| Date: | 17 February 2022 |
| Location: | Online Webinar |
| Start / end time: | 13:00 - 14:00 |
| Attendees: | NHSmal Intune Team and LAs from February onboarding organisations. |
| Objectives & purpose: | To provide an overview of key Intune features so LAs can understand the platform in greater detail and demo the Group Management application. |
| End goal: | Attendees understand more about Intune specifics and know how to access and use the Group Management app. |

| Housekeeping |
|--|
| <ul style="list-style-type: none">• 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 one of these, please raise your hand. Alternatively, please use 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. |



Session 5



Intune Features & Group Management

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 5** will focus on providing more detail on the key features of Intune to enable LAs to **understand the platform in greater depth** and demonstrate how to use the Security Group Management application.

Objectives of this session

- Provide a **detailed overview** of key Intune features and explain how they work.
- Explain **technical terms** and Intune specifics.
- Support organisations to access and use the **Security Group Management App** and demonstrated what creation and management actions can be completed via the app.
- **Answer any questions** related to Intune feature or the Security Group Management App.

Agenda

Session 5: Intune Features & Group Mgmt.

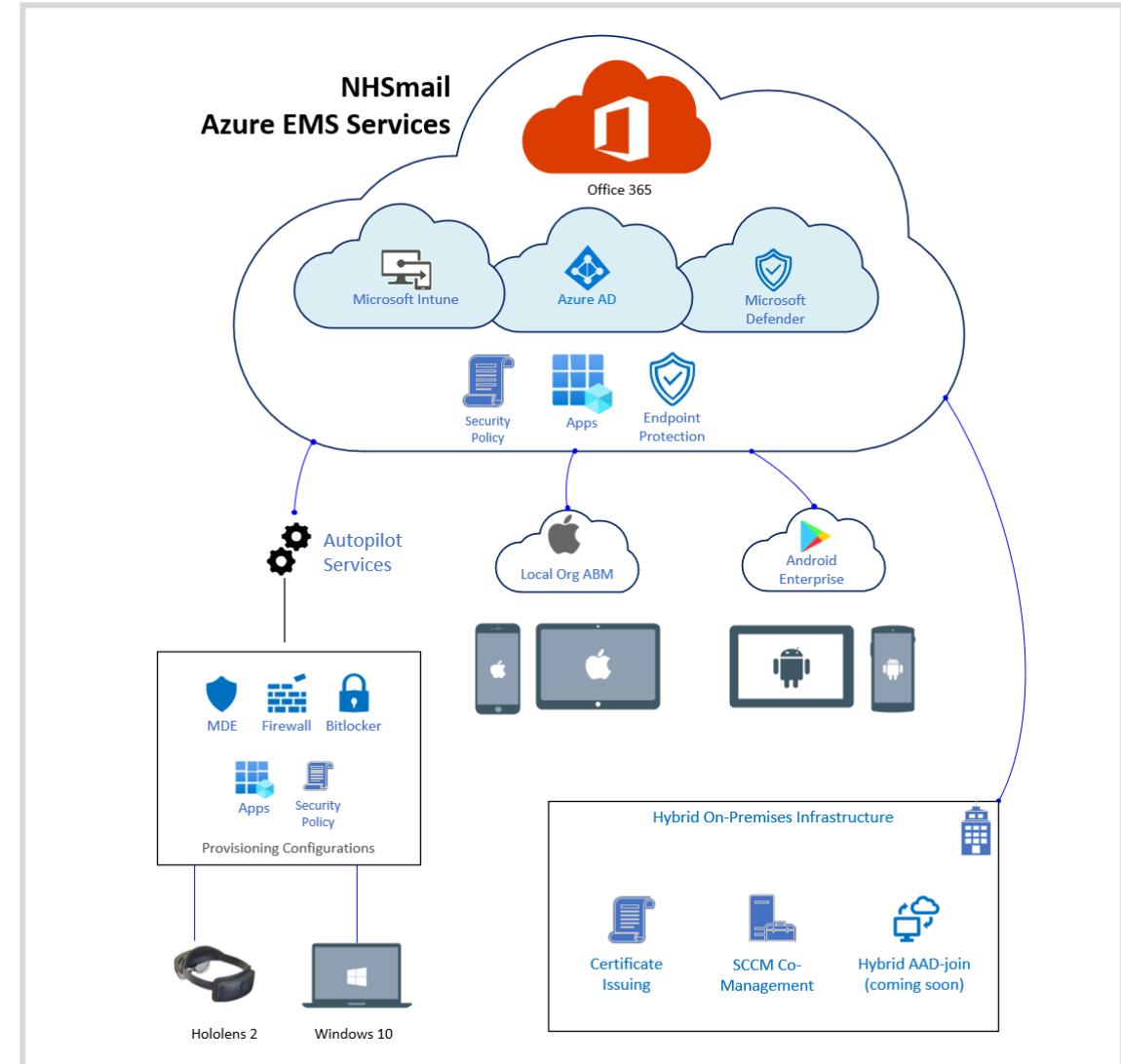
Menti code: 5868 7964

- 01** Overviews and Objectives
- 02** NHSmail Intune Solution
- 03** RBAC & Security Baselines
- 04** Scope Tags
- 05** Naming Standards
- 06** Enrolment Restrictions
- 07** Configuration Profiles
- 09** Compliance Policies
- 10** Group Management App Overview
- 11** Group Management App Demo
- 12** Questions and Close

Intune Features| NHSmail Intune Solution

The NHSmail Intune solution builds upon existing infrastructure to provide a seamless experience for LAs and end users

- The NHSmail Intune solution builds upon existing infrastructure to provide a seamless experience for LAs and end users.
- The solution leverages existing NHSmail Azure capabilities, including Azure AD (AAD), Intune and Microsoft Defender for Endpoint (MDE).
- NHSmail Intune offers **centralised device management of technology platforms** (Windows 10, Apple iOS/iPadOS, HoloLens 2 and Android OS).
- The solution offers **devolved powers and rights** between NHS Digital and individual orgs.
- A '**standardised NHSmail baseline**' is defined globally across the NHSmail Intune platform. This refers to a set of standardised apps, settings and policies configured and deployed for each technology platform. For Windows 10 there is a centralised Security Baseline policy which is enforced to all Windows 10 'Cloud' devices enrolled into Intune. There are also "pencilled-in", customise-able baselines available for all device types.
- Although centrally managed, an **Intune Role Based Access Control (RBAC) model enables LAs to maintain control** over their organisation's devices.
- The NHSmail Intune service will **enable organisations to Co-Manage devices** with SCCM and Intune as well as connect on-premises **Certificate Issuing** services for VPNs, Wifi, etc.
- A hybrid-join experience for Windows 10 will be available soon.



Intune Features | RBAC Overview

Overview of what RBAC permissions are, who is granted them, what the permissions allows LAs to do and why they are important for NHSmail Intune



WHAT ARE ROLE BASED ACCESS CONTROL (RBAC) PERMISSIONS?

- Role Based Access Control (RBAC) permissions provides LAs with the ability to administer configuration items within NHSmail Intune, including devices, Groups, applications and policies.
- Any LA trying to enrol and manage an organisation's devices within NHSmail Intune, **who does not have the correct RBAC permissions, will be unable to complete most basic enrolment and device management tasks.**



WHO IS GRANTED RBAC PERMISSIONS WHEN AN ORG. ONBOARDS?

- When completing the Onboarding Request Form, organisations were asked to confirm which LAs from their organisation would need to be assigned custom RBAC permissions. **These LAs were provided with RBAC permissions during the technical onboarding process which the NHSmail Intune Team completed.**
- Organisations **can request for additional LAs to be provided with RBAC permissions by raising a Service Request at any time.** There is **no limit** to the number of LAs who can be given RBAC permissions at any organisation.



WHAT CAN LAS WITH RBAC PERMISSIONS DO?

- Custom RBAC permissions on Intune allow LAs to complete all required device enrolment and device management tasks for iOS/iPadOS, Android, Windows 10 (and later) and HoloLens 2 devices.
- LAs can view specific details of these RBAC permissions via the Intune Portal. **These are set centrally, and additional permissions can't be added.**
- Although Group creation and management tasks on NHSmail Intune need to be completed via the Security Group Management Application, the RBAC permissions provided to LAs at onboarded organisations **also permit the ability to complete all Group creation and management tasks via that custom application.**



WHY ARE RBAC PERMISSIONS IMPORTANT TO NHSMAIL INTUNE?

- The custom roles provided to nominated LAs at onboarded organisations allow LAs at different organisations to **administer the management of their device estate in isolation from other organisations,** despite all onboarded organisations using a shared Intune tenant.

Intune Features | RBAC and Security Baselines

The NHSmail Intune solution includes baseline settings which individual organisations can apply policies and settings on top of

NHSmail Intune RBAC

Baseline Policies and Delegated Policies

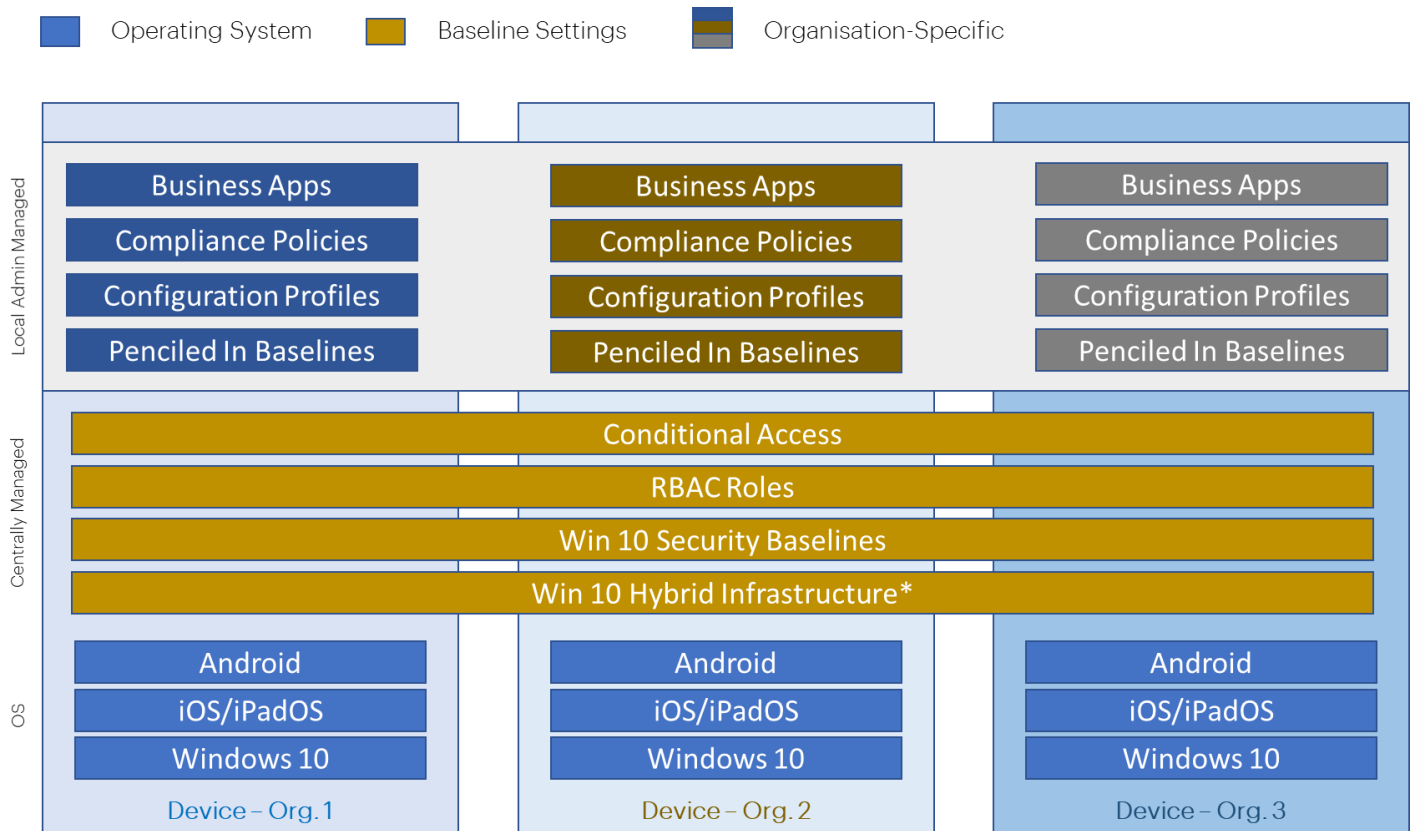


Intune will be configured to provide a core set of centrally managed Windows 10 Security Baselines. Organisations will be able to view these settings via the Intune Portal but will not be able to change them. On top of these baselines, there are “pencilled-in” policies and settings which can be changed by LAs.



Local Administrators at onboarded organisations will be able to set up their own Groups, Policies, Profiles and Apps on top of the centrally managed settings ensuring a high degree of customisation, oversight and local autonomy.

NHSmail Baselines

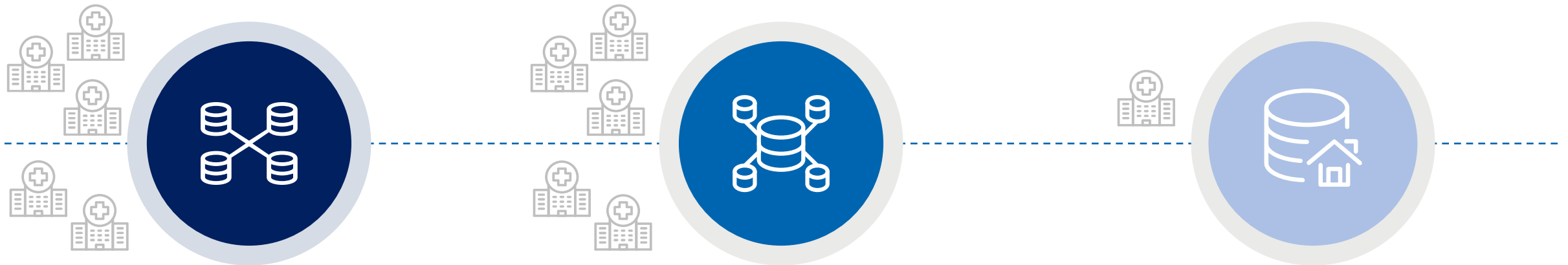


*Coming soon

Intune Features | Configuration Items

NHSmal Intune allows segregation of overarching configuration settings into two distinct categories; settings that are 'tenant-wide' and settings that can be delegated to LAs (via Roles). The settings delegated to LAs are limited in scope to ensure that they only affect the devices and settings a LA is assigned to

NHSmal Intune enables LAs to administer their configuration items in isolation from other organisations'. This includes administering their own devices, policies, and apps via Intune. It is important that any changes made by an LA only affect the devices and users within their organisation. To facilitate this requirement, NHSmal Intune has a **robust RBAC model** to provide general-purpose roles for every day admin tasks, as well as **custom roles provided for a more fine-grained approach** to permission management.



Set by central NHSmal IT Admins

TENANT-WIDE CONFIGURATIONS

- MDM Authority
- Apple MDM Push Certificate
- Manage Google Play account
- Android Enterprise – corporate owned fully managed enrolment
- Android Enterprise – Enrolment Profiles
- Device Clean-up rules
- Conditional Access – requires AAD permissions

Set by central NHSmal IT Admins

CENTRAL NHSMAIL CONFIGURATIONS

- Intune Company Portal - Branding and customisation
- Custom notifications
- RBAC and Scope Tags (Provided to LAs)
- Windows 10 Security Baselines
- Android Enterprise – Corporate Owned Dedicated Device

Delegated to organisations' Local Admins

LOCAL ADMIN CONFIGURATIONS

- Apple Automated Device enrolment
- Autopilot deployment profiles
- Device & App management
- Device compliance policies
- Device & App configuration profiles
- Apple VPP tokens & iOS app provisioning profiles
- Terms of use
- Update policies for iOS/iPadOS

Intune Features | Scope Tags

Scope tags determine which objects are visible to LAs and provide logical groupings within Intune



WHAT IS A SCOPE TAG?

- At the most basic level, a scope tag in Intune is an **identifier**.
- Scope tags need to be given a name and can then be applied to objects within Intune, allowing LAs to control the visibility of objects.



WHY ARE THEY USED IN INTUNE?

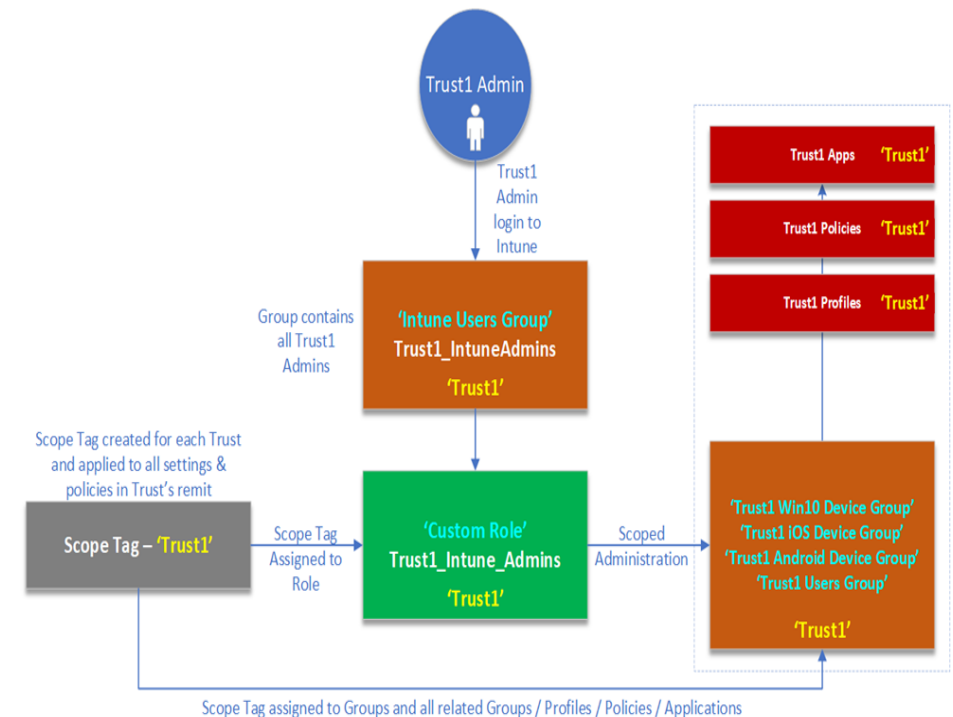
- Scope tags provide a **logical grouping** of users, devices, policies and settings tied to a specific role.
- Scope tags ensure that LAs have the right visibility to objects within Intune and prevent LAs from different organisations accessing another organisation's policies or devices.



ARE THE SCOPE TAGS ALREADY CREATED?

- Each organisation which onboards to NHSmail Intune will have scope tags created as **part of the technical onboarding process**.
- The naming convention of these scope tags for onboarded organisations is [ODS Code].

Scope tags and custom roles example:



Important: Any new device group must be added into the scope tag to enable visibility of the devices in Intune.

Intune Features | Naming Standards

Naming standards allow LAs using NHSmail Intune on the shared tenant to identify their devices, groups, profiles and settings with ease

There are several instances within NHSmail Intune, wherein LAs will need to follow the naming standards outlined in the [Operations Guide for Local Administrators and Onboarding Managers](#). Failure to follow the correct naming standards when creating groups of devices, profiles, policies and settings will cause problems and make it much harder to identify your objects or configuration items.



The **naming convention** within the Intune environment will utilise each organisation's unique Organisation Data Service (ODS) code.



This helps **differentiate** each organisation's scoped grouping of configuration items when viewed either by an LA or the Intune Live Service Team.

AAD group naming standards are in place to ensure that both 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 LAs can easily identify what is contained within a AAD group.



<ODS>-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>-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.**

Example Naming Standards:



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

Intune Features | Enrolment Restrictions

There are several enrolment restrictions in place which LAs need to be aware of before beginning the enrolment of devices



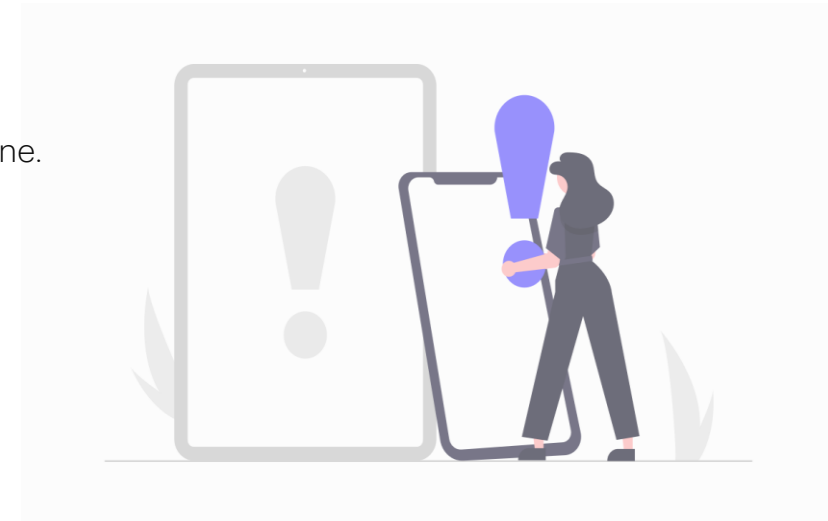
NUMBER OF DEVICES

- There is a limit to the number of devices that can be linked to a user or administrator in Intune.
 - Administrator limit: **15 devices**
 - End user limit: **5 devices**



TYPES OF DEVICES & MINIMUM OS

- Personal devices **should not** be enrolled onto NHSmail Intune.
- Only the supported platforms should be enrolled: iOS/iPadOS, Android, Windows 10 and (later) HoloLens.
- Devices will need to meet minimum OS requirements to be enrolled onto the platform.
- LAs should refer to the [Operations Guide for Local Administrators and Onboarding Managers](#) for full details on the specific minimum OS required.



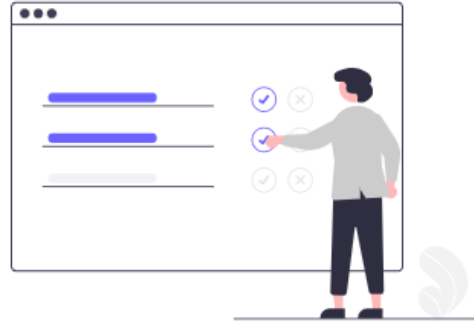
Intune Features | Configuration Profiles

Configuration profiles allow LAs to determine what settings are applied to a device



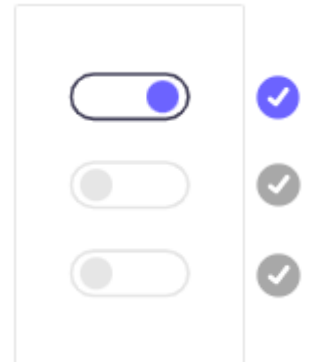
WHAT ARE CONFIGURATION PROFILES?

- Configuration profiles are policies or settings that configure devices.
- These profiles allow LAs to add and configure settings, and then push these settings to specific groups of devices.
- Configuration profiles operate in a similar manner to group policies in SCCM.



WHAT CAN LAS DO?

- LAs can use configuration profiles to manage what end users can do and see on their devices.
- For instance, LAs can do the following using configuration profiles, for example:
 - ✓ allow or disable features
 - ✓ set password rules
 - ✓ allow or restrict specific policies
 - ✓ apply backgrounds
 - ✓ pin apps to the start bar for all devices
- LAs can maintain granular control over device settings by using configuration profiles.
- Configuration profiles can be found for each platform under devices on the Intune Portal.
- The [Operations Guide for LAs and Onboarding Managers](#) includes a full list of configuration profiles which can be changed by LAs and instructions on how to create and assign configuration profiles for each device type in NHSmail Intune.



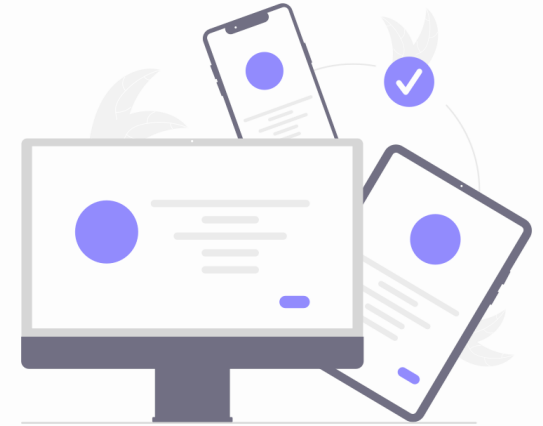
Important: Any deviation from the pencilled-in baseline settings and configuration should be done with consideration and prior testing. Organisations are solely responsible for changes made by their LAs that have been provided with Intune RBAC permissions.

Intune Features | Compliance Policies

Compliance policies are policies which help protect organisational data by enforcing requirements that users and devices need to meet

Compliance policies are sets of rules and settings which devices and end users must meet to be compliant. In practical terms, compliance policies support LAs at onboarded organisations to increase and assure the security of devices and data and monitor their entire device estate easily.

- Intune compliance policies can include actions that will apply to all devices which are non-compliant, such as alerts to users to complete certain actions so that their device/s are compliant with the compliance policy configured.
- When combined with **Conditional Access** (available soon), compliance policies can be configured by organisations to block end users and devices which are non-compliant.



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**.

These are the baseline ‘pencilled-in’ settings.



Compliance Policy Settings

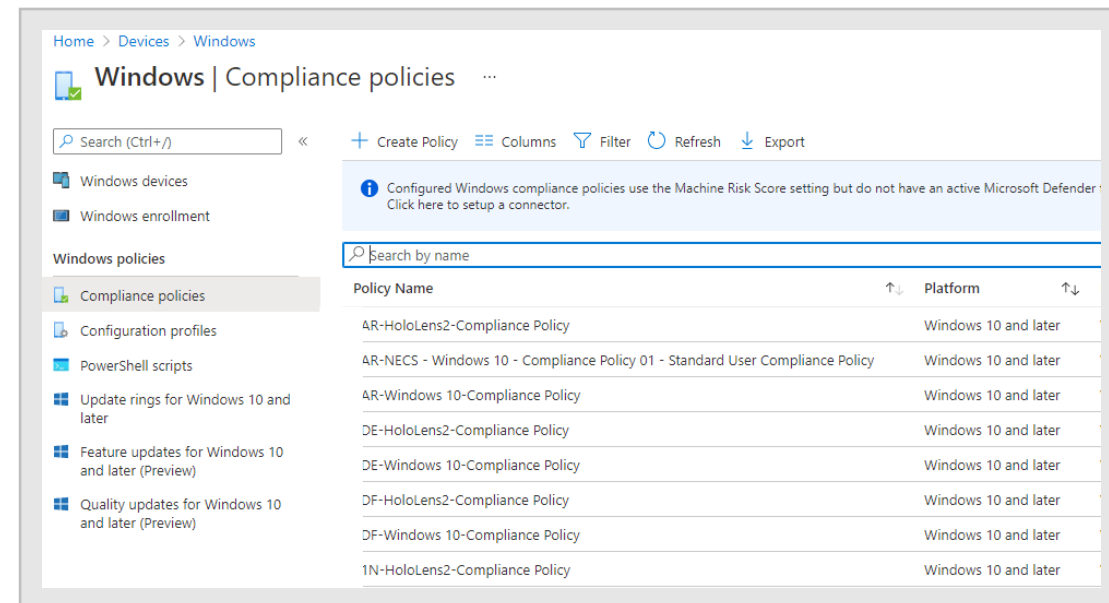
Compliance policy settings are **tenant-wide** settings that are like built-in compliance policy which every device receives. **These settings are not editable by individual organisations.**



Device Compliance Policy

Device compliance policy settings are **platform-specific rules** LAs **configure and 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.



Intune Features| Policy Conflicts

Planning is important to minimise any potential rework associated with setting up conflicting policies when configuring devices



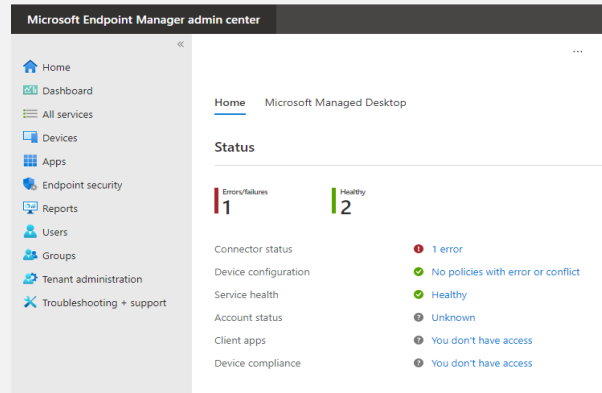
- RBAC permissions allow LAs to configure their devices as required, but it is recommended that planning is completed prior to configuration to avoid policy profile conflicts.
 - For example, if your organisation needs to set a **compliance policy** that requires passwords to be **6 characters or longer** but your organisation also set a **device restriction policy** which requires an **8 character password or longer** to reset devices, these policies will conflict and neither will be successfully applied to the target devices.
 - The most likely policies to have conflicts are apps, compliance policies and especially, configuration profiles.
- ✓ A full list of recommended policy settings is available as part of the [Operations Guide for Local Administrators and Onboarding Managers](#).



SPOTTING CONFLICTS



LAs will be able to see any conflicts across policies in the monitoring section of the Intune Portal. Conflicts may also show up on the policy itself if relevant.



LAs can click on the conflict to find out more about the specific details of the conflict including the profiles involved, in order to then rectify the issue.

RECOMMENDATIONS

In order to avoid the frustration of setting conflicting policies and the rework required to identify these and reconfigure them, it is recommended that LAs at onboarded organisations bear the following in mind:



It is advised that organisations have their own high-level design for their policies to ensure that all policies will meet requirements and can operate alongside one another.







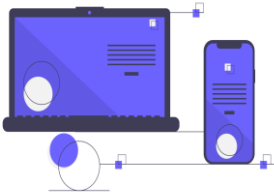
Organisations should not begin pushing policies to their devices until there has been some planning of policies.

Intune Features | Shared Device Modes

Overview of Shared Device Modes available on Intune-enrolled devices including key features, licencing requirements and expected end user experience

Beyond single user, the NHSmail Intune Solution supports several Shared Device Modes, enabling organisations to decide which mode will work best for their specific context.

| Platform |  |  |  |  |
|---|--|--|---|--|
| Shared Device Mode | iPadOS Non-User Affinity / Guest Mode | iOS Managed Apple ID | Windows 10 Autopilot Device Registered with Intune MDM | Android Shared Device Mode (Dedicated) |
| Licences Required | No user licence For Apple devices, app licences are required to be deployed via ABM as per standard app deployment process. | No user licence For Apple devices, app licences are required to be deployed via ABM as per standard app deployment process. | EMS E3 and AADP2 | No user licence |
| Password required for session log-in? | No | Yes | Yes | Can be set by LAs |
| Can LAs deploy apps? | Yes | Yes | Yes | Yes |
| Features / Capabilities & User Experience | <ul style="list-style-type: none">✓ No user log-in✓ Ease of use as end users are not required to remember credentials✓ Session history deleted when user logouts to ensure security✗ End users are not able to create personalised user profile | <ul style="list-style-type: none">✓ Sign-in / Out functionality allows end users to create a customised user profile✗ End users are required to remember sign-in credentials to maintain device security and create a customised user profile | <ul style="list-style-type: none">✓ Sign-in / Out functionality allows end users to create a customised user profile. Any user with a NHSmail ID and licence can log in✗ End users are required to remember sign-in credentials to maintain device security and create a customised user profile | <ul style="list-style-type: none">✓ QR code enrolment is fast and simple for end users |

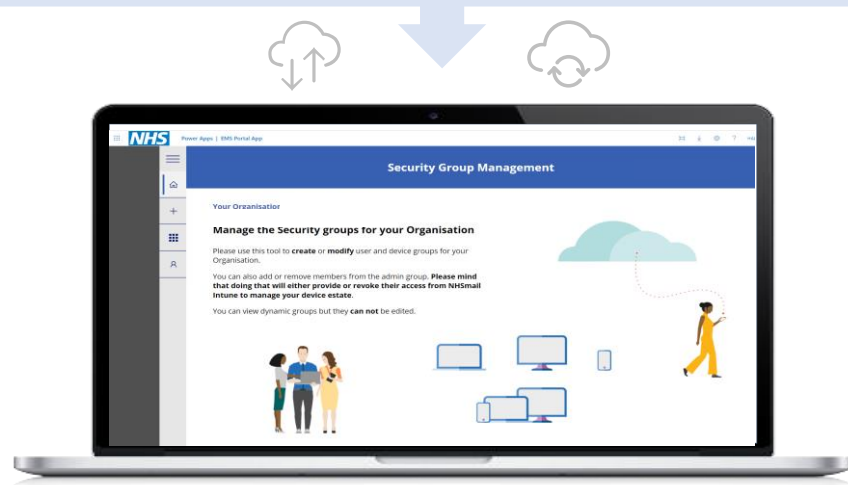


Intune Features | Group Management App

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.



- ✓ 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 Win 10 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 Win 10 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.

DEMO

Security Group Management Application



Group Mgmt. App | Journeys Overview

The following demo will cover the below 5 journeys. These 5 journeys do not cover every action possible but do demonstrate the most common actions



JOURNEY 1: FIRST TIME LOGIN

- ✓ Access the Group Management App for the first time
- ✓ SSO login should work for all future logons



JOURNEY 2: VIEW & SEARCH

- ✓ View Groups created during technical onboarding of your organisation
- ✓ Use the search function to find Groups you have created
- ✓ You will be able to view and search all Groups assigned to your ODS scope tag



JOURNEY 3: CREATE GROUPS

- ✓ Create additional Groups to enable the management of groups of users and Win 10 devices
- ✓ These Groups should always be assigned to the scope tag for your organisation



JOURNEY 4: USER SEARCH

- ✓ View a full list of users
- ✓ Check which users are assigned to which Groups



JOURNEY 5: ADD/DELETE MEMBERS AND GROUPS

- ✓ Add and remove other LAs to the Group Management app without needing to request access for them

Group Mgmt. App | Journey 1

Accessing and using the Group Management App for the first time



West View NHS Foundation Trust has recently onboarded to NHSmail Intune Service, and its staff predominantly use Apple and Windows 10 devices.



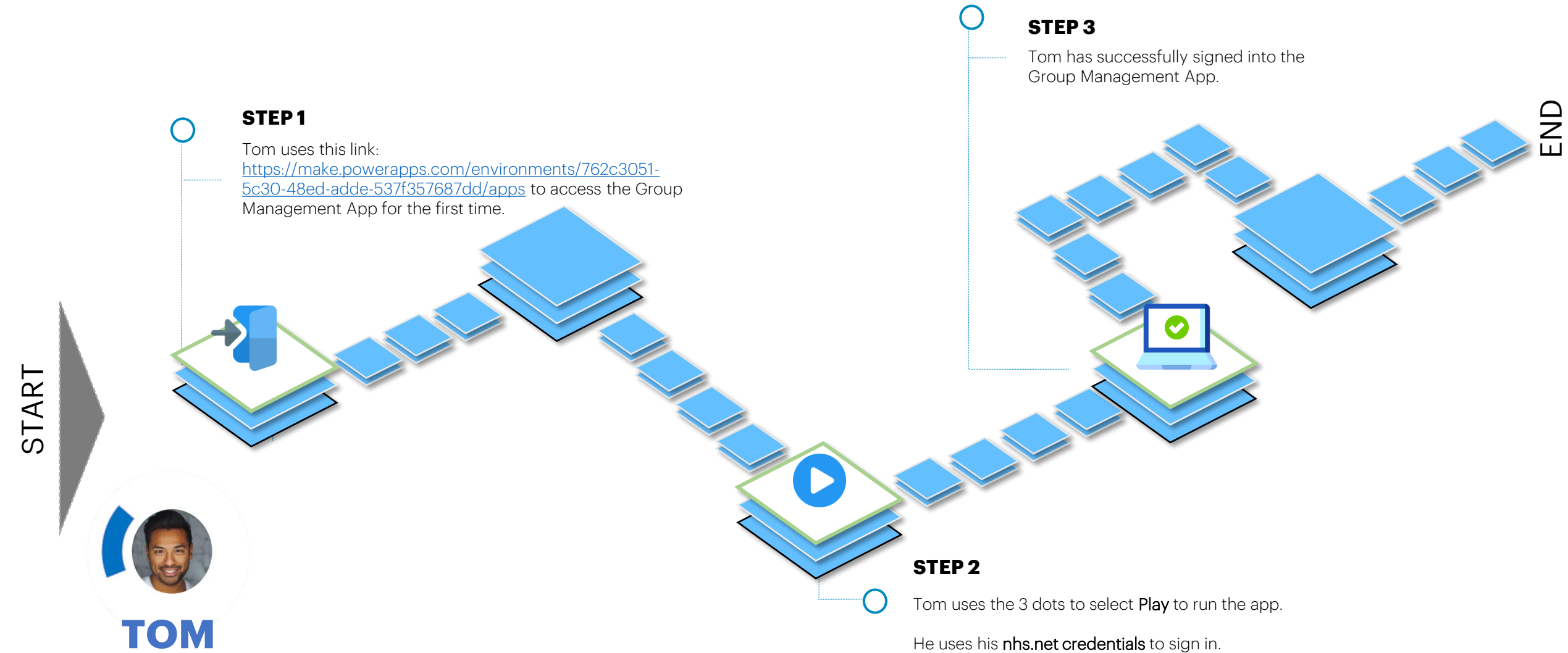
Tom is an **LA** at West View NHS Foundation Trust. He will be testing NHSmail Intune and enrolling some devices to understand how the platform works and the functionality available.

Tom would like to review the Group Management application to see how it works. This is Tom's **first time logging** in to the **Group Management App**.



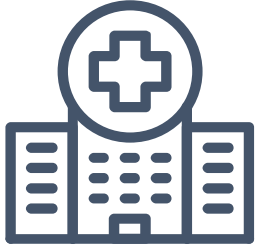
Key takeaway: Once an LA has accessed the Security Group Management Application, the steps which will be shown next will not need to be followed for subsequent logins. After the initial login - provided the LA is logged in with their nhs.net credentials - they should be able to use SSO to login.

Group Mgmt. App | Journey 1: First time login



Group Mgmt. App | Journey 2

Viewing and searching for Groups within the Group Management application



West View NHS Foundation Trust has recently onboarded to NHSmail Intune Service, and its staff predominantly use Apple and Windows 10 devices.



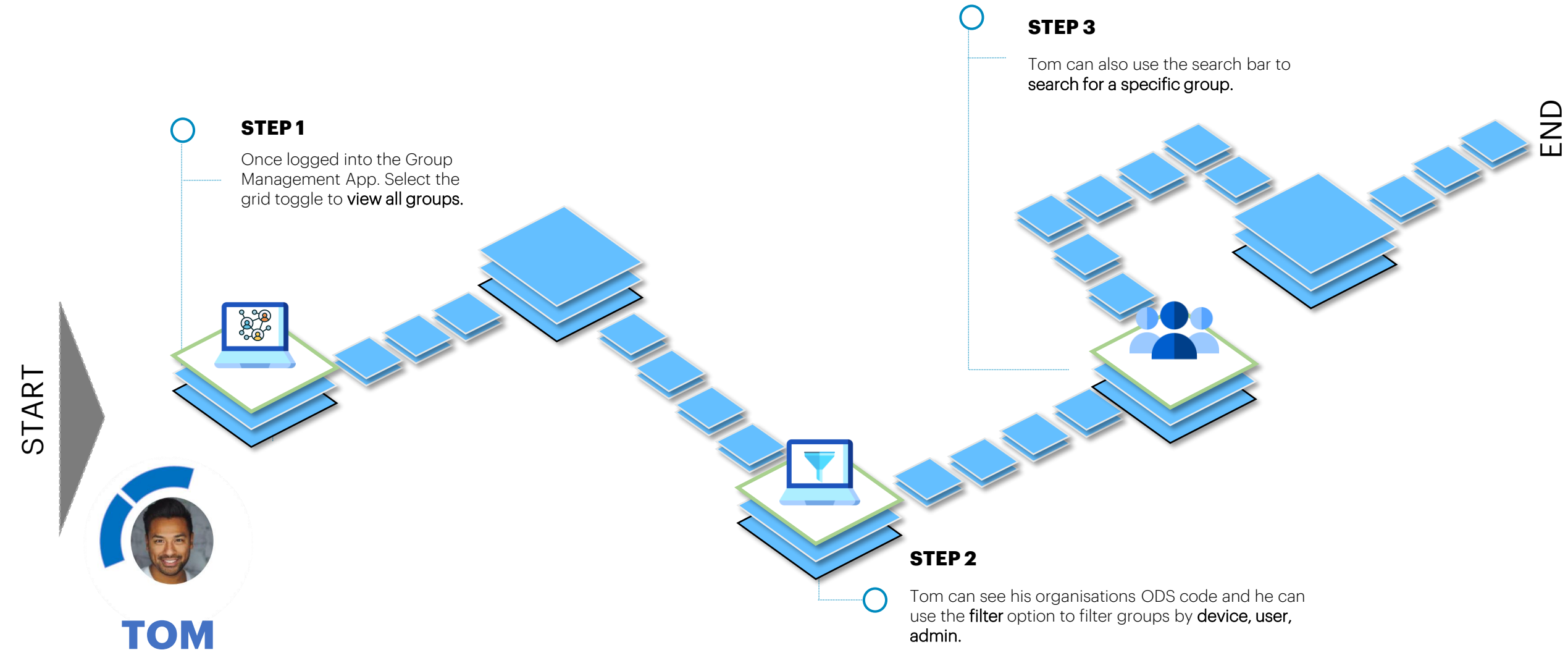
Having successfully logged into the app for the first time, Tom would now like to **view the groups** which have already been set up for this organisation as part of the technical onboarding process. There should be several standard pre-configured Groups available for Tom to use, including an Intune Admins Group.

Tom would also like to check that the search function can be used to **filter** Groups.



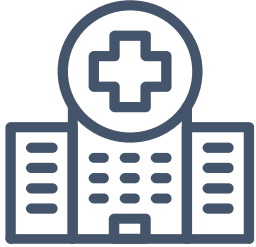
Key takeaway: LAs will be able to view and search all Groups assigned to their organisation's ODS scope tag.

Group Mgmt. App | Journey 2: View and Search



Group Mgmt. App | Journey 3

Creating Groups in the Group Management App



West View NHS Foundation Trust has recently onboarded to NHSmail Intune Service, and its staff predominantly use Apple and Windows 10 devices.



Tom has found and viewed the groups which had already been set up for this organisation. He now wants to **create some additional groups** using the Group Management app in order to better manage devices and users at his organisation.

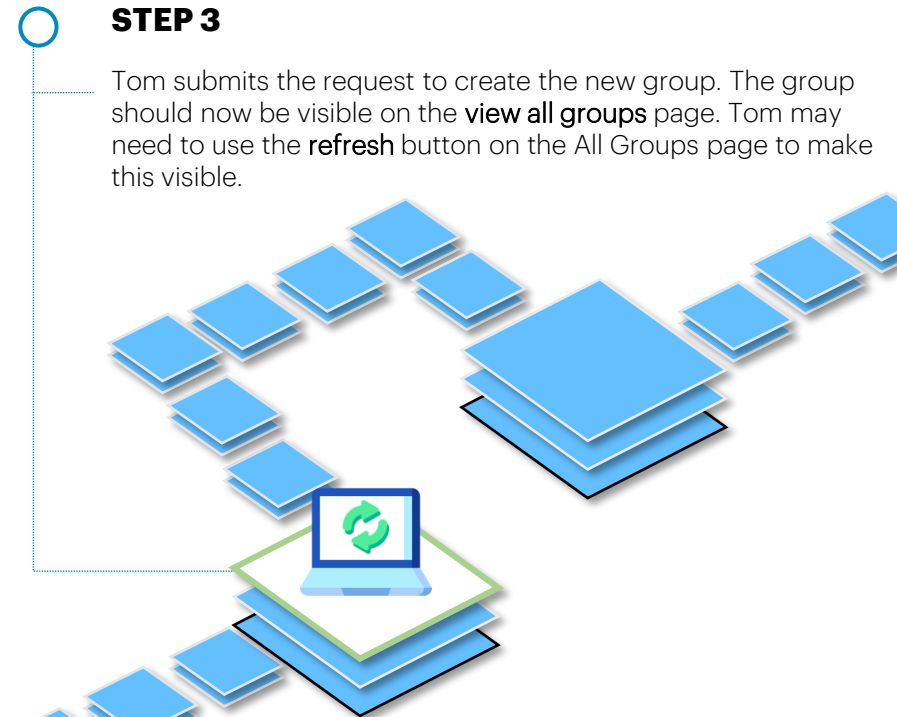
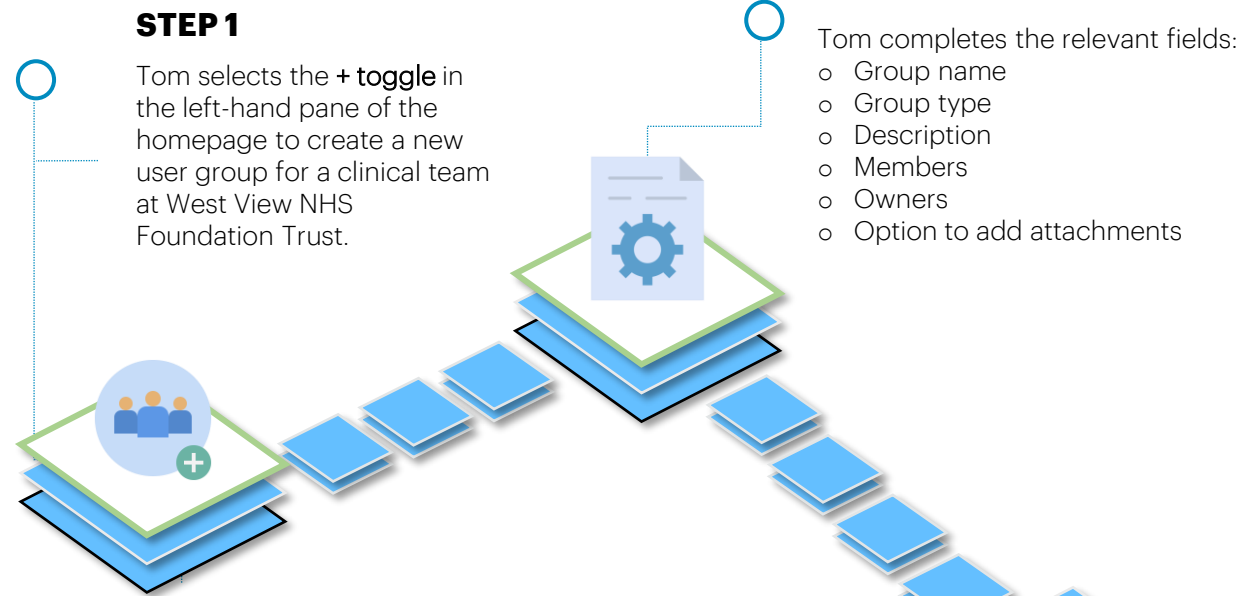
Specifically, Tom would like to **create a separate user group** for the community nursing team at West View NHS Foundation Trust so he can apply specific policies to this user group.

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 via [Helpdesk Self-Service](#).



Key takeaway: Any new groups created should be assigned to the scope tag (your organisation's ODS code) in NHSmail Intune.

Group Mgmt. App | Journey 3: Create Groups



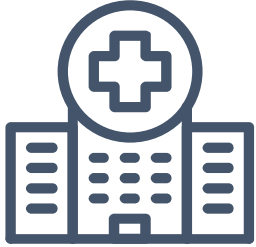
END

START

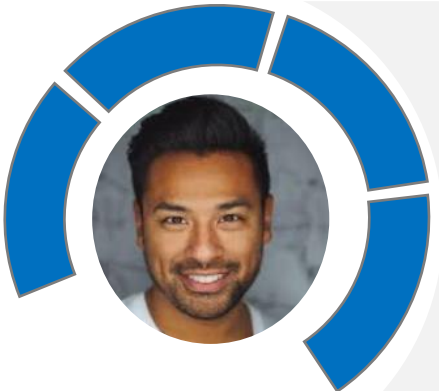


Group Mgmt. App | Journey 4

Search a list of users in order to check that users are all assigned to the correct Groups



West View NHS Foundation Trust has recently onboarded to NHSmail Intune Service, and its staff predominantly use Apple and Windows 10 devices.



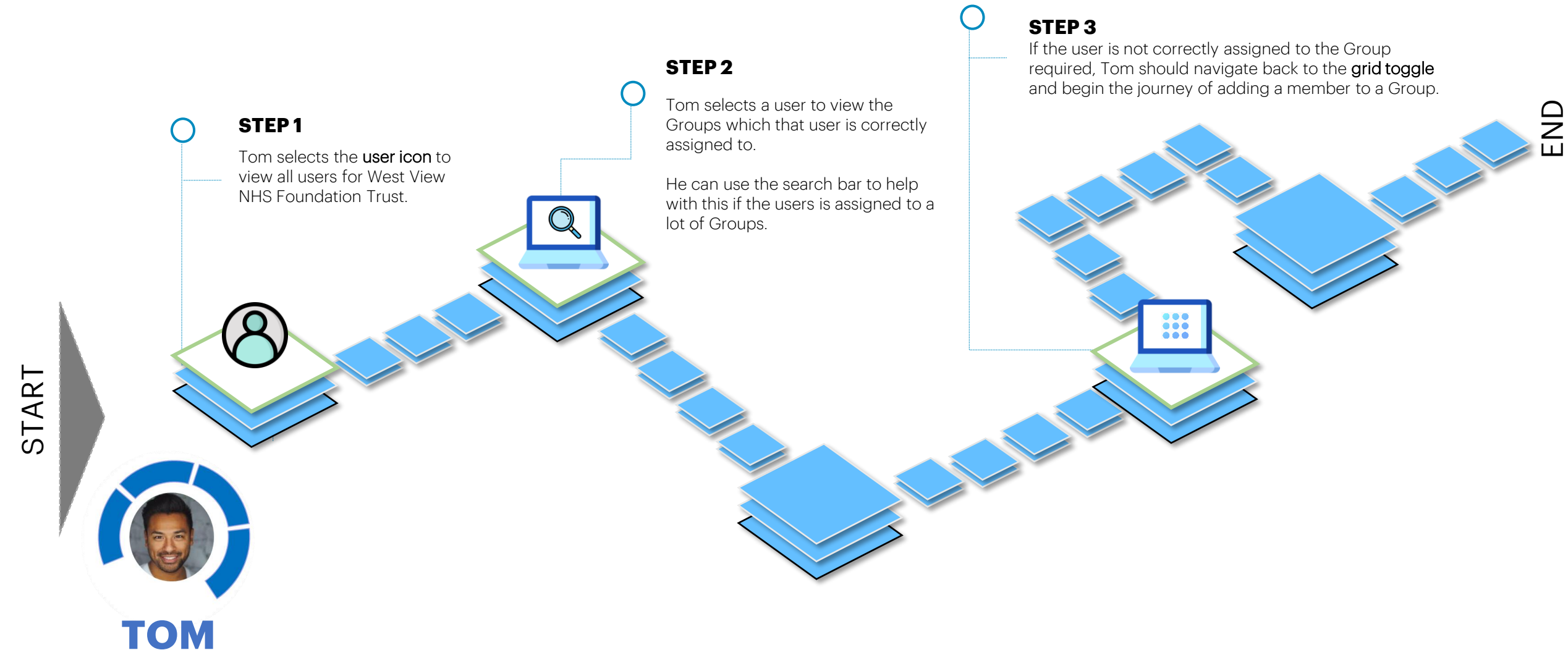
Tom has now created lots of additional groups using the Group Management App but one member of his team isn't able to manage a Group which he should be able to manage. Tom needs to check that this team member has been correctly assigned to the Group in question.

He discovers that the team member has not been correctly assigned to the Group, so Tom now needs to add them to the Group.



Key takeaway: Group memberships can always be checked to see whether access issues are the result of LAs not being correctly assigned to Groups.

Group Mgmt. App | Journey 4: User Search

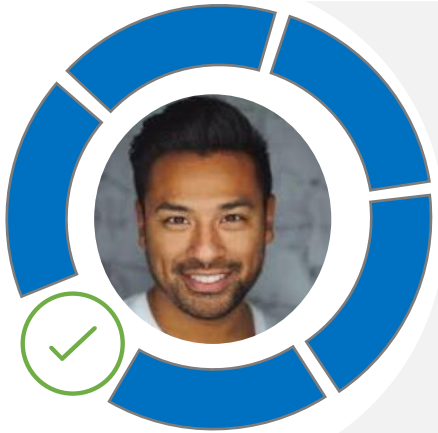


Group Mgmt. App | Journey 5

Completing several Group management tasks including adding members to Groups and deleting members from Groups



West View NHS Foundation Trust has recently onboarded to NHSmail Intune Service, and its staff predominantly use Apple and Windows 10 devices.



Tom now needs to make some updates to the Groups for his organisation. These actions will become part of Tom's regular Group management tasks as he will need to ensure that all Groups are up-to-date regularly so policies can be applied correctly to devices and users.

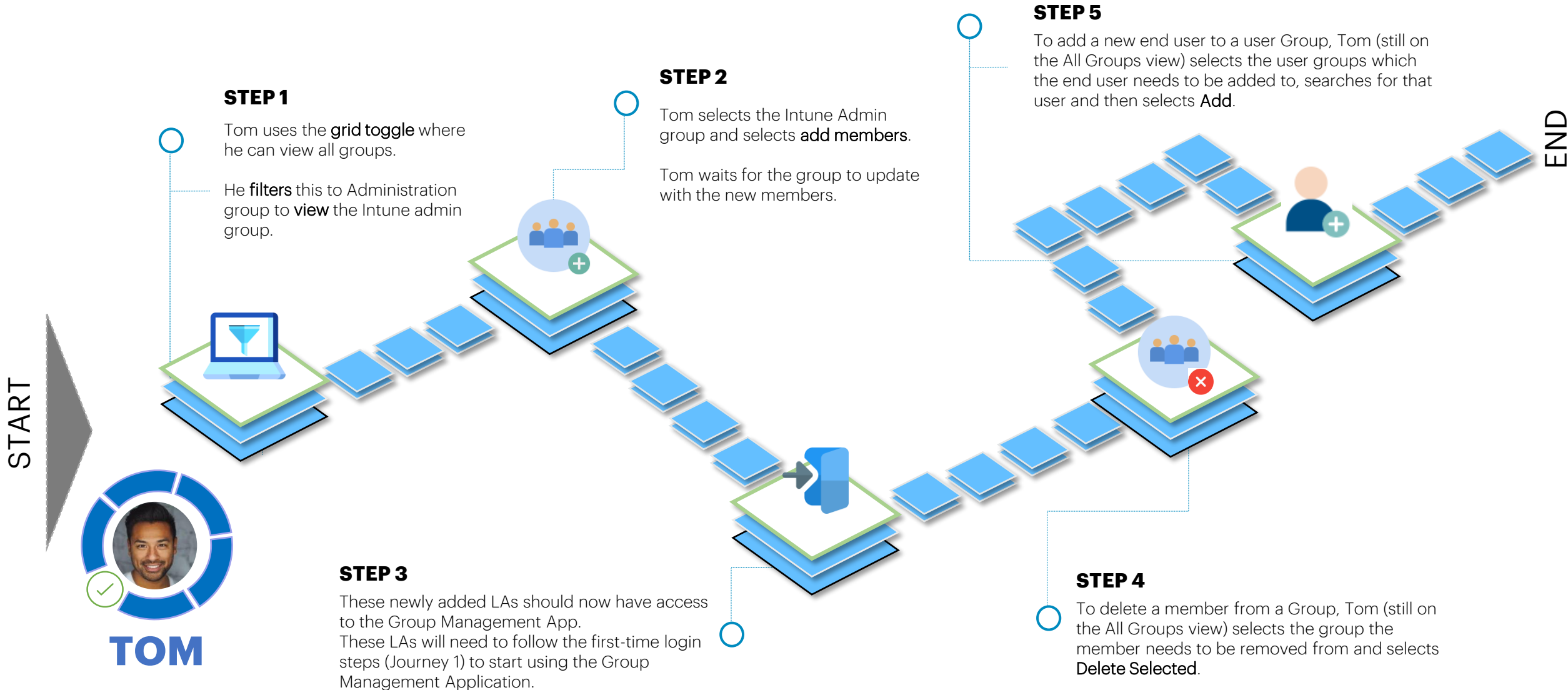
He needs to add an LA to the Intune Administration Group for his organisation, delete an LA who has left the organisation from the Group and delete a Group which is now longer needed.

He also needs to add some end users to a user Group in order to push some new profiles to their devices.



Key takeaway: The Security Group Management Application allows users 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.

Group Mgmt. App | Journey 5: Add/Delete Members & Groups



THANK YOU