

Mail for Exchange for Nokia smartphones

NOKIA
Connecting People

Guide for IT Managers



Mail for Exchange for Nokia smartphones

Guide for IT Managers

Contents

1. About this document	3	7. Arranging connectivity	8
2. Overview	3	Make Exchange Server accessible from the Internet	8
3. Supported servers	3	Verifying that Exchange ActiveSync is enabled	8
4. Compatible Nokia smartphones	3	8. Installing and configuring Mail for Exchange ...	8
5. Deployment considerations	3	Installing	8
Battery life considerations	3	Upgrading	8
<i>Access point impact</i>	4	Configuring mailbox	8
Device management	4	<i>Mail for Exchange integrated on the smartphone</i>	8
<i>Open Mobile Alliance (OMA) standardisation</i>	4	<i>Installable Mail for Exchange application</i>	9
<i>Managing Mail for Exchange</i>	4	9. How should I proceed?	9
<i>Autodiscovery</i>	5	Case 1 – You are an Exchange admin currently using other ActiveSync clients	9
6. Security considerations	5	Case 2 – You are an admin using Exchange 2003 SP2 or later with no mobile devices	9
Are your devices ‘provisionable’?	5	Case 3 – You are an admin not yet using Exchange ..	9
Mail for Exchange with Exchange 2003 SP2	5	10. Best practices	9
Mail for Exchange with Exchange 2007 (no SP)	5	Use SSL	9
Mail for Exchange with Exchange 2007 SP1 and later	5	Enable device lock policies	9
Remotely wiping devices	6	Verify network configuration	10
Using SSL certificates	6	Understanding device logging	10
Using Certificate-Based Authentication (CBA) with Symbian Anna smartphones	6	Appendix – Supported Exchange Server Security Policies	11
<i>Overview</i>	7		
<i>Pre-requisites</i>	7		
<i>Steps to set up CBA</i>	7		

1. About this document

This document applies to Nokia smartphones with S60 3rd Edition Feature Pack 1 and Feature Pack 2 (S60 3.1 and 3.2), S60 5th Edition (S60 5.0) as well as Symbian OS with Symbian Anna software.

2. Overview

This document discusses the deployment options to enable compatible Nokia smartphones to synchronise Email, Contact and Calendar information with the Microsoft® Exchange Server utilising the Microsoft® Exchange ActiveSync® protocol. Mail for Exchange ensures that your business users have an intuitive solution that:

- Always has up-to-date Email, Contacts and Calendar on their Nokia smartphones and desktop
- Has the ability to look up email recipients from Exchange Server directly from the mobile device

For IT departments Mail for Exchange is a secure solution that supports:

- Direct, secure connectivity between Nokia smartphone and Exchange Server
- Exchange Server Security Policies
- Industry standard device management via the Open Mobile Alliance Device Management (OMA-DM) and Device Configuration & Provisioning (OMA-CP) standards

Mail for Exchange is supported with a wide range of Nokia smartphones. The latest models running Symbian Anna software and connecting to Exchange Server 2010 SP1 support new features such as grouping and preview of threaded conversations and certificate-based authentication (CBA), and introduce more Exchange ActiveSync policies.

3. Supported servers

The following Microsoft Exchange Server versions are supported by Mail for Exchange

- Microsoft Exchange 2003 Service Pack 2 (SP2)
- Microsoft Exchange 2007
- Microsoft Exchange 2010
- Microsoft Exchange 2010 SP1
- Exchange Online Service (BPOS and Office 365)

For further information about the Microsoft Exchange solution and the Exchange ActiveSync protocol, please go to <http://www.microsoft.com/exchange>

and <http://www.microsoft.com/exchange/en-us/mobile-email-with-exchange-activesync.aspx>

4. Compatible Nokia smartphones

The Symbian OS has evolved over the years from menu-based and button-based user interfaces of Series 60 to the full touch experience of Symbian OS with Symbian Anna today. Mail for Exchange has evolved in conjunction with these platform changes from an aftermarket installable application to a core part of the Symbian platform.

Please visit www.nokia.com/mailforexchange for the latest availability of three versions of Mail for Exchange applications designed for specific Symbian releases.

The ability to support Exchange security policies is dependent on both Mail for Exchange application version and Exchange Server version. See section 5 Security Considerations for more details.

5. Deployment considerations

When you are designing, planning and deploying a managed mobile messaging infrastructure for your business, there are four main areas to focus on:

- What are your goals around increasing productivity?
- What will deliver satisfaction among people actually using the devices?
- How critical is the ability to manage devices from a central (and remote) point?
- How will the devices be managed locally by end users themselves?

The answers to these questions will drive how you manage and configure Mail for Exchange on your Nokia smartphones.

Battery life considerations

Mail for Exchange supports Microsoft Direct Push and uses this during 'always on' connections. The following is Microsoft's description of direct push and heartbeat interval:

"Direct Push is a client initiated HTTP connection to the server where the device opens a connection to the Exchange Server and keeps it alive for a duration known as the heartbeat interval. Basically the client sets up the connection, chooses the appropriate heartbeat interval and tears down and re-establishes the connection if and when necessary. The server sends notifications about new items over this connection and the client synchronises to get the new items."

Visit <http://technet.microsoft.com> and search: 'understanding direct push'. The link has some recommendations for correcting or preventing low heartbeat.

In summary, higher heartbeat intervals result in longer battery life. Mail for Exchange adapts the heartbeat for changing network conditions to the highest possible value. The maximum heartbeat possible with Exchange is typically 45 minutes, although this is not common. Heartbeat intervals of 8-10 minutes are recommended. Over five minutes is generally acceptable, but if heartbeat drops to one minute the negative impact on battery life may be dramatic.

The latest version of Mail for Exchange detects low heartbeat intervals and synchronises until the interval is optimised. With Exchange 2007 and later servers there are alerts generated when heartbeat is too low: [http://technet.microsoft.com/en-us/library/bb218291\(EXCHG.80\).aspx](http://technet.microsoft.com/en-us/library/bb218291(EXCHG.80).aspx).

Access point impact

Service provider specific access point settings may have additional impact on heartbeat interval (and battery life) that can't be managed by Mail for Exchange, Microsoft Internet Security and Acceleration (ISA) Server, Microsoft Exchange Server or firewall settings. The access point your service provider has provided for general web use (browsing, WAP, etc.) may not be optimised for Direct Push. The service may be dropping connections after one minute, for example, when there is no data being transferred. Direct Push relies on long connections to the server with no data activity.

When disconnected this way and the user has selected the 'always on' synchronisation setting, Mail for Exchange must reconnect to the network. This uses a relatively high amount of battery power.

However, the same service provider may offer multiple access points. Make sure that your users have subscriptions to an access point that allows long connections with no data traffic, or recommend that they use polled (i.e. every 30 minutes) or manual synchronisation. For all firewalls and network appliances, set the idle session timeout to 30-45 minutes. This will ensure that your users get higher heartbeat intervals.

Device management

Device management comprises several operations to remotely manage a mobile device. It is a generic term for the systems that can be used by or on behalf of users to configure, manage and update mobile devices.

With device management Enterprise IT can help employees use new services and applications, as well as

modify the configuration of existing ones with minimal effort. It also enables simple device management practices to be used, such as an inventory of the enterprise's devices.

Certain applications such as personal information synchronisation, network access and email all require separate configuration settings, making them more time-consuming to configure manually. By simplifying configuration, device management helps save time and resources. It can be crucial for companies with many mobile users and devices to ensure efficient usage and cost-effective management.

Open Mobile Alliance (OMA) standardisation

Nokia uses OMA standardised device management technology and has been active in OMA standardisation work. OMA Device Management is designed to work in the wireless environment and makes it possible to add, modify and remove parameters, to provide new services and applications and to perform troubleshooting by identifying configuration issues.

The following examples demonstrate the advantages of a full device management solution:

'Out-of-the-box' provisioning – For a new device, services and applications can be deployed and configured using device management systems.

Proactive and reactive provisioning of new service settings – Mobile users may request new settings for a service or they can be automatically prompted, for example for upgrades.

Troubleshooting – If incorrect settings cause problems for mobile users your company's help desk should be able to check the settings, determine what caused the problem and fix it by sending the correct settings to the device.

Mass configuration – Administrators can configure services and applications across their entire fleet of mobile devices.

Managing Mail for Exchange

Mail for Exchange settings such as the user's credentials and sync profile can be configured remotely with a compatible OMA Device Management solution. Over-the-air management capability helps to take the burden from mobile users to manually configure each device with the correct Microsoft Exchange server settings. Device management provides a powerful tool to large scale enterprise Microsoft Exchange ActiveSync email deployments.

Find more information on over-the-air device management solutions:

<http://europe.nokia.com/find-products/nokia-for-business/software/device-management>

Autodiscovery

This option is available if Exchange 2007 Server or later is being used. Autodiscover is a Microsoft feature that allows easier configuration of Mail for Exchange.

When Mail for Exchange is first launched, the user is prompted for email address and password (Symbian OS and Symbian Anna), username, password, domain and an access point (all other versions). If your environment is configured properly for Autodiscover, these are used to obtain the servername and other sync profile information. Otherwise, manual entry of this information is required, which means you will have to provide this information to your users.

Visit <http://technet.microsoft.com> and search: 'configure autodiscover Exchange ActiveSync'

6. Security considerations

Exchange allows you to configure security policies that apply to mobile devices. For example, you can enable the device lock and set the lock code parameters. As there are differences between Nokia smartphones with regard to these parameters, the following sections explain the differences and your options for configuration.

See Appendix for the current set of Exchange Server Security Policies supported by Mail for Exchange.

Are your devices 'provisionable'?

Devices capable of enforcing security policies are termed 'provisionable'.

As a general guide:

- All Nokia Eseries smartphones
- All S60 3.2.3 and 5.0 smartphones
- All Symbian OS smartphones

Mail for Exchange with Exchange 2003 SP2

Provisionable devices:

Mail for Exchange can enforce all Exchange 2003 SP2 security policies, when installed on a provisionable device.

It is also possible for the admin to remotely wipe a provisionable device. This will restore the device to factory settings and erase the memory card. With Exchange 2003 the Microsoft Exchange ActiveSync Mobile Administration Web Tool must be downloaded from technet.microsoft.com (search: 'Microsoft mobile administration tool') and installed to perform remote wipe operations.

Non-provisionable devices:

If you wish to support Nokia smartphones that cannot enforce security policies, there is a setting called 'Allow access to devices that do not fully support password settings' in the Exchange System Manager (see Mobile Services>General tab>Device Security button). This must be set or synchronisation will not be allowed by the server.

View details/screenshots <http://technet.microsoft.com> and search: 'configure and manage mobile device access on the exchange server'.

In the same Exchange System Manager dialogue box, it's also possible to allow specific users of non-provisionable devices by specifying an exception list. This is a list of user accounts that are exempt from security enforcement. See Exchange Server documentation for details.

Mail for Exchange with Exchange 2007 (no SP)

Provisionable devices:

Mail for Exchange can enforce all Exchange 2007 security policies, when installed on a provisionable device.

It is possible for the admin to remotely wipe a provisionable device. Mail for Exchange responds to the wipe command by restoring the device to factory settings and erasing the memory card. It is also possible for the user to remotely wipe a provisionable device. Remote wipe is performed via the Outlook Web Access (OWA) interface.

Non-provisionable devices:

If you wish to use a Nokia smartphone that cannot enforce security policies, there is a setting in the same dialogue box as where other policies are set. It's labelled 'Allow non-provisionable devices'.

Mail for Exchange with Exchange 2007 SP1 and later

Provisionable devices:

Exchange 2007 SP1 has added many security policies. A Nokia smartphone with S60 3.2.3 (or later) may be required to take advantage of some policies. With Exchange 2007, groups of users can have separate policies, so you can have a group of all Nokia users with different policies.

It is possible for the admin to remotely wipe a provisionable device. Visit <http://technet.microsoft.com> and search: 'how to perform a remote wipe on a device'. Mail for Exchange responds to the wipe command by restoring the device to factory settings and erasing the memory card. It is also possible for the user to remotely

wipe a provisionable device. This will restore the device to factory settings and erase the memory card. Remote wipe is performed via the OWA interface.

Non-provisionable devices:

If you wish to use a Nokia smartphone that cannot enforce security policies, there is a setting in the same dialogue box (see Mobile Services>General tab) where other policies are set. It's labelled 'Allow non-provisionable devices'.

Visit <http://technet.microsoft.com> and search: '2007 Understanding Exchange ActiveSync mailbox policies'.

Remotely wiping devices

In Exchange Server Administration you can select the option to enable remote wiping of device memory and memory card. Visit <http://technet.microsoft.com> and search: 'understanding remote device wipe'.

For a remote wipe to be successful, the 'lost' phone must still have connectivity to the server as the device needs to be able to receive the wipe command. This is true for all ActiveSync clients, including Mail for Exchange. The wipe command is received the next time the device and the server communicate.

There are some situations that may affect device wipe:

Lost phone is turned off – Wipe command cannot be received and data cannot be accessed. When the device is powered up and next makes communication with the server it will receive the wipe command.

Lost phone is out of coverage (or in offline mode) – Wipe command cannot be received, but data can be accessed until the device lock timeout expires. Make sure the device lock timeouts are set low enough to protect data. When the device is next able to communicate with the server it will receive the wipe command. Nokia recommends a relatively short device lock timeout to mitigate the above situation.

Lost phone has SIM replaced – This requires a reboot. On boot, if device lock is enforced the data cannot be accessed without the lock code. If Mail for Exchange detects the same carrier's SIM card it will receive the wipe command when the device next communicates with the server. However, if there's a different carrier's SIM card, Mail for Exchange may not be able to communicate with the server and cannot receive the wipe command. If a wireless access point was being used and the device comes within range of the defined Wi-Fi access point, it will receive the wipe command.

Lost phone is booted with SIM card removed (or in offline mode) – This requires reboot. On boot, if device lock is enforced, data cannot be accessed without the lock code. No new data will be synchronised with device. Mail for

Exchange is unable to communicate with the server so cannot receive the wipe command.

Security unlock code input incorrectly by end user – When keypad lock is activated, administrators can set devices to carry out a local wipe after a given number (usually three to five) of failed attempts to unlock the keypad. So it's important that end users remember their security code.

Wipe has different meanings for provisionable and non-provisionable devices. For provisionable devices, the phone is restored to factory state. This means after wipe it will behave as if it is being powered on for the first time. As such, all data and applications will be lost and the contents of the memory card will be deleted. For non-provisionable devices, the data being synchronised is also removed from the device.

The server will continue to send the 'wipe' command until instructed otherwise by the user or administrator. This means that if the device is recovered and partnered with the server it will be wiped again.

Using SSL certificates

Most admins will use secure sockets layer (SSL) and will have installed a certificate on their Internet Security and Acceleration (ISA) Server as well as their Exchange Server. Installing a certificate that is also pre-installed on the Nokia smartphone is recommended. The list of preinstalled certificates may vary by device. See the 'certificate management list' (in 'security settings') or details in the user guide for the device. If a certificate from this list (established certificate authorities) is used, you will not have to distribute and install certificates on all managed devices, which will save time and reduce support costs.

Usage of self-created certificates is possible, but not highly recommended, since they are very difficult to support.

Using Certificate-Based Authentication (CBA) with Symbian Anna smartphones

In most Exchange environments, Basic Authentication is required; meaning the server requests and the client submits a username and password. To support this, the credentials are stored on the device and sent over the air, usually encrypted via SSL (highly recommended), during authentication.

Client certificate-based authentication is used in more secure environments. During setup, in addition to the user's credentials, a digital certificate is used to verify an identity. After setup, the credentials are removed from the client and only the certificate is used for authentication. Access to the server is controlled not

only by the mailbox permissions, but by the validity of the certificate. Certificates are valid for a defined period and may also be revoked.

To use certificate-based authentication with Nokia smartphones with Symbian Anna software, a certificate specific to each user must be requested by the user and installed in the Exchange environment and on the Nokia smartphone.

Overview

Certificate-based authentication uses a digital certificate in addition to the user name and password to verify the identity. A digital certificate consists of two components: the private key that is stored on the Nokia smartphone and the public key that is installed on the Exchange server. If you configure Exchange 2010 to require certificate-based authentication for Exchange ActiveSync, only devices that meet the following criteria can synchronise with Exchange 2010:

- The device has a valid client certificate installed that was created for user authentication.
- The device has a trusted root certificate for the server to which the user is connecting to establish the SSL connection.

To learn more about certificated-based authentication and how to deploy it within your Exchange environment, contact your Microsoft Support representative or review the documents on Microsoft TechNet.

Visit <http://technet.microsoft.com> and search: 'How to Configure Certificate-Based Authentication for Exchange ActiveSync'.

Pre-requisites

- Your Exchange server environment is configured properly for client certificate authentication, including Exchange settings and certificate authority.
- (OPTIONAL) You have downloaded the latest version of Nokia Configuration Tool (NCT) that supports certificate transfer. NCT can be downloaded here: <http://europe.nokia.com/support/download-software/nokia-configuration-tool>.
- You have Nokia smartphones with Symbian Anna software with Mail for Exchange that supports CBA.

Steps to set up CBA

In general, setup of CBA involves the following steps:

1. Export the user certificate from the Exchange server
2. Import the authentication certificate to the device
3. Initiate synchronisation with Mail for Exchange

Exporting the user certificate from Exchange

Export the certificate from Exchange in a file format that is compatible with Nokia smartphones.

Compatible format details here:

http://www.forum.nokia.com/info/sw.nokia.com/id/a60ed5ab-c2fc-486c-89d0-2695b67ffec4/Installing_Certificates_to_S60_3rd_Edition_Devices_v1_1_en.pdf.html.

Importing the authentication certificate to the device

There are two ways to import the authentication certificate from the Exchange server to the device. The recommended method is to use the Nokia Configuration Tool. Alternatively, you may use manual steps to copy the certificate to the smartphone.

When using the Nokia Configuration Tool, the tool will provide detailed instructions to guide you on installing the certificate on the device.

If you choose to use the manual process to install the certificate the following steps should be followed.

1. Copy the certificate file to the device while the smartphone is connected to a PC in Mass storage mode, or by using a removable memory card.
2. Browse to the certificate file using the File Manager application on the smartphone and select the file.
3. When prompted for the location, choose 'Personal' for best user experience.
4. If nothing occurs, the file is probably in the wrong format. You should try the process again by re-exporting the user certificate from the Exchange server.

Synchronisation

If the certificate was manually imported, it's necessary to launch Mail for Exchange and create a mailbox profile.

If the certificate and settings were provisioned via the Nokia Configuration Tool, launch the Mail for Exchange settings and provide the credentials and, depending on the version of Mail for Exchange, the access point (under Advanced settings).

In both cases, after creating the profile the initial sync will start. When Mail for Exchange determines that CBA is required and configured properly, the credentials will be removed from the device. The Mail for Exchange settings will reflect CBA being used for authentication by showing that username and password are not required.

7. Arranging connectivity

Make Exchange Server accessible from the Internet

Make sure port 443 is open on your firewall. If your company uses Outlook Web Access, port 443 is most likely already open. It is possible to use other port numbers, but 443 is the default for SSL.

Make sure the Domain Name System (DNS) server for your network returns a single, externally routable address to the Exchange ActiveSync server for both intranet and internet clients. This is so the device can use the same IP address for communicating with the server when both types of connections are active.

Verify that a server certificate is installed on the front-end Exchange server. Then in the Authentication Method properties, turn on basic authentication (only) to require an SSL connection to the Microsoft Server ActiveSync directory of your IIS.

Verifying that Exchange ActiveSync is enabled

Exchange 2003 SP2 – To enable these features at an organisational level visit <http://technet.microsoft.com> and search: 'how to enable and disable Exchange ActiveSync features at the organisational level'.

Exchange 2007 and later – ActiveSync should be enabled by default when you have installed the client access server (CAS) role. To verify or enable ActiveSync visit <http://technet.microsoft.com> and search: 'how to enable Exchange ActiveSync'.

Publishing Exchange Server via ISA 2006 (optional) – If you are already using Outlook or other Exchange clients, this step may not be necessary. Otherwise, you will have to publish Exchange. This means creating both a web listener as well as an Exchange web client access publishing rule.

To get started visit <http://technet.microsoft.com> and search: 'publishing Exchange Server with ISA Server 2006'.

It's important to verify that a server certificate is installed and to update the public domain name system (DNS) to properly resolve incoming connections. ISA 2004 can also be used.

8. Installing and configuring Mail for Exchange

Installing

On many recent Nokia smartphones, Mail for Exchange is preloaded. However, configuration still needs to be performed using the email 'wizard' on the device. Please consult your device's user guide and the Configuring section below for further instructions.

For older devices, the latest version of Mail for Exchange may be available via the ovi store on the Internet or via the ovi application on the device. After accessing the ovi store, search for 'Mail for Exchange', and the latest version of Mail for Exchange that is recommended for the device will be available for download and installation.

Upgrading

Latest Nokia smartphones are updateable via over-the-air download. When Nokia provides an updated application or firmware, the Software Update application on the device will prompt users to download. Alternatively, users can launch the Software Update application on their device to check if new updates such as Mail for Exchange are available for download.

On older devices, the updated version of Mail for Exchange can be installed without uninstalling the previous version, in most cases. Refer to the Mail for Exchange release notes <http://europe.nokia.com/get-support-and-software/download-software/mail-for-exchange/compatibility-and-download> for exceptions.

Configuring mailbox

Unless you will be configuring the device for your users, you will have to share the information with them so they can configure it. The following mandatory settings are required:

Mail for Exchange integrated on the smartphone

- Email address
- Password
- Domain*
- *Server name**

*Needed only if Autodiscover is not configured on the server.

Installable Mail for Exchange application

- Username
- Password
- Access point
- Domain
- SSL settings
- *Server name**

*Needed only if Autodiscover is not configured on the server.

There are also a number of optional settings with recommended default values. You may want to inform your users of your preferences.

For larger deployments Nokia provides a PC-based tool called the Nokia Configuration Tool (NCT) which can be used to pre-configure your Nokia smartphones before deploying to your users. For more information on the Nokia Configuration Tool, visit <http://europe.nokia.com/find-products/nokia-for-business/device-management>.

There are third party solutions available for pushing settings to users via the Open Mobile Alliance Device Management (OMA-DM) and Client Provisioning (OMA-CP) standards. Information about compatible device management solutions can be found by visiting <http://europe.nokia.com/find-products/nokia-for-business/device-management>.

9. How should I proceed?

Determining which steps to follow when setting up and configuring Mail for Exchange depends on your readiness to deploy devices. We've grouped the steps into three main scenarios.

Case 1 – You are an Exchange admin currently using other ActiveSync clients

1. Verify your SSL Certificate
2. Consider your security policies
3. Install and configure Mail for Exchange
4. Optionally configure your Open Mobile Alliance Device Management (OMA-DM) solution to remotely configure your Nokia smartphones

Case 2 – You are an admin using Exchange 2003 SP2 or later with no mobile devices

1. Make Exchange accessible from the internet
2. Optionally configure Autodiscover
3. Consider your security policies

4. Install and configure Mail for Exchange
5. Optionally configure your Open Mobile Alliance Device Management (OMA-DM) solution to remotely configure your Nokia smartphones

Case 3 – You are an admin not yet using Exchange

1. Purchase and prepare your Exchange Server environment

View details of server operating system and hardware requirements for Exchange at <http://www.microsoft.com/exchange/en-us/default.aspx> and search: 'Exchange system requirements'. Find out more about ISA 2006 and its benefits <http://technet.microsoft.com> and search: 'ISA 2006'. View details of ISA operating system and hardware requirements by visiting <http://technet.microsoft.com> and search: 'ISA server 2006 system requirements'.

2. Make Exchange accessible from the internet
3. Optionally configure Autodiscover
4. Consider your security policies
5. Install and configure Mail for Exchange
6. Optionally configure your Open Mobile Alliance Device Management (OMA-DM) solution to remotely configure your Nokia smartphones

10. Best practices

Use SSL

Secure Sockets Layer (SSL) is a protocol that provides several layers of security for users of a web server. It encrypts data between the device and the server. This ensures that if the data is intercepted it cannot be interpreted. It also prevents data from being changed or replaced between the client and server. This requires installation of a certificate on the server.

Enable device lock policies

Policies are enforced to Mail for Exchange users through the ActiveSync connection. Policies cannot be disabled by the mobile user.

As an Exchange Administrator your tasks include Create Exchange ActiveSync Mailbox Policy and/or Add Mail for Exchange users to Exchange ActiveSync Mailbox Policy.

These are the Exchange ActiveSync Mailbox Policy options to configure device lock:

- Require a password for device lock
- Require alphanumeric password

- Minimum password length
- Prevent simple passwords
- Track password history
- Password expiration days
- Maximum inactivity timeout
- Maximum password attempts
- Local wipe after maximum attempts

Visit <http://technet.microsoft.com> and search: 'understanding Exchange ActiveSync mailbox policies'.

In Exchange 2007 (and later) groups of users can have separate policies. See Appendix for the list of Exchange security policies supported by Mail for Exchange.

For more information about security on Nokia smartphones, please see <http://europe.nokia.com/find-products/nokia-for-business/security>.

Verify network configuration

In the Authentication Method properties, you should verify that a server certificate is installed on the front-end Exchange server and then turn on basic authentication only. This requires an SSL connection to the Microsoft Server ActiveSync directory of your internet information services (IIS).

Understanding device logging

Mail for Exchange does not display a specific error message for errors that are not commonly encountered, have an unclear solution or a known complex solution. Instead, these errors are logged to files on the device.

The admin logs are located in the \MailForExchange directory. These logs can be viewed by using the device's File Manager application or by moving them via data cable or Bluetooth® to a PC. You may even ask your users to email them to you if possible. Many HTTP and GPRS errors are visible in these logs. If you need help interpreting these admin logs, please contact Nokia for support or visit the Nokia support discussion forum.

Appendix – Supported Exchange Server Security Policies

Server version where introduced	Category	Description	Value
2003 SP2	General policies	This setting defines how frequently the mobile phone updates the Exchange ActiveSync policy from the server.	Policy refresh interval
2003 SP2	Password policies	This setting specifies how many times an incorrect password can be entered before the mobile phone performs a wipe of all data.	Maximum failed password attempts
2003 SP2	Password policies	This setting specifies the length of time that a mobile phone can go without user input before it locks.	Maximum inactivity time lock
2003 SP2	Password policies	This setting specifies the minimum password length.	Minimum password length
2003 SP2	Password policies	This setting enables the mobile phone password.	Password enabled
Exchange 2007	Password policies	This setting enables or disables the ability to use a simple password such as 1234. The default value is \$true.	Allow simple password
Exchange 2007	Password policies	This setting enables the administrator to configure a length of time after which a mobile phone password must be changed.	Password expiration
Exchange 2007	Password policies	This setting specifies the number of past passwords that can be stored in a user's mailbox. A user can't reuse a stored password.	Password history
Exchange 2007	Password policies	This setting specifies whether the storage card must be encrypted. Not all mobile phone operating systems support storage card encryption. For more information, see your mobile phone and mobile operating system.	Require storage card encryption
Exchange 2007	Sync policies	This setting enables attachments to be downloaded to the mobile phone.	Attachments enabled
Exchange 2007	Sync policies	This setting specifies the maximum size of attachments that are automatically downloaded to the mobile phone.	Maximum attachment size
Exchange 2007 SP1	Advanced policies	This setting specifies a list of applications that cannot be run in ROM.	Unapproved InROM application list
Exchange 2007 SP1	Device policies	This setting specifies whether a mobile phone allows Bluetooth® connections. The available options are Disable, HandsFree Only, and Allow.	Allow Bluetooth®
Exchange 2007 SP1	Device policies	This setting specifies whether the mobile phone camera can be used.	Allow camera
Exchange 2007 SP1	Device policies	This setting specifies whether the mobile phone can synchronise with a computer through a cable, Bluetooth® or IrDA connection.	Allow desktop sync
Exchange 2007 SP1	Device policies	This setting specifies whether the mobile phone can access information that's stored on a storage card.	Allow storage card
Exchange 2007 SP1	Device policies	This setting specifies whether wireless Internet access is allowed on the mobile phone.	Allow Wi-Fi
Exchange 2007 SP1	General policies	This setting enables access to files that are stored on Windows file share (UNC) shares.	UNC file access
Exchange 2007 SP1	General policies	This setting enables access to files that are stored in Microsoft Windows SharePoint Services document libraries.	WSS file access
Exchange 2007 SP1	Password policies	This setting requires that a password contains numeric and non-numeric characters.	Alphanumeric password required
Exchange 2007 SP1	Password policies	This setting enables encryption on the mobile phone. Not all mobile phones can enforce encryption. For more information, see the phone and mobile operating system documentation.	Device encryption enabled
Exchange 2007 SP1	Password policies	This setting specifies the minimum number of complex characters required in a mobile phone password. A complex character is any character that is not a letter.	Minimum device password complex characters
Exchange 2007 SP1	Password policies	This setting specifies whether device encryption is required. If set to \$true, the mobile phone must be able to support and implement encryption to synchronise with the server.	Require device encryption
Exchange 2007 SP1	Sync policies	This setting specifies the maximum range of calendar days that can be synchronised to the mobile phone. The value is specified in days.	Maximum calendar age filter
Exchange 2007 SP1	Sync policies	This setting specifies the maximum number of days' worth of email items to synchronise to the mobile phone. The value is specified in days.	Maximum email age filter
Exchange 2007 SP1	Sync policies	This setting specifies the size beyond which HTML-formatted email messages are truncated when they are synchronised to the mobile phone. The value is specified in kilobytes (KB).	Maximum HTML email body truncation size
Exchange 2007 SP1	Sync policies	This setting specifies the size beyond which email messages are truncated when they are synchronised to the mobile phone. The value is specified in kilobytes (KB).	Maximum email body truncation size
Exchange 2007 SP1	Sync policies	This setting specifies whether the mobile phone must synchronise manually while roaming. Allowing automatic synchronisation while roaming will frequently lead to larger-than-expected data costs for the mobile phone plan.	Require manual synchronisation while roaming