Welcome to the NHSmail Anti-Spoofing Webinar

- The webinar will begin at 10.30am.
- Participant lines will be muted during the presentation.
- The webinar will be recorded.
- You can use the chat messaging feature to ask questions. Please only use this for questions, not general comments.

NHSmail
Anti-Spoofing Webinar
26 October 2018

Information and technology
for better health and care

Agenda

- **Introductions and housekeeping**
  Catherine Anderson-Selby NHS Digital
- **Background information and pipeline activities**
  John McGhie NHS Digital
- **Suggested steps and advice**
  Tom Blackmore Accenture / Kieran Brough NHS Digital
- **Additional resources**
- **Questions**

Background Information

NHSmail in numbers

The most widely used application inside the NHS based on number of users, screen time and N3 bandwidth

USERS

1.279M
Users on the Platform

MAILBOXES

1.435M
Mailboxes on the Platform

MOBILE

622K
Connected Mobile Devices

ADMINISTRATION (PER MONTH)

64K
Joiners, Movers and Leavers

700K
Automated Self-Service Requests

13K
NHS Organisations

2.05M
Azure AD Objects – Largest Globally

25K
Service Desk Interactions

16K
Local Administrators

COMPUTE

21PB
Storage

5.5K
CPU Cores

66TB
Memory

MIGRATIONS

120K
Users Migrated in 1 Day – Fastest Globally

124
New Organisations Committed – 354K Users

SECURITY

1B
Malicious Emails Blocked / Month

Anti-spoofing

The anti-spoofing project has been introduced to prevent the practice of **spoofing from the internet** from an @nhs.net email address:

- Email communications are being sent to the spoofing email addresses of the organisations that are currently spoofing.
- Phase one of this project is to divert any spoofed emails that are received to recipients' 'Junk' mailboxes – this will commence from the **31 October 2018**.
- Phase two will block any spoofed emails from the NHSmail platform completely, so these won't reach a user's mailbox at all. This is expected to take place in early spring 2019 and exact dates will be confirmed nearer the time.
- Further information is available within the 'NHSmail News' section of the Service Status page, within the 'Anti-spoofing' area.

Why is spoofing being stopped?

- NHSmail is introducing an approach to prevent emails being sent from spoofed @nhs.net addresses from being delivered into NHSmail inboxes.
- This is being introduced to protect the NHSmail service and to ensure that senders are sending emails legitimately from @nhs.net addresses.
- Reduces the risk of phishing emails being sent through @nhs.net

Enabling POP IMAP SMTP

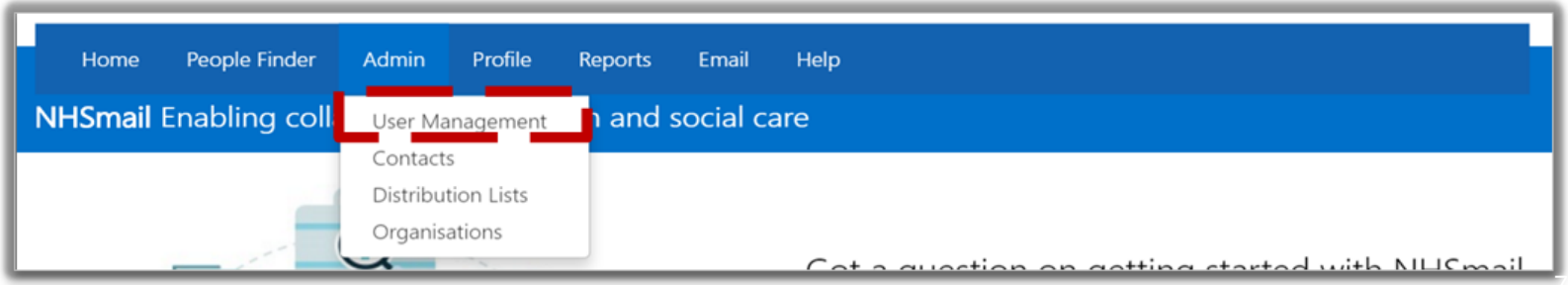
Performing action behalf of users

Enabling POP IMAP SMTP

Local Administrators will be able to enable or disable this for users as required – this will enable / disable these protocols connecting from either the internet or the transition network / HSCN.

To enable this feature:

1 Click **Admin** in the navigation bar at the top of the screen and select **User Management** from the drop down menu



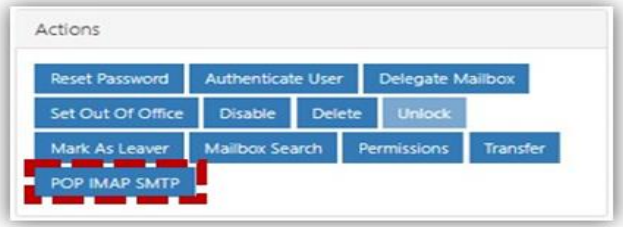
Enabling POP IMAP SMTP

2 Use the search box to find the account you wish to change the protocols for

Refer to the *Searching for an Entry* section for more information

3 Click on the user's **Display Name** to open the User Details Page

4 From the User Details Page, click the **POP IMAP SMTP** button in the **Actions box**

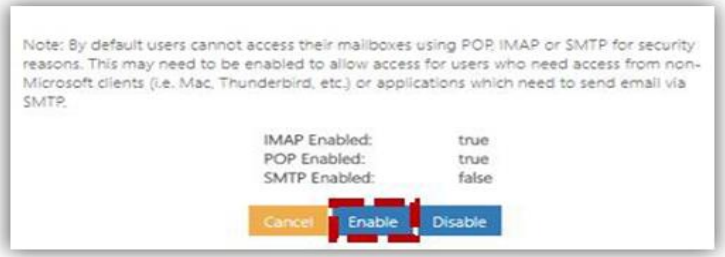


5 Click **Enable**

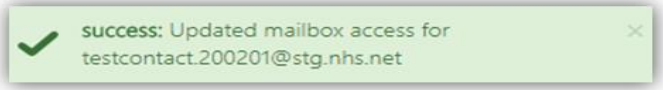
Enabling POP IMAP SMTP

Enabling and disabling POP IMAP SMTP

Performing actions on behalf of users



The following message will be displayed:



6 Click **Update** at the bottom of the page

Connection details

- **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.
- 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	imap.nhs.net	993	SSL	Yes
POP	Receiving email	pop.nhs.net	995	SSL	Yes
SMTP	Sending	send.nhs.net	587	TLS	Yes

Connection details

- Connection via the protocols on the previous slide 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 / TN 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

Connection details

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

- The IP address of your server must be registered on the HSCN / TN, as our 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.**

Additional resources

- Guidance on spoofing
- Service Status page
- Applications Guide
- Portal Local Administrator Guide

Questions?

NHS Digital

www.digital.nhs.uk

@nhsdigital

enquiries@nhsdigital.nhs.uk

0300 303 5678

Information and technology
for better health and care