

Mail for Exchange

Security Overview

NOKIA
Connecting People

Data sheet

Our global economy is changing the way people in many professions work. Increasingly, they are spending less time at their desks and more time in meeting rooms collaborating with colleagues, out of the office with their customers or business partners, and seeking new opportunities with travel to other cities or overseas. It's estimated that there will soon be one billion mobile workers. So today's business challenge is to seamlessly free people from their desktop technologies in a way that helps them remain productive while also being cost effective. The solution is Mail for Exchange.

Mail for Exchange uses Microsoft® Exchange ActiveSync® data synchronisation technology to push information to Nokia devices. Read more about Mail for Exchange business email solution at www.nokia.com/mailforexchange.

When implementing a business mobility solution, security and reliability are top considerations for business professionals and enterprise IT decision makers. Mail for Exchange includes several measures to safeguard business professionals' and consumers' confidential information on their Nokia devices.

Secure network connection

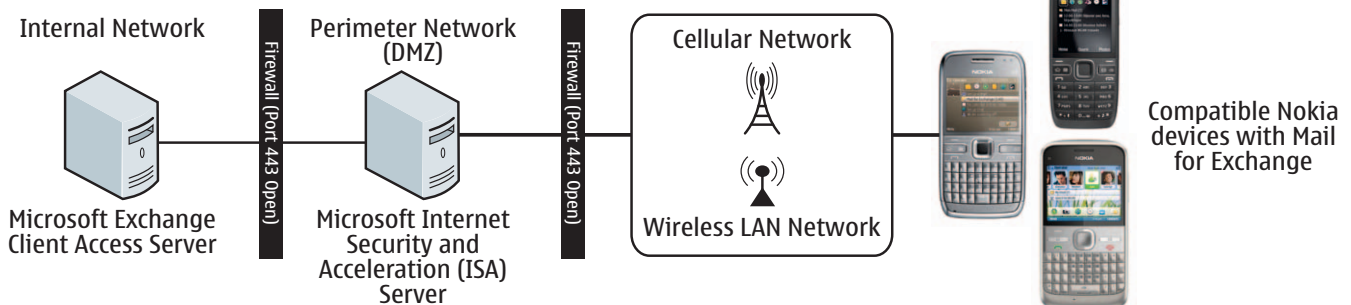
Mail for Exchange supports the use of Secure Sockets Layer (SSL)/Transport Layer Security (TLS) authentication and data encryption to establish a secured end-to-end https connection between a Microsoft Exchange front-end server and a Nokia device. Because Mail for Exchange is a direct access solution, data is routed directly from email server to user Nokia device. Security certificates from leading Certificate Authorities (CA) are preloaded in Nokia smartphones. These include: Baltimore,

Entrust.net, Equifax, GeoTrust, GlobalSign, Go Daddy, GTE, S60 Nokia Online CA, Starfield, Thawte, ValiCert, and VeriSign. Additionally, an enterprise has the option to use its own self-signed certificate.

Mail for Exchange connection can also be tunnelled through mobile VPN. Nokia Mobile VPN client, which is preloaded in our Nokia Eseries smartphone range, uses Internet Protocol Security (IPSec) standard, and is compatible with Alcatel-Lucent VPN Gateways, Check Point VPN-1 NGX, Cisco ASA, Nokia IP VPN and VPN Concentrator Gateway, and Nokia Siemens Networks I-WLAN Solution.

Device control and policies

Microsoft Exchange Server administrators can enforce security policies to Mail for Exchange users with compatible Nokia devices to ensure that confidential corporate information is protected. In addition to Nokia Eseries, many Nokia devices support Terminal Administration Rights Model (TARM) which enables key security policies to be enforced.



To give an Exchange Server administrator control of the user devices, a comprehensive set of Microsoft Exchange ActiveSync policies are supported with compatible Nokia devices, including:

- Required device lock password
- Required alphanumeric password
- Minimum password length
- Prevention of simple passwords
- Track password history
- Password expiration days
- Maximum inactivity timeout
- Maximum password attempts
- Wipe data after maximum number of password attempts
- Remote wipe* of device memory and memory card
- Device policy refresh
- Control non provisionable devices access
- Allow attachments to be downloaded on the device
- Allow HTML email viewing
- Allow synchronisation while roaming
- Set maximum attachment size (kB)
- Maximum calendar age filter
- Maximum email age filter
- Maximum email body truncation size

*Confirmation email is generated on successful wipe.

Enterprises that need specific additional policies or want to manage Mail for Exchange policies with a device management system instead of Exchange Server can implement Open Mobile Alliance (OMA) standards-based device management solutions. Solutions compatible with Nokia devices include: Fromdistance, HP MDM, InnoPath, Mformation, Nokia Siemens Networks, Perlego, Smith Micro, and Sybase Afaria. Read more about device management at www.nokia.com/business.

Device data protection

Protecting both business and personal data stored on a mobile device or in-transit is important. Nokia devices support a number of security measures to prevent unauthorised access of confidential data.

Device lock

Nokia smartphones support the use of device lock codes to prevent unauthorised use of the mobile device. The user has the option to automatically lock the device when it has not been used for a defined time. Furthermore, the user has the option to trigger remote phone locking via a predefined text message, should the device be lost or stolen.

An IT administrator can mandate the use of device lock through the ActiveSync mailbox policy or via a compatible OMA device management server to configure and manage device and lock policies remotely.



To prevent use of the device with an unauthorised SIM card, it can be set to prompt for a phone lock code whenever a different SIM card is inserted.

Encryption

Nokia Eseries smartphones have an on-board dedicated crypto co-processor that performs hardware-accelerated AES 256 + XTS encryption on data in the phone memory, as well as the memory card.

Encrypting the data is a powerful option to protect against device theft or loss. Once the user encrypts the data stored on the phone memory or memory card, unauthorised access via a memory card reader on a PC is not possible.

Data wipe

A remote wipe of data stored in the device, in case of loss, is supported with Nokia devices implementing TARM. An IT administrator can issue a remote wipe command from a Microsoft Exchange Management Console or a compatible Device Management application. The user also has the option to issue the remote wipe command using Microsoft Outlook Web Access. Upon success, a notification is sent from the device to Exchange email confirming the wipe succeeded.

Similarly, support for local wipe after a predefined number of failed lock code attempts is available. All data stored on both the device memory and memory card are formatted and the device is restored to factory default settings.

Secure platform

Nokia smartphones use the Symbian operating system and implement Symbian Signed policy to prevent malware. Symbian Signed is a process whereby application developers need to submit their applications to the Symbian Foundation for signing before they can use the more sensitive features of the phone. In addition to Symbian Signed, the Nokia Symbian platform also uses established security principles like data caging and process separation.

An application whose origin is unknown (that is one which has not been signed) will not be able to access sensitive functionality of the phone and warning prompts are triggered to the user if an attempt is made to install such an application.

Symbian Signed policy effectively reduces the risk of virus attack on Nokia smartphones.

Mail for Exchange on Nokia smartphones offers enterprises and business professionals a highly secure and reliable mobile solution that enhances business efficiency and productivity.

See www.nokia.com/business for more information.

NOKIA
Connecting People