guide for administrators

Mail for Exchange for Nokia devices with Microsoft Exchange ActiveSync

NOKIA
Connecting People

Nokia for Business

Contents

1. INTRODUCTION

Mail for Exchange is the Nokia implementation of ActiveSync. A large part of the total solution is Microsoft Exchange, so previous experience with Exchange and other ActiveSync clients is helpful.

This guide is for administrators who need to increase their understanding of Nokia's implementation of ActiveSync. It will also improve admins' experience of Mail for Exchange, which means fewer support issues, higher security, longer battery life, better user experience and enhanced connectivity. The number of steps required depends on your previous experience and current use of ActiveSync devices.

In this guide, there are three main scenarios, presented as 'cases':

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

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

Case 3 – You are an admin not using Exchange yet

Supported servers

Microsoft Exchange 2003 Service Pack 2 (SP2)

Microsoft Exchange 2007

Microsoft Exchange 2007 SP1

Key features for admins

Security (SSL, device lock and device wipe)

Policies and settings to reduce bandwidth

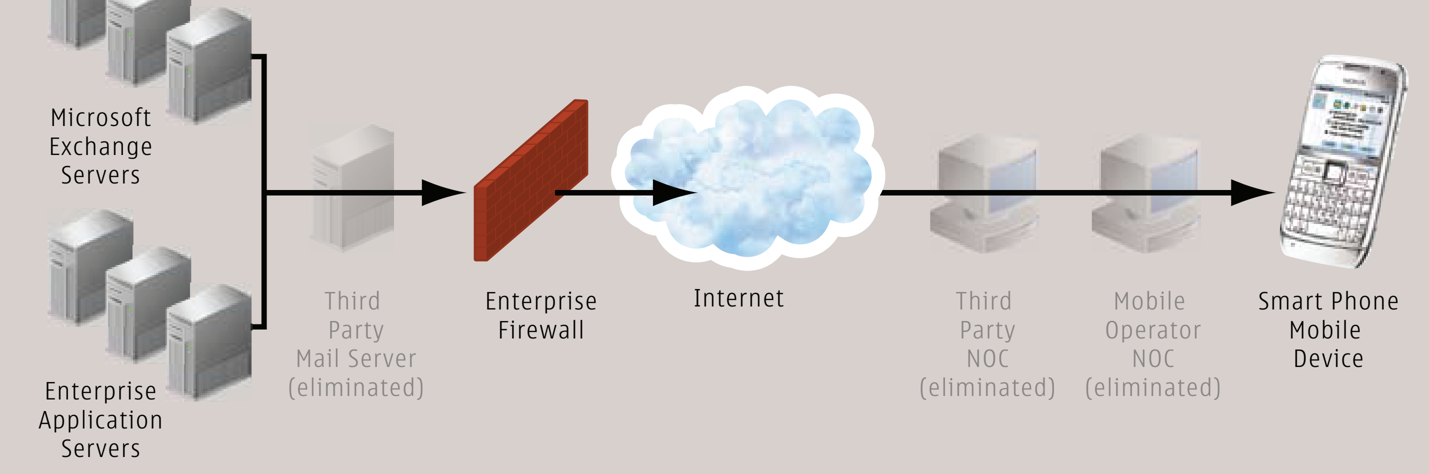
Supported by Nokia

Things to consider

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?

Nokia Mail for Exchange leverages a company's existing Microsoft infrastructure and does not require third-party middleware, gateways, a network operations centre or complicated configurations.


Microsoft Exchange Servers
Enterprise Application Servers
Third Party Mail Server (eliminated)
Enterprise Firewall
Internet
Third Party NOC (eliminated)
Mobile Operator NOC (eliminated)
Smart Phone Mobile Device

2. CASE 1 – YOU ARE AN EXCHANGE ADMIN CURRENTLY USING OTHER ACTIVESYNC CLIENTS

This is the simplest scenario, which includes the following issues:

2.1 Verifying your SSL Certificate

Most admins will use secure sockets layer (SSL) and will have installed a certificate on internet security and acceleration (ISA) and Exchange.

ⓘ *Installing a certificate that is also pre-installed on the Nokia device 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.

ⓘ Available from established certificate authorities, if a certificate from this list is used, you will not have to distribute and install certificates on all managed devices, which will save time and reduce support costs.

Warning – using self-created certificates is possible, but very difficult to support.

2.2 Consider your security policies

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 devices with regard to these parameters, please consider points 2.2.1 to 2.2.4 when partnering with Nokia devices.

2.2.1 Are your devices ‘provisionable’?

Devices capable of enforcing security policies are termed ‘provisionable’.

As a general guide:

- Eseries devices are provisionable
- Nseries devices previous to S60 3.0 Feature Pack 2 (FP2) are not provisionable
- Nseries devices after S60 3.0 FP2 may be provisionable
- Supported devices not designated Eseries or Nseries may or may not be provisionable

2.2.2 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 Administation Web Tool must be downloaded from technet.microsoft.com and search:
‘Microsoft mobile administration tool’ and then installed to perform remote wipe operations.

Non-provisionable devices:

If you wish to support Nokia devices 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 synchronization will not be allowed by the server.

ⓘ View details and screenshots http://technet.microsoft.com and search:
‘configure and manage mobile device access on the exchange server’

In the same Exchange System Manager dialog 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.

2.2.3 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 device that cannot enforce security policies, there is a setting in the same dialog as where other policies are set. It’s labeled ‘Allow non-provisionable devices’.

2.2.4 Mail for Exchange with Exchange 2007 SP1

Provisionable devices:

Exchange 2007 SP1 has added many security policies. For the latest list of supported policies, see the Mail for Exchange release notes.

ⓘ A Nokia device with Series 60 3rd Edition Feature Pack 2 (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 device that cannot enforce security policies, there is a setting in the same dialog box (see Mobile Services>General tab) where the other policies are set. It’s entitled ‘Allow non-provisionable devices’.

ⓘ Visit http://technet.microsoft.com and search:
‘2007 Understanding Exchange ActiveSync mailbox policies’

2.3 Battery life – understanding the impact of your network and operator

Mail for Exchange supports Microsoft Direct Push and uses this during 'always on' connections. Here's 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 reestablishes the connection if and when necessary. The server sends notifications about new items over this connection and the client synchronizes to get the new items."

Visit http://technet.microsoft.com and search: 'understanding direct push'

The link above has 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, but 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.

Latest version of Mail for Exchange detects low heartbeat intervals and synchronises until the interval is optimised.

With Exchange 2007 there are alerts generated when heartbeat is too low: http://technet.microsoft.com/en-us/library/bb218291(EXCHG.80).aspx

2.3.1 Operator impact

There is one issue that can have a negative impact on heartbeat interval (and battery life) that can't be overcome by Mail for Exchange, ISA, Exchange or firewall settings.

The access point your operator has provided for general web use (browsing, WAP, etc.) may not be optimized for Direct Push. The operator 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 'Always on', Mail for Exchange reconnects to the network. This uses a relatively high amount of battery power.

However, the same carrier 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 synchronizing.

For all firewalls and network appliances, set the idle session timeout to 30-45 minutes. This will ensure that your clients get higher heartbeat intervals.

2.4 Understand 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. http://discussions.europe.nokia.com/discussions/

2.5 Installing Mail for Exchange and configuring

2.5.1 Installing

On many recent Nokia devices, Mail for Exchange is preloaded, which means that the installation file is already on the phone from the factory.

However, installation still needs to be performed using an email 'wizard'. Please consult your device's user guide for further instructions.

View the product specific installation guide www.nokia.com/email

The latest version of Mail for Exchange may be available via the Download! application on your device. After refreshing the catalogue, the latest version of Mail for Exchange that is recommended for the device will be available for download and installation.

Please note that in the most advanced models, such as Nokia E75, Nokia E55 and Nokia E52, there's an advanced email client that supports ActiveSync protocol. For these devices, no separate client is required. The set-up procedure is initiated by inputting your server settings and credentials into the set-up wizard on the device homescreen.

2.5.2 Upgrading

On recent Nokia devices, Mail for Exchange may be updateable. After refreshing the catalogue (by opening the Download! menu, selecting Options > Refresh list), the latest version of Mail for Exchange that is recommended for the device will be available for downloading and installation.

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.

Please note that the latest models, such as Nokia E75, Nokia E55 and Nokia E52, have a dedicated upgrade mechanism and the clients from Download! Service are not compatible and do not work on these devices.

2.5.3 Configuring

Unless you will be configuring the device for your users, you will have to share the information with them so they can configure it.

If Autodiscover is configured properly on the server, you will have to provide the following mandatory settings to users:

- username
- password
- access point
- domain (in some configurations)
- SSL settings (particularly if SSL is not currently used)

If Autodiscover is not configured properly on the server, you will also have to provide:

- server name

There are also a number of optional settings with recommended default values. You may want to inform your users of your preferences, notably for the setting 'sync while roaming'.

Alternatively, there are some Nokia (www.nokia.com/business) and third party solutions available for pushing settings to users.

For larger deployments, a compatible device management solution is recommended (see next section 2.6).

2.6 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.

Applications such as personal information synchronization, 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.

2.6.1 Open Mobile Alliance (OMA) standardization

Nokia uses OMA standardized device management technology and has been active in OMA standardization 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.

2.6.2 Managing Mail for Exchange

Mail for Exchange settings such as server name, domain name, username 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 an essential 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

3. CASE 2 – YOU ARE AN ADMIN USING EXCHANGE 2003 SP2 OR LATER WITH NO MOBILE DEVICES

Most of this section relates to configuring your environment for ActiveSync. There are links to a number of Microsoft TechNet pages that provide help for ActiveSync clients, including Mail for Exchange.

3.1 Make Exchange 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) 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.

3.2 Verify that Exchange ActiveSync is enabled

Exchange 2003 SP2

To enable these features at an organizational level visit http://technet.microsoft.com and search:
'how to enable and disable Exchange ActiveSync features at the organizational level'

Exchange 2007

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'

3.3 Publish Exchange via ISA 2006 (optional)

If you are not using ISA you can ignore this section.

If you are already using Outlook or other Exchange clients, this 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 2007 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.

3.4 Configure Autodiscover (optional)

This option is available if Exchange 2007 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, username, password, domain and an access point. If your environment is configured properly for Autodiscover, these are used to obtain the servername. Otherwise, manual entry of the servername is required, which means you will have to provide this information to your mobile users.

Visit http://technet.microsoft.com and search:
'configure autodiscover Exchange 2007 ActiveSync'

3.5 Next steps

All the Mail for Exchange considerations are provided in Section 2 (Case 1).

4. CASE 3 – YOU ARE AN ADMIN NOT USING EXCHANGE YET

To get started there are certain hardware and software requirements, including purchasing servers, installing the correct Windows server operating system, installing Exchange and getting familiar with Mail for Exchange.

There are entire books devoted to planning and constructing an Exchange environment. This section is not a substitute for these, but it will help administrators to get started.

This section references Microsoft TechNet articles to help you get started, but it may be necessary to consult Microsoft if you have detailed queries.

4.1 Obtain and prepare your server environment

You will have to install the correct Windows Server OS and then install Exchange. This section assumes that you will use Exchange 2007.

View details of server operating system and hardware requirements for Exchange at http://technet.microsoft.com and search:
'Exchange 2007 system requirements'

Find out more about ISA 2006 and its benefits at http://technet.microsoft.com and search:
'ISA 2006'

View details of ISA operating system and hardware requirements http://technet.microsoft.com and search:
'ISA server 2006 system requirements'

From here, follow the installation guides provided by Microsoft.

4.2 Next steps

Enable ActiveSync by following the instructions in Section 3 (Case 2).

Review the Mail for Exchange considerations provided in Section 2 (Case 1).

5. BEST PRACTICE (IN ALL CASES)

5.1 Using 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. See Section 2.1 for more information.

5.2 Enable device lock policies

Policies are enforced to Mail for Exchange clients 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 groups of users can have separate policies. See Section 2.2 for more information about policies.

For more information on security on Nokia devices, please see www.nokia.com/business

5.3 How to wipe your 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.

We recommend 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 wifi 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 syncronised with device. Mail for Exchange is unable to communicate with the server so cannot receive the wipe command.

- Security unlock code incorrectly inputted 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.

5.4 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).

Work together. Smarter.

Nokia Corporation
P.O.Box 100, FI-00045
Nokia Group, Finland
Tel. +358 7180 08000
Fax +358 7180 34003

www.nokia.com/business

NOKIA
Connecting People