FastTrack Benefit Description for the NHS

This Benefit Description is current as of ***February 18, 2025.***

Microsoft works with a network of certified partners (FastTrack Ready Partners, or FRPs) who provide expertise in deploying Microsoft 365 solutions. These partners help organisations navigate the deployment process, customise the approach to meet your specific needs and provide additional support to ensure successful adoption to drive effective utilisation of your services. Partners also recommend additional services (in addition to the FastTrack benefit) for a fee to enhance your deployment experience. Those services are determined case-by-case based on your particular requirements and wants.

The **FastTrack Benefit Description for the NHS** identifies the scope of guidance that FRPs will provide to the National Health Service (NHS) Organisations engaged in this programme. The specific workloads and guidelines have been customised to the unique central tenant configuration utilised by NHS and is subject to change.

There are four (4) sections to each workload:

1. **FastTrack Guidance Details** (definition of the in-scope activities)
2. **Source Environment Expectations** (system requirements)
3. **The following is out of scope** (activities that are not covered by this program)
4. **Organisation responsibilities include** (tasks that may be required of the NHS Organisation Local Administrator)

This **FastTrack Benefit Description for the NHS** is subject to change. Before entering into an engagement between an NHS Organisation and FRP, the current **FastTrack Benefit Description for the NHS** should be downloaded and referenced to ensure that all parties are clear as to what workloads are included, as well as the activities that are in and out of scope for these workloads.

This programme is exclusive and only available to the NHS for the duration of the NHSmail and Custom FastTrack Ready programme, which completes on **June 30th, 2026**.

M365 Applications

FastTrack Guidance Details

We provide remote deployment guidance for:

- Addressing deployment issues.
- Installing Office Mobile apps (like Outlook Mobile, Word Mobile, Excel Mobile, and PowerPoint Mobile) on your iOS or Android devices.
- Configuring update settings using the Office 365 Deployment Tool. Selection and set-up of a local or cloud installation.
- Creation of the Office Deployment Tool configuration XML with the Office Customisation Tool or native XML to configure the deployment package.

Source Environment Expectations

- Online client software must be at a minimum level as defined in the System requirements for Microsoft 365 and Office.
- Test your network connectivity Microsoft 365 network connectivity test (office.com).
- Enablement and management of M365 Apps by ~~SCCM~~, group policies and Intune.

The following is out of scope:

- Microsoft 365 Admin Center/Cloud Policy access. This is restricted for use at the Tenant level only; all settings are universal to the Organisations and cannot be customised or accessed by the Organisations. *Partner to provide guidance as to what settings are needed for Local Administrator to create service request.*
- M365 Cloud policies are not enabled at the Organisation level and are out of scope.

Organisation responsibilities include:

Alignment with Microsoft's principals of network connectivity is vital to the successful onboarding of FastTrack Services. As such, FastTrack provides remote guidance to obtain and interpret data from a customer's environment subject to the terms of the customer agreement to verify this alignment. This highlights a company's network score which directly impacts migration velocity, user experience, service performance, and reliability. FastTrack also guides our customers through necessary remediation steps highlighted by this data to help improve the network score.

Organisation's Local Administrator will need to initiate service requests as needed to turn on/off capabilities, correct access roles, etc.

Microsoft Defender for Endpoint (MDE)/Microsoft Defender Advanced Threat Protection (MDATP)

FastTrack Guidance Details

Microsoft Defender for Endpoint is a platform designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats. We provide remote guidance for:

- Assessing the OS version and device management (including Microsoft Endpoint Manager, Microsoft Endpoint Configuration Manager, Group Policy Objects (GPOs), and third-party configurations).
- Onboarding Microsoft Defender for Endpoint P1 and P2 customers. Organisations should contact mdefeedback@nhs.net for further guidance.
- Providing recommended configuration guidance for Microsoft traffic to travel through proxies and firewalls restricting network traffic for devices that aren't able to connect directly to the internet.
- Enabling the Microsoft Defender for Endpoint service by explaining how to deploy a Microsoft

Defender for Endpoint (MDE) endpoint detection and response (EDR) agent profile using one of the supported management methods.

- Deployment guidance, configuration assistance, and education on:
    - Threat and vulnerability management
    - Attack surface reduction (ASR), including Web Protection*
    - Next-generation protection
    - EDR
    - Automated investigation and remediation
    - Secure score for devices
    - Microsoft Defender SmartScreen configuration using Microsoft Endpoint Manager
    - Device discovery, including auto tagging. Please contact mdefeedback@nhs.net for further guidance.**
- Reviewing simulations and tutorials (like practice scenarios and fake malware.
- Overview of reporting and threat analytics features.
- Walkthrough Microsoft Defender for Endpoint in the portal view.
- Onboarding and configuration of the following operating systems:
    - Windows 10/11.
    - Windows Server 2012 R2***
    - Windows Server 2016***
    - Windows Server 2019***
    - Windows Server 2022***
    - Windows Server 2019 Core Edition***
    - Supported macOS versions (see System requirements for more details).
    - Android****
    - iOS****

*Only attack surface reduction rules, controlled folder access, and network protection are supported. All other attack surface reduction capabilities aren't in scope. See the following **out of scope** section for more details.

Only some aspects are device discovery are supported. See the following **out of scope section for more details.

***Windows Server 2012 R2 and 2016 support is limited to the onboarding and configuration of the unified agent. All Windows versions must be managed by Configuration Manager or Microsoft Endpoint Configuration Manager 2017 (with the latest hotfix updates or greater).

****Constraints are set at the central tenant level. See the following **out of scope** section for mobile threat defense details.

Source Environment Expectations

Most Organisation may already be configured for MDE Admin Roles, as they are centrally configured. New Organisations not already configured must contact mdefeedback@nhs.net prior to FastTrack enrollment.

The following is out of scope:

- Onboarding and enablement guidance for preview features.
- Project management of the customer's remediation activities.
- Complex issues and unknown errors during engagement.
- Management of break/fix issues.
- On-site support.
- Ongoing management and threat response.
- Onboarding or configuration for the following Microsoft Defender for Endpoint agents:
    - Windows Server 2008. o Linux.
    - Virtual Desktop Infrastructure (VDI) (persistent or non-persistent).
- Server onboarding and configuration below:
    - Configuring a proxy server for offline communications.
    - Configuring Configuration Manager deployment packages on down-level Configuration Manager instances and versions.
    - Servers not managed by Configuration Manager.
    - Integrating Defender for Endpoint with Defender for Servers (Defender for Cloud).
- macOS onboarding and configuration related to:
    - JAMF-based deployment.
    - Other mobile device management (MDM) product-based deployment.
    - Manual deployment.
- Mobile threat defense onboarding and configuration (Android & iOS):
    - Unmanaged bring your own devices (BYOD) or devices managed by other enterprise mobility management systems.
    - Set up app protection policies (like mobile app management (MAM)).
    - Android device admin-enrolled devices. Assistance with co-existence of multiple VPN profiles.
    - Onboarding devices to Intune. For more information on onboarding assistance, see the **Microsoft Intune** section.
- Configuration of the following attack surface reduction capabilities related to:
    - Hardware-based app and browser isolation (including Application Guard).
    - App control.
    - Device control.
    - Exploit protection.
    - Network and endpoint firewalls.
- Configuration or management of account protection features like:
    - Credential Guard.
    - Local user group membership.
- Configuration or management of BitLocker.
  Note: For information on BitLocker assistance with Windows 11, see Windows 11.
- Configuration or management of network device discovery.
- Configuration or management of the following device discovery capabilities:
    - Onboarding of unmanaged devices not in scope for FastTrack (like Linux).

    - Configuring or remediating internet-of-things (IoT) devices including vulnerability assessments of IoT devices through Defender for IoT.
    - Integration with third-party tooling.
    - Exclusions for device discovery.
    - Preliminary networking assistance.
    - Troubleshooting network issues.
- Attack simulations (including penetration testing).
- Enrollment or configuration of Microsoft Threat Experts.
- Configuration or training reviewing API or security information and event management (SIEM) connections.
- Training or guidance covering advanced hunting.
- Training or guidance covering the use of or creation of Kusto queries.
- Training or guidance covering Microsoft Defender SmartScreen configuration using Group Policy Objects (GPOs), Windows Security, or Microsoft Edge.
- Some Windows 365 features including:
    - Troubleshooting project management of customer Windows 365 deployment
    - Configuration of Windows 365 Cloud PC
    - Third-party app virtualisation and deployment
    - Custom images
    - All other areas not listed as in-scope for Windows 365.

Organisation responsibilities include:

New Organisations not already configured for Microsoft Defender for Endpoint must contact mdefeedback@nhs.net prior to FastTrack enrollment.

Microsoft Intune

FastTrack Guidance Details

We provide remote guidance on getting ready to use Intune as the cloud-based mobile device management (MDM) and mobile app management (MAM) provider for your apps and devices. The exact steps depend on your source environment and are based on your mobile device and mobile app management needs. The steps can include:

- Licensing your end users.
- Configuring identities to be used by Intune by leveraging either your on-premises Active Directory or cloud identities (Microsoft Entra ID). NHS Mail portal by Local admin or Intune to configure.
- Adding users to your Intune subscription, defining IT admin roles, and creating user and device groups.
- Providing MDM guidance for:
    - Configuring tests groups to be used to validate MDM management policies.

    - Configuring MDM management policies and services like:
        - App deployment for each supported platform through web links or deep links.
        - Conditional Access policies.
        - Deployment of email, wireless networks, and VPN profiles if you have an existing certificate authority, wireless network, or VPN infrastructure in your organisation.
        - Connecting to the Intune Data Warehouse.
- Enrolling devices of each supported platform to Intune.
- Providing app protection guidance on:
    - Configuring app protection policies for each supported platform.
    - Targeting the appropriate user groups with the previously mentioned MAM policies.
    - Using managed-apps usage reports.
- Providing migration guidance from legacy PC management to Intune MDM.

Certificate delivery

We provide remote guidance for:

- Simple Certificate Enrollment Protocol (SCEP) and the Network Device Enrollment Service (NDES).
    - Configuring Enterprise Certificate Authority related items.
    - Creating and issuing a SCEP certificate template.

    o Installing and configuring NDES. Installing and configuring the Microsoft Intune Connector for SCEP.
    - Installing and configuring Azure AD o Application Proxy and Azure AD Application connectors.
    - Creating and assigning a trusted certificate device configuration profile in Microsoft Endpoint Manager.
    - Creating and assigning a SCEP certificate device configuration profile on Microsoft Endpoint Manager.
- Public-Key Cryptography Standards (PKCS) and PFX (PKCS#12) certificates.
    - Configuring enterprise Certificate Authority related items.
    - Creating and issuing a PKCS certificate template.
    - Creating and assigning a trusted certificate device configuration profile in Microsoft Endpoint Manager.
    - Creating and assigning a PKCS certificate device configuration profile in Microsoft Endpoint Manager.

Source Environment Expectations

- IT admins need to have existing Certificate Authority, wireless network, and VPN infrastructures already working in their production environments when planning on deploying wireless network and VPN profiles with Intune.

- The customer environment should have an existing healthy PKI before enabling PKCS and SCEP certificate delivery with Intune.
- Endpoint devices must be managed by Intune.

Note: The FastTrack benefit doesn't include assistance for setting up or configuring Certificate Authorities, wireless networks, VPN infrastructures, or Apple MDM push certificates for Intune.

Note: The FastTrack benefit doesn't include assistance for setting up or upgrading either the Configuration Manager site server or Configuration Manager client to the minimum requirements needed to support cloud-attach.

The following is out of scope:

- Helping customers with their public key infrastructure (PKI) certificates or enterprise Certificate Authority.
- Supporting advanced scenarios, including:
    - Using imported PKCS certificates.
    - Configuring Intune certification deployment using a hardware security module (HSM).

Organisation responsibilities include:

- Organisation Local Administrator to submit Service Requests as needed to gain access to Intune as prescribed by the Intune Onboarding Process NHSmail Intune Service | Overview – NHSmail Support.
- Organisation Local Administrator will provide Intune baseline usage metrics from the Intune Admin Portal to NHS England (via email to england.nhsfrp@nhs.net or other method as directed by NHS England) prior to FastTrack engagement as well as monthly thereafter to track growth. Metrics should be submitted five (5) working days after the start of every month for the previous month. (Example: Organisation Local Administrator provides the number of active Intune devices by 7 February for January metrics).
    - *Please note that no personal or sensitive data will be shared with Microsoft or the FastTrack Ready Partner (FRP).*
    - *Refer to the Microsoft Privacy Statement for more information.*
- Organisation will follow the Device naming conventions as published in the NHSmail Intune Operations Guide.

Windows Autopilot

IT admins are responsible for registering their devices to their organisation by either having the hardware vendor upload their hardware IDs on their behalf or by uploading it themselves into the Windows Autopilot service. Please refer to this article on Autopilot for more provisioning information.

Cloud-attach

FastTrack Guidance Details

FastTrack provides remote guidance to customers to cloud-attach existing Configuration Manager environments with Intune. This includes:

- Configuring supported workloads to switch to Intune.
- Installing the Configuration Manager client on Intune-enrolled devices.

Source Environment Expectations

- Must have existing System Center Configuration Manager (SCCM) client (on prem).
- Must have access to Microsoft Intune at the Organisation level, see article on the Hybrid track. *Organisation Local Administrator will need to register using the Intune Registration Form.*

The following is out of scope:

- Changing any policies managed at the Organisation level; these settings are established by the Tenant Administrators and are not editable or accessible by the Organisation.
- Providing guidance setting up Microsoft Entra ID hybrid join.
- Providing guidance on setting up Microsoft Entra ID for MDM auto-enrollment. **Requires* Organisation *Local Admin to raise Service Request.*
- Organisation should refer to Hybrid Track – NHSmail Support for more direction on hybrid join prerequisites.

Organisation responsibilities include:

- Organisation Admin to submit Service Requests as needed to gain access to Intune as prescribed by the Intune Onboarding Process NHSmail Intune Service | Overview – NHSmail Support.
- Organisation Admin to submit Service Requests as needed to enable Cloud-based policies (managed at the Tenant level).

Microsoft Teams (Including Teams Phone and Teams Rooms)

FastTrack Guidance Details

Microsoft Teams core (including chat, collaboration, and meetings) FastTrack provides remote guidance for:

- Teams prerequisites:
    - Identities enabled in Microsoft Entra ID for Microsoft 365.

    - Exchange mailboxes are present (online and on-premises in an Exchange hybrid configuration).
    - Users are enabled for SharePoint Online and OneDrive.
    - Microsoft 365 Groups are enabled.
- Network readiness:
    - Network port and enablement checks
    - Domain Name System (DNS) settings
    - Proxy settings
    - Connection quality checks
    - Bandwidth checks
- Security and compliance readiness:
    - Develop governance and compliance policies including hardware security and account security, like multi-factor authentication (MFA) guidance and password policies.
- Teams chat and collaboration:
    - Teams basics
    - Managing and Organising Teams
    - Presence
    - Messaging policies
    - Channels (standard, shared, and private).
- Teams meetings and Audio Conferencing:
    - Meeting settings and policies
    - Service number acquisition
    - Guidance for conference bridge settings
    - Assignment of dial-in numbers to meeting organisers.
- Enabling Teams live events and webinars:
    - Organisation setup of live events and webinar policies.

Microsoft Teams Rooms

FastTrack provides remote guidance for:

- Network, security, and compliance readiness:
    - Validation of network, security, and compliance readiness requirements for Teams Rooms.
- Resource accounts:
    - Creation and configuration of resource accounts needed for supported Teams Rooms devices including license assignment and mailbox configuration – details how to create resource mailbox in the central tenant are covered in this article: Resource mailboxes – NHSmail Support
- Device setup:
    - Guidance on the out-of-box experience of a new Teams Rooms device.
- Device management:
    - Device management, including Teams admin center, Microsoft Intune, and Teams Rooms Pro Management service.

- Certified devices:
    - Guidance on using the Teams Device Catalog to find and purchase certified devices.

Microsoft Teams Phone

FastTrack provides remote guidance for:

- Network, security, and compliance readiness:
    - Validation of network, security, and compliance readiness requirements for Teams Phone.
- Operator Connect:
    - Enabling Operator Connect
    - Emergency addresses
    - Assigning numbers - Inventory Type Change for Numbers
- Teams Phone Mobile:
    - Teams Phone Mobile license acquisition and assignment
    - Enabling a mobile operator
    - Assigning numbers, guidance on how to assign/change numbers is provided here: Inventory Type Change for Numbers
- Calling Plans:
    - Local number porting guidance for the central tenant is available in the following article: Onboarding (Calling Plans) – NHSmail Support
    - License assignment, license requirements for NHSMail Teams Phone System in this article: Licensing for NHSmail Teams Phone System
    - Phone number acquisition and assignment, guidance on how to acquire and assign numbers for the central tenant in this article: Inventory Type Change for Numbers
- Direct Routing:
    - Guidance on Direct Routing, onboarding guidance for the central tenant in this article: Onboarding (Direct Routing) – NHSmail Support
    - Session Border Controller (SBC) configurations and connectivity, details and guidance on how to configure SBCs for the central tenant in this article: Configure Session Border Controllers (SBCs) | Direct Routing – NHSmail Support
    - Call routing policies, call routing configuration guidance for the central tenant in this article: Voice Routing and Voice Routes (Direct Routing)
    - Media bypass and local media optimisation, media bypass and local media optimisation guidance for the central tenant in this article: Connectivity and Optimisation
    - Assigning numbers guidance on how to assign/change numbers in this article: Inventory Type Change for Numbers

The following is out of scope:

- A/V and conference rooms design and installation.
- Device procurement.

- Third-party integrations (like Cloud Video Interop (CVI)).
- Carrier Session Initiation Protocol (SIP) trunk configuration.
- Session Border Controller (SBC) trunking to carrier or legacy Private Branch Exchange (PBX).
- Troubleshooting existing deployments.
- End user training.
- Hands-on keyboard support.
- Production of live events or webinars.

Organisation responsibilities include:

If implementing Teams Rooms, Organisation may need to purchase additional licenses.

Windows Client OS Deployment

Windows 11

FastTrack Guidance Details

We provide guidance for updating to Windows 11 Enterprise from Windows 7 Professional, Windows 8.1 Professional, and Windows 10 Enterprise. **Note:** PCs must meet these system requirements.

We provide remote guidance for: • Planning for

your Windows 11 deployment.

- Assessing your source environment and the requirements (ensure that Microsoft Endpoint Configuration Manager {SCCM} is upgraded to the required level to support the Windows 11 deployment).
- Deploying Windows 11 Enterprise and Microsoft 365 Apps using Microsoft Intune or Configuration Manager.
- Recommending options for you to assess your Windows 11 app and driver readiness.
- Microsoft 365 Apps compatibility assessment by leveraging the Office 365 readiness dashboard in Configuration Manager or with the stand-alone Readiness Toolkit for Office plus assistance deploying Microsoft 365 Apps.
- Creating a remediation checklist on what you need to do to bring your source environment up to the minimum requirements for a successful deployment.
- Providing update guidance for Windows 11 Enterprise devices that meet Windows 11 system requirements.
- Providing update guidance for in-place updates from Windows 10 to Windows 11 using Windows Update for Business and guidance for Windows 11 servicing using Windows Update for Business and Intune.
- Providing guidance for new Windows 11 device deployment using Windows Autopilot.

- Providing guidance using Endpoint analytics and Windows Update for Business reports to see eligible devices and monitor device deployments.
- Providing guidance for enabling co-management and moving the update workload to Intune.
- Providing guidance for using Windows Update for Business with Configuration Manager.
- Providing guidance to help your organisation stay up to date with Windows 11 Enterprise and Microsoft 365 Apps.

BitLocker

We provide remote guidance for:

- Assessing your Windows 11 environment and hardware for BitLocker configuration.
- Recommending best practices for configuring BitLocker policies from Microsoft Endpoint Manager.
- Enabling compliance reporting of BitLocker from Microsoft Endpoint Manager and Microsoft Endpoint Configuration Manager.
- Providing guidance on configuring BitLocker for Windows Autopilot scenarios.
- Providing guidance on BitLocker key recovery best practices.

Windows Hello for Business

We provide remote guidance for:

- Assessing your Windows 10/11 environment and hardware for Windows Hello for Business configuration.
- Enabling Windows passwordless authentication using Windows Hello for Business cloud trust.
- Planning guidance for Windows Hello for Business hybrid key or certificate trust.

Windows Autopatch

We provide remote guidance for:

- Helping you understand the features of the Windows Autopatch service, validating environment prerequisites, and how the service relates to other Microsoft update tools.
- Assessing your readiness for Windows Autopatch onboarding using the Readiness Assessment tool and addressing issues identified by the tool.
- Understanding the process to enroll into the Windows Autopatch service.
- Registering physical and virtual devices into the Windows Autopatch service.
- Validating device updates and understanding reports.

<u>Source Environment Expectations</u>

For PC update, you must meet these requirements: •

Source OS: Windows 10 Enterprise or Professional.

- Devices: Desktop, notebook, or tablet form factor.

- Target OS: Window 11 Enterprise.

For infrastructure upgrade, you must meet these requirements:

- Microsoft Endpoint Configuration Manager.
- The Configuration Manager version must be supported by the Windows 11 target version and Configuration Manager must be cloud-attached. For more information, see the Configuration Manager support table.

The following is out of scope:

- Upgrading Configuration Manager to Current Branch.
- Creating custom images for Windows 11 deployment. Creating and supporting deployment scripts for Windows 11 deployment.
- Converting a Windows 11 system from BIOS to Unified Extensible Firmware Interface (UEFI).
- Enabling Windows 11 security features.
- Configuring Windows Deployment Services (WDS) for Preboot Execution Environment (PXE) booting.
- Using the Microsoft Deployment Toolkit (MDT) to capture and deploy Windows 11 images.
- Using the User State Migration Tool (USMT).

Organisation responsibilities include:

Nothing unique identified at this time.

Windows 365

FastTrack provides remote guidance for onboarding to Windows 365 Enterprise, Windows 365 Frontline, and Windows 365 Government. Windows 365 takes the operating system to the Microsoft Cloud, securely streaming the full Windows experience—including all your apps, data, and settings—to your personal or corporate devices. Organizations can provision Cloud PCs (devices that are deployed on the Windows 365 service) instantly across the globe and manage them seamlessly alongside your physical PC estate using Microsoft Endpoint Manager. This desktop-as-a-service (DaaS) solution combines the benefits of desktop cloud hosting with the simplicity, security, and insights of Microsoft 365.

We provide remote guidance for:

- Assigning licenses to users.
    - The assignment and licensing policy is handled by NHS Administration, where the Organisation would be responsible for managing that request
- Utilising Provided Gallery Images
- Editing of preconfigured provisioning policies

Note Creation and deletion of policies not supported on central tenant.

- Deploying Windows Update policies for Cloud PCs using Intune.
    - Autopatch, Update Rings and WUfB supported
- Deploying apps (including Microsoft 365 Apps for enterprise and Microsoft Teams with media optimizations) to Cloud PCs using Intune.
- Securing Cloud PCs, including multifactor authentication (MFA), and managing Remote Desktop Protocol (RDP) device redirections.
- Managing Cloud PCs on Microsoft Endpoint Manager, including remote actions, resizing, and other administrative tasks.
- Optimizing end user experience.
- Finding other support for Windows 365

Source Environment Expectations

- Windows 365 licensing requirements must be met.
    - Note, as of March 2025, NHS Trusts must purchase additional licensing
- Within the NHS Tenant only MS Hosted is supported at this time

The following is out of scope:

- Creation of Azure subscription features including Azure Virtual Networks (VNets), ExpressRoute, and Site-to-Site (S2S) VPN.
- Support for advanced networking topics.
- Customizing images for a Cloud PC on behalf of customers.
- Standalone use of Configuration Manager for managing Cloud PCs.
- Deploying Windows updates for Cloud PCs using Configuration Manager.
- Migrating virtual desktop infrastructure (VDI) or Azure Virtual Desktop virtual machines to Windows 365.
- Migrating Configuration Manager or Microsoft Deployment Toolkit (MDT) images to Azure.
- Migrating user profiles to or from Windows PCs.
- Configuring network appliances on behalf of customers.
- Programmatic actions against Microsoft Graph API.
- Support for third-party integrations.
- Support for Windows 365 Business.

Organisation responsibilities include:

- Intune administrator (to ensure license applied, pre-requisites, etc.)
- If applicable, Azure knowledge
- Please see source expectations