



NHSmail Intune

Technical Deep Dive Webinar

06th December 2022



Agenda

Technical Deep Dive

- 01** Introduction
- 02** Current capabilities
- 03** Android / iOS
- 04** Windows 10/11
 - Cloud
 - Hybrid
 - Cloud + SSO
- 05** Co-management
- 06** Conditional Access
- 07** NHSmail Intune Roadmap
- 08** Microsoft Feature Update
- 09** Q & A

NHSmail Intune Service

Overview & Context

- NHSmail Intune is a new **corporate device management service integrated with existing NHSmail capabilities**
- Centralised device management delivered in this manner will allow local orgs. to maintain a **degree of oversight and local autonomy, through the use of RBAC controls.**
- Onboarded organisations can access technical support to successfully rollout Intune across their device estates from both the **Intune Live Service Team** and the **Microsoft FastTrack Team.**
- Positive feedback has been received from onboarded organisations especially Android enrolment / management and support available.

Devices



Uptake & Onboarding



143 organisations currently using the service



>220 Local Admins using Intune Teams channel

To onboard:

Organisations wishing to onboard onto the service should complete this [registration form](#).

Benefits

- ✓ Improved device estate security via defined postures
- ✓ Centralised Intune platform with local autonomy
- ✓ SSO to NHSmail apps for end users
- ✓ Licence consolidation
- ✓ 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)



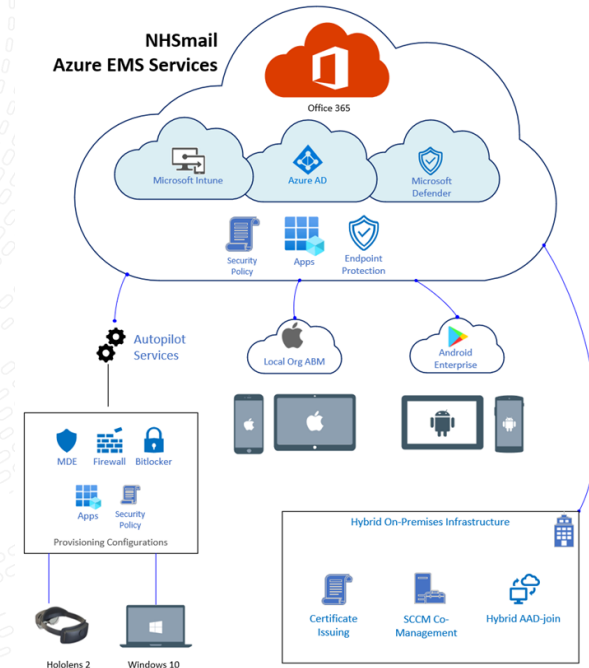
EMS E3 & AADP2 licenses in NHS Tenant



ABM link to NHSmail Intune (for Apple only)



Reset devices to factory settings

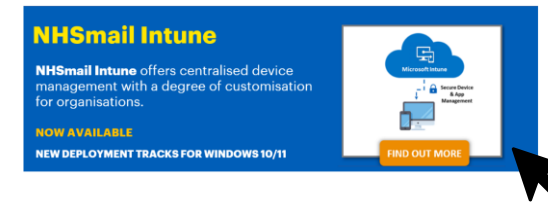


NHSmal Intune Support & Community



Support Documents

<https://support.nhs.net/article-categories/intune/>

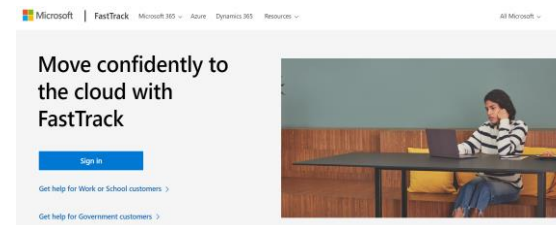


Teams Channel

Join here:

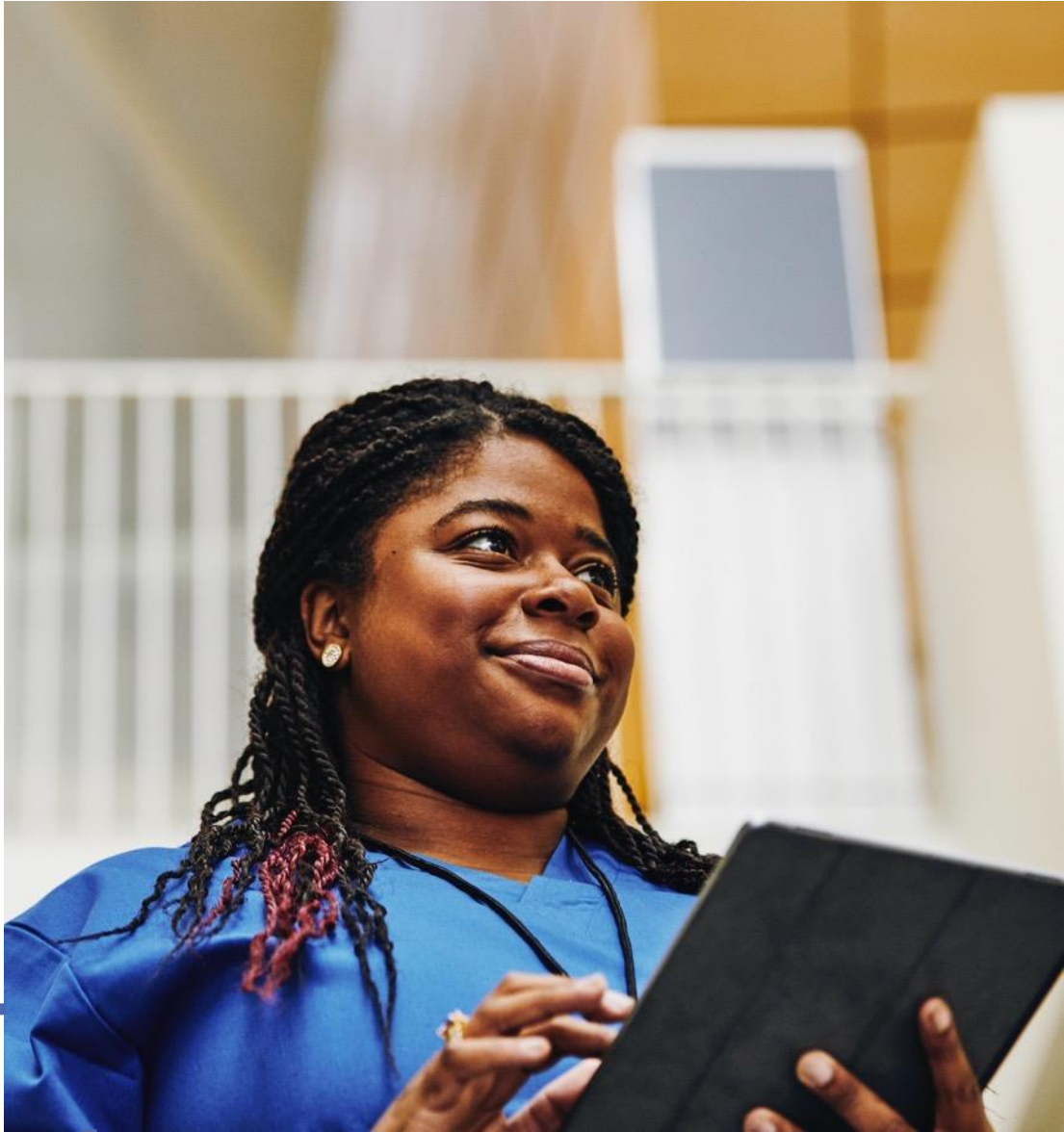
https://teams.microsoft.com/l/team/19%3a_RUbfd7jHHWjT6eyxI3otRTiUozzEwcVJvA-WN8-IJw1%40thread.tacv2/conversations?groupId=9cbf9175-58de-4ca8-94d4-157544c080eb&tenantId=37c354b2-85b0-47f5-b222-07b48d774ee3

Microsoft FastTrack



Intune Live Service

Dedicated Intune service support team



Current capabilities

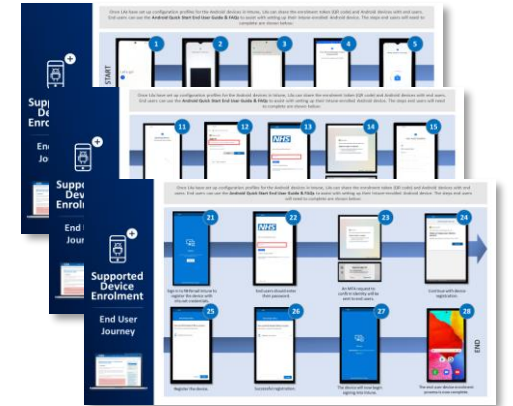
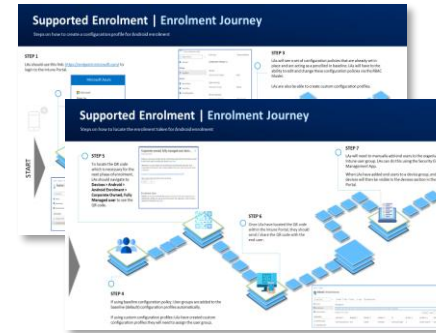
- Corporate device management integrated with NHSmail supporting single and shared user Android, iOS, Windows 10 /11 and HoloLens 2
- NCSC / CIS Security Baselines
- SCCM / MECM Integration and Co-Management
- Samsung Knox enrolment
- First-line RBAC role
- 3 ways to manage Windows 10/11 devices
- Mobile Application Management (MAM) Policies
- Multi-organisation management
- Conditional Access
- Surface Hubs



Android



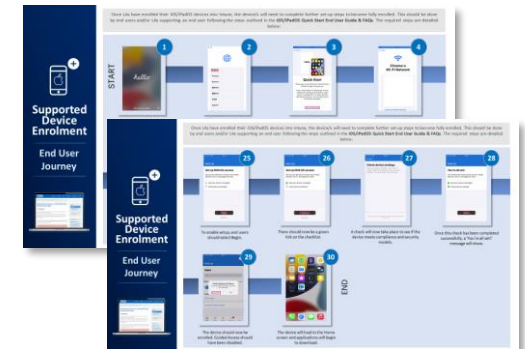
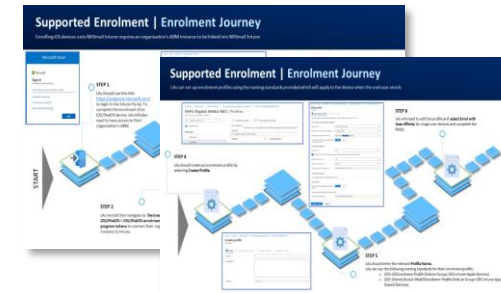
Samsung Knox can be used for easier mass enrolment of devices



iOS



Requires link with NHSmail Apple Business Manager (ABM)



Windows 10 / 11 Tracks

3 ways to manage Windows devices

Cloud

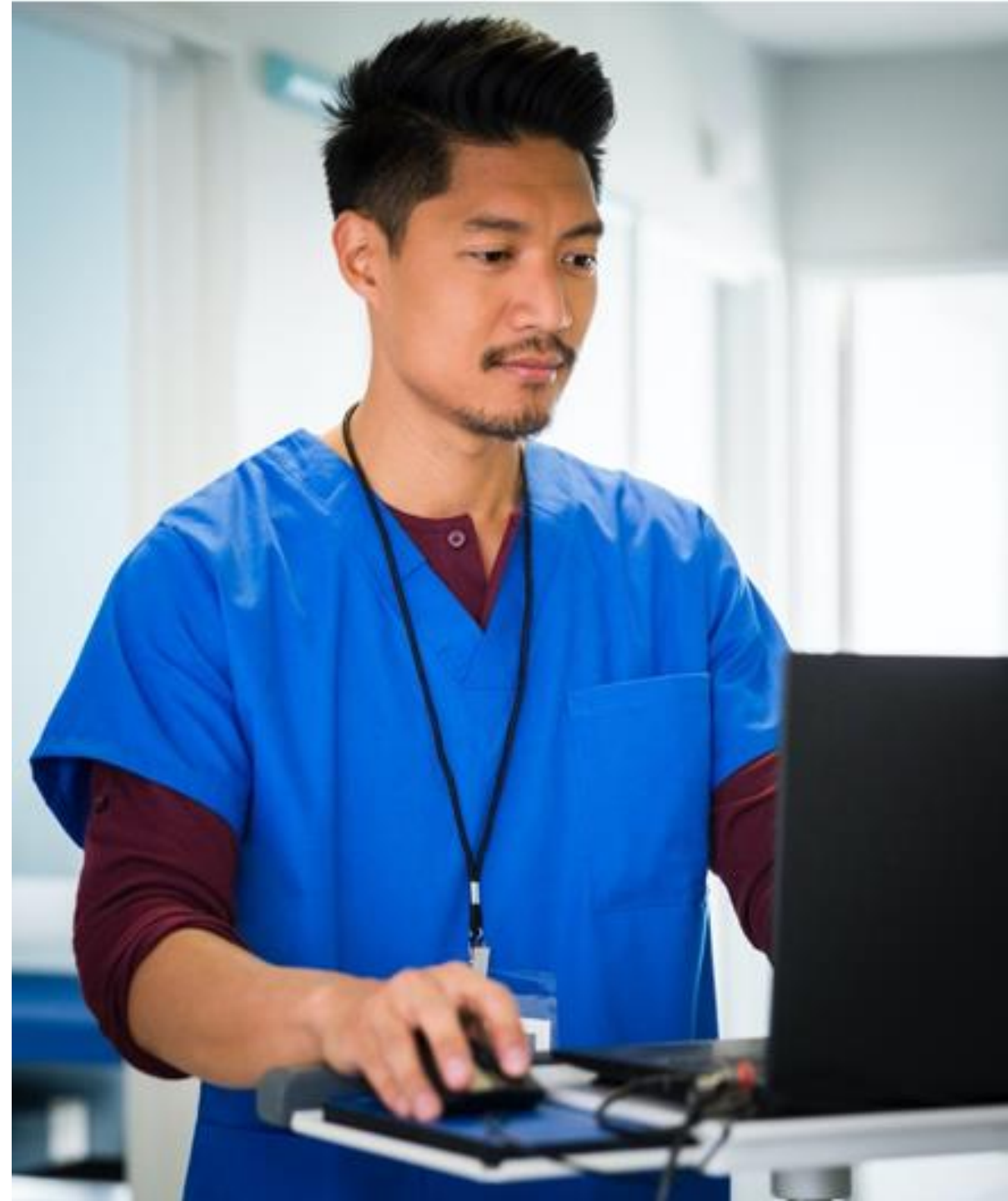
Allows devices to be deployed and managed solely through the NHSmail Intune tenant.

Hybrid

Allows devices to be managed in the NHSmail Intune tenant but remain domain-joined with local Active Directory.

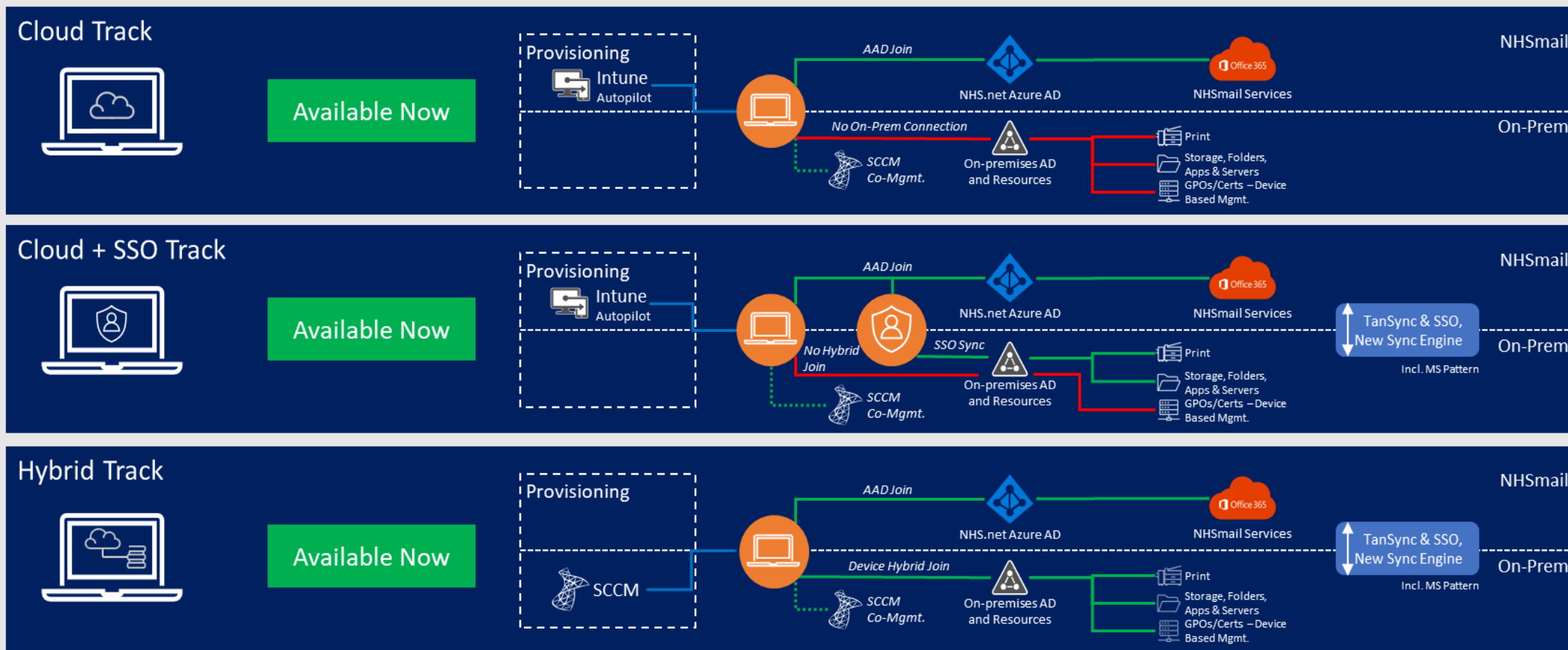
Cloud + SSO

Allows devices to be managed in the NHSmail Intune tenant with Local Active Directory User Identity enhancements.



Technical solutions

No Connectivity



Pre-Requisites

1

Configure TANSync/BDS

An identity management solution which synchronises user objects between NHSmail and local active directory

2

Configure Same Sign On

A solution which enables bi-directional synchronisation of passwords between NHSmail and local active directory

3

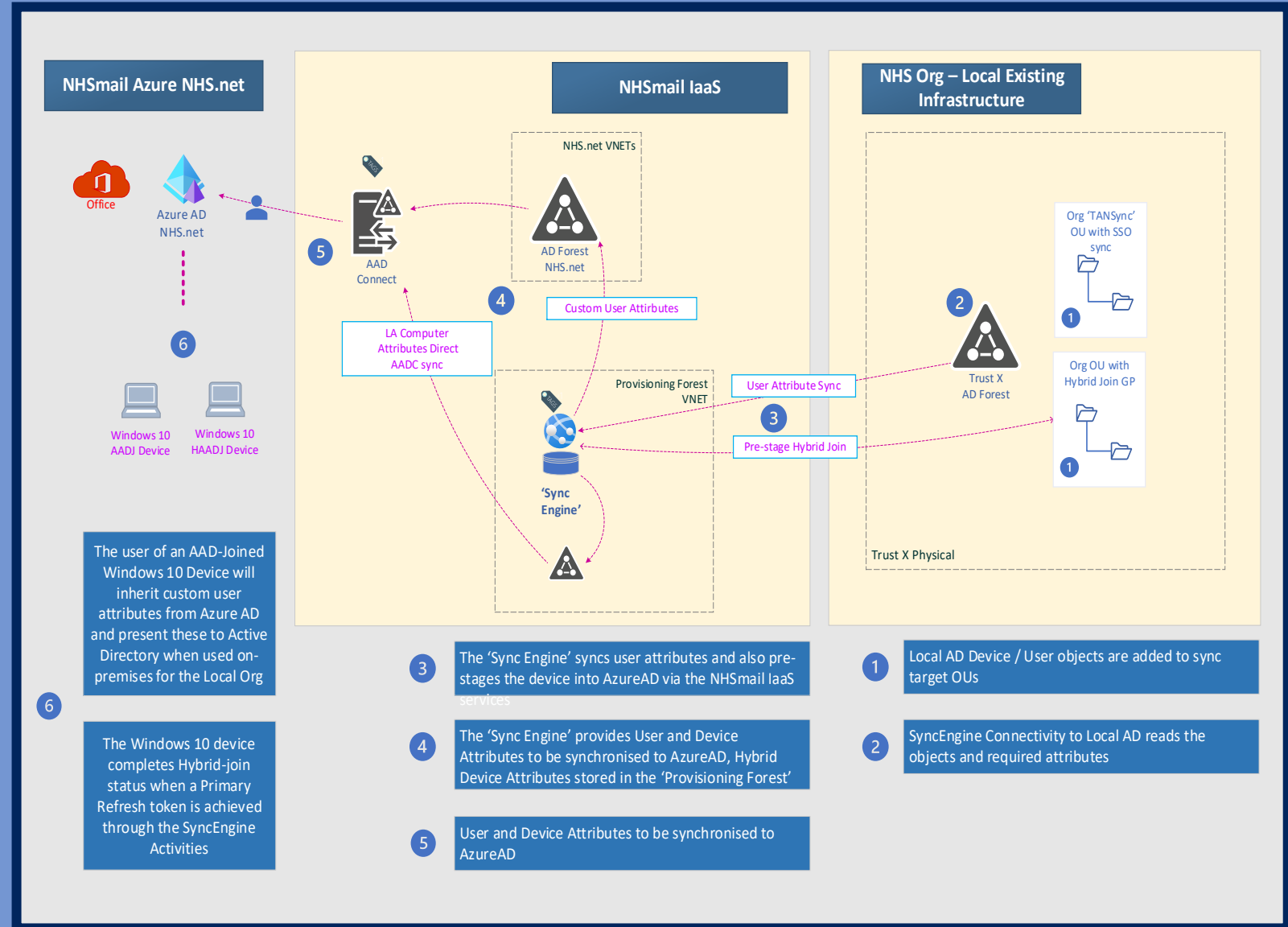
Assist setting up S2S VPN Connection

Stand up a dedicated DC to ensure there is connectivity and a Sync Engine can be provisioned



Windows 10 / 11 Tracks

Hybrid solution schematic



Windows 10 / 11 Management

Co-Management

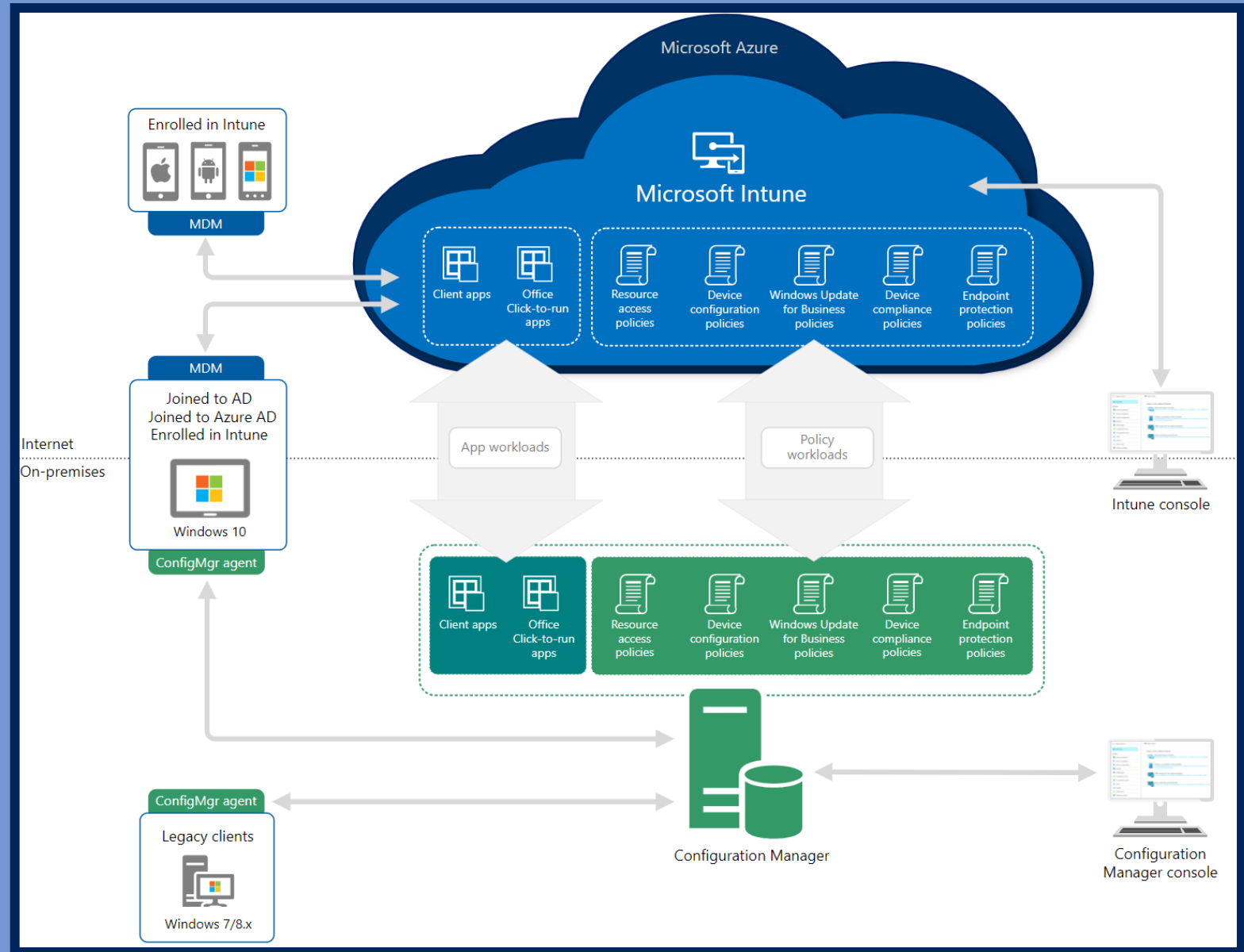
Co-management allows LAs to link their existing on-prem environment with the Microsoft 365 Cloud.

The NHSmail Intune service provides Hybrid solution to enable organisations to Co-Manage their devices with Configuration Manager (SCCM) and Intune.

LAs can choose which workloads they'd like to be managed via SCCM and which via Intune. Workloads:

- Compliance Policies
- Device Configuration
- Endpoint Protection
- Client Apps
- Windows Update Policies

Existing workloads and deployments can be preserved in the existing SCCM Site configuration if required with others applied via Intune, concurrently.



Windows 10 / 11 Management

Co-Management

Co-Management can be achieved in the below two pathways.

Existing Configuration Manager:

- Domain Joined Windows 10 Device with Configuration Manager client installed
- Join Windows 10 device to Hybrid Azure AD (Hybrid Track)
- Enroll into Intune
- Enable Co-management on configuration Manager and Share workloads

New internet-based devices:

- Windows 10 Device Azure AD joined and enrolled into Intune with configuration manager client installed
- Request a public SSL certificate for the cloud management gateway (CMG)
- Enable Azure services in Configuration Manager
- Deploy and configure CMG (Cloud Management gateway)

Co-Management – NHS.net Tenant

Co-management services for Intune on-boarded organisations does not require the deployment of additional Resource Types to O365 Azure tenants and can therefore continue as planned

(Co-management enables both Intune and SCCM to manage a device. Without a CMG, the SCCM client will then need connectivity to the on-premises SCCM site via VPN/Internet Client method)

- ✓ Organisations with NO existing Co-management facility will enrol devices into the NHSmail tenant as part of Hybrid/On-boarding



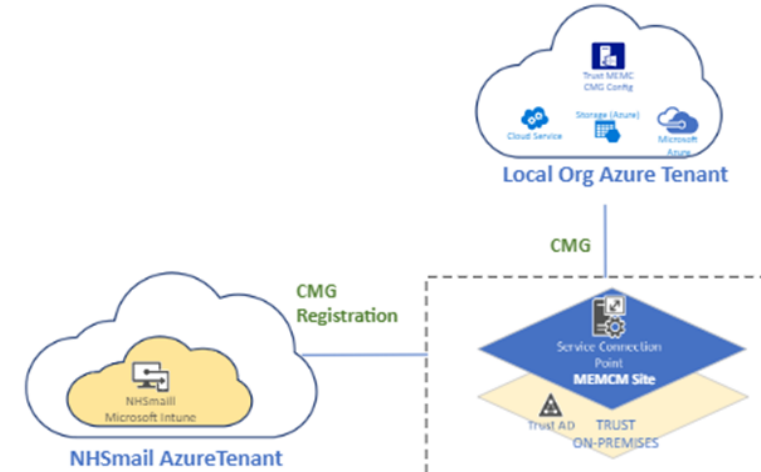
CMG - Local Org Azure Tenant

- ✓ Org can Deploy CMG Resource Types to their own Azure Subscription:

- Microsoft.ClassicCompute
- Microsoft.Storage
- Microsoft.Network

- ✓ Organisations will then register their CMG (additionally) in the NHS.net tenant for client connectivity

- ✓ Org can alternatively configure their Native On-premises SCCM to provide CMG internet client connectivity



Conditional Access

Conditional Access provides a way to secure access to Azure services, apps or data based on pre-qualified 'conditions', prescribed through policies.

The Conditional Access Policies are configured by Central Tenant Administrators and applied to all users.

Policies apply to: Cloud apps and resources, requiring that service access is being performed on a secure & managed device

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



- ✓ Mark a device as '**non-compliant**' according to the (time) setting configured in the 3 postures (Baseline, Enhanced, Restrictive)



- ✓ When a device is non compliant: the **user sign in will be blocked** and the user will be required to remediate the 'non-compliance' items



Bring Your Own Device

Added security controls for BYODs

The aim is to provide **security controls** for personal and Bring Your Own (BYO) Devices accessing **NHSmail O365 services**.

Personal and BYO Devices are defined as mobile devices (iPhone, iPadOS and Android) and Windows 10/11, MacOS and Linux devices that are:

personally owned and unmanaged, or
corporate devices but **unknown to the NHSmail tenant**.

KEY BENEFITS



Reduces security risks on organisations' BYODs that access NHSmail services



Autonomy for LAs to manage and secure their organisation's BYODs

- ✓ LAs will be able to **opt-in or opt-out users** from Conditional Access policies
- ✓ BYO controls will be available to **both Intune and non-Intune organisations**
- ✓ BYO controls will be available using **standard NHSmail licences**

LICENSES



NHSmail E3R & AADP2



EMS

Specifically for orgs enrolled and managing devices on Intune



NHSmail Intune Roadmap

Items in development



Zebra Mobility Extension

Added security features
for Android



Read only RBAC permission

Additional RBAC
permission ideal for new
users



Autopilot Manufacturer Provisioning

Easier provisioning of
new devices



Windows Store

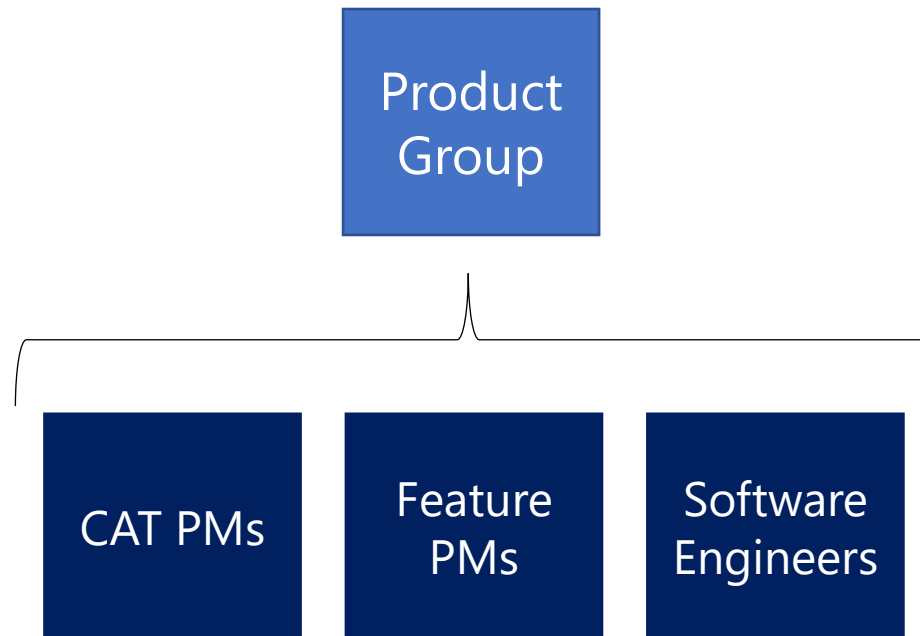
Integration with
NHSmail Intune
following the
deprecation of Microsoft
Store

Microsoft Intune

- **Introduction to the team**
- **Product investment areas**
- **FastTrack Assistance**

What is Customer Acceleration Team?

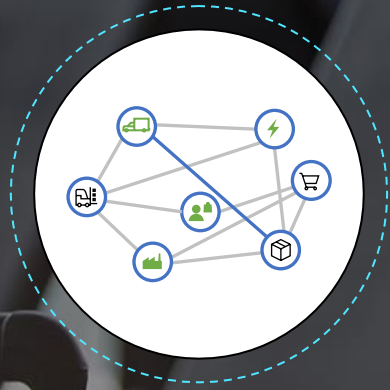
- Product Group owns the end-to-end lifecycle of one or more products
 - All the orgs are part of Engineering
- Key in deepening relationships between Microsoft and our customers



What is CAT (contd..)



Provide strategic
guidance



Deep technical
advice and
deployment
assistance



Understand your
scenarios and
business
challenges



Part of the
Product Group

Our goal is a long-term relationship for mutual benefit

Microsoft Intune – Top-level priorities

Service basics:
security, availability,
scalability, quality,
compliance

Supporting our
internal partners

Advanced
Management

Windows
Commercial

Mobile Application
Management

Frontline Workers

Analytics

Integrations

Microsoft Intune – Focus Areas



THE YEAR OF MAM



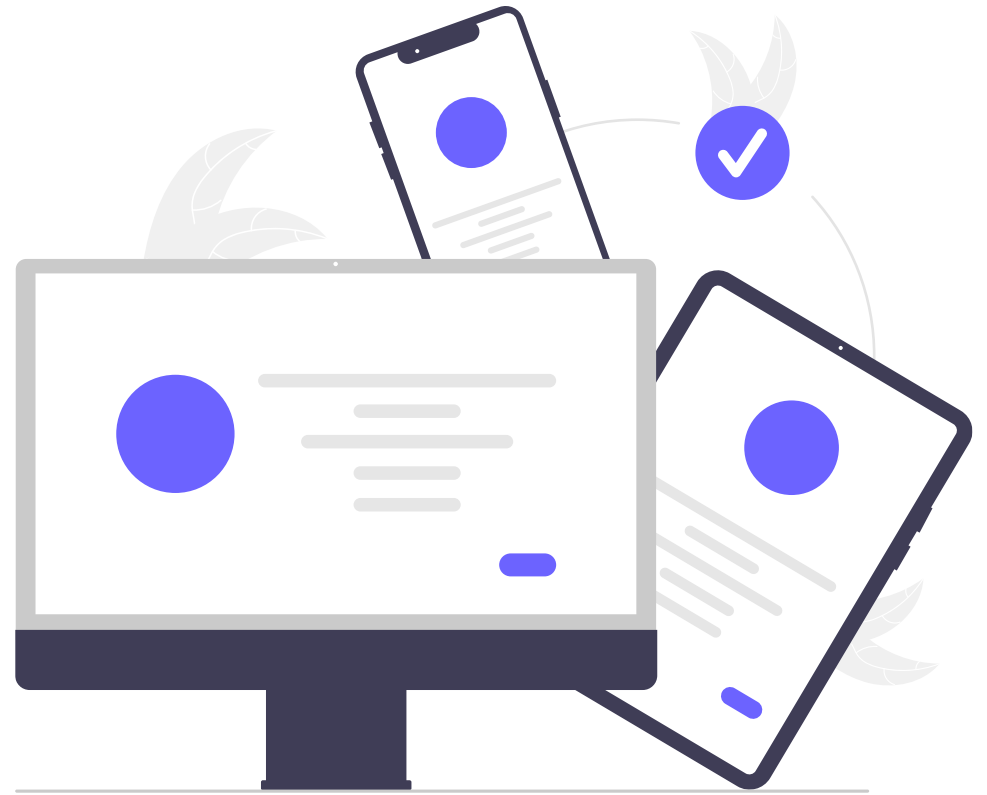
SHARED DEVICES



ANALYTICS

FastTrack Support for Microsoft 365

- FastTrack is a benefit designed to help you deploy Microsoft 365 (included in eligible subscriptions) at no additional cost. You can use FastTrack services with a new or existing qualifying subscription.
- Organisations can request FastTrack assistance via this NHSmail Support Site article - [Microsoft FastTrack Support – NHSmail Support](#)



Q & A

A woman with curly hair, wearing a blue cardigan over a white shirt, is smiling and pointing at a tablet held by an elderly woman with short blonde hair. The elderly woman is sitting in a dark green armchair, wearing a light pink long-sleeved shirt. They are in a bright, modern living room with large windows in the background showing green plants. In the foreground, there is a small round black table with a white teapot, a white cup and saucer, and a small potted plant. The text "Thank you" is overlaid in the center in a large, white, sans-serif font. A white arrow points to the right, positioned below the text.

Thank you

