NHSmail

the secure communication solution

Android with TouchDown installed supports encryption at rest.

**Please refer to sections two and three for further information

Android running the native email client (TouchDown not installed) does support encryption at rest, but email content may be compromised by some downloaded and installed applications.

**Please refer to sections two and three for further information

NHSmail mobile configuration guide Android mobile devices

Version: V.10

Date: June 2013

THIS INFORMATION IS FOR NHS STAFF AND IS NOT TO BE DISTRIBUTED OR COPIED OUTSIDE OF THE NHS

Contents

1. Android mobile devices

Android is an operating system that can be found on many mobile handsets available today. Most Android mobile devices can be configured with either an:

- Exchange ActiveSync email account; or an
- IMAP email account; or a
- POP email account.

This guide will demonstrate how to configure your Android mobile device to access your NHSmail account using Exchange ActiveSync.

Before configuration you must ensure that you have backed up the device. Installation will by default replace all the contacts, calendar items and tasks currently held on the device with what is held in your NHSmail account.

Important note: some mobile devices provide an initial synchronisation option of replacing the Calendar and Contact information in your NHSmail account with the data held on the device. If you select this option all existing calendar and contact information in your NHSmail account will be removed and replaced with the data on your device and it could, as a result, be left blank.

If you erroneously select this option there is no way to recover your NHSmail Calendar and Contacts unless you have your own personal backup. This is because although it is possible to recover deleted items in NHSmail up to 14 days after the event, your handset has instructed the service to change, not delete, the data in your account.

If you require any assistance setting up your device, please contact your local helpdesk.

Devices that have been modified by techniques such as ‘Jailbreaking’ or ‘Rooting’ should never be connected to NHSmail as the security/integrity of the device is no longer guaranteed.

Your organisation will also need to confirm that a Windows Server client access licence and an Exchange server client access licence is allocated to your mobile device.

2. NHSmail mobile device security policy

Devices connecting to NHSmail must adhere to the NHSmail mobile device policy which is automatically applied:

- A password is required to unlock the device
- The inactivity timeout should be set to 20 minutes. After this time, or if the device goes into standby mode, the password has to be entered to unlock the device
- If an incorrect password is entered eight times in succession, the phone will be automatically wiped of ALL data and restored to its default factory settings
- The maximum message size is 500KB. You can receive messages over this size in your NHSmail mailbox but not on your phone
- Only one month’s worth of email will be synchronised to the device to reduce the risk of data loss as well as improve synchronisation times / reduce cost
- You are required to change the device password every 90 days
- Encryption at rest will be enabled on devices with the built-in capability to support it.

Note: currently some Android devices do not have a built-in encryption at rest capability, therefore these devices should not be used until you have approval from your employing organisation or unless TouchDown for Android is purchased and installed. Please refer to your mobile device manufacturer to check whether your device has in-built encryption. For those devices that **do have inbuilt encryption at rest, please refer to the next section for configuration instructions.

Encryption at rest encrypts the data on the phone and can only be read after the phone is unlocked by the user, preventing access should it fall into the wrong hands.

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

It is important to remember that receiving data on your device may incur a financial cost to you or your organisation, especially if using the device abroad where costs are particularly high. You may wish to set your device to manually update. Check with your organisation for more information regarding data plans and tariffs.

3. Android with in-built encryption

Android released a new operating system in February 2011 which provides in-built encryption at rest to many Android devices. The new operating system is known as Android OS 3 (or higher) or Honeycomb, and encryption is only present on those devices that were manufactured after the release date. Any device that runs the new operating system will not require additional software to provide encryption functionality.

Note: Please refer to your mobile handset manufacturer to check whether you are running the new Android operating system and that your handset has in-built encryption.

** Please also note that although Android devices running Android OS 3 or greater have in-built encryption, once the device is unlocked there is a possibility that an application already on the device, or one that you have downloaded to the device from an App Store, may be able to gain access to any of the data it holds. We would therefore advise that if a device is used to transmit patient data you should only configure your nhs.net email account with a pre-installed application, such as Touchdown. Touchdown encapsulates the email data it holds and prevents other applications from gaining unknown access to it.

4. TouchDown for Android

Touchdown is an application, available to purchase from a third party company called Nitrodesk, which is compatible with most Android handsets. More information on Touchdown can be found at: http://nitrodesk.com/nhs.aspx.

Please Note; Touchdown is only required on Android if your mobile device is running operating system version 2 or older. We would also advise that it is installed on any handset with third party applications installed. Please check with your device manufacturer in order to confirm your operating system version.

5. Configuring TouchDown with NHSmail

5.1. Purchasing and downloading TouchDown

Note: ensure that you download TouchDown version 5.0.0002 or higher. Older versions of TouchDown don’t have encryption at rest capabilities.

- On the Android device click the **Market** application
- Click the **Search** option

- Type in ‘TouchDown’ and click the **Search** button
- The application search result should include ‘Exchange by TouchDown’
- If you have a Droid or Nexus device (any Android 2.0/2.1 device) you should select the ‘Exchange for Android 2.0/2.1’ application
- If neither ‘Exchange by TouchDown’ or ‘Exchange for Android 2.0’ appear you may have the option of selecting ‘TouchDown (Non Cupcake)’
- Don’t select ‘Exchange by TouchDown Key’ unless you are purchasing a license
- After you have selected your chosen application, click the **Install** button
- Follow the prompts to download and install the application.

What if TouchDown is not available in the market place?

If TouchDown is not displayed in the market place on your handset you can download it directly from NitroDesk:

If your phone is a Droid/Nexus/Milestone (firmware version 2.0 or above):

- Point your G1 browser to http://nitrodesk.com/tddownloads/nitroid-droid.apk

If your phone runs Android Cupcake firmware version 1.5 or above (most phones fall in this category):

- Point your device browser to http://tinyurl.com/tchdwn

Otherwise:

- Point your device browser to http://tinyurl.com/td-nocupcake and the latest TouchDown version will be downloaded. Click the downloaded file to install it and follow the prompts.

Please note: if your NHSmail password contains certain characters it will prevent your Touchdown client from synchronising with NHSmail. A list of characters that are valid can be found at: http://www.asciitable.com.

If you require assistance, please contact NitroDesk directly at support@nitrodesk.com. The NHSmail helpdesk does not support this application.

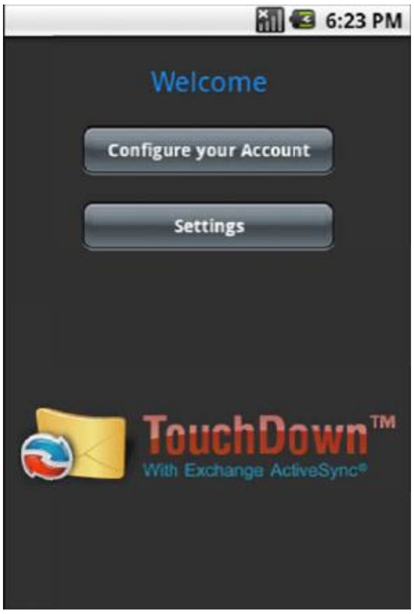
5.2. Configuring TouchDown

Once you have installed the TouchDown software you will need to follow the onscreen configuration settings.

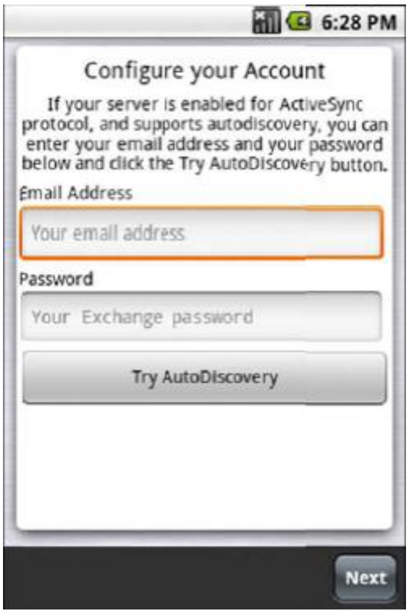
To begin configuring TouchDown, first navigate to the TouchDown icon on the main menu of your Android device.

You will be presented with a license agreement which you will need to read and accept in order to continue. Once you have read it click **I Accept**.

When you launch TouchDown for the first time, the following dialog will open up. Click **Configure Your Account**:



You will now be presented with the Configure Your Account screen as shown below:



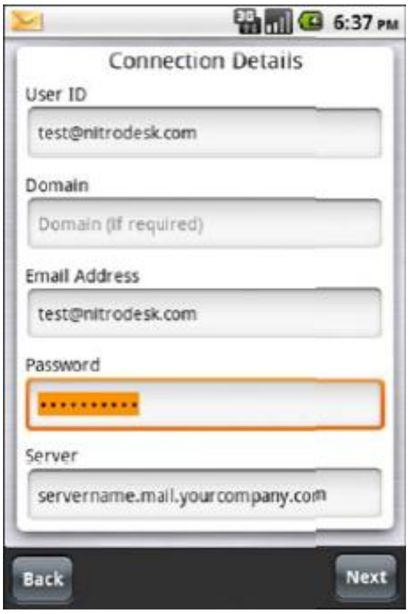
Configure your Account

If your server is enabled for ActiveSync protocol, and supports autodiscovery, you can enter your email address and your password below and click the Try AutoDiscovery button.

Enter your NHSmail email address and your NHSmail password. Click **Next**.

You will now need to enter your connection details:

User ID – Your full NHSmail email address
Domain – Leave blank
Email Address – Your full NHSmail email address
Password – Your NHSmail password
Server – eas.nhs.net



Connection Details

User ID: test@nitrodesk.com

Domain: Domain (If required)

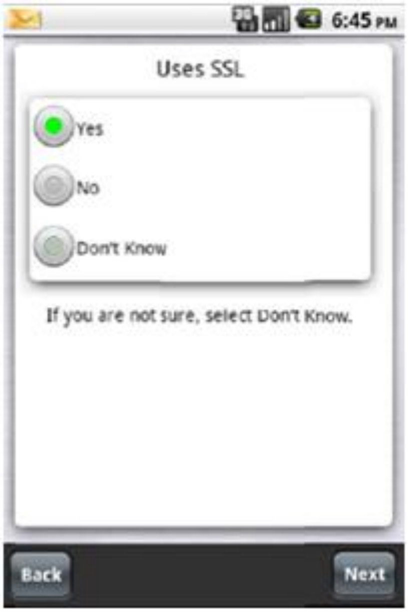
Email Address: test@nitrodesk.com

Password: ••••••••••

Server: servername.mail.yourcompany.com

Click **Next**.

Next you will need presented with the Uses SSL screen. Select **Yes** and click **Next**:



Uses SSL

● Yes

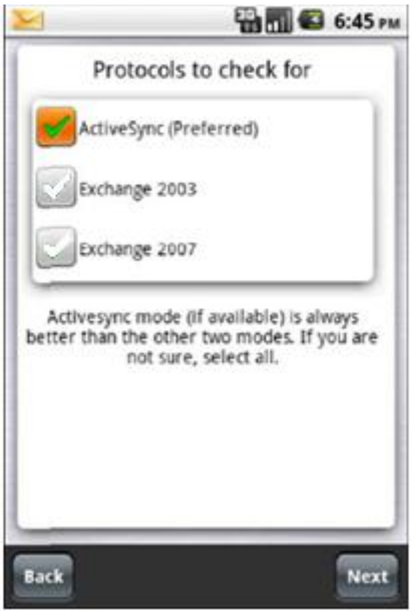
○ No

○ Don't Know

If you are not sure, select Dont Know.

You will now be presented with a screen entitled Protocols to check for.

Select **ActiveSync** and click **Next**:



Protocols to check for

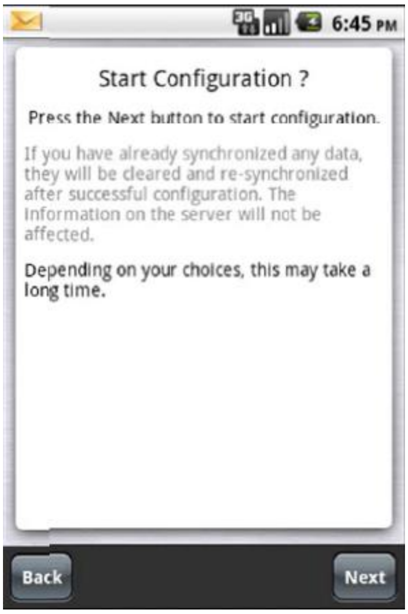
☑ ActiveSync (Preferred)

☐ Exchange 2003

☐ Exchange 2007

Activesync mode (if available) is always better than the other two modes. If you are not sure, select all.

Click **Next** on the screen below:



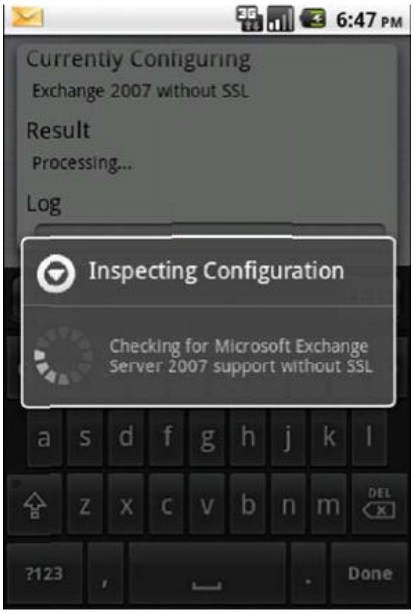
Start Configuration ?

Press the Next button to start configuration.

If you have already synchronized any data, they will be cleared and re-synchronized after successful configuration. The Information on the server will not be affected.

Depending on your choices, this may take a long time.

TouchDown will now attempt to complete the configuration:



Currently Configuring

Exchange 2007 without SSL

Result

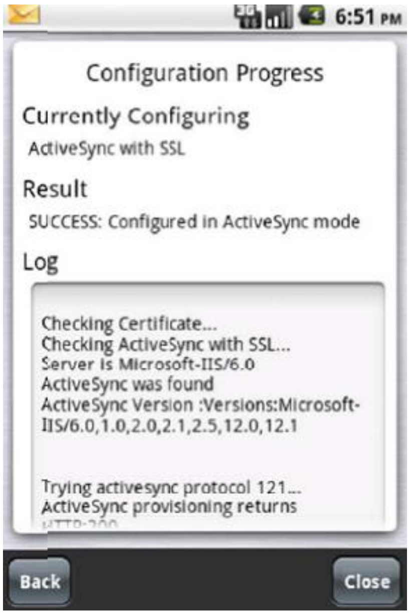
Processing...

Log

Inspecting Configuration

Checking for Microsoft Exchange Server 2007 support without SSL

Your configuration is now complete. Click **Close**:



Configuration Progress

Currently Configuring

ActiveSync with SSL

Result

SUCCESS: Configured in ActiveSync mode

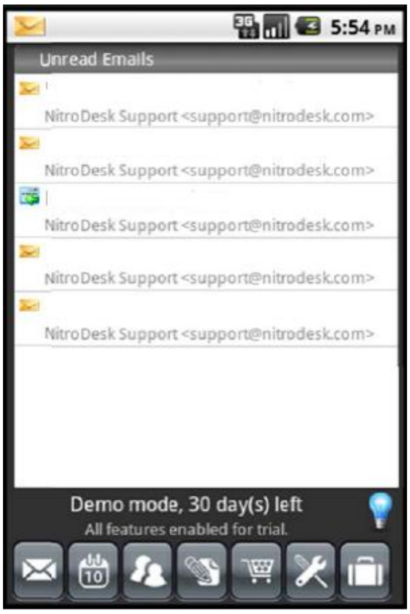
Log

```
Checking Certificate...
Checking ActiveSync with SSL...
Server is Microsoft-IIS/6.0
ActiveSync was found
ActiveSync Version :Versions:Microsoft-IIS/6.0,1.0,2.0,2.1,2.5,12.0,12.1


Trying activesync protocol 121...
ActiveSync provisioning returns
HTTP:200
```

You will be requested to create a PIN for Touchdown. Enter a PIN which must have more than four digits and click the green tick to confirm. Confirm the new PIN again by clicking the green tick.

You will now be directed to the email inbox screen as shown below:



Unread Emails

NitroDesk Support <support@nitrodesk.com>

NitroDesk Support <support@nitrodesk.com>

NitroDesk Support <support@nitrodesk.com>

NitroDesk Support <support@nitrodesk.com>

NitroDesk Support <support@nitrodesk.com>

Demo mode, 30 day(s) left

All features enabled for trial.

Moxier Mail for Android

Moxier Mail is an encryption application, available to purchase from a third party company called Moxier, which is compatible with most Android handsets. More information on Moxier can be found at http://www.moxier.com.

Moxier is available to Android users but although it provides encryption at rest, it only encrypts the body of the email. This means that the calendar, contacts, email attachments and subject are not encrypted in the latest version of Moxier. It is advised that you only user Moxier on your Android device if you are not exchanging patient and confidential data. If you do install Moxier and exchange patient data you will need to seek approval from your local organisation to do so.

Q&A

I currently use an Android device but am unable to update the firmware since installing NHSmail. I need to de-encrypt the device before the firmware update will take place but this option is now greyed out, how do I do it?

This has occurred previously with devices such as the Samsung Galaxy. In this instance the NHSmail email profile needed to be removed and the device un-encrypted so that the firmware upgrade could take place. Once these steps had been taken the NHSmail email profile would need to be re-installed.

For clarity we recommend that you contact your device manufacturer.