Mobile configuration guide for NHSmail

Version 3

Published July 2017

Glossary of Terms

Term / Abbreviation	What it stands for
Encryption at rest	Data stored in phone (handset) storage is encrypted and can only be read with the secret key needed to decrypt it. If a device does not have encryption at rest, data could be read if copied.

Contents

NHSmail and mobile devices overview

Purpose of document

Target Audience: End users of NHSmail who wish to access the service via a mobile device. This document will only provide support for mobile devices that are still under mainstream support by the vendor.

Mobile device features

The NHSmail service provides features for mobile users such as wireless synchronisation of the calendar and 'always on email'.

Key features at a glance:

- You will receive any new or updated item as soon as it arrives on the NHSmail server – there is no need to set up a synchronisation schedule.
- Email, calendar items, contacts, and tasks are synchronised 'over the air' with the device – no additional synchronisation activities are required to replicate changes between the mobile device and other devices.
- Security features are automatically applied to devices that are able to support security policies, e.g. an automatic screen lock after the device has been inactive for 20 minutes; self-service device password reset and remote wipe facility if the handset is lost or stolen.
- The service is available on different devices including Windows Mobile, Nokia, Blackberry, Android, Apple iPhone 5 / 6 / 7 and iPad.
- Supports flags enabling you to manage your email and flag items for later action.
- Rich HTML formatting of mail for mobile devices renders tables, fonts, formatting and images correctly. You can control whether you want to view HTML or plain text email.
- Many bandwidth saving features help reduce costs and the time taken to deliver data over slow wireless networks.
- Forward, reply, or reply-all to a meeting request.
- You can set up an automatic reply (out of office) from your mobile device.
- Easy setup for most devices – all you need to know is your email address and password.

Note: Exchange ActiveSync does not support shared mailboxes or delegate access.
It is important to remember that receiving data on your device may incur a financial cost to you or your organisation. You may wish to set your device to manually update. Check with your organisation for more information regarding data plans and tariffs.

Important: should you wish to use either a personal device to connect to NHSmail, or a mobile device that cannot be encrypted or allow the policies to be applied, please ensure you have approval from your own organisation to ensure compliance with local information governance policies.

Devices that have been modified by techniques such as 'Jailbreaking' or 'Rooting' must never be connected to NHSmail as the security/integrity of the device cannot be guaranteed. Devices should be kept up to date with the latest software available via the manufacturer.

Mobile device configuration

This guide does not provide configuration information for individual device types. For full guidance on each device type, please refer to your manufacturer's instruction guide on setting up your email account.

The table below provides a brief overview of configuration information for a selection of devices (only devices that support the latest operating system by the vendor).

Device	Configuration
Windows Phone 10	Uses the 'Autodiscover' feature so the user will only have to type in their email address and password. There is a known issue when configuring Windows Phone 10 – a workaround is on the NHSmail support pages: https://portal.nhs.net/Help/servicestatus
Apple iPhone 5, 6, 7 and iPad	Uses the 'Autodiscover' feature so the user will only have to type in their email address and password.
Blackberry devices with operating system (OS) 7.1 or earlier running AstraSync / NotifySync software	Manual settings / Autodiscover Older Blackberry models (7.1 or earlier) can only be configured with NHSmail if either AstraSync or NotifySync software is purchased and installed. Please refer to your handset provider to check your device operating system version.
Blackberry with operating system (OS) 10 and ActiveSync	Blackberry with OS10 uses the 'Autodiscover' feature so the user will only have to type in their email address and password. **Note: encryption will need to be enabled manually on the device.**
Android with Touchdown	Many older Android devices (running Android 5 lollipop or older) do not include the encryption at rest capability and third party Symantec Touchdown software must be installed prior to configuration. Please check with your handset manufacturer should you need any specific device information.
Android with native email client	Newer Android devices (running Android 6 marshmallow or newer) do include an encryption at rest capability. Android devices have built-in ActiveSync client which will allow connection to Exchange. There is a significant data leakage risk with versions of Android below version 6 (Android 6 Marshmallow) that could allow any app on the device to access and covertly export the mail data.

Configuration guides (click to follow links):

- Set up email on Windows Phone 10
- Set up email on iPhone, iPad, or iPod Touch
- Set up email on an Android

Only devices which support the Exchange Active Sync protocol and have inbuilt encryption at rest capability should be connected to NHSmail. See manufacturer websites for further information.

For those devices that require manual configuration, the following settings are required:

Configuration	**Set as:**
ActiveSync Server URL	eas.nhs.net
ActiveSync Domain Name	<leave blank>
Username	<your NHSmail email address>
Password	<your NHSmail password>

Protecting a mobile device

Making NHSmail more secure on mobile devices

If you have a mobile device set up to access NHSmail, you may notice a range of security features are automatically applied to it. This is to minimise the risk of data loss.

Security features include:

- An encrypted connection between the mobile device and the NHSmail service.
- Implementation of a password to access the mobile device.
- A limit on the size of email attachments that can be downloaded – by default 10MB.
- A remote-wipe facility, meaning that the data held on the mobile device can be deleted if it is lost or stolen.

In addition, some mobile devices automatically encrypt the data they contain ‘at rest’, in other words the data held on the phone is encrypted and can only be read after the phone is unlocked by the user, preventing access should it be lost or stolen. Encryption at rest is automatically enabled on connection to NHSmail on those devices that support this feature.

It is important that sensitive or patient identifiable data isn’t held on any mobile devices that don’t have a built-in encryption at rest capability or those where encryption at rest cannot be remotely enabled. It is a mandatory Department of Health requirement that only encrypted devices carry such data. Email encryption using NHSmail is covered later in this document.

If your mobile isn’t listed in the compatible mobile devices section of this document, please contact your local IT helpdesk / Local Administrator for further guidance before it is used to hold or transmit sensitive or patient identifiable information.

NHSmail mobile device security policies

Once you have set up your device to work with NHSmail, a security policy will be applied. The default NHSmail security policy is:

Category	Policy Setting	NHSmail policy
Loss Protection	Mobile device password required	Yes
	Minimum mobile device password length	Four characters
	Maximum inactivity time lock	20 mins
	Maximum fail mobile password attempts[1]	Eight
	Mobile password expiry (The device password will never expire. You will still need to reset your NHSmail password every 90 days or fewer.	90 days
	Policy refresh interval	1 hour
Data aggregation	Maximum attachment size[2]	10 MB
	Maximum e-mail body truncation size	64 KB
	Maximum HTML e-mail body truncation size	Unlimited
	Maximum e-mail age filter	1 month
Encryption	Enforces encryption at rest on devices that support this feature?	Yes

[1] The phone will be automatically wiped of all NHSmail data and restored to its default factory settings after the last failed attempt. Refer to the device's manufacturer guide for non-NHSmail data (photos, documents) stored on the device.

[2] This size only applies to a mobile device. Attachments over this size will be received by your NHSmail mailbox.

Once the policies have been applied to the device they can only be removed by performing a factory reset (format) of the device.

If the policies aren't applied to your device, you must inform your local IT helpdesk to ensure you are not in breach of local information governance policies

Compatible mobile devices

The tables below lists the device version used to connect to NHSmail and whether or not the device supports encryption at rest. If the device does not support encryption at rest, you should check with your handset manufacturer first. You should also contact your local IT helpdesk / Local Administrator for further guidance before it is used to hold or transmit sensitive or patient identifiable data.

Please be aware that the Microsoft Outlook mobile app does not work with NHSmail as it uses a different configuration. Instead, email should be accessed via the mail feature on your mobile device.

Note: the list provided below is not a complete list of every device on the market and only includes those devices that are in mainstream support (e.g. they are still supported for updates by the vendor). If you have a device that cannot be matched to the information in this guide, please contact the device manufacturer for further information.

Android

DeviceUserAgent	Device / application	Supports encryption at rest?
Android 6.0 (Marshmallow) and later	Android - Marshmallow	Yes

Apple

DeviceUserAgent	Device / application	Supports encryption at rest?
Apple-iPhone5C1/ Apple-iPhone5C2	iPhone 5	Yes
Apple-iPhone5C3/ Apple-iPhone5C4	iPhone 5C	Yes
Apple-iPhone6C1/ Apple-iPhone6C2	iPhone 5S	Yes
Apple-iPhone7C1/ Apple-iPhone7C2	iPhone 6 iPhone 6+	Yes
Apple-iPhone8C1/ Apple-iPhone8C2	iPhone 7 iPhone 7+	Yes

Apple-iPad3C4 and later	iPad and iPad 2 iOS 4.3 and later	Yes

Please check with your device manufacturer should you have any concerns.

Blackberry

DeviceUserAgent	Device / application	Supports encryption at rest?
NotifySync/4.7 NotifySync/4.8 NotifySync/4.9 NotifySync/4.10 And later	NotifySync	Yes
RIM-Z10 RIM-Z30 RIM-Q5 RIM-Q10 RIM-Leap RIM-Passport RIM-Classic Most newer Blackberry models will show in the reports as “RIM-…”.	Blackberry ActiveSync	Yes – but encryption must be manually switched on by the user

Windows Mobile

DeviceUserAgent	Device / application	Supports encryption at rest?
WindowsMail/17.5.9600…	Windows Mobile 10	Yes – encryption may have to be manually switched on by the user. Please check with the manufacturer

Email encryption using NHSmail on a mobile device

Mobiles that support encryption at rest and other security policies

The following mobiles automatically encrypt the data at rest and automatically apply the NHSmail security features:

- Apple iPhone 5/6/7/ and the Apple iPad.
- Blackberry with NotifySync 4.7 or higher installed – users which already have it installed can continue using it, but for new devices it is not required.

- Blackberry OS 10 and greater.
- Devices running the Windows Mobile 10 operating system.
- Android devices with Symantec Touchdown installed - users who already have it installed can continue using it, but for new devices it is not required.

Vendors are continually releasing new products. Any new mobile device must have the built-in capability to encrypt the data and implement the security policy requirements to connect to NHSmail.

Apple iPhone 5, 5s, 6, 6s, 7 & iPad

Help from Apple to identify the model of iPhone you are using.

All iPad versions include encryption at rest which is enabled by default and cannot be disabled.

Windows Mobile devices with operating system 10

Help from Microsoft to identify the model of Windows Mobile device you are using.

Blackberry configured with ActiveSync running OS10)

Currently the encryption at rest capability on these devices requires manual activation. You must ensure that you are aware of information governance policies enforced by your local organisation regarding the requirement to encrypt the memory of any portable device. Disabling the security features of your mobile handset may mean you do not comply with local policies and could result in disciplinary action.

Blackberry with NotifySync 4.7 or higher installed

The Blackberry running NotifySync version 4.7 physically encrypts the data at rest. Once NotifySync has been installed on the Blackberry it means that there will be two encryption options available – the encryption at rest built into the Blackberry handset (native encryption) and encryption at rest written into the NotifySync software.

When running NotifySync to connect to NHSmail, native encryption at rest should NOT be switched on. If it is switched on, Contacts and Calendar will not sync and only access to email will be available.

Android devices

Android devices with Symantec Touchdown installed can continue using it, but it is not required for new encrypted devices. Newer Android devices do include an encryption at rest capability.

Frequently Asked Questions

What does 'mobile device' mean – does it include laptops or computers used away from work?
No, it means mobile phones, handsets or tablets that can be used to make phone calls as well as connect to NHSmail. Your organisation should have policies in place outlining how to keep information secure when accessed on laptops or other computers outside of your organisation.

What will happen if my mobile device cannot be encrypted and doesn't meet the policy requirements?
You will be able to connect to NHSmail but must not hold any sensitive or patient identifiable data on the device. It is a mandatory Department of Health requirement that only encrypted devices carry such data. If you are unsure as to whether you should continue to use your mobile device with NHSmail, you should check with your organisation.

What about Google Android phones?
Users who already have Symantec Touchdown installed can continue using it, but for new devices it is not required. Android supports encryption at rest after version 6.0.

What is the policy on connecting personal devices with NHSmail?
You must obtain approval from your own organisation to use a personal device with NHSmail to ensure you comply with your local information governance requirements.

If my device does not support encryption at rest does this mean that if I use it to transmit data via email it is not secure?
When we talk about encryption at rest, we are referring to the security (encryption) of the data that is *held* on a device. When the data is transmitted it is encrypted between the handset and NHSmail service, even if the device used to send it is not an encrypted device. It is Cabinet Office and NHS policy to not store any personal data on non-encrypted devices.