Applications Guide for NHSmail

Version 13
July 2021

Contents

Introduction

This document provides guidance on how to configure local mail-enabled applications to work with NHSmail. The document provides information on connection settings over various types of networks, considerations that must be taken into account when setting up an application, examples and frequently asked questions.

It details the APIs that can be used and the functionality offered by each. This guidance focuses only on native Microsoft APIs for Exchange, which are currently the only published NHSmail APIs.

About NHSmail

NHSmail is a national secure collaboration service for health and social care, designed to enable the secure exchange of information by email and other methods such as Microsoft Teams. The NHSmail service is available through the Internet and the Relay service on the Health and Social Care Network (HSCN).

Please note, if an automated system's behaviour threatens the service, the accounts may be automatically disabled without notification. This should be included in the hazard log for any clinical system.

The following protocols are available for use:

- SMTP
- POP
- IMAP

If your application needs to use these protocols, you will need to contact your Local Administrator (LA) within your organisation to enable these protocols locally due to the security risks associated with these protocols as they do not support modern authentication. Where not used for some time, these protocols may automatically be disabled to minimise attack surfaces.

Considerations

There are certain considerations that must be noted when setting up your application to work with NHSmail. These are listed below.

Authentication policy

All protocols require an authenticated connection using the full NHSmail email address (as the username) and the accompanying NHSmail password. Additionally, the 'from' address of all sent emails must match the email address of the sending account.

If your application does not support authentication, is on the HSCN and can send using an nhs.uk address then NHSmail provides a solution that will allow your application to transmit the email through a relay server. A mail relay server uses the SMTP protocol to forward emails from another server or application to its destination.

NHSmail hosted relay service can be used by any NHS organisation on the HSCN network with a nhs.uk email domain. When sending email through the relay server it must use the valid nhs.uk domain for the organisation sending the email. If the 'from' address is spoofed the mail will be marked as spoofed and will either be delivered to the 'Junk' email folder or may not be delivered at all. Further information about how NHSmail guards against spoofing can be found in the NHSmail Spoofing Guide.

Please note: emails containing any patient or confidential data must be sent via NHSmail only. Non-patient and non-confidential data, such as alerts, can be sent through the relay service. Emails sent through the relay service and NHSmail will be virus and spam checked.

Please refer to the connection details section in this document for more information on setting up a connection to the relay server.

For further help please contact the relay helpdesk on 0333 200 4333, or by email: relayhelpdesk@nhs.net.

Changing your NHSmail account to an 'application account'

You can request, via Helpdesk Self Service, to change the account that your application is using from a standard user to an application account type. There are key differences between user and application account types:

- A more complex password – as it is unlikely a person will be reviewing the mailbox regularly and they would normally send more emails, there is more risk to the service if the account becomes compromised.

- Reduced email retention – as these accounts are high volume sending accounts, we have removed the 180-day email retention. Please refer to the Data Retention Policy for more information.

Password policy

NHSmail has been designed as a secure service and as such passwords must be kept secure and not shared[1]. If your application is configured to store an NHSmail password, access to the application must be strictly controlled and audited to prevent unauthorised access to the NHSmail account, which could have patient / sensitive data within it. If the application is used to exchange patient data it must be treated as a clinical system with the appropriate controls / security mechanisms in place, as per your local governance and clinical safety policies.

Caching or 'banking' the passwords of multiple NHSmail accounts is strictly forbidden unless done so with a Password manager such as Azure Key vault and configured in line with NCSC guidance on the use of password managers. Caution must be taken as if multiple NHSmail passwords are stored in a single application and that application becomes compromised, the security and integrity of many NHSmail accounts will be put at risk. The NHSmail email account used by your application must adhere to the NHSmail password policy (a standard active directory complex password policy):

- Password must NOT include your username (prefix of your email address)
- It does not require a mix of character types
- It must not be detected as a common or breached password (undertaken as a real time check at password change)
- It must be ten or more characters long
- It cannot be any of your four previous passwords
- It must be changed every 365 days

If you set your NHSmail account to an 'application account' as per the previous section of this document then you will need to adhere to the above password policy, with the exception of the below:

- It must be at least 20 characters long.
- It must be changed every 12 calendar months.

Lockout policy

You must be aware of the constraints of the NHSmail lockout policy when integrating your application:

- The account must be active and in an unlocked state, to work with your application
- If the account is locked or disabled, then you will need to contact your Local Administrator to have the account unlocked
- You have a number of attempts to enter the password correctly, before the account is locked

[1] See section 3.1.5 of the NHSmail Acceptable Use Policy at https://portal.nhs.net/Home/AcceptablePolicy

Should any account credentials become compromised the account may be locked out and/or forced to change the password. If locked it will require an administrator to be unlocked.

Spam policy

NHSmail checks all emails handled by the system, in an effort to limit the amount of spam that reaches users' mailboxes. There are multiple layers of checking and defence to give the best protection possible.

More information can be found in the NHSmail Cyber Security Guide and the NHSmail Spoofing Guide.

Support

The NHSmail helpdesk is available, to support clients recommended for use with NHSmail, 24 hours a day, 365 days a year, by calling 0333 200 1133 or by emailing helpdesk@nhs.net.

Information about supported clients can be found in the NHSmail Desktop Configuration Guide.

Support for a self-coded application will not be provided by the NHSmail helpdesk. Advice will be given around connection types, but application / coding issues will need to be diagnosed by your local support team.

Sending automated email

It is possible to create an application that integrates with NHSmail, to send automatic email messages.

Certain criteria must be followed to ensure that the application works seamlessly with NHSmail, as listed in the following sections.

Connection details

To successfully connect your application to NHSmail, you must use the following settings with a valid NHSmail account:

Protocol	Purpose	Hostname	Port	Encryption	Authentication required?
IMAP	Receiving email	outlook.office365.com	993	SSL	Yes
POP	Receiving email	outlook.office365.com	995	SSL	Yes
SMTP	Sending	smtp.office365.com	587	TLS	Yes

Note: for SMTP, POP and IMAP to work you may need to make changes locally via your Local Administrator, as well as requesting the protocols to be enabled for the application account being used on NHSmail.

Connection via the above protocols is the preferred option. However, if your application does not support these protocols, you may choose to transmit your email through our relay server on the HSCN network using a valid nhs.uk domain name; using an nhs.net address will result in the email being marked as spoofed and it may not be delivered. The connection details are:

Server name	relay.nhs.uk
Server IP addresses	155.231.210.221, 155.231.210.253
Port number	25
Authentication type	Anonymous access

You must ensure that the firewall rules on your SMTP server allow outbound traffic through the IP address and port numbers above.

The IP address of your server must be registered on the HSCN, as the relay service carries out a reverse lookup when transmitting email messages. If you do not register the IP address, the relay will check that a Domain Name System (DNS) record exists on the HSCN / TN when carrying out its reverse lookup. If the IP address of the relay requestor is not registered, the relay request will be refused and the email will not be routed to its destination.

To ensure a resilient service, best practice approach should be implemented; **do not use hardcoded IPs, but instead use the DNS name - relay.nhs.uk.**

Note: you only need to register your IP address with the DNS team if you are sending via relay.nhs.uk with no authentication. Other connection methods (IMAP, POP etc.) do **not** require you to register your server with the DNS team.

To register the IP address of your server on the HSCN / TN, contact the DNS team at dnsteam@nhs.net.

Further information is available on how to use the NHS relay service.

To send email using your application:

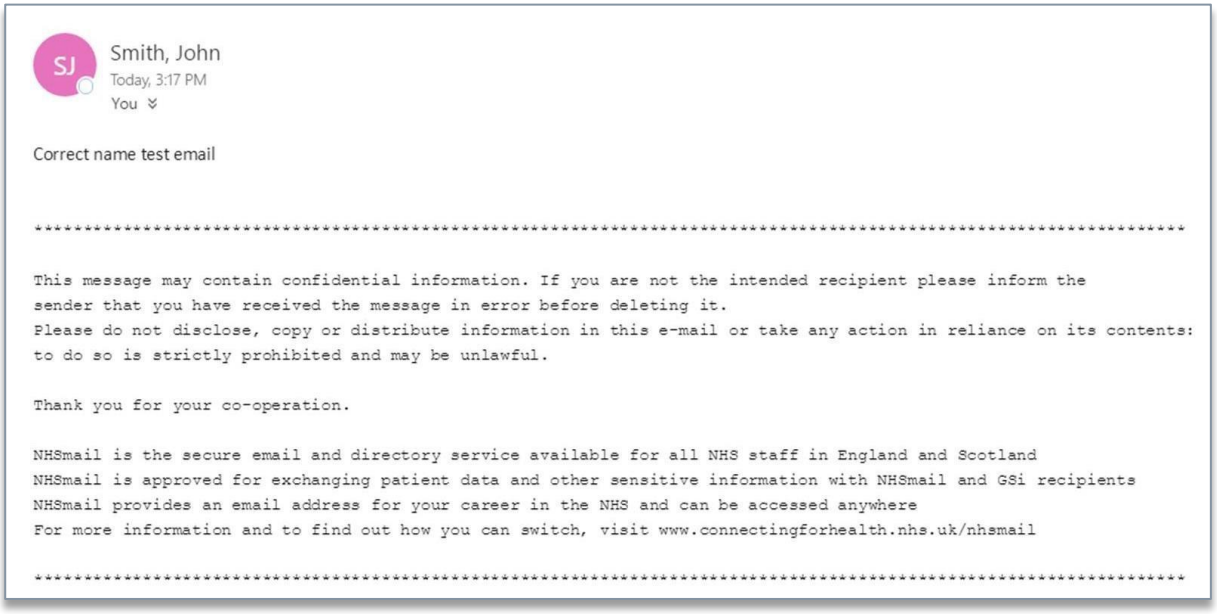
- Where the connection must be authenticated, the full email address of the NHSmail account must be entered as the username (for example, test@nhs.net)

- Outbound (SMTP) connections must use TLS and not SSL
- The ‘from’ field must match the email address that you are using to send from. If a different ‘from’ address is used, the message may be rejected as spam
- IMAP is recommended, rather than POP, for receiving email as it is a more feature rich / robust protocol
- The mailbox must be within quota. If the mailbox is over quota then any emails will not be sent
- The mailbox size must be managed in the same way as a regular user mailbox. If you are sending large volumes, then you should regularly check the status of the account to ensure it is within quota
- Individual messages must not exceed 35mb in size
- Emails cannot be sent to more than 5000 recipients in a single email, unless an NHSmail distribution list is used
- When sending to distribution lists, the application should be configured to send at a minimum of 30-minute intervals
- You must use a separate, application email account for your application. This will make it easier to manage the account in terms of keeping it under quota, monitoring replies and setting permissions
- The reply to email address must be valid. Non-delivery addresses, such as noreply@nhs.net, must not be used. Applications found using non-delivery addresses may be blocked from NHSmail
- You must ensure the system has an in-built error messaging capability to highlight any messages that are not delivered using the application. This is to protect your business process and to ensure any errors are highlighted to the sender, in order for the error to be fixed as soon as possible

IMAP and POP display name field

If you configure an NHSmail account using POP or IMAP with an application, you must ensure that the display name field is populated correctly. This applies to any configured application, be it Outlook or a coded application. For example, in Outlook the field is called ‘your name’. When sending to a non-NHSmail address, this is the name that will show in the recipient’s mailbox. The name must be entered as Lastname, Firstname (ORGANISATION NAME).

In the example below, an NHSmail account has been configured using POP and ‘Smith, John’ has been entered in the ‘your name’ field. An email has been sent to a non-NHSmail email address and the recipient’s mailbox shows the following:



Office 365 Sending and Receiving Limits

NHSmail uses Office 365 which has a range of mailbox, sending and receiving limits as detailed here:

https://docs.microsoft.com/en-us/office365/servicedescriptions/exchange-online-service-description/exchange-online-limits

You need to ensure you configure your applications not to exceed any of the mailbox and receiving limits. If you have a business need to send higher volumes then a separate email relay will be provided to support high volume sending accounts.

If there are any service outages or Office365 limits exceeded, you need to ensure your application is able to queue and retry messages automatically.

Application Programme Interface (APIs)

The NHSmail APIs are native Microsoft APIs that provide a bridge to make it possible for you to connect your local, regional or national applications or services to NHSmail, in a selfservice manner. This will allow your organisation to increase the benefits of using the platform.

Through APIs, NHSmail is enabling functionality in an open but controlled and secure manner, to enable collaboration in a way that is immediately accessible for in-house innovation within local health and social care organisations, as well as third parties.

APIs are not just technical products – they are powerful business tools for developing an ecosystem around the NHSmail platform, however they do require local technical skills to implement. We have provided links to further Microsoft technical information for the APIs that

can be used with the NHSmail service, throughout this guidance document. The NHSmail management team reserves the right to restrict users' access to specific APIs, if they are being utilised in a way that is impacting performance of the platform.

When referring to the 'NHSmail APIs' throughout this guidance document, this includes Microsoft Exchange APIs. The NHSmail Exchange APIs are open-source, although an NHSmail account is needed to access the APIs.

NHSmail uses native Microsoft APIs that are transferrable to other instances. Several webbased platforms and SDKs (Software Development Kits) are available, which make it easy to access the APIs and understand how to use them.

See below for high level supporting notes on the recommended APIs that are currently available for NHSmail, as well as links to further information.

Exchange APIs

Exchange Web Services (EWS) has a variety of available APIs that provide access to email and calendar-related functionality that can be integrated into other apps, web-services and programmes.

Exchange Web Service (EWS) Managed API 2.0

The EWS Managed API is the recommended interface for developing client applications that use EWS and Autodiscover, to communicate with Exchange. EWS Managed API is an opensource, simple and full-featured interface that can be used to work with email messages, calendar, task and contact information and to allow programmatic access to mailboxes. Client applications implementing 'Managed' EWS will be compatible with later versions of Exchange including Office365.

For more information on the EWS Managed API, refer to:
https://msdn.microsoft.com/enus/library/office/jj220535(v=exchg.150).aspx

Exchange Web Service (EWS) API

EWS provides a set of operations that client applications use to access and manage Exchange store items. Just like the EWS Managed API, EWS can be used to work with email messages, calendar, task and contact information and to allow programmatic access to mailboxes, public folders and public folder mailboxes. Data is sent to and from the Exchange server by means of XML that is based on a schema definition. Client applications implementing basic EWS may not necessarily be compatible with future releases of Exchange including Office365.

For more information on the EWS API, refer to:
https://msdn.microsoft.com/enus/library/office/bb204119(v=exchg.150).aspx

The correct URL for EWS will change depending on the mailbox being accessed or if the mailbox is moved within the service. It is recommended that the Autodiscover service is used, to return the correct endpoint.

For further information on how to use this within your code, refer to:
https://msdn.microsoft.com/en-us/library/office/jj900155(v=exchg.150).aspx

SOAP Autodiscover

The SOAP Autodiscover service was introduced in Exchange 2010. We recommend that you use the SOAP Autodiscover service to get client configuration data from Exchange. The legacy POX Autodiscover service should not be used.

For more information, refer to:
https://msdn.microsoft.com/en-us/library/office/dd899340(v=exchg.150).aspx.

Enterprise Directory (LDAP)

The Enterprise Directory (ED) is an implementation of a Lightweight Directory Access Protocol (LDAP) service, containing full details of the organisations, departments, sites and people registered in the NHSmail service. It can be used by any NHSmail subscriber to integrate identity data from the service into local applications and services.

Acceptable use of NHSmail APIs

The NHSmail platform and APIs have a number of safeguards to protect against inappropriate use. NHS Digital encourages appropriate use of the NHSmail APIs. The APIs have rate limiting controls that will prevent inappropriate use. The NHSmail management team reserves the right to restrict users' access to specific APIs, if they are being utilised in a way that is impacting performance of the platform.

System updates & changes

Updates to the NHSmail system will occur as needed and not on a set schedule. Forewarning of these changes, where possible, will be posted onto the NHSmail Service Status pages.

Testing

NHS Digital does not provide an environment for development testing. It is the responsibility of the developer to perform testing. The production NHSmail system must not be used for

development testing. All developers are advised to create their own safe environment for application testing and to use an iterative approach for development.

Clinical Safety

If your application is used to exchange clinical data your local safety case must take into accounts hazards associated with email such as non delivery, delivery delays, out of sequence delivery and unavailability.

Further guidance and contact information

Further information about the NHSmail APIs, and developing apps for the NHS more generally, can be found on the health developer network webpages: https://developer.nhs.uk/. You can also contact the health developer network, if required.

If you are intending to create an app to connect with NHSmail, please contact us at feedback@nhs.net.

Frequently asked questions

Can my application be run from the Internet?

Yes and this will be subject to your own local governance with your application. However, if you require the use of SMTP over the internet you will need to speak with your Local Administrator who can enable this protocol to work over the internet.

I am not an employee of an NHS organisation. How do I get an NHSmail account to integrate my application with the NHSmail APIs?

To gain third-party access to NHSmail, please visit the joining NHSmail section of the Portal help pages and follow the instructions for 'registering a commissioned / independent organisation providing or supporting publicly funded health and social care'.

Who is the best person to speak to from a technical perspective, if I am wishing to develop an interface with an API?

There are a large number of Microsoft resources, and information from other sources, on the internet around developing against the native Exchange APIs. You should work with your local developer resources in the first instance, using the online information.

If your developers experience any difficulty connecting to the APIs, or the responses are not as expected, then please contact feedback@nhs.net detailing the issue.

Do I need to seek any approvals to use an API on the NHSmail platform?

There are no approvals to use any of the APIs but developers should follow the guidance contained within this guidance document.

What happens if the APIs change centrally - how will I be informed?

APIs do change over time, but it is the Microsoft standard APIs that are available, so will be well documented and as with Microsoft normal policies they usually give good notice of change. Where possible we will cascade known change communications to the Local Administrator community and ensure it is published on the NHSmail Portal help pages, for all

users to read. Developers are encouraged to subscribe to TechNet and monitor Microsoft streams of work.

What policies should I consider when interfacing an API to an existing system?

Guidance in this document should be adhered to but it is important to consider local information governance policies and those relating to clinical safety, for example, DCB0129.

Can I use Autodiscover for EWS?

The correct URL for EWS will change depending on the mailbox being accessed or if the mailbox is moved within the service. It is recommended that the Autodiscover service is used to return the correct endpoint.

For further information on how to use this within your code, refer to:
https://msdn.microsoft.com/en-us/library/office/jj900155(v=exchg.150).aspx