NHSmail roadmap

Roadmap for digital collaboration services across health and social care

Presented by:
NHSmail team

Live on NHSmail service

- ✓ Active Directory Bi-directional Sync / TANSync
- ✓ Address Book Sync
- ✓ All user's security group
- ✓ Authorisation User Portal Management
- ✓ Bring Your Own Device (BYOD)
- ✓ Calendar Federation
- ✓ Changed Settings Reporting
- ✓ Centre of Excellence
- ✓ CIS Identity Matching
- ✓ CIS2 / NHS.net identity mapping
- ✓ Clinical Safety
- ✓ Compromised Accounts Detection
- ✓ Conditional Access for MFA
- ✓ Data protection Impact Assessment (DPIA)
- ✓ ESR Integration JML
- ✓ Federation Ecosystem Active Directory Bi-directional Sync
- ✓ Federation Ecosystem Third Party SSO
- ✓ Federation Ecosystem ESR Integration
- ✓ Governance Portal Administration
- ✓ ICB Identity Patterns
- ✓ Identity Patterns
- ✓ Identity Protection – (IDP)
- ✓ Local AD Integration
- ✓ M365 Licensing
- ✓ Microsoft Defender for Endpoint
- ✓ Microsoft SharePoint team store, app store & add ins
- ✓ Mobile Application Management (MAM)
- ✓ Mobile services (iOS, Android, iPad OS)
- ✓ Modern Authentication for Basic Auth (POP,IMAP and EWS)
- ✓ Multi-factor Authentication & FIDO2
- ✓ Native Self-Service Password Reset
- ✓ NHSmail Admin Portal
- ✓ O365 Company Communicator
- ✓ O365 Privacy alerts / Safety Net
- ✓ O365 Security Groups
- ✓ Onboarding & Offboarding Tooling Guide
- ✓ One Drive Delegate Access
- ✓ Password Synchronisation / Same Sign On
- ✓ Phishing Remediation
- ✓ Phone System Direct Routing/ Calling Plans
- ✓ Power BI New Workspace
- ✓ Power Platform
- ✓ Project for the Web / Visio Lite
- ✓ PST Ingestion Service
- ✓ Risky Login, and Risky Sign-in Monitoring and alerting
- ✓ Relay Service
- ✓ Safe Links /Safe Attachments (Exchange)
- ✓ Secure Email (DCB1596)
- ✓ Sensitivity Labels
- ✓ Single Sign On
- ✓ Virtual Visits
- ✓ Windows 10/HoloLens2 (AAD join)

To find out more please visit a feature on NHSmail support site
Owing to information security concerns, certain features are not made public..

NHSmail Strategy Timeline

Jan-Mar Q1
Apr-Jun Q2
Jul-Sep Q3
Oct-Dec Q4

Q3 / Q4, 2023

- Microsoft Teams Shared Channels
- MDO >> Teams Protect
- MDO >> Spoofing intelligence
- MDO >> Impersonation intelligence
- MDO >> SafeLink's Safe attachments on Teams and Office
- Mailbox/SharePoint/OneDrive Capacity uplifts
- Blocked filetypes
- Adaptive scopes
- Sub domain branding within NHS.net
- Actionable Emails
- AFE device-based licenses
- eDiscovery (premium)
- Audit (premium)
- Safe Documents

Q1, 2024

- Licence renewal changes and uplifts
- Centralised MDI Microsoft Defender for Identity
- External Authentication method
- Advanced Security Reports
- Rules-based automatic retention policies
- Machine Learning-based retention
- Teams message retention policy
- Revised JML processes
- Application secret and certificate renewal services
- Risk Based CA policies
- Admin units (enable native console access – Exact capabilities TBC)
- Native Intune and MDE integrations
- Account Secret
- Office 365 Cloud Apps Security
- Defender for Cloud apps

Q2, 2024

- localised MDI Microsoft Defender for Identity
- Windows 365/ Windows 11 & Microsoft Managed desktop
- Intune Device migration capabilities
- Data Loss Prevention (DLP) for emails and Files
- DLP for Teams chat
- Endpoint DLP
- Authentication only account
- Alternative Data Loss Prevention (DLP) policies
- Viva Connections – Local organisation deployment
- Individual single seat licence allocation
- Office 365 enhanced backups/retention capabilities review
- Advanced Message Encryption
- Customer Key
- Attack simulation

Long Term Strategies

- Automatic sensitivity labelling in Office 365 apps (**Q3, 2024)**
- Automatic sensitivity labels in Exchange, SharePoint, and OneDrive (**Q3, 2024**)
- Automatic labelling in the AIP plugin (**Q3, 2024**)
- Sensitivity labels based on advanced classification (ML, EDM) (**Q3, 2024**)
- Communication Compliance (**Q4, 2024**)
- Records Management (**Q1, 2025**)
- Phone system – Operator Connect (**TBC**)
- Government roam and Wi-Fi (**TBC**)
- Enhanced local backup capability (**TBC**)
- Microsoft Purview Insider Risk Management (**Q4, 2024**)
- Information Barriers (**Q4, 2024**)
- Customer Lockbox (**Q4, 2024**)
- Privileged Access Management (**TBC**)
- Microsoft 365 Copilot (TBC)
- Unattended RPA (TBC)

NHSmail Identity & Security Capability Roadmap

Jan-Mar Q1
Apr-Jun Q2
Jul-Sep Q3
Oct-Dec Q4

Q3 / Q4, 2023

- MDO >> Teams Protect
- MDO >> Spoofing intelligence
- MDO >> Impersonation intelligence
- MDO >> SafeLink's Safe attachments on Teams and Office
- Blocked filetypes
- Microsoft Advanced Threat Analytics (F5 S&C)
- Safe Documents (F5 S&C)

Q1, 2024

- Centralised MDI Microsoft Defender for Identity (F5 S&C)
- External Authentication methods
- Advanced Security Reports (F5 S&C)
- Revised JML processes
- Application secret and certificate renewal services
- Risk Based CA policies (F5 S&C)
- Cross Tenant Sync
- Account Secret
- Office 365 Cloud Apps Security (F5 S&C)
- Defender for Cloud apps (F5 S&C)

Q2, 2024

- localised MDI Microsoft Defender for Identity Data Loss Prevention (DLP) for emails and Files (F5 S&C)
- DLP for Teams chat (F5 S&C)
- Endpoint DLP (F5 S&C)
- Authentication only account
- Alternative Data Loss Prevention (DLP) policies (F5 S&C)
- Advanced Message Encryption (F5 S&C)
- Customer Key (F5 S&C)
- Attack simulation (F5 S&C)

Q3 / Q4, 2024

Automatic labelling in the AIP plugin (F5 S&C)

Sensitivity labels based on advanced classification (ML, EDM) (F5 S&C)

Communication Compliance (F5 S&C)

- Access Reviews (F5 S&C)
- Entitlement Management (F5 S&C)
- Microsoft Purview Insider Risk Management (F5 S&C)
- Information Barriers (F5 S&C)
- Customer Lockbox (F5 S&C)

Long-term

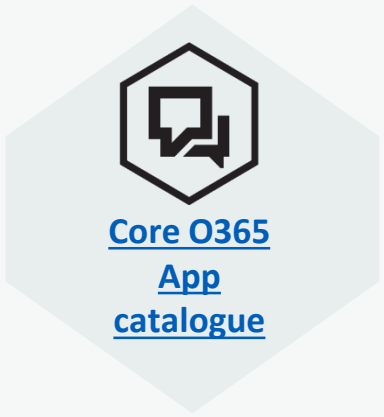
- Privileged Access Management (TBC)

NHSmail Application Guidance

Request an application assessment

This guidance provides detailed information about the process involved in Requesting:

- a SharePoint app from the SharePoint Store to be added
- custom/third-party app
- new Teams app to be added to the Teams App Store
- new Office 365 Store App (Add-ins from App Source)
- new Global Term Group
- requesting to manage the Terms in the Group



Core O365 App catalogue

This guidance outlines all the core 365 (SharePoint, App Source add-ins, Teams) applications approved for the NHSmail platform.
These applications have passed a hurdle assessment conducted by the Technical Design Authority (TDA).

Custom & 3rd party apps

This article outlines the third party and custom applications which are available with the NHSmail Azure AD / Office 365.

Rejected Applications

This article provides a view of all application requests that have been rejected by the NHSmail Technical Design Authority (TDA). A justification will be provided as to the rationale behind the decision.

Intune Enhancements Roadmap 2023-24

High Level Overview

Q3-23

- Windows Autopatch
- Sync Engine Multiple OU (front end)[1]
- Managed Home Screen[2]
- PatchMyPC (PoC)
- Android (FOTA) Deployments[3]

Q4-23

- MacOS Deployments
- Android Devices Renaming
- Baseline App Protection Policies
- Baseline Device Compliance Policies
- MDE Mobile Tagging
- Windows Hello for Business Kerberos trust PoC
- BYOD Simplification

Q1-24

- Android Work Profiles
- 3rd Party App Patching[4]
- Quest Migrations Pilot
- AAD Cloud Connect assessment
- Windows 365 Pilot

Q2-24

- RBAC Endpoint Security UI
- Scoped[4] Windows Autopatch
- Windows 11 Baseline
- Central App Store[4]

(1) Hybrid Enhancement
(2) Private Preview
(3) Requires Intune Suite 2 or Add-on
(4) Further evaluation in progress

Completed

Proposed / Not yet confirmed

accenture | NHS

Phone System Development Per Quarter

High Level Overview

Q3-23

- Upload and update the audio files for Call Queues
- Correction of ODS tagging for PSTNCallRecords
- ODS code & Primary Org name – fetch from Portal
- Increase PowerApp Admin Licence Limit to 10*
- Remove custom policies when user removed
- Call Queue Special character check.
- Support for M365 E5 licence*

Q4-23

- Acceptable file format hint text under call queue attachments.
- Fix for custom policies being removed when utilizing bundle licences
- High-detail error logging across all functions
- Improved process for managing Excel files under number upload process.
- Handling duplicate queue messages from Portal
- Support ticket creation when converting numbers from Auto Attendant to Call Queue and vice versa.
- Fix to embedded URL
- Enhanced on-screen guidance for releasing numbers and licencing resource accounts
- Contrast ratios, tab indexes and focused border added to controls to improve accessibility

Phone System Development Per Quarter

High Level Overview

Q1-24

- Number format hint text to be added
- Upgrade PowerShell Module
- Fix for policy name changes in Portal and resulting duplicate entries
- VN170 – licencing resource account
- Enhanced Accessibility

TBC

- Changes to Call Queue - additional option been added by Microsoft (exception handling)
- Ability to prevent Org. consuming minutes when exceeded allowance
- Bulk unassignment of numbers
- Internal notification of 80%/100% usage orgs
- Common Area Phones
- Enhanced Reporting
- Teams 1:1 Meeting Call Recording for Phone System disabled based user policies *
- Portal API output limit 500 for Groups*

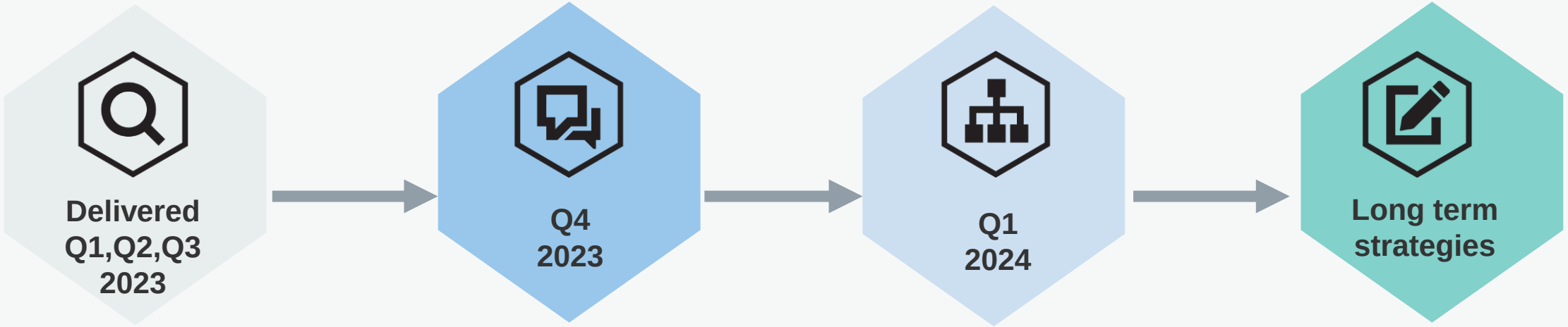
accenture | NHS

* Pending Portal Release/Prioritisation

✓ Completed

MDE Timeline

Jan-Mar Q1
Apr-Jun Q2
Jul-Sep Q3
Oct-Dec Q4



- ✓ Indicator pool
- ✓ MDE test environment
- ✓ MS Monitoring Agent (MMA) Update
- ✓ MS Server & Linux scoping
- ✓ Local M365D Tenant Monitoring MVP
- ✓ MacOS scoping
- ✓ Device Discovery Pilot
- ✓ Mobile IOS/Android scoping
- ✓ MDVM Premium Trial

- ✓ Deliver Device Discovery Auto-Tagging phased rollout
- ✓ Attack Surface Reduction (ASR) Configuration
- ✓ Unified RBAC Permission Model
- ✓ SIEM Integration Pilot
- ✓ Basic Live Response Pilot

- ✓ Local M365D Tenant Monitoring Maturity
- ✓ Enhanced Tamper Protection
- ✓ Unified agent adoption
- ✓ MDAV best practice and configuration guidance

- ✓ MDE Tenant Attach
- ✓ Enhanced Network Discovery
- ✓ API migration to Graph
- ✓ SIEM Integration Service
- ✓ Device Discovery Endpoint onboarding
- ✓ MDI RBAC Unified scoping
- ✓ MDO RBAC Unified scoping
- ✓ NHS Central Shared Tenant MDE & MEM / InTune integration
- ✓ EDR in Block Mode
- ✓ MDE Indicator Pool enhancement
- ✓ MDE enhanced Standard Device Discovery
- ✓ SIEM Integration full rollout
- ✓ MDE Enhanced Device Isolation
- ✓ MDE Device Containment

Improving Resilience | Improving Visibility | Enhancement | Customer Integration

Nationally available, locally funded

MDE Features (Q4) 2023 Overview

Basic Live Response Pilot

Enhanced diagnostic and response tools for local organisations.
Benefits include additional advanced threat hunting and incidence response capabilities.

1

SIEM integration for NHS organisations

Ability to ingest MDE information into local SIEMs for all organisations.
Benefits include better local analysis of MDE information and correlation to local sources.

2

Device Discovery Auto – Tagging Phased Rollout

Provides local NHS organisation with visibility for newly MDE discovered assets to be presented alongside existing onboarded assets in the MDE Device Inventory.

3

Attack Surface Reduction (ASR) Configuration

Knowledge campaign that is aimed at NHS estates who use Microsoft Defender Antivirus as the primary active AV to help further harden the IT estate from cyber intrusion.

4

Unified RBAC Permission Model

Granular access providing foundation across M365D family components.
Benefits include the improved targeting of security permissions and opportunity to provide access to additional capabilities.

5

Improving Resilience | Improving Visibility | Enhancement | Customer Integration

MDE Features (Q1) 2024 Overview

Enhanced Tamper Protection

Protect Microsoft Defender Anti-Virus (MDAV) configuration from bad actors.
Benefits include the prevention of bad actors disabling MDAV or changing configuration.

MDE Universal Agent UA Adoption

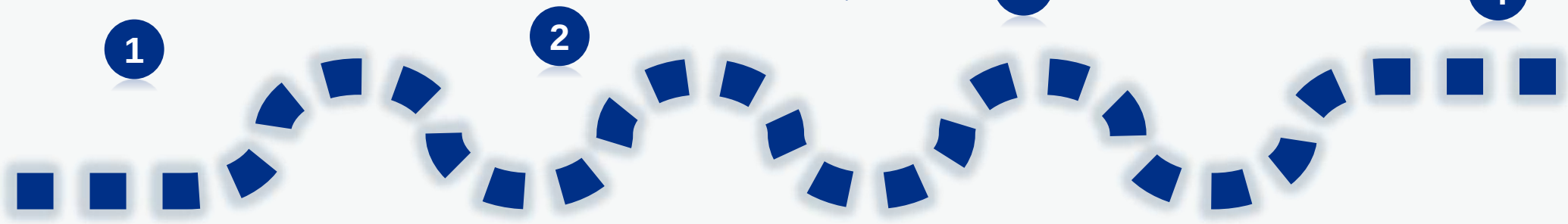
Replaces the need to use MMA for certain Windows Server OS versions and provides an expanded feature set for Server 2012 R2 and 2016 on MDE.

MDAV Best Practice and Configuration

Information campaign to support Microsoft Defender for Endpoint enabled estates with the use and uptake of Microsoft Defender Antivirus based on Microsoft best practice. .

Local M365D Tenant Monitoring Maturity

Enhanced cyber monitoring for local NHS tenants.



Improving Resilience | Improving Visibility | Enhancement | Customer Integration

NHSmail Deprecation Roadmap

Delivered

Basic Auth in Exchange Online
Microsoft turned off Basic Auth for the following protocols: POP,IMAP,EWS,MAPI,RPC,OA,EAS, RPS (Remote PowerShell)

Microsoft Office 2013
Office 2013 ended extended support on April 11, 2023.

Team Phone System for GPs
Teams Phone System for outbound calls is reserved specifically for GP practices. Decommissioned by Primary Care.

Microsoft Office Products
End of support for: Office Professional 2013, Visio Professional 2013, Project Professional 2013

Microsoft Teams Rooms Licensing Policy Enforcement. These should be properly licensed by 30 September 2023.

End of Support for Cortana on Microsoft Teams Room on Windows and Teams Displays (Lenovo ThinkSmart View) - Come end of September 2023, we will no longer support Cortana voice assistance, both push-to-talk capability and wakeword detection, on all MTR-W devices and Teams Displays, specifically Lenovo ThinkSmart View.

Reminder: Windows 11, version 21H2 end of servicing (Home & Pro) From 10 October 2023, devices running this version will no longer receive monthly security and preview updates.

Microsoft Office 2016 & 2019
Connection to M365 is no longer be supported from October 10, 2023. Office versions will still be able to connect but end users may experience performance or reliability issues.

In progress

Stream
Microsoft will be retiring Stream (Classic) and moving to Stream (on SharePoint). Expected: **February 2024**

Classic Teams users to be updated to new Teams after 31 March 2024 - From 31 March 2024, Microsoft will be deprecating classic Teams and users will be moved to the new version of Teams. Further information is available following a recent announcement by Microsoft.

Yammer
Microsoft will soon be moving Yammer to Native mode from legacy version. In Native Mode, all Yammer users are in Azure AD, all groups are Microsoft 365 groups, and all files are stored in SharePoint Online **Expected: April 2024**

Stream (Classic) Sets Retirement Date of April 15, 2024, Microsoft will retire Stream (Classic) on April 15, 2024. Additionally, end users will be blocked from uploading new videos to Stream (Classic) on September 15, 2023. Also end user will not be able to access Stream (Classic) at all after October 15, 2023, unless you delay this changes by using the new migration settings in Stream (Classic) admin centre.

Windows Server 2008/R2 - You will receive an extra year of ESUs if you utilise Windows Server 2008/R2 on Azure; these will expire on January 9, 2024. Windows Server 2008/R2 will no longer receive security updates or support. Customers are left with little choice except to update to the newest version.

Outlook REST API v.2.0 and beta endpoints – Every call to Outlook REST v2.0 after March 31, 2024 will result in (Not found error) Please consider switching to Microsoft Graph. This change will have no effect on Outlook add-ins that use Outlook REST.

Windows Mail and Calendar are becoming Outlook - The new Outlook for Windows helps people be more productive and in control of their inbox: Expected: end of 2024

Long-term

TLS 1.0 and TLS 1.1 will be disabled in future Windows OSEs. Transport Layer Security (TLS) is the most common internet protocol for setting up an encrypted channel of communication between a client and server **Expected: TBC**

Windows Microsoft Monitoring Agent (MMA)
Azure will no longer accept connections from older versions of the Windows Log Analytics agent, also known as MMA that uses an older method for certificate handling. The affected versions are Windows 7 SP1, Windows 8.1, Windows Server 2008 R2 and Windows Server 2012 R2/2016. The new minimum supported MMA version is 10.20.18053.0
MMA is due to be fully retired by Microsoft ETA: 31st August 2024.

EWS in Exchange Online – from **1 October 2026** there will be a block placed for EWS requests from non-Microsoft apps to Exchange Online. This also applies to EWS SDKs for Java and .net. We recommend transferring to Microsoft Graph. There are no changes to EWS in Exchange Server, there do not affect Outlook for win or Mac, Teams or any other Microsoft product.

Thank You

@nhsengland

company/nhsengland

england.nhs.uk