accenture NHS

NHSmail Intune Service

Session 7:

Windows 10/11 Deep Dive

28th July 2022

Upskilling Series | Housekeeping

Event name:	Session 7: Windows 10/11 Deep Dive
Date:	28 July 2022
Location:	Online Webinar
Start / end time:	13:30 – 14:30
Attendees:	NHSmail Intune Team and LAs.
Objectives & purpose:	To provide an in-depth overview of Win 10/11 devices on NHSmail Intune and the different offerings/tracks available for these devices.
End goal:	Attendees feel more informed about how to enrol and manage Win 10/11 devices & the different offerings/tracks available.

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 using the chat functionality.
• Any questions submitted in the chat which we don't have time to answer in the session will be answered via follow-up email after the session where appropriate.
• Information outlined in red indicates key information.
• We would appreciate any feedback on this session as this will help us to provide upskilling sessions to organisations which are useful and impactful. If you would like to provide some feedback, please email nhsmail.intune-comms@nhs.net.

Upskilling Series | Sessions

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

12 sessions over 4 weeks

All sessions are optional

Recordings and session materials available

Suggested further reading & resources

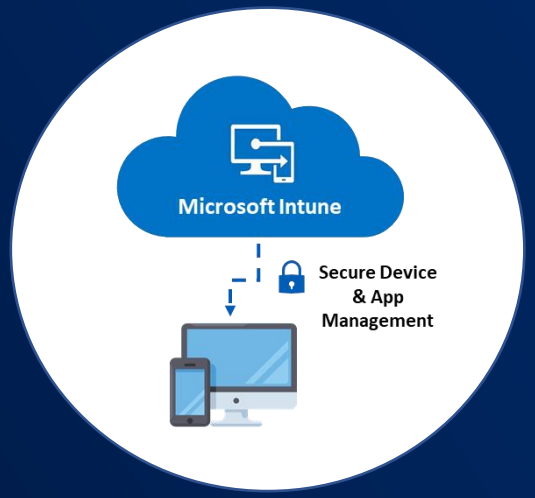
Supported upskilling

KEY		Intune Fundamentals	Onboarding and Support Basics	Mobile Devices	Windows 10/11	HoloLens 2	MAM	Intune Advanced

Week	Date	Focus	Session Title	Session Content	Duration	Session Audience	Preparations prior to session	Target Audience
1	19/07	Onboarding and Support Basics	Introductory Session	Pre-requisites, licencing, how to get started using NHSmail Intune	1 hour	All organisations	None required	All LAs
	20/07		Support Model, Raising a ticket and Supporting Documentation Walkthrough	Overview of the NHSmail Intune Support Model, how to raise an ticket via Helpdesk Self-Service and walkthrough of the key supporting documentation available to all onboarded organisations	1 hour	All organisations	None required	All LAs
	21/07	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
	22/07		Intune Features and Group Management App	Session exploring the specific features of NHSmail Intune and a demo of the Security Group Management App	30 minutes	All organisations	None required	All LAs
2	26/07	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
	27/07		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
	28/07	Windows 10/11	Windows 10/11 Deep Dive and Offering	Deep dive session focused on managing Windows 10 devices on NHSmail Intune and preparations required for the Hybrid-Join feature	1 hour	Organisations with Windows 10 devices	None required	LAs from organisations interested in enrolling Win 10/11 devices with access to both cloud and/or on-premises resources
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	01/08	Mobile Application Management	Mobile Application Management (MAM) Overview	Overview of MAM policies on NHSmail Intune and how to use them	1 hour	All organisations	None required	LAs wishing to deploy Mobile Application Management policies to devices
	02/08	Supported Enrolments	Supported Device Enrolment Session (Android)	Guided enrolment session with Q & A	30 minutes	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
	03/08		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
	04/08		Supported Device Enrolment Session (Windows 10/11)	Guided enrolment session with Q & A	30 minutes	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
Recording			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
3	05/08	Intune Fundamentals	Intune Wrap-Up and Readiness	Summary of the full upskilling series and a focus on the initial steps to start your journey of enrolling devices on NHSmail Intune	1 hour	All organisations	None required	All LAs

Organisations can register to attend any of these sessions by signing up on the July 2022 NHSmail Intune Upskilling page.

Session 7



Win 10/11 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 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.
- Session 7 will provide a detailed insight into enrolling and managing Azure AD-Joined Windows 10/11 devices on NHSmail Intune, including Win 10/11 specifics and the different track offerings available. The session will also provide the opportunity for attendees to ask any questions specific to enrolling and managing Azure AD-Joined Windows 10/11 devices on NHSmail Intune.

Objectives of this session

- Inform organisations of the device enrolment process for Azure AD-Joined Win 10/11 devices & provide details on Intune-enrolled Windows 10/11 management and features.
- Provide an overview of the different Windows 10/11 tracks and outline the difference between Azure AD-Joined and Hybrid-Joined Win 10/11 devices.
- Outline key prerequisites which will need to be met by organisations in order to enrol and manage 'hybrid' devices.

Agenda

Session 7: Win 10/11 Deep Dive

01 Overview & Objectives

02 High-Level NHSmail Intune Solution

03 Device and Software Requirements

04 Windows 10/11 Enrolment & Post Enrolment

05 Wipe / Reset Windows 10/11 with Intune

06 Introduction to Hybrid

07 Hybrid Technical Benefits

08 Different Tracks Available

09 Hybrid Prerequisites

10 Same Sign On

11 TanSync

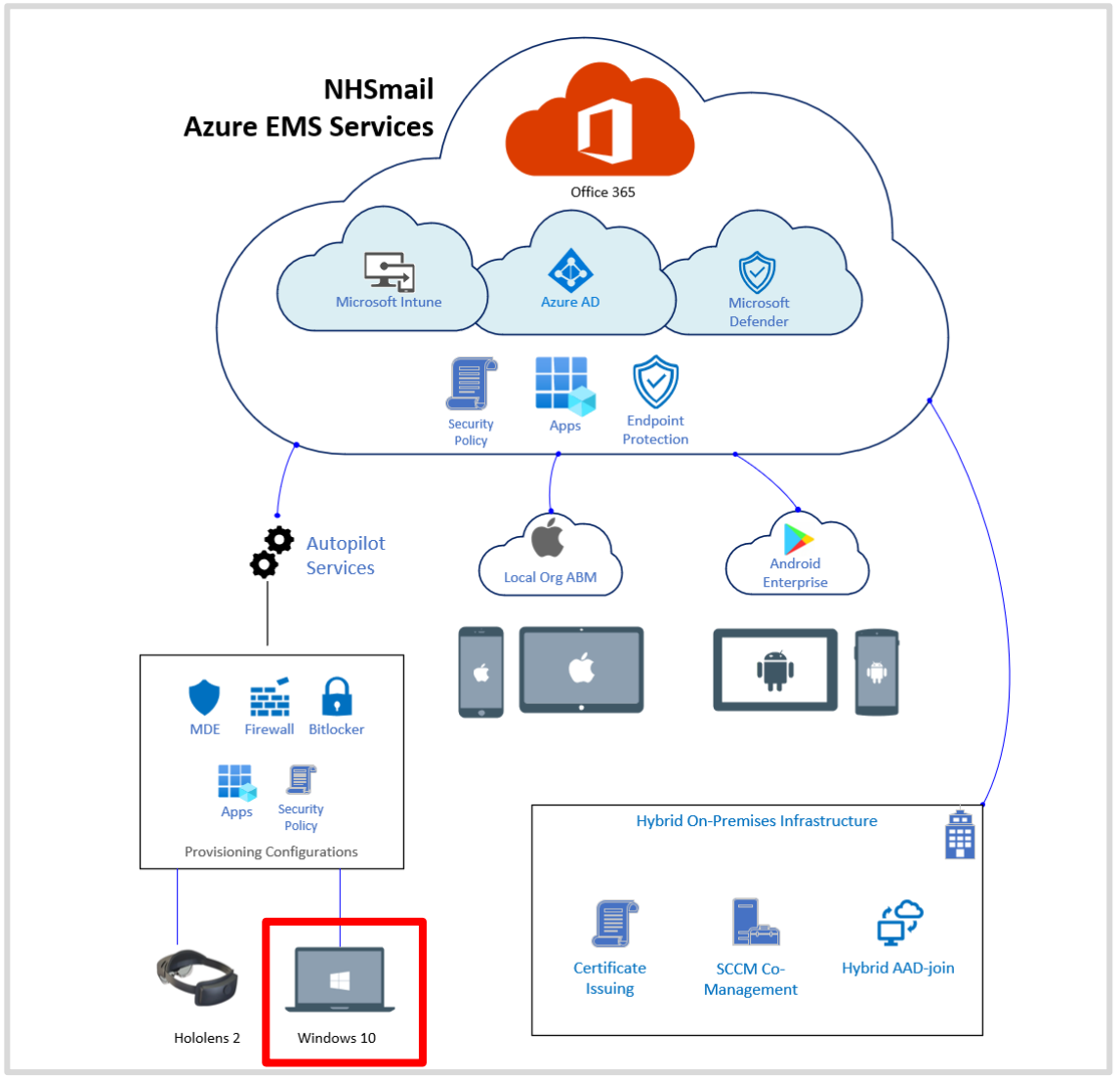
12 Windows 10/11 Service Requests

13 Questions & Close

Win 10/11 Deep Dive | High-level 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 10/11, Apple iOS/iPadOS, HoloLens 2 and Android OS).
- The solution offers **devolve 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
- 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 provides different track offerings (including Hybrid) to **enable organisations to Co-Manage devices** with SCCM and Intune as well as connect on-premises **Certificate Issuing** services for VPNs, Wifi, etc.



Win 10/11 Deep Dive | Device & Software Reqs.

Key requirements to check prior to enrolling any Windows 10/11 devices onto NHSmail Intune

Supporting Documentation for Win 10/11:

- ✓ Operations Guide for Local Administrators and Onboarding Managers
- ✓ Windows 10/11 Quick Start End User Guide
- ✓ Windows 10/11 End User FAQs

Windows 10 Pro/Enterprise version standardised at 21H2, or Windows 11 with relevant OS licence

Note: A 'base' Windows version of 2004 is required to support a direct upgrade path to Windows 11. Earlier versions do not provide this pathway.

Ensure TPM 2.0 is enabled in the BIOS / UEFI settings

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: A device estate can be split across different MDM solutions, but individual devices can only be enrolled into one MDM at a time.

Existing AD-joined Windows 10/11 devices will need to be rebuilt / reset to factory settings in order to enrol to Intune as an Azure joined device

Win 10/11 Deep Dive | Windows 10/11 Enrolment

At a high-level, there are 3 steps to complete in order to enrol a Windows 10/11 device into Intune. End users will then need to complete several set-up steps on the device/s

1. GATHER HARDWARE HASHES

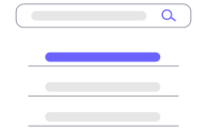
There are **4 methods** LAs can use to collect the hardware hash of their Windows 10/11 devices. Once the hashes have been extracted, these will need to be exported into a .csv file ready to be uploaded into Intune. This is a manual process, but hardware hashes can be uploaded in batches.

2. ADD GROUP TAG

Before uploading the hardware hashes into Intune, a Group Tag **must** be added to the .csv file containing the device hardware hashes. If this step is missed, the device/s will not be assigned an Autopilot enrolment policy and the enrolment will fail.

3. ADD AUTOPILOT DEVICES INTO INTUNE

Via the Intune Portal, LA should now be able to import the Windows 10/11 devices into Intune, if the .csv file is formatted correctly. **Profiles should be assigned to devices as soon as they are added**, as imported Autopilot devices cannot have a scope tag assigned.



Naming Standards

Windows 10/11 devices are subject to the same naming device, policy and Group requirements as other devices and all naming standards should be followed as outlined in the Operations Guide for Local Administrators and Onboarding Managers.

Enrolment Times:

The time needed for a Windows 10/11 enrolment to complete will likely vary between organisations. LAN / Wi-Fi strength and reliability is a key factor, so we would advise completing enrolment with a strong reliable internet connection if possible.

If an enrolment takes **longer than 90 minutes**, please raise a ticket with Helpdesk Self-Service.

Note: Surface Hub devices can be deployed using the same methods as Windows 10/11 devices

Windows (Cloud Only) Supported Device Enrolment Session: 4th August at 13:30 - 14:00

Win 10/11 Deep Dive | Post Device Enrolment

Once Windows 10/11 devices have been successfully added into NHSmail Intune, LAs can then move forward with the following actions to set up each device as required ahead of deploying to end users

Assign Autopilot deployment profiles

A centralised Autopilot Deployment profile determines the deployment mode and allows customisation of the OOBE (Out-of-Box-Experience) for end users. Autopilot deployment profiles are used to configure the Autopilot devices.

For Windows 10/11 devices, an **Autopilot Deployment profile** is assigned to the device when it is enrolled with AutoPilot.

Assign device configuration and compliance policies

LAs can deploy **custom configuration profiles** and **compliance policies** to groups of Windows 10/11 devices. The configuration profiles allow LAs to determine what settings are applied to a Windows 10/11 device, by allowing or disabling features. The compliance policies define requirements for devices, like minimum operating systems or the use of disk encryption.

Add device/s to Groups using the Security Group Management App

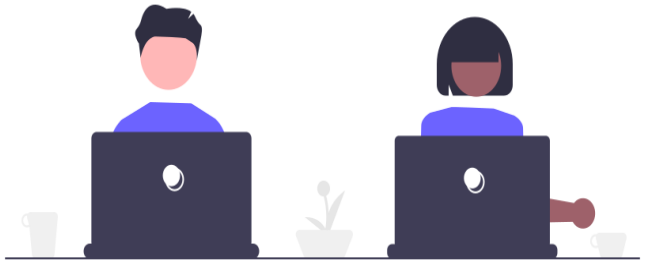
The Security Group Management Application allows LAs granular control over the creation, editing and deletion of their organisation's device (including Windows 10/11) and user Groups within Intune and permit LA's to closely and independently manage Groups scoped to their organisation.

LAs who manage Windows 10/11 devices should use the app to manage **Win 10/11 device Groups**.

Push applications

LAs have the ability to manage and distribute applications to Windows 10/11 devices via the **Microsoft Store**.

Applications should be added to Intune before being deployed to Windows 10/11 devices. **Microsoft 365 applications** or **custom applications** can be added to Windows 10/11 devices.



Win 10/11 Deep Dive | Wiping / Resetting Devices

Windows 10/11 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 also have permissions to remotely wipe and remove Windows 10/11 devices from the NHSmail Intune platform. There are several options for wiping and resetting Windows 10/11 devices which are explained fully in the Operations Guide for Local Administrators and Onboarding Managers.

❑ RETIRE / DELETE

The retire action removes app data, settings and Intune managed email profiles from the device.

To remove stale devices immediately, use the delete action.

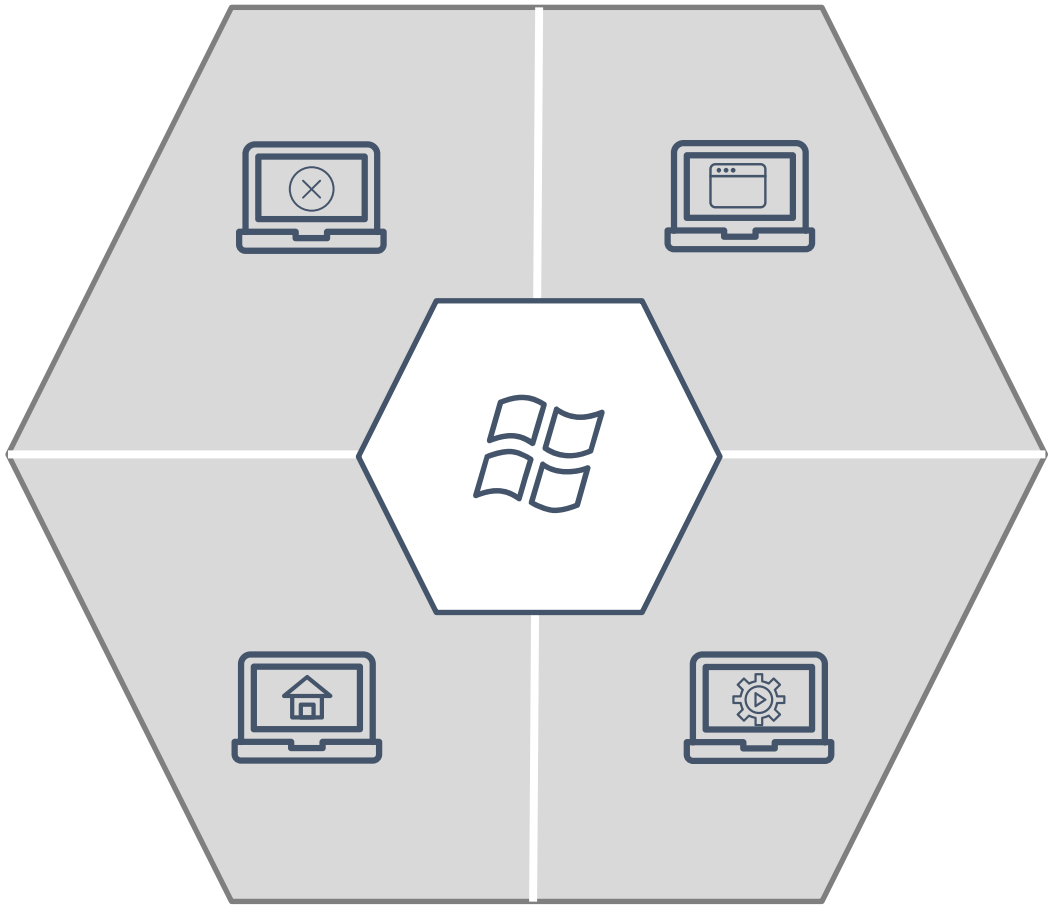
Retire / Delete are the best options for devices which are no longer needed. All access to the device is removed immediately.

❑ FRESH START

The fresh start action is very similar in function to the wipe action, however fresh start helps to remove pre-installed (OEM) apps that are typically installed on a new device.

Fresh start offers the option of retaining user data, otherwise the device is restored to the default OOBE.

LAs can use this option if they would like to reassign a device.



❑ WIPE

The wipe action will restore a device to its default settings.

All data, apps and settings can be removed using the wipe action which is why the **wipe action is useful for resetting a device before it will be given to a new user, or when the device has been lost or stolen**.

❑ AUTOPILOT RESET

Autopilot Reset removes all files, apps and settings and user data on a device but retains the connection to Azure AD and Intune.

Autopilot reset also maintains the region/language/keyboard, any machine provisioning and Wi-Fi connections.

Autopilot Reset is the best option for re-using a working device. The last user is removed, and the device can be handed over the next user.

Hybrid Overview | Introduction to Hybrid

NHSmail Intune allows Windows 10/11 devices to be enrolled onto the platform as Azure Hybrid-joined devices as well as Azure AD-joined devices

Why Hybrid?

1. In order for organisations to achieve a full, Cloud-Only Device immediately, some organisations may find the effort and transformation prohibitive.
2. The NHSmail EMS Windows 10/11 'Hybrid Track' solution is designed to accelerate cloud adoption by providing an interim solution.
3. Organisations can more widely deploy and adopt Cloud benefits in NHSmail by:
    1. Adopting a 'Cloud + SSO Track' (AAD-joined)
    2. Adopting an interim 'Hybrid Track' (Hybrid-AAD-Joined)

Benefits & Limitations

- ✓ Device identity managed in nhs.net Azure AD
- ✓ Augmented access to resources in the organisation's on-premises Active Directory
- ✓ Microsoft Intune & Co-management with SCCM
- ✓ Org AD Users / (Hybrid-joined) Devices synchronised to NHS.net AAD
- ✓ Windows Autopilot builds for AAD-joined devices
- ✗ Org AD User & Device Groups not synced to AAD

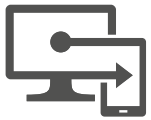
What's available for organisations?

1. Option to progress with an AAD-joined device with Cloud adoption simultaneously
2. A Kick-off assessment will identify the main track opted for and align support accordingly.

Hybrid Overview | Technical Benefits

By adopting Hybrid Windows 10/11 devices, organisations can accelerate the adoption of key **secure NHSmail cloud services** to reduce IT effort and enhance user experience

Intune



Intune Cloud Management

Deploy and manage AAD-Joined devices with Autopilot and Intune.

Hybrid-joined device management can be migrated from On-premises SCCM to cloud via 'Co-management' workloads.

Conditional Access

Enhanced Device Compliance

Provides a pathway to applying conditional access to users' devices to access key NHS resources:

- Require Device Compliance
- Require approved apps

Cloud and On-Premises access

Single-Sign-on to resources

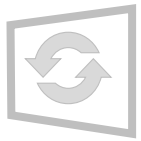
Enhanced access to Cloud and existing on-premises resources for AAD-Joined devices such as printing, existing apps, Active Directory and more.

Defender for Endpoint (ATP)

On-board cloud-based security

Leverage Microsoft Defender for endpoint with Intune to keep devices secure. Migrate & Retire existing AV and threat protection solutions.

Windows Updates



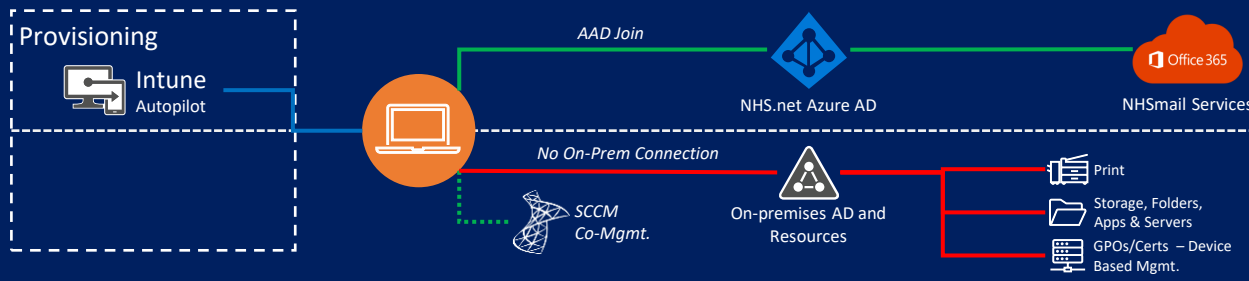
Enhanced Windows updates & Features

Automate and centralise Windows 10/11 updates and features with Intune-based 'Deployment Rings' and an evergreen approach.

Different Tracks Available

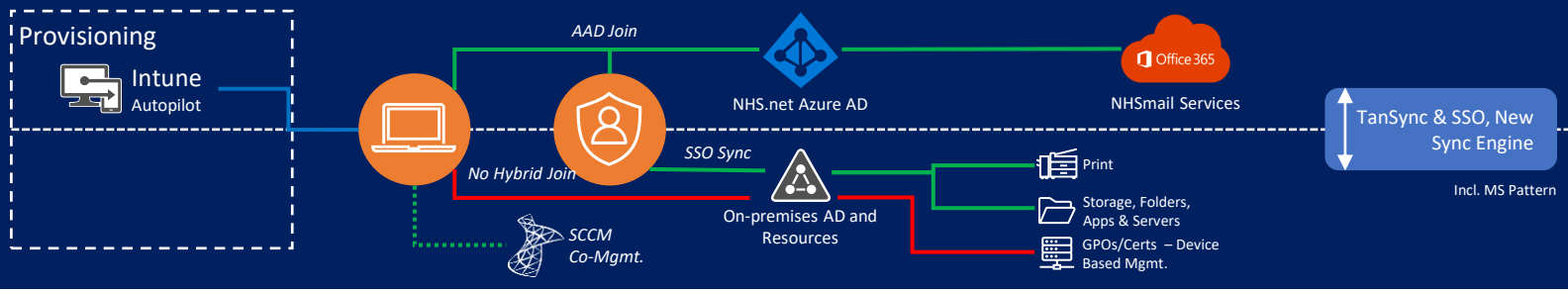
Cloud Track

Available Now



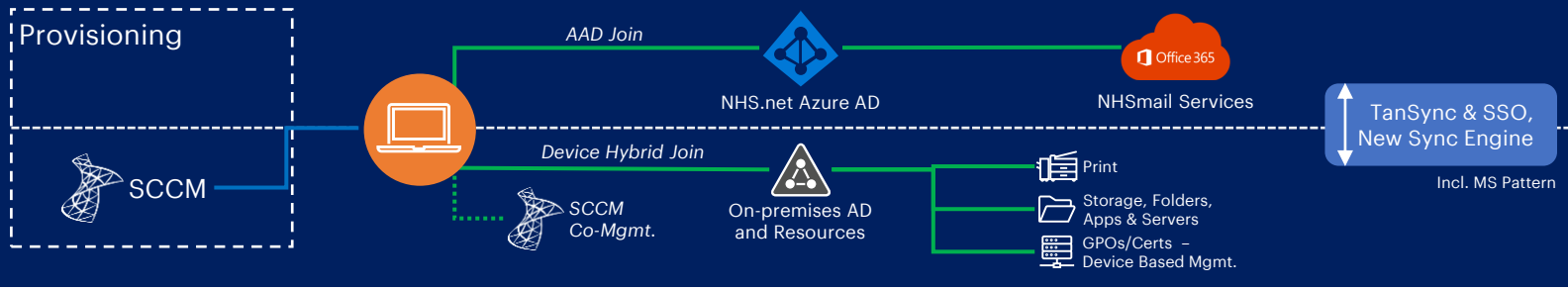
Cloud + SSO Track

Available Now



Hybrid Track

Available Now



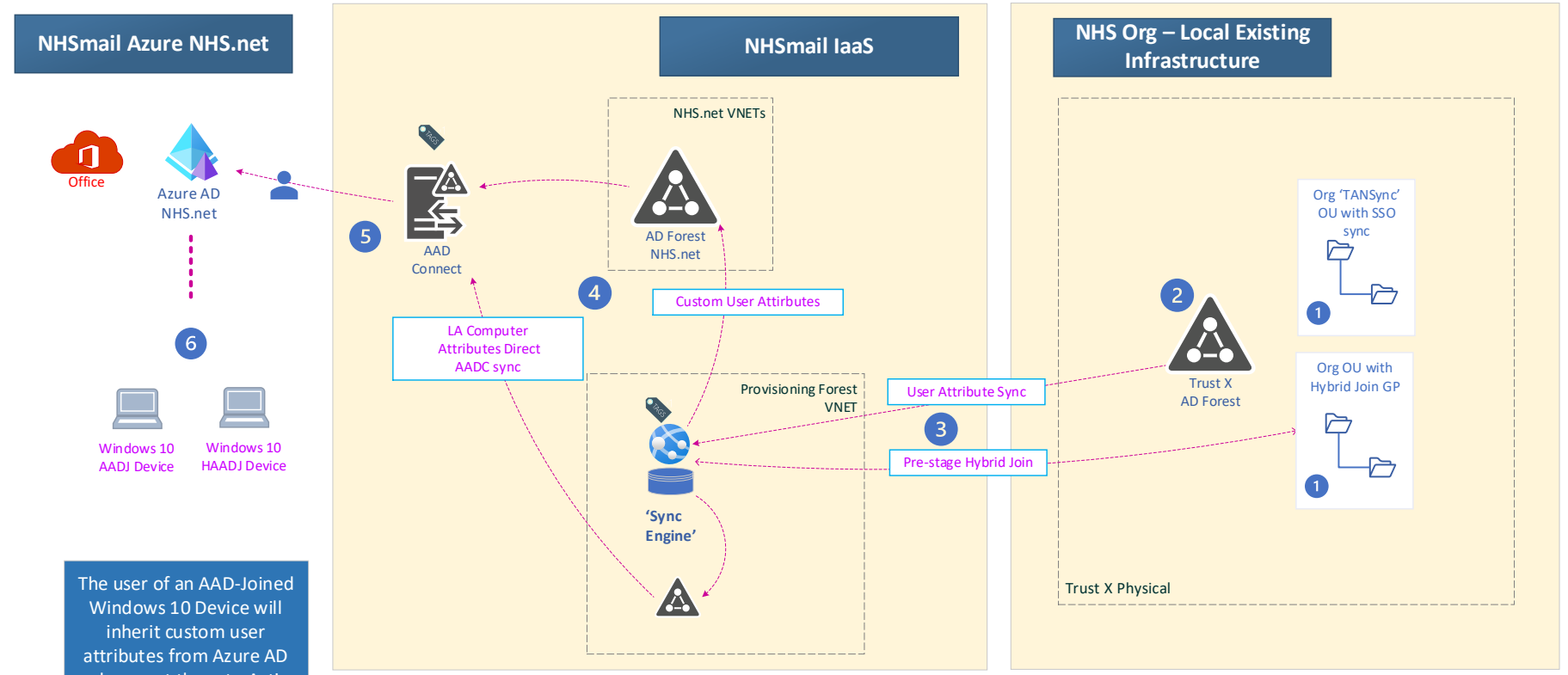
Dotted Line Indicates Optional

Connectivity

Provisioning

No Connectivity

Hybrid Overview | Solution Schematic



6 The user of an AAD-Joined Windows 10 Device will inherit custom user attributes from Azure AD and present these to Active Directory when used on-premises for the Local Org

6 The Windows 10 device completes Hybrid-join status when a Primary Refresh token is achieved through the SyncEngine Activities

3 The 'Sync Engine' syncs user attributes and also pre-stages the device into AzureAD via the NHSmail IaaS

4 The 'Sync Engine' provides User and Device Attributes to be synchronised to AzureAD, Hybrid Device Attributes stored in the 'Provisioning Forest'

5 User and Device Attributes to be synchronised to AzureAD

1 Local AD Device / User objects are added to sync target OUs

2 SyncEngine Connectivity to Local AD reads the objects and required attributes

Hybrid Overview | Prerequisites

Below is a high-level overview of the prerequisites required to be met before an organisation can begin using the Hybrid solution

1

CONFIGURE SAME SIGN ON

The NHSmail solution for Event-driven Password Sync with NHS.net Azure identities will be deployed on a Local Org Domain Controller

2

CONFIGURE/CHECK TANSYNC/MIM/BDS

The Local Org will require the use of a custom identity solution to support User provisioning via the NHS Portal and API (Cloud service, details will be provided by team or equivalent BDS config secured)

3

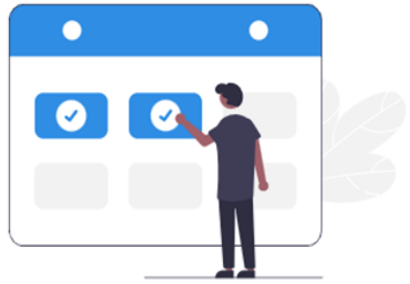
DEDICATED VLAN/EDGE NET

Local Orgs will need to set up an isolated / edge network to host an AD Domain Controller to provide an endpoint to the 'Sync Engine'

4

STS VPN TUNNEL FACILITY (IKE V2)

Pre-prepared config file will be provided to Local Orgs with Tunnel definition



5

SECURE A DEDICATED AD DOMAIN CONTROLLER IP ADDRESS SPACE

The NHSmail Intune team will advise on IP address range for the Local Organisation 'Edge' network

6

STAND UP A DEDICATED AD DC

A specific domain controller will be set up in the edge network outlined above with routing to internal Domain Controllers

7

VALIDATE AD REPLICATION to 'INTERNAL' DCS

The domain controller needs to be part of the Domain replication set

8

CREATE EXTERNAL FOREST TRUST & DELEGATIONS

A Forest External Trust need to be set up to the NHSmail EMS 'Provisioning Forest' to allow SyncEngine LDAP access

9

NHS.NET USER IDENTITIES

Define the accounts for testing that will be used, provision and test regular user functions

10

PREPARE 2 HYBRID-JOINED WINDOWS 10 TEST DEVICES

Windows 10 Devices should be built with existing on-premises methods (with apps deployed) and made available for Hybrid-join status

11

PREPARE 2 AAD-JOIN WINDOWS 10 TEST DEVICES

Windows 10 Devices should be built from EMS Intune Autopilot (including apps required), deployed from Intune or SCCM (additionally requires SCCM 'co-management' setup) and made available for 'AAD+SSO' sync

Hybrid Overview| Same Sign On

An outline of the Same Sign On prerequisites required before an organisation can begin adopting the Hybrid solution

Overview

Currently, the majority of NHS organisations operate Local Directories which are typically standalone and do not link with any of the directories within the NHS. This means that users must manage two separate passwords, one for NHSmail to access their mailbox, and one for their local AD to log into their workstation.

This causes a high volume of password reset tickets to organisations' local service desks.

The NHSmail Same Sign On (SSO) solution enables bi-directional synchronisation of passwords between NHSmail and organisations' local active directories.

Key Benefits

✓ Reduce overhead on password management for users

✓ Reduce overhead on the service desk to support password reset

✓ Unified Password Policy across the two services

Hybrid Overview | TANSync

An outline of the Identity Sync prerequisites required before an organisation can begin using the Hybrid solution

Overview

TANSync is a **customised Identity Management Solution which synchronises user objects between NHSmail and local Active Directory (AD)** using Microsoft Identity Manager.

No Microsoft licenses are required and there are therefore **no ongoing licenses costs**.

Key Benefits

✓ Exchanging contacts to and from your Local AD

✓ Creating accounts in NHSmail – with Local AD being authoritative

✓ Creating users in Local AD – with NHSmail being authoritative

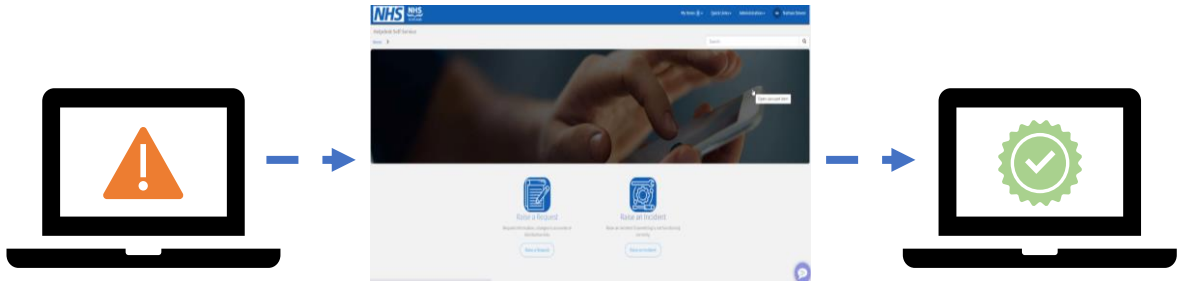
Additional Resources:

- Windows 10/11 Overview
- Cloud Track
- Cloud + SSO Track
- Hybrid Track
- Surface Hubs Guidance
- Co-Management and Certificates

Note: Organisations can alternatively adopt the equivalent 'BDS' or custom Identity sync solution as an alternative to TANSync

Win 10/11 Deep Dive | Service Requests

List of Windows 10/11 specific Service Requests which can be raised and when these should be raised by LAs enrolling and managing AD-joined devices



Ticket Type			Reason for Ticket	Requestor/s
Onboarding Tickets		Intune Registration Form	• Submission of key information about an interested organisation and current readiness for Intune, in order to register interest in onboarding onto the platform.	LA from an interested organisation ONLY.
		Onboarding Request Form	• Submission of the Onboarding Request Form to request the technical onboarding of an organisation on to the NHSmail Intune Service. • **Please note:** This form will only be visible to LA/s listed on your organisation's entry on the NHSmail Intune SharePoint.	LA from interested organisation ONLY who have been invited to complete this form.
		Licence Onboarding Request Form	• Request to move procured licences into the NHS Shared Tenant in order to be able to assign them to LAs and end users.	LA from interested/onboarded organisation. Helpdesk can support with completing form if needed.
Service Support		Service Requests	• **Windows 10/11 BitLocker recovery key** • Request an Android enrolment profile (Shared Device) • Request to offboard an organisation from the NHSmail Intune Service • Request to onboard your organisation's Apple Business Manager (ABM) for Apple Devices • Request to add a certificate connector • Request to add a multi-organisation • Query related to Security Posture • **Request for Cloud + SSO Track and Hybrid Join Track** • Other	LA from concerned organisation. Helpdesk can support with completing form and submitting if needed.
		Incidents	• Organisation onboarding • Device enrolment • Intune Role Based Access Control (RBAC) Permissions • Device configuration and policies (LA Delegated) • Intune Group Management Tool • Resetting Devices • Applications • Conditional Access • Centrally managed configuration (security posture) • Other	LA from concerned organisation. Helpdesk can support with completing form and submission if needed.

Windows 10/11 Service Requests:

1. WINDOWS 10/11 BITLOCKER RECOVERY KEY

- LAs have the ability to **rotate** BitLocker keys for Windows 10/11 devices as part of their RBAC permissions.
- BitLocker **recovery** keys for Windows 10/11 devices need to be requested via Helpdesk Self-Service and raised as a service request.
- Recovery requests will then be reviewed by the NHSmail Intune Technical Team and a resolution communicated back to you.
- It is **hoped that this action will be able to be delegated to LAs in the future**, although no timeframe has yet been confirmed.

2. REQUEST FOR CLOUD + SSO TRACK AND HYBRID JOIN TRACK

- LAs can raise a service request if they are interested in the Cloud + SSO Track or the Hybrid Join Track (as opposed to the standard Cloud Only Track).
- A session is then scheduled with the Live Service Team to look into the viability of this i.e. does organisation setup accommodate this, can pre-requisites be met etc.

THANK YOU