NHSmail Portal Release Note

Version: 1.1

Release Date: w/c 27/02/2023

Release Name: Dickson

Connect. Communicate. Collaborate.

Document Version Control

Document Information

File Name:	NHSmail Portal Release Notes – Dickson
Author(s):	Lewis O'Nions, Shail Kumari
Version:	1.1

Document Revision History

Version	Date	Changed By	Change
1.0	10/02/2023	Shail Kumari	Created release note for Dickson
1.1	15/02/2023	Lewis O'Nions	Release note updates

Document Distribution

Name	Role	Date	Status
Chris Coveyduck	Accenture Enterprise Technical Architect	w/c 27/02/2023	
Judith Revels	Accenture Service Lead	w/c 27/02/2023	
David Middleton	NHS England Service Lead	w/c 27/02/2023	
Matt Brownhill	NHS England Senior Technical Architect	w/c 27/02/2023	
Mark Ward	NHS England Technical Architect	w/c 27/02/2023	
Chris Parsons	NHS England Programme Manager	w/c 27/02/2023	
John McGhie	NHS England Service Delivery Owner, Operations Group	w/c 27/02/2023	
Mike Fisher	NHS England Senior Project Manager	w/c 27/02/2023	
Cell Six	NHS England	w/c 27/02/2023	

1 Release

1.1 Objectives of the Document

The objective of this release note is to detail the contents of the Dickson portal release.

This document lists the new features and bug fixes that shall be deployed w/c 27/02/2023, alongside any known errors found during testing.

1.2 Objectives of the Release

The objective of Dickson is to deploy into Production an updated set of changes to the Portal application that have been completed by the development team. A release can contain:

- New features (**P**roduct **B**acklog **I**tems aka PBI's)
- Defect resolutions (aka Bug Fixes)

1.3 Release Content

The content of this release are as follows:

1.3.1 Product Backlog Items

1.3.1.1 Portal Application Functionality

ID	Title
47507	Update Guest Inviter role and workflow within Portal
59614	New MFA Status Report - to include MFA Status & Compromised Account related details
67686	B2B Approver & Invite Guest Users Roles Permissions Update
68768	New MFA Status values
69039	Removal of MFA Authentication Type from the Mailbox Report
70222	MAC Email Notification Logic - PLAs/LAs at Parent organisations
70928	Updating Marked as Compromised email notification
48742	Auto-mapper needs to enabled for additional mailboxes where the user has access to
56119	Add dial-out capacity per User Policy
56210	Add dial-out capability for an organisation
58913	My Approval Requests page refactoring
59615	MFA - Add banner to User Details pages for user accounts that are marked as Compromised
59893	When renaming a distribution list, do a check in the DB and AD/Exchange on update to ensure the proxy address does not already exist on the platform
61001	My Profile Page - Update Support Site link

64186	SharePoint PnP module - Update to code to replace the Credential object with App and Certificate details
66372	Dial-Out Capability - Addition of ability to dial out nationally (Policy & Org Level)
66770	Update to Tooltips for Auto-Expanding Archive Feature (User Management & Organisation Level)
68933	New Account Hygiene Columns
69169	Update Portal Carousel to include 'NHS Care Identity (Smartcard) Sign in' Slide as fifth slide
70782	Update Portal Carousel to include 'NHSmail account – use it or lose it' Slide as first slide
67874	'Accessibility Issue' (Accessibility Scan): Elements with role=listbox must contain or own an element with role=option
68199	'Accessibility Issue' (Accessibility Scan): The visual label must appear in the accessible name of links and controls
68202	'Standards Issue' (Accessibility Scan): CSS Validation Error
68229	'Standards Issue' (Accessibility Scan): Invalid CSS color value
68230	'Standards Issue' (Accessibility Scan): Too many values for CSS property
67685	ATP_Approver & ATP_Local_Admin Permissions Update
63015	VN137 - Create a portal API to disable MFA when CA is enabled

1.3.2 Bug Fixes

1.3.2.1 Portal Application

ID	Title
53675	Teams are intermittently being created without the ResourceProvisioningOptions property set, this can lead to the team's status sync hangfire job updating their status to deleted in the DB
71975	CSV Bulk Update Accounts Failing - Password Validation
49230	PODS - If attempt to register with a care provider site that is already registered for NHSmail, error message should be displayed always
52221	Sponsor 2 receives the 'Action required – Azure B2B Request has been raised' email separately for external organisation access requests
59894	Static DL's get stuck in pending once approved if they encounter any error during the approval
68681	Teams Locale Hangfire Job code refactor
71105	RemoveMailTipForActiveUsers Hangfire job improvements

2 Initial Proposed Release Functionality

2.1 High-level Functionality

The following section provides details of the initial proposed release functionality that is being delivered as part of the Dickson release.

2.1.1 Product Backlog Items

2.1.1.1 Portal Application Functionality

- **47507- Update Guest Inviter role and workflow within Portal**

  As part of this PBI, the "Invite Guest Users" role is updated to only be able to view the requests associated to the Organisation in which the user has Invite Guest Users roles access as mentioned below:

  - When a user has a Global Admin and (B2B Approver & Invite Guest Users) role the admin will have the ability to perform the following actions: View/Add/Re-Invite/Restore/Delete for all guest users across the platform.
  - When a user is a Local Admin of Organisation A and (B2B Approver & Invite Guest Users) of Organisation B they will have the ability to perform the following actions for Organisation B only: View/Add/Re-Invite/Restore/Delete for all guest users under Organisation B.
  - When user has B2B Approver & Invite Guest Users role at Organisation A they will have the ability to perform the following actions for Organisation A only: View/Add/Re-Invite/Restore/Delete for all guest users under Organisation A.

- **59614- New MFA Status Report - to include MFA Status & Compromised Account related details**

  This PBI implements a new admin report called ***'MFA Status Report'*** which is presented under Reports tab within NHSmail Portal.

  This report will provide the following details related to a user's MFA status on the NHSmail platform: MFA status, MFA authentication type, the user's compromised status, alongside metadata of when a user was compromised, remediated, who it was compromised by, who it was remediated by and the overall compromised tally per user.

  Please note, the compromised and remediated data will only be present if a user has ever been marked as compromised or remediated.

- **67686- B2B Approver & Invite Guest Users Roles Permissions Update**

  As part of this PBI, B2B Approver & Invite Guest Users has been updated to only be able to view the requests associated to the Organisation in which the user has B2B Approver & Invite Guest Users access too. This feature change is focusing on the B2B admin section, alongside the B2B "My Approvals" requests.

  - When a user has B2B Approver & Invite Guest Users roles at Organisation A, they will only be able to view "External Organisations" and "External Federated Groups" associated with Organisation A.
  - When a user has B2B Approver & Invite Guest Users roles at Organisation A, they will be able to view the B2B related approval requests associated with Organisation A via the "My Approvals" page.

- **68768- New MFA Status values**

  As part of this PBI, new MFA status values has been introduced into NHSmail to define how MFA (Multi-Factor Authentication) was either granted or remove from a user account. The following scenarios highlight how MFA has either been granted or removed:

  - **User Enabled** - when a user enables MFA via the Self-Enrol flow
  - **User Disabled** - when a user disables MFA via the Self-Enrol flow

- **Admin Enabled** - when an admin enables MFA via User Management
- **Admin Disabled** - when an admin disables MFA via User Management
- **MFA Enforced ATP Group** - for a user that is added to an ATP Role (this act enables MFA for this user) - This applies for when granted ATP Approver through the DL and also when added to a ATP group.
- **MFA Disabled ATP Group** - for a user that is removed from an ATP Role (this acts as disabling MFA for this user) - This applies when you have ATP Approver role removed from your account and/or when removed from ATP group.
- **MFA Enforced Admin Role** - for a user that is given an admin role (Local Admin, Primary Local Admin, Global Admin, Global Helpdesk etc)
- **MFA Disabled Admin Role** - If (Local Admin, Primary Local Admin, Global Admin, Global Helpdesk etc) is removed from the user account MFA is removed.
- **MFA Enforced Compromised** - for a user whose account has been marked as compromised

These new MFA status values will be reflected in the new MFA status report.

- **69039- Removal of MFA Authentication Type from the Mailbox Report**

  As part of this PBI, MFA Authentication Type column is removed from Mailbox Report.

- **70222- Mark As Compromised Email Notification Logic - PLAs/LAs at Parent Organisations**

  As per this PBI, if a user has been marked as compromised, and the associated organisation does not have any users with Local Admin or Primary Local Admin role, the notification email will attempt to send to the Local Admin or Primary Local Admin of the associated parent organisation.

  If the associated parent organisation does not have any users with Local Admin or Primary Local Admin role, the notification email will then attempt to send to the Local Admin or Primary Local Admin of the associated grandparent organisation.

- **70928- Updating Marked as Compromised Email Notification**

  The email template content has been updated for the “Mark As Compromised” workflow which Local Admins and Primary Local Admins receive when a user under their associated organisation has been Marked As Compromised by either a Global Admin or Global Helpdesk user.

- **48742- Auto-mapper needs to enabled for additional mailboxes where the user has access to**

  This PBI auto-enables the Delegated mailboxes all users with additional mailboxes. The change will appear updates to the relevant Active Directory PowerShell cmdlets to simultaneously edit both the msExchDelegateListLink and msExchDelegateListBL attributes with the relevant delegate permissions values as these attributes are dependent on one another.

- **56119- Add dial-out capacity per User Policy**

  As part of this PBI, we have introduced the dial-out functionality as part of the Dial-in Add-on licence. The dial-out capability will give users the ability to dial-out internationally from Microsoft Teams. By default, all User Policies with a dial-in add-on licence will be set to dial-out national as per Microsoft's default setting.

- **56210- Add dial-out capability for an organisation**

  This PBI will introduce the capability of switching the dial-out international toggle ON for all User Policies with a dial-in add-on licence under your Organisation. This setting will be available on your organisation settings page. By default, the international toggle will be switched OFF.

- **58913- My Approval Requests page refactoring**

  The development of this PBI is to improve the performance of the "My Approvals" page under the admin tab. This page will automatically load 0 results, but the following guidance will be presented in order to refine the results further: "Please enter a search criteria to see results".

  If the request returns more than 500 results, a blue banner will appear stating the following: "Only the 500 most relevant results have been returned for your search. Please refine your search to return less than 500 results to see them all."

  This will require you to refine your result set further to find the required results needed.

- **59615- MFA - Add banner to User Details pages for user accounts that are marked as Compromised**

  This PBI adds a new blue information banner at the top of the User Details page for a compromised account: "This account has been marked as compromised. Please proceed with caution".

  Once a user account is remediated, the blue information banner will be removed.

- **59893- When renaming a distribution list, do a check in the DB and AD/Exchange on update to ensure the proxy address does not already exist on the platform**

  This PBI implements an error growl message when a user updates a distribution list email address where the distribution list alias already exists. This is an additional validation change to ensure the reuse of aliases is not available on the platform, alongside providing relevant information to end users of why the update failed.

- **61001- My Profile Page - Update Support Site Link**

  This PBI updates a hyperlink for "here" (within the textbox below the "Self-enrol for Azure MFA" button), on the Self-Service tab of "My Profile" page.

  https://support.nhs.net/article-categories/multi-factor-authentication-mfa/

- **64186- SharePoint PnP module - Update to code to replace the Credential object with App and Certificate details**

  This PBI updates the existing 'Connect-PnPOnline' cmdlet with 'Connect-PnPOnline -ClientId $ClientID -Url $siteURL -Tenant $tenantName -Thumbprint $Thumbprint'.

- **66372- Dial-Out Capability - Addition of ability to dial out nationally (Policy & Org Level)**

  As per this PBI, this is in addition to the dial-out changes which have been developed under 56119 and 56210. This PBI focuses on the user interface tooltip changes as well as the toggle functionality between the relationship of dial-in and dial-out.

  - If dial-in is switched OFF within the user policy, neither the dial-out nationally nor internationally will be able to be toggled ON.
  - If dial-in is switched ON, dial-out nationally will be switched ON by default with dial-out internally switched OFF.
  - If dial-in is switched ON and dial-out internationally is switched ON the dial-out nationally will also be switched ON as this is a default capability.

- **66770- Update to Tooltips for Auto-Expanding Archive Feature (User Management & Organisation Level)**

  - This PBI is to update the text tooltip displayed for the auto-expanding archive feature both at a User Detail level and Organisation level.User Details auto-expanding archive feature tooltip:
  - "Once this feature has been enabled, it can never be disabled. For further information, please read the "Data Retention and Information Policy - Office 365" article on https://support.nhs.net/knowledge-base/data-retention-and-information-management-policy-office-365/"Organisation auto-expanding archive feature tooltip:

  "Once this feature has been enabled, it can never be disabled for any of the users in your organisation. For further information, please read the "Data Retention and Information Policy - Office 365" article on https://support.nhs.net/knowledge-base/data-retention-and-information-management-policy-office-365/"

- **68933- New Account Hygiene Columns**

  This PBI adds a new table in the database "AccountLifecycle" which will be used by the service team for the new account hygiene process.

- **69169- Update Portal Carousel to include 'NHS Care Identity (Smartcard) Sign in' Slide as fifth slide**

  As part of this PBI, a new slide has been added to the carouselto include the following: "'NHS Care Identity (Smartcard) Sign". This item on the carousel will be presented in the 5th slide.

- **70782- Update Portal Carousel to include 'NHSmail account – use it or lose it' Slide as first slide**

  As part of this PBI, a new slide has been added to the carousel to include the following: "NHSmail account – use it or lose it". This item on the carousel will be presented in the 7th slide.

- **67874- 'Accessibility Issue' (Accessibility Scan): Elements with role=listbox must contain or own an element with role=option**

  As part of this PBI, the issue identified is related to the HTML role=listbox tag. This has now been replaced with the role=option value to meet accessibility standards.

- **68199- 'Accessibility Issue' (Accessibility Scan): The visual label must appear in the accessible name of links and controls**

  In this PBI the appropriate visual label has been added to accessible name of links and controls. This will ensure users who use speech control to select elements using the visual label displayed on screen.

- **68202- 'Standards Issue' (Accessibility Scan): CSS Validation Error**

  This PBI has been implemented to resolve a broken link with a CSS validation error. The appropriate CSS change has resolved this issue as part of the most recent accessibility scan.

- **68229- 'Standards Issue' (Accessibility Scan): Invalid CSS colour value**

  As part of this PBI, the invalid CSS colour values are resolved and updated to the valid values (rules for CSS colours specified as per accessibility scan tool).

- **68230- 'Standards Issue' (Accessibility Scan): Too many values for CSS property**

  This PBI implements the resolution to resolve the excess CSS property values issue flagged within the accessibility scan.

- **63015- VN137 - Create a portal API to disable MFA when CA is enabled**

  As part of this PBI, if a user is within a Conditional Access group that either disables MFA or applies MFA via a conditional access setting this will take precedence over MFA settings enabled via the Portal UI until the user is removed from the Conditional Access group.

  With regard to accounts that have been Marked As Compromised, MFA will automatically be enforced and will not be disabled if that user is added to a Conditional Access group. Only upon remediation will this account be able to have MFA removed when added to the Conditional Access group.

2.1.2 Bug Fixes

2.1.2.1 Portal Application

- **53675- Teams are intermittently being created without the ResourceProvisioningOptions property set, this can lead to the teams status sync hangfire job updating their status to deleted in the database**

As part of this bug fix, a resolution has been put in place to ensure any newly created Microsoft Teams via Portal have the Exchange ResourceProvisioningOptions property set to “Team”. This fix will prevent the Teams Status Sync hangfire job from failing by incorrectly marking the Microsoft Team group as Deleted within the NHSmail Portal.

- **71975- CSV Bulk Update Accounts Failing - Password Validation**

  The bug fix is implemented to remove password validation within the CSV upload functionality when updates to other field properties are included within the CSV updates.

  For example, if a user attempted to update the JobTitle property with a value which didn’t match the NHSmail Portal criteria, the validation of the file will return a validation error against the wrong CSV column.

- **49230- PODS - If an attempt is made to register a care provider site that is already registered for NHSmail, error message should be displayed**

  After the bug fix, when a care provider site has already registered for NHSmail, then the error message will be displayed if a user attempts to register with the same postcode more than once. This error will provide guidance to end users that the care provider is already registered.

- **52221- Sponsor 2 receives the 'Action required – Azure B2B Request has been raised' email separately for external organisation access requests**

  This bug fix is focused on when an External Organisation Access request is raised and has both a Primary and a Secondary sponsor listed. , The request notification will include both sponsors in the CC field rather than sending separate emails to each.

- **59894- Static DL's remain in pending once approved if they encounter any error during the approval**

  This bug fix has been resolved for situations where static distribution lists remain in a pending status after an admin approves the static distribution list changes performed by an owner. This fix will no longer see distribution lists remaining in a pending state after an approval or rejection operation.

- **68681- Teams Locale Hangfire Job code refactor**

  After the bug fix, once a MS Teams Site locale has been updated from US to UK, the original MS Teams site owner will be added, and the tenant admin user will be removed.

  The original bug was around the tenant service account remaining as the Microsoft Teams owner rather than being removed with the original teams owner after the Microsoft Teams Local ID change occurred.

- **71105- RemoveMailTipForActiveUsers Hangfire job improvements**

  After the bug fix, the following mail-tips for Active Leavers and Disabled status users are removed once the associated operations of “Mark As Joiner” and “Enable” user have successfully occurred. The related Hangfire

job will run on schedule to remove these mail-tips from any accounts which no longer require this mail-tip notification.

3 Items dropped from Release after Testing

This section will be updated post testing detailing any items that have been removed from the release due to failing testing or not working as designed.

Any items de-scoped will re-enter the product backlog for prioritisation into a future release.

3.1.1 Product Backlog Items

ID	Title	Rationale

3.1.2 Bug Fixes

ID	Title	Rationale

4 Known Defects going into the Release

ID	Work Item Type	Title	Severity	Comments	Target Release

5 RFC Dependencies

RFC Reference	RFC Title	Work Item Reference	Work Item Title	Implementation Date
CHG0874571	Production - Update 'ResourceProvisioningOptions' to 'Team' for all teams missing this property	53675	Teams are intermittently being created without the ResourceProvisioningOptions property set, this can lead to the teams status sync hangfire job updating their status to deleted in the db	02/03/2023
CHG0874588	Production - Create Certificate based Azure App for SharePoint PnP	64186	SharePoint PnP module - Update to code to replace the Credential object with App and Certificate details	16/02/2023
CHG0879606	Production – Update Teams Dial Out Policy	56119	Dial-out Capacity	02/03/2023

RFC Reference	RFC Title	Work Item Reference	Work Item Title	Implementation Date
CHG0879606	Production – Update Teams Dial Out Policy	56210	Add dial out capability for an organisation	02/03/2023
CHG0879606	Production – Update Teams Dial Out Policy	66372	Dial-Out Capability - Addition of ability to dial out nationally (Policy & Org Level)	02/03/2023

6 Release Deployment Approval

This section will be completed prior to the final release note being issued. The following approval will be provided by the Accenture NHSmail Service Delivery Lead or a suitably empowered representative to confirm that the release can be deployed into the production environment.

Name	Role	Date	Approved/Rejected
Stuart Glen	NHSmail Service Lead		

7 Post-Release Review

This section will be completed 5 working days after the release has been deployed in Production. It will cover any post-release issues that have been investigated and found to be directly related to the release/release items.

Post-release issues: Yes/No (delete as applicable)

Issue	Date logged	Remediation Agreed