accenture NHS

NHSmail Intune Service

Android Deep Dive

Agenda

Android Deep Dive

01 Overview & Objectives

02 Device and Software Requirements

03 Device Enrolment

04 Configuration Profiles

05 Compliance Policies

06 Device Management

07 Application Management

08 Samsung Knox

09 Wiping and Removing an Android device

10 Questions and Close

Android Deep Dive

Overview & Objectives

Overview

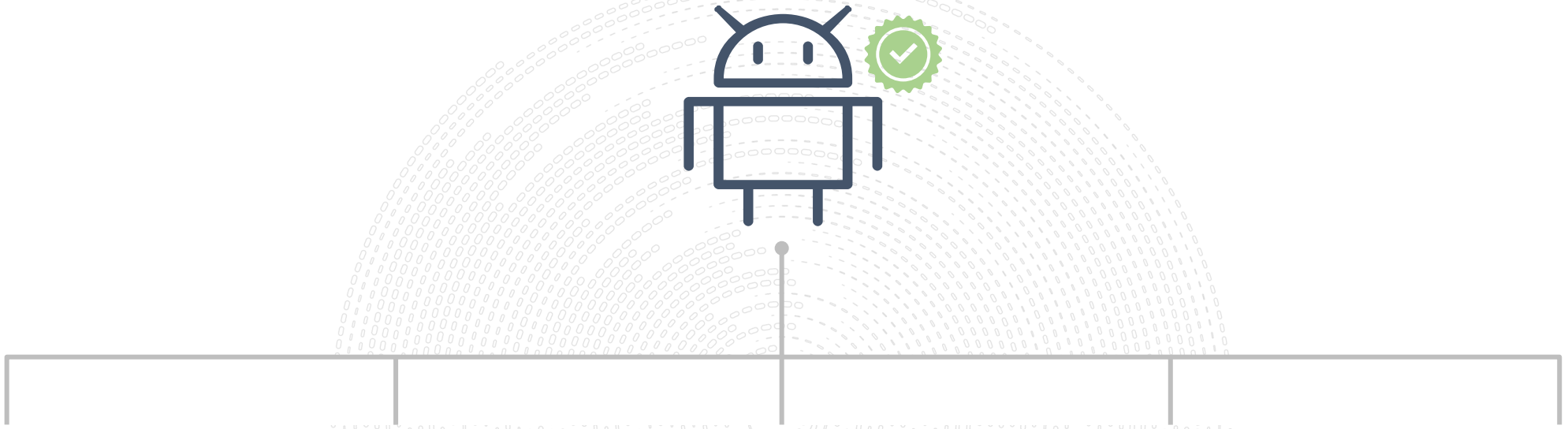
- As a result of organisations having the opportunity to purchase EMS E3 and AADP2 licenses, Intune for Mobile Device Management (MDM) capabilities has been enabled, in a way that supports the shared NHSmail tenant multi-organisation model.
- The NHSmail Intune Service is a supported live service with 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.
- This session will focus on providing a detailed look at the managing and using Android devices on NHSmail Intune, including Android-specific features such as the managed Google Play Store and Samsung Knox.

Objectives of this session

- Inform organisations on device enrolment process for Android devices.
- Provide details on Android management and features.
- Answer any questions specific to Android device enrolment and management.

Android Deep Dive | Device and Software Reqs.

Key requirements to check prior to enrolling any Android devices onto NHSmail Intune to ensure a successful enrolment



Android devices must run Android OS 8.0 or above.

Note: Newer, lower specification Android phones that run the Android 'go' version are not supported for Android Enterprise 'Fully Managed' enrolment.

Connect to a Wi-Fi network for a stable connection.

EMS E3 and AADP2 licences have been assigned to each LA / end user with a *single-user* device.

Unenroll devices from any existing device management platforms.

Note: Device estates can be split between different MDMs. Single device must only be managed by one.

Android device must have a functioning camera to scan the QR enrolment code.

Android Deep Dive | Device Enrolment

Android devices can be enrolled for single users or as shared devices. The enrolment processes for single and shared devices differ slightly

Below is a high-level overview of the steps required to enrol either a single-user Android device or shared Android device onto NHSmail Intune. Full steps are included in the Operations Guide for Local Administrators and Onboarding Managers and we will be going through these enrolment steps in more detail during the Upskilling Sessions.

Single User Android Device Enrolment

1

Setup Android Configuration Profiles

Once the configuration profile has been set up, ensure you add your Trust user group to the assignments.

This is a vital step as it allows policies and apps to be pushed to end users.

2

Obtain Enrolment Token

Once devices profiles have been added, you can then forward the enrolment token to users.

The end user will be provided with a QR code as their enrolment token which they scan using their Android device.

During this enrolment process we will be manually **adding the user** to your organisations specific device group.

Shared Android Device Enrolment

1

Setup Android Configuration Profiles

To enrol a shared android device, there will be a separate enrolment profile for the shared devices.

If an LA wants to set up a shared device, they will need to apply the shared device enrolment profile to that group.

2

Obtain Enrolment Token

This step is the same as is required for the Single User Android Device Enrolment.

Android Deep Dive | Configuration Profiles

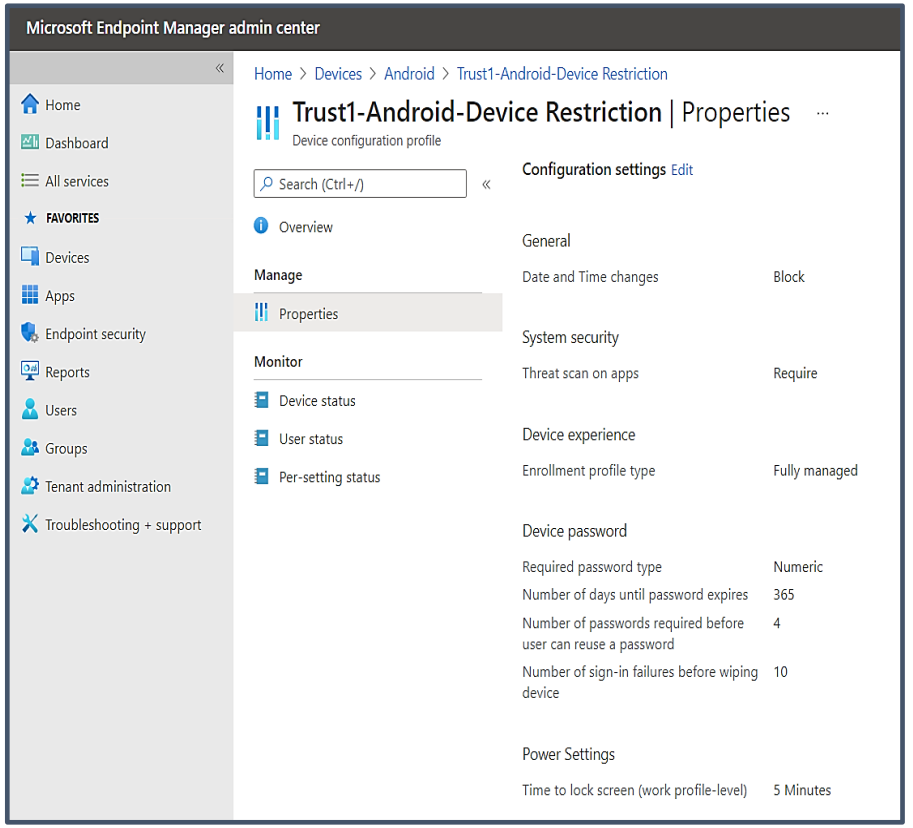
Configuration profiles allows LAs to set up specific features on Android devices. Configuration profiles allow LAs to manage what end users can do on their devices

WHAT ARE ANDROID CONFIGURATION PROFILES?

- Android configuration profiles are the different policies that you can control for Android devices; providing the ability for LAs to allow or disable features, set password rules, allow, or restrict specific policies.
- Configuration profiles allow LAs to determine what settings are applied to a device. They operate in a similar manner to group policies in SCCM for example.

WHAT CAN LAS DO WITH ANDROID CONFIGURATION PROFILES?

- LAs have the rights to change the recommended polices to suit their organisation.
- LAs can assign policies to groups. Once the policy has been assigned to a particular group, all the Android devices in that group will have that policy applied to it.



Reminder: 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.

Android Deep Dive | Compliance Policies

Compliance policies are a feature of Intune which gives LAs the ability to set requirements on Android devices

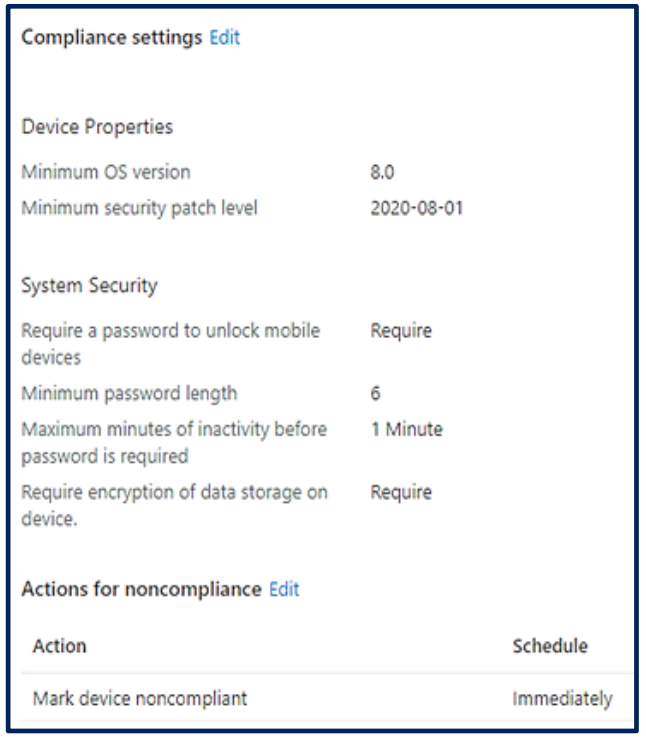
WHAT ARE ANDROID COMPLIANCE POLICIES?

- Android compliance policies determine what makes your Android device compliant.
- They are platform-specific rules you 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.

WHAT CAN LAS DO WITH COMPLIANCE POLICIES?

- Include actions that apply to devices that are noncompliant; actions for noncompliance can alert users to the conditions of noncompliance and safeguard data on noncompliant devices.
- Be combined with Conditional Access, which can then block users and devices that don't meet the rules and are noncompliant until the device is compliant.
- LAs can view a report (from the monitoring section of the Intune Portal) detailing all devices which are noncompliant as well as also viewing reports that will help troubleshoot policies that have conflicts or errors.
- Compliant devices – the device will have access to resources.
- Noncompliant devices (with conditional access) – the device will be unable to access resources until the compliance requirements are met by the end user. For example, adding a password to unlock the device.

<ODS>-Android-Compliance Policy



Compliance settings Edit

Device Properties

Minimum OS version	8.0
Minimum security patch level	2020-08-01

System Security

Require a password to unlock mobile devices	Require
Minimum password length	6
Maximum minutes of inactivity before password is required	1 Minute
Require encryption of data storage on device.	Require

Actions for noncompliance Edit

Action	Schedule
Mark device noncompliant	Immediately

Reminder: 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.

Android Deep Dive | Device Management

Organisations can manage Android devices through the Intune Portal. Below is a high-level overview of device management for Android devices

DEVICE CONFIGURATION SETUP

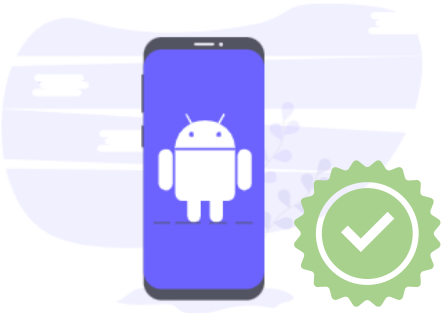
- Device Configuration Setup gives LAs the ability to change configurations policies to fit their organisation.
- LAs will have the ability to customise various policies allowing them to block, enable or set polices to not configured with the use of the RBAC model.

ASSIGNING DEVICE PROFILES

- Configuration profiles can be applied to devices via Azure AD groups or via filters.
- During onboarding, groups will be created and should be managed by LAs via the Security Groups Management App. These groups will be a manual creation that will include user Groups and device Groups.
- Each organisation will have setup their own set of standard groups for Android, and each group will be assigned their Scope tag (ODS Code).
- Each group will follow a particular naming standard that will be involve the ODS code, the OS platform and whether it's a user or device Group.

ANDROID DEVICE ONGOING MANAGEMENT TASKS

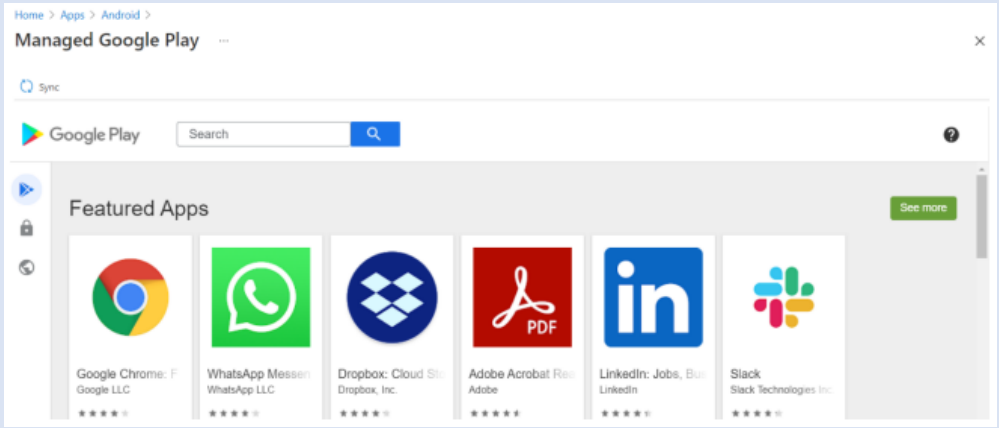
- ❑ Ensure Android devices are always updated to the latest version/OS
- ❑ Review policies fairly frequently to ensure all are applying properly
- ❑ Stay updated on latest Google / Microsoft updates for example, updates from Microsoft on Device Configuration Profiles



Android Deep Dive | Application Management

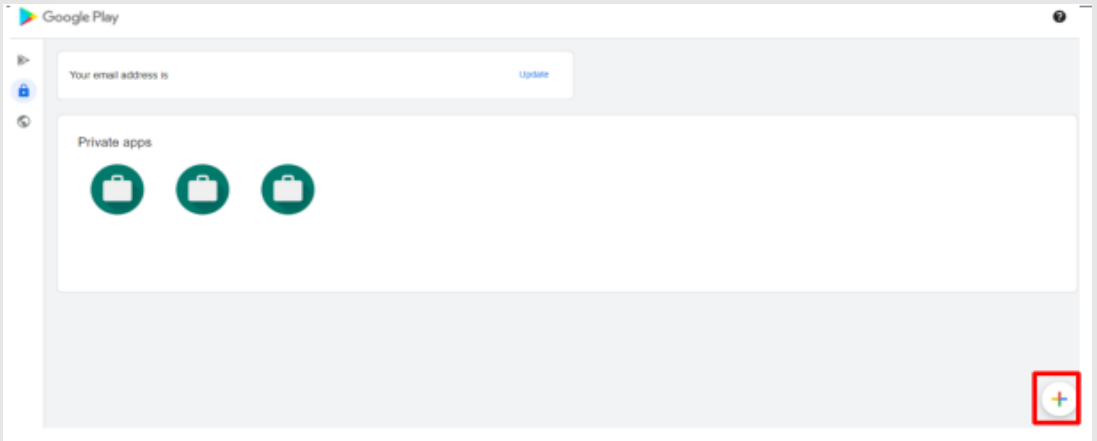
Organisations can assign and manage applications, including custom applications for Android devices via the Google Play Store

MANAGED GOOGLE PLAY STORE



- The Managed Google Play Store is the **sole method of app deployment for Android Enterprise devices**.
- This is a central store, so it is possible for common apps e.g., Outlook to already be approved within the environment.
- Any deleted application can be approved and imported again.
- Apps can be assigned by **selecting the app** and **assigning your AAD Group.**

CUSTOM ANDROID APPLICATIONS



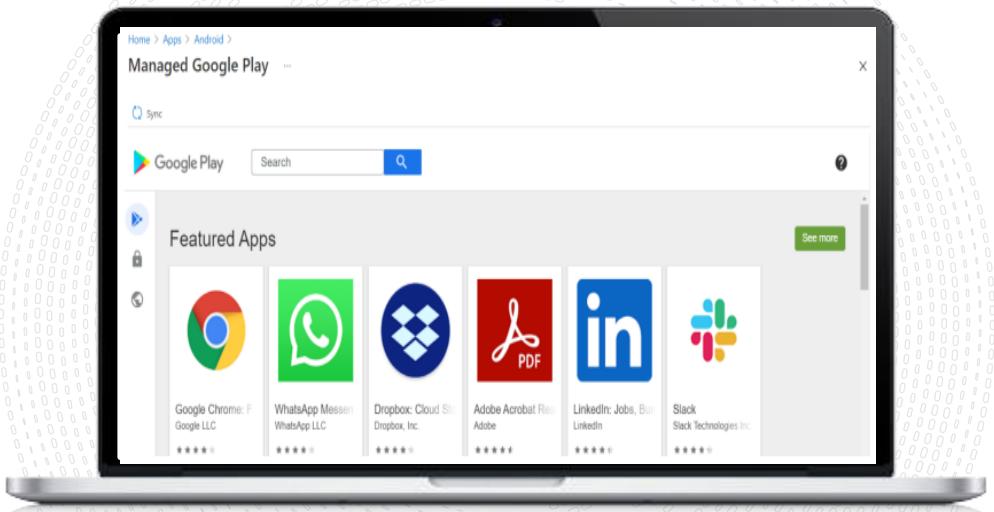
- LAs have the ability to **add custom apps** through the Google Play Store.
- In the managed Google Play Store, these are referred to as private apps.
- Once the private apps are **added and synced** to the Google Play Store, the custom app can then be **assigned to an organisation's AAD group**.

There are **no** limits to number of applications you can deploy and there are **no** restrictions on application types. The only restrictions for applications are regarding storage on the device.

Android Deep Dive | Application Management

Assigning applications to Android devices via the Google Play Store will require LAs to understand and consider the below

When assigning applications to Android devices, LAs should be aware of the following:



VISIBILITY

- LAs can see other organisation's groups on the Intune tenant.
- LAs should not be concerned if they see another organisation assigned to the same application.

SCOPE TAGS

- LAs should not unassign the default scope tag from Android apps.
- This will remove the ability for other LAs within Intune to assign apps to their organisation.
- The default scope tag can be readded by the LST.

GROUPS

- LAs will only be able to assign groups which are covered under their RBAC role.
- LAs should not amend any AAD Group which is assigned to an Android app which does not belong to their organisation.

OTHER ORGS' APPLICATIONS

- LAs should not unapprove/delete any application that is already approved within the Google Play Store.
- If an LA does unapprove/delete an application, the app will be removed from the Intune tenant and therefore will be removed from all organisations on NHSmail Intune who had this app.

Android Deep Dive | Samsung Knox

From January 2022, onboarded organisations will be able to use Samsung Knox on their NHSmail Intune-enrolled Android devices

- Samsung Knox is a proprietary security framework pre-installed on most Samsung mobile devices. It's primary purpose is to provide organisations with a toolset for managing mobile devices. Many NHS organisations already use Samsung Knox on their Android devices, and there was a clear requirement to enable this feature as a part of the NHSmail Intune offering.
- Samsung Knox Mobile Enrolment (KME) is a Zero Touch provisioning solution. This solution fully automates the enrolment of new, or factory reset devices into an MDM solution like Microsoft Intune.
- Full details on how to enrol and manage an Android device with Samsung Knox are included in the Operations Guide for Local Administrators and Onboarding Managers.

Samsung Knox Prerequisites

A Microsoft Intune environment up-and-running with at least one Corporate-owned enrolment profile enabled.

Samsung devices with Knox 2.8 or higher.

A Samsung Knox account to access the Samsung Knox portal.

Samsung Knox Mobile Enrolment

The following outlines, at a high-level, how an LA would use Samsung Knox with NHSmail Intune on Android devices:

1. Create MDM profile

- In the Samsung Knox Portal, activate the Knox Mobile Enrolment to create an MDM profile.
- Obtain the enrolment token from Intune and apply it to the MDM profile you are creating in the Samsung Knox portal.

2. Connect Samsung Knox to Intune

- In the Intune portal, add and approve the Knox Service Plugin application from the Managed Google Play Store.
- Once approved, create a configuration profile associating the Knox plugin app.

Any issues pertaining to enrolling onto an NHSmail Intune-enrolled Android device, which cannot be resolved by referring to the Operations Guide, should be raised as an incident ticket.

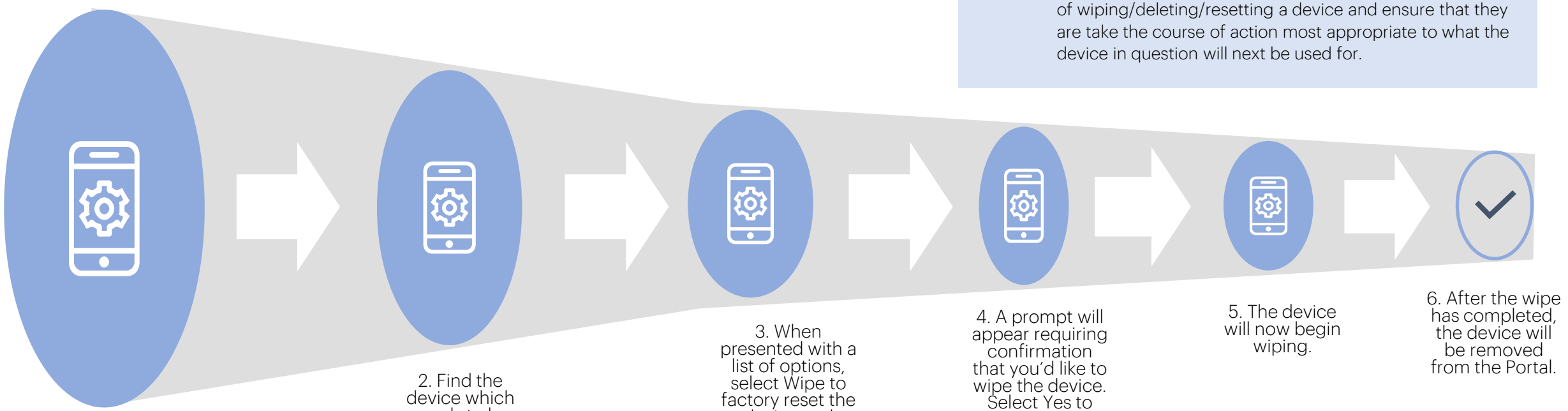
Android Deep Dive | Wiping and Removing

Android devices enrolled onto NHSmail Intune can be remotely wiped and removed from the platform by LAs with the correct RBAC permissions

- With delegated RBAC controls, LAs have the permissions to remotely wipe and remove iOS/iPadOS and Android devices from the NHSmail Intune platform. This action should be performed only as a last resort for devices experiencing issues and LAs are not required to seek support from the Intune Live Service Team to complete this.
- Devices can be wiped via the Intune Portal by following the below steps:

Important note:

LAs should always consider the data retention implications of wiping/deleting/resetting a device and ensure that they are take the course of action most appropriate to what the device in question will next be used for.



1. Sign into the Intune Portal and select the Devices page.
2. Find the device which needs to be wiped and select this device.
3. When presented with a list of options, select Wipe to factory reset the device and remove all data.
4. A prompt will appear requiring confirmation that you'd like to wipe the device. Select Yes to progress.
5. The device will now begin wiping.
6. After the wipe has completed, the device will be removed from the Portal.

Android devices may still be visible in the Portal even after they have been wiped. This is a known issue for Android devices, but it does not mean that the wipe has been unsuccessful.

THANK YOU