accenture NHS

NHSmail Intune Service

Introductory Pack 1

For organisations considering registering their interest

Contents

Introductory Pack 1

Introductory Pack 1 is intended to provide organisations who are interested in registering for the NHSmail Intune Service with a very high-level overview of the service, the technical solution and an introduction to the pre-requisites required of organisations to be able to onboard.

See Introductory Pack 2 for further information on the NHSmail Intune Service.

NHSmail Intune

OVERVIEW

NHSmail Intune Service

Overview

Overview & Context

- NHSmail Intune is a new **corporate device management service integrated with existing NHSmail capabilities**. Intune natively supports the multi-organisational nature of NHSmail.
- Centralised device management delivered in this manner will allow local orgs. to maintain a **high degree of oversight and local autonomy, through the use of RBAC controls**.
- NHSmail Intune is now **a supported live service** after successful testing and piloting with a group of organisations with all device types to be supported. Onboarding of organisations onto NHSmail Intune will be through a **phased approach.**

Devices

Device platforms supported:

iOS/iPadOS

Windows 10/11

Android

HoloLens 2

Device types supported:

Corporate devices only

Clinical and Non-Clinical devices

Recommendation:

It is recommended that all organisations devise and follow a **ramp-up plan** when onboarding users and devices onto Intune and carefully consider current levels of Intune knowledge among LAs.

Typical Benefits

- ✓ Improved device estate security via defined baselines
- ✓ Centralised Intune platform with preserved local autonomy
- ✓ SSO to NHSmail apps for end users
- ✓ Supports staff to work mobile securely
- ✓ Licence consolidation
- ✓ Future-ready cloud hosted solution
- ✓ Autonomy for LAs to manage Intune groups
- ✓ LA documentation and end user guides
- ✓ Remote, cloud management of all devices

Key Pre-Requisites

(Full list to be provided before onboarding)

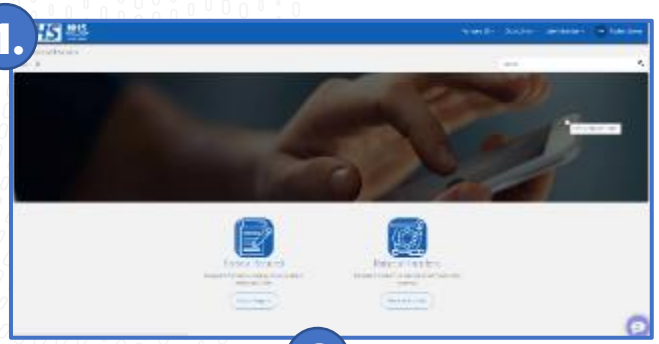
EMS E3 & AADP2 licenses in NHS Tenant

ABM link to NHSmail Intune (for Apple only)

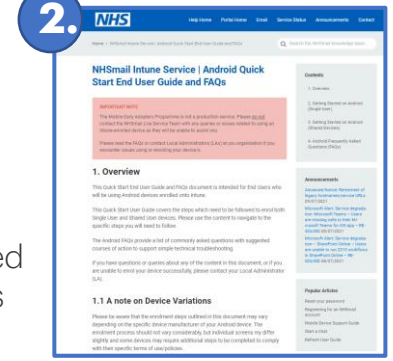
Reset devices to factory settings

Support

1. All requests, including to onboard onto the NHSmail Intune Service, and once onboarded, service requests and incidents should be actioned via Helpdesk Self-Service.



2. All supporting LA and end user documentation will be available on the NHSmail Support Site. Links will be provided to you once your technical onboarding has been completed.



NHSmail Intune

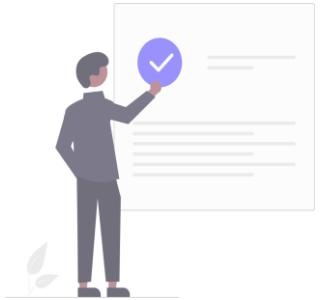
FEATURES AND BENEFITS

NHSmail Intune Service | Features & benefits

NHSmail Intune offers the following features & benefits to organisations, LAs and end users.

The NHSmail Intune Solution **centralises device management** under NHSmail's Intune tenant while maintaining a **high degree of customisation, oversight and local autonomy for local organisations**.

Monitoring of **device compliance is visible at both centralised and local levels;** organisations can also expect a range of additional benefits including:



REDUCED COMPLEXITY

- Simplified cloud-hosted device management, provisioning and remote configuration
- Out-of-the-box standardised policies and device configurations across local organisations
- Individual orgs. provided granular management of their device estate via the Intune native multi-org RBAC permissions model
- Create and manage Intune user and device groups with bespoke app

SECURITY & DATA PROTECTION

- Seamlessly update security configurations for different technology platforms
- Ability to remotely wipe and lockdown lost or stolen devices
- Provides monitoring of device compliance
- Set device policies such as device restriction profiles
- Set local device compliance policies such as minimum OS requirements

TIME SAVINGS & CONSOLIDATION

- Consolidate MDM licence costs and enable a return on investment of EMS licences purchased
- Transition away from existing legacy MDM capabilities
- Staff time savings for LAs resulting from standardised, modern, streamlined and simplified device management via single console
- Out-of-the-box standardised policies and device configurations to speed up org. onboarding

USER EXPRIENCE

- Intune is the single tool to manage iOS/iPadOS, Android, Windows 10/11 & HoloLens 2
- LAs will be able to remotely set-up a device creating a bespoke and org. personalised unboxing and first touch use experience
- Using Intune with the NHSmail Azure AD (AAD) identity platform will enable SSO to NHSmail services
- Remote assistance from LAs for enrolment, onboarding and resets

NHSmail Intune device management will provide **critical digital infrastructure** that can support the **mobile and flexible NHS workforce.**

NHSmail Intune

TECHNICAL SOLUTION

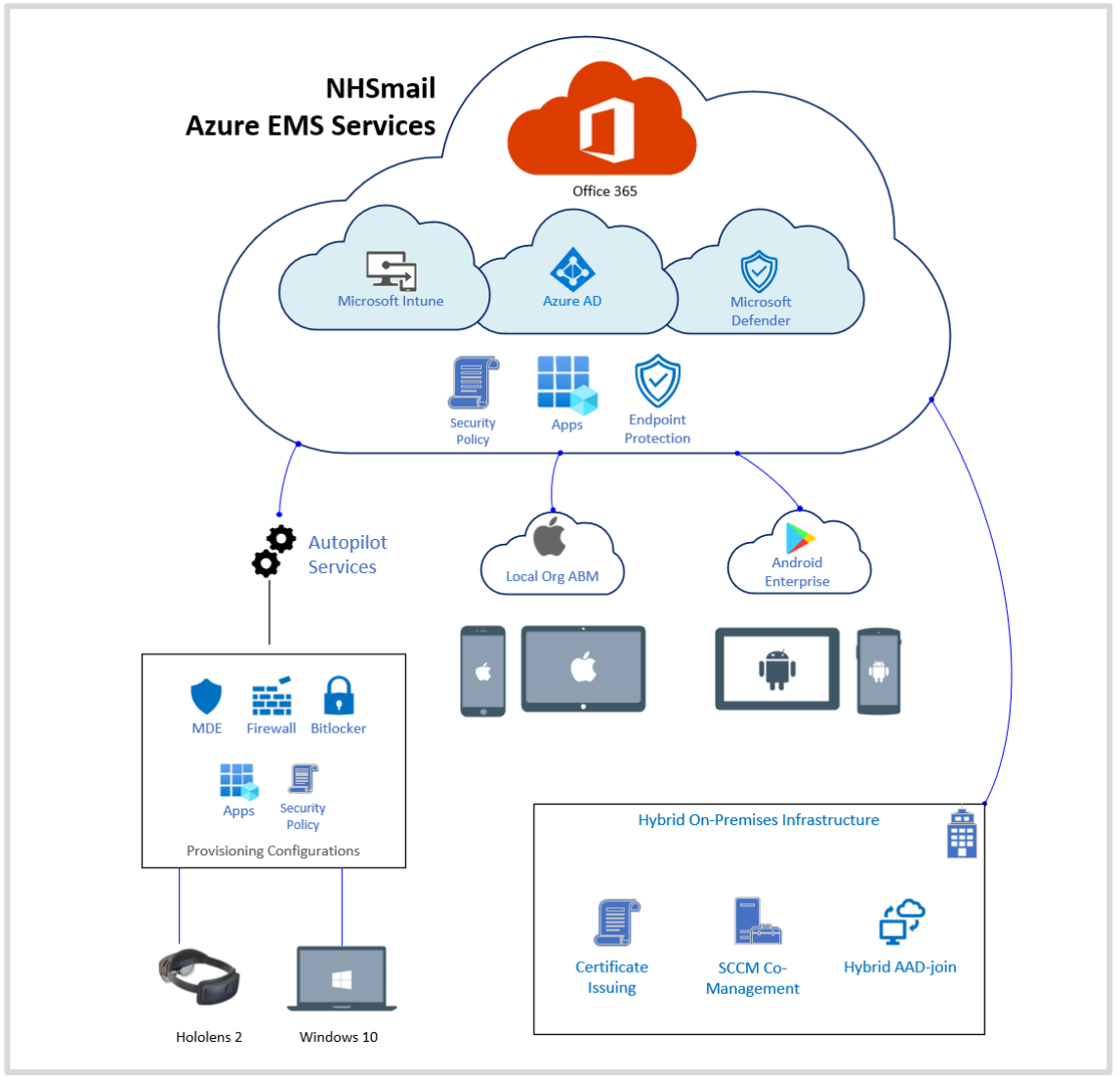
NHSmail Intune Service | High-Level Intune Solution

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 10/11, 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 10/11 there is a centralised Security Baseline policy which is enforced to all Windows 10/11 'Cloud' devices enrolled into Intune. There are also "pencilled-in", customisable 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 **enables organisations to Co-Manage devices** with SCCM and Intune as well as connect on-premises **Certificate Issuing** services for VPNs, Wifi, etc.

<u>Available now:</u>

- **3 ways to manage Windows 10/11 devices** in addition to the **Cloud track** which will enable your organisation to accelerate its journey to the cloud. Our **Hybrid track** enable organisations to continue to consume on-premise resources (e.g., printing and network storage drives), whilst enabling organisations to adopt the NHSmail Intune Service and the benefits associated with cloud device management.



NHSmail Intune Service | RBAC & NHSmail baseline

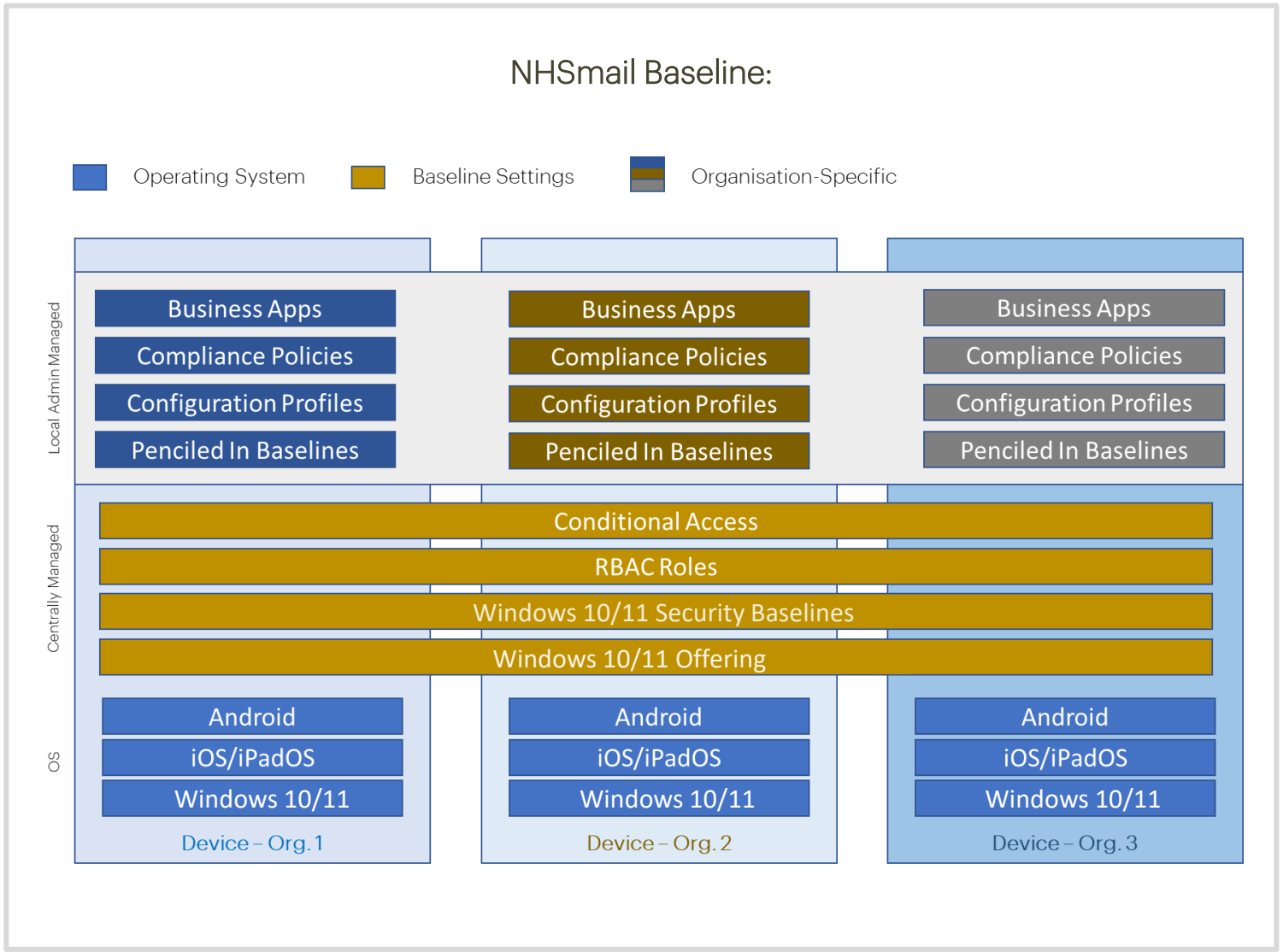
The NHSmail Intune solution includes baseline settings which individual organisations can apply policies and settings on top of.

NHSmail Intune RBAC

Baseline policies and delegated policies

Intune will be configured to provide a core set of centrally managed Windows 10/11 Security Baselines. Organisations will be able to view these settings 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.

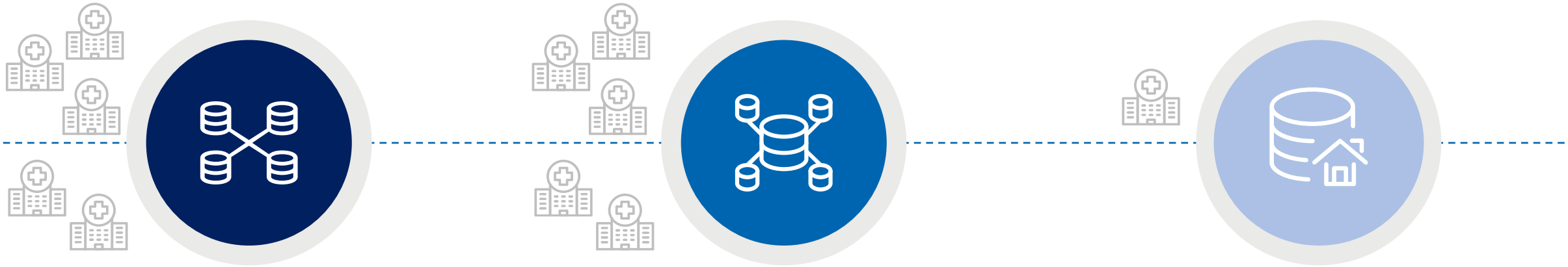
Local Administrators at onboarded organisations will be able to set up their own Groups, Policies, Profiles, Apps and Security Baselines on top of the centrally managed settings ensuring a high degree of customisation, oversight and local autonomy.



NHSmail Intune Service | Configuration items

NHSmail 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.

NHSmail 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, NHSmail 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 NHSmail 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 NHSmail IT Admins

CENTRAL NHSMAIL CONFIGURATIONS

- Intune Company Portal - Branding and customisation
- Custom notifications
- RBAC and Scope Tags (Provided to LAs)
- Windows 10/11 Security Baselines
- Android Enterprise – Corporate Owned Dedicated Device

Delegated to Organisations' Local Admins

LOCAL ADMIN CONFIGURATIONS

- Apple Automated Device enrolment
- Autopilot deployment profiles
- Device Categories & Policy Sets
- 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

NHSmail Intune

PRE-REQUISITES

NHSmail Intune Service | Key pre-requisites

A selection of key pre-requisites and requirements of any organisation wishing to onboard onto the NHSmail Intune Service. This is not an exhaustive list.

Below are the key pre-requisites for organisations wishing to onboard onto Intune. For all pre-requisites, see the NHSmail Intune Service Terms of Reference.

Enrolment

- ✓ Organisations will need to remove devices from existing device management and then reset devices to factory settings prior to enrolling devices onto Intune.
- ✓ LAs will be required to support end users with data back-up to avoid any data loss during device reset and enrolment.
- ✓ Device enrolment will involve leaving the existing organisation On-Prem domain and joining NHSmail's Azure AD; hybrid solution is not yet available.

Licencing

- ✓ Relevant and required device and Operating System licencing (e.g., Windows 10/11).
- ✓ EMS E3 and AADP2 licences should have already been procured and moved into the NHSmail shared tenant.
- ✓ Procured EMS and AADP2 licences should be allocated to your organisation prior to user assignment in the NHSmail LA portal.
- ✓ EMS E3 and AADP2 licences are required for end users and LAs who will be using the Intune service.**

Devices & users

- ✓ For Windows devices, Windows 10/11 Pro/Enterprise version 1809 or higher with relevant OS licence will be supported.
- ✓ For HoloLens 2, device running the Windows Holographic build version 20H2.
- ✓ For iOS/iPadOS 14.4 and above.
- ✓ For Android OS 6.0 and above.
- ✓ All end users and LAs must have an NHS.net account.
- ✓ End users can be in either clinical or non-clinical roles and can work any hours.*

Service support

- ✓ All service requests and Level 3 issues should be raised as a ticket via Helpdesk Self-Service (HSS).
- ✓ All LAs should have access to Helpdesk Self-Service (HSS).
- ✓ It is expected and the responsibility of organisations that LAs are upskilled in Intune device management sufficiently to be able to enrol and provide Level 1 (e.g., service desk and deskside support) and Level 2 support (via delegated RBAC controls) to their end users.

ABM link

- ✓ Organisations wanting to enrol Apple devices (iOS and iPadOS) will require those devices to exist in an ABM instance already.
- ✓ Organisations will be required to associate their ABM instance with NHSmail Intune.
- ✓ Org. ownership and management of Apple Business Manager (ABM) for iOS iPads/iPhones is to be maintained, including Apple IDs.
- ✓ Administrator or Device Enrolment Manager role should be assigned to the Apple ID being used to connect into Intune.

*Organisations will need to complete a clinical safety assessment in line with safety standard DCB0160 if using Intune-enrolled devices for clinical purposes. **This applies to all single user devices but not all shared device modes.

NHSmail Intune

NEXT STEPS

NHSmail Intune Service

Next steps

To submit a request to begin onboarding onto the NHSmail Intune Service, please follow these five next steps:

REVIEW THE NHSMAIL INTUNE INTRODUCTORY PACK (PART 1)

This is the first step in the journey to onboarding onto NHSmail Intune – which you've now completed. Please follow the steps below to begin onboarding your organisation.

01

REVIEW THE NHSMAIL INTUNE INTRODUCTORY PACK (PART 2)

Interested organisations should review the Introductory Pack (Part 2) which contains further information on the NHSmail Intune Service.

02

COMPLETE AND SUBMIT THE INTUNE REGISTRATION FORM

Interested organisations **who have not already completed the NHSmail Intune Information Gathering Survey** should complete the Intune Registration Form, available here. This will help us to understand your readiness for NHSmail Intune. If you meet the prerequisites, your organisation's information will be added to the NHSmail Intune SharePoint.

03

RECEIVE A PROVISIONAL SLOT TO ONBOARD

You will receive an email stating that a provisional slot has been offered to your organisations on the NHSmail Intune SharePoint. Organisations will need to either accept or decline this slot. If accepted, your organisation will receive an invitation to complete the Onboarding Request Form (ORF), available via Helpdesk Self-Service.

04

REVIEW THE TERMS OF REFERENCE AND COMPLETE THE ORF

Please review the Terms of Reference document to ensure that your organisation is aware of all pre-requisites which will need to be fulfilled to onboard onto NHSmail Intune, and then complete the ORF. This form will be visible **only** to PLA/LAs who are listed on your organisation's entry on the NHSmail Intune SharePoint.

05

AWAIT CONFIRMATION OF TECHNICAL ONBOARDING

Once a PLA/LA from your organisation has completed and submitted the Onboarding Request Form, you can then expect to receive a confirmation of technical onboarding email. This confirms that all required permissions, Groups etc. have been set up for your organisation and you can begin enrolling devices.

NHSmail Intune

GLOSSARY

NHSmail Intune Service | Glossary

Full list of key terms and acronyms used throughout this pack explained.

Term/Acronym	Full Term	Description
AD	Active Directory	Directory service by Microsoft providing directory based identity-related services.
AAD	Azure Active Directory (Azure AD)	Microsoft's cloud-based identity and access management service.
ABM	Apple Business Manager	Apple portal allowing IT Admins to bulk manage and deploy corporate-owned devices.
AADP2	Azure Active Directory Premium P2	Azure Active Directory Licence type allowing Conditional Access. This licence may have been included as part of a suite licence like Enterprise Mobility and Security (EMS E3/E5).
ATP	Advanced Threat Protection	Advanced Threat Protection refers to a category of security solutions that defend against malware targeting sensitive data.
BYOD	Bring Your Own Device	Refers to personal device/s employees may use to complete work tasks, connect to organisational networks and access work related systems.
EMS	Enterprise Mobility Security	Collection of security and management products from Microsoft that work seamlessly with Office 365.
EMS E3	Enterprise Mobility Security E3 licence	Enterprise Mobility Security licence type which provides the necessary permissions for using Intune.
HSS	Helpdesk Self-Service	All onboarding requests (licence onboarding and organisation onboarding), service requests and Level 3 incidents should be raised as tickets via Helpdesk Self-Service on the NHSmail Portal.
Level 1 and Level 2	Level 1 and Level 2 Support	Local Administrators will provide Level 1 and 2 support to their end users in the first instance. Level 1 and Level 2 support refers to service desk and deskside support. Activities covered include: device enrolment and wiping, password resets, support via RBAC permissions etc.
MDM	Mobile Device Management	Solution for the management of corporate devices or devices through which employees can access corporate services and data.
ODS Code	Organisation Data Service Code	Unique code created by the Organisation Data Service within NHS Digital, and used to identify organisations across health and social care.
OS	Operating System	Software which handles communication between the computer user and computer hardware, allowing other types of software to run on the device.
RBAC	Role Based Access Controls	A method of managing who has access to organisation's resources and what they can do with those resources.
SSO	Single Sign-On	Authentication method that enables users to securely authenticate with multiple applications and websites by using just one set of credentials.
SCCM	System Center Configuration Manager	Enables the management, deployment and security of devices and applications across an enterprise.