

Nexor Enforcer for Outlook 6.0

Building upon Nexor's experience of providing security solutions for mission critical communications around the world, Nexor Enforcer for Outlook implements the very latest in Internet security standards.

Enforcer combines three key technologies to ensure the secure electronic transfer of information within your organisation:

- **Security** – the cryptographic protection of the message
- **Role processing** – ensuring that all the people who need to be able to read the message can read the message
- **Access control** – ensuring that all the people the message is being sent to are allowed to receive the message

Enforcer extends the functionality of Microsoft Outlook and Nexor Defender for Outlook, allowing the user to continue to use the tools and interfaces with which they are familiar.

Product Features

Cryptographic Protection

Enforcer uses the S/MIME v3 standard to digitally sign and encrypt messages. Messages that are both signed and encrypted can be triple wrapped allowing intermediate gateways and mail list agents to process the secure message during its transfer.

Enforcer has been designed to be able to secure:

- Military messages in conjunction with Nexor Defender for Outlook
- Standard Outlook messages
- Any custom Outlook message.

Security Policy

Messages within an organisation may need to be classified, based on their content. Enforcer provides a configurable way to support organisational security policies. The security policy is defined in a standard format, in a Security Policy Information File (SPIF) [SDN801]. These SPIFs are:

- Signed to ensure the integrity of the policy
- Downloaded from a directory to allow the propagation of changes
- Used to determine the security label that can be applied by the user

Clearance Checking

Using the organisational security policy, together with a clearance assigned to individuals, Enforcer can perform an "access control" check to ensure that all the recipients are "cleared" to receive the message. This check can be performed on:

- Origination - to prevent the message being sent to recipients that are not appropriately cleared
- Reception – to ensure that recipients can not read messages they have received for which they are not cleared

Enforcer can also perform access controls on the originator of the message ensuring that they cannot create a security label for which they are not "cleared"

Message

Security Features

The message can be secured using the S/MIME version 3 [CMS] to provide:

Signature

- Non repudiation with proof of origin. This proves that a particular individual sent the message
- Content Integrity to ensure that no-one has tampered with the message
- Non repudiation with proof of receipt to prove that a particular individual has read the message

Encryption

- Content confidentiality to ensure that only the appropriate people can read the message

Enhanced Security Services

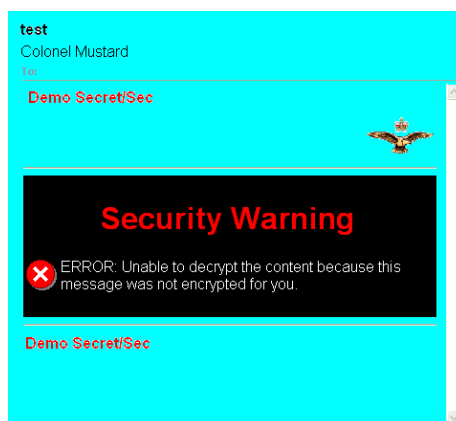
In addition to S/MIME v3, Nexor Enforcer for Outlook provides enhanced security services in accordance with [ESS].

These include:

- Security labels bound to the message
- Signed receipts - includes requests, generation and correlation
- Content hints to provide information about the protected message

Platforms

- Microsoft Outlook 2003 / 2007
- Windows 2003 / XP



connect transform protect

NEXOR®

Standards

- RFC3852 - Cryptographic Message Syntax [CMS]
- RFC2634 - Enhanced Security Services [ESS]
- RFC2251 - Lightweight Directory Access Protocol [LDAPv3]
- RFC3854- Securing X.400 Content with S/ MIME [X400WRAP]
- RFC3855- Transporting S/ MIME Objects in X.400 [TRANSPORT]
- SDN801 - Access Control Concept and Mechanisms (SDN.801)
- WP7 – Electronic Labelling of NATO Information [WP7]
- PKCS#12 - Personal Information Exchange Syntax Standard
- PKCS#11 - Cryptographic Token Interface Standard
- CAPI - Microsoft Cryptographic API

Product Features

Roles Based Messaging

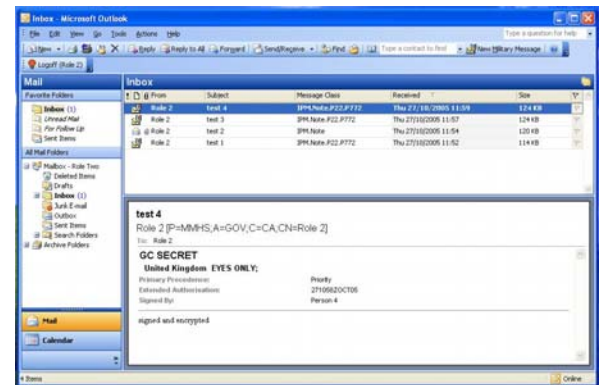
Within an organisation, if a message is addressed to a role, e.g. "Support Desk", then several people may need to be able to read the message. Enforcer will ensure that all the people who perform the role can read the message.

This role can be expanded to include:

- Alternate recipients – if the original recipient cannot be reached and the message is redirected by Nexor Overseer to another user.
- Gateways – that may need to be traversed in order to reach a recipient.

Message Preview and Printing

Enforcer supports the use of the Outlook message preview pane allowing secure messages to be displayed in a user customisable HTML format.



Content Encoding

Enforcer can be configured to encode messages using:

- X.400 to support STANAG 4406 Edition 2
- MIME to support S/MIME v3

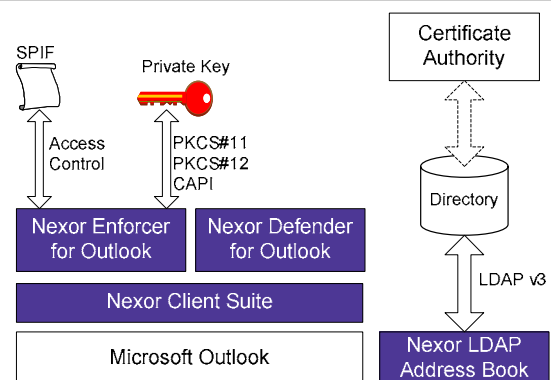
Policy

Enforcer can be configured to ensure that messages are signed and encrypted consistently within an organisation. This includes automatically signing or encrypting all messages or applying a signature or encryption based on the security classification of a message.

Product Architecture

Nexor client products share a common interface to Outlook ensuring that Enforcer closely integrates with the services of:

- Nexor Defender for Outlook which can immediately virus scan a message after it has been decrypted and will also display any military elements of service
- Nexor LDAP Address Book which provides a lookup service for E-mail addresses, Certificates, Certificate Revocation Lists and SPIFs using multiple servers and advanced caching for offline working.



Enforcer is not tied to any particular CA vendor or cryptographic service. It has been successfully integrated with:

- PKCS#11
- Microsoft CAPI
- Microsoft Certificate Services
- PKCS#12
- Entrust CA

www.nexor.com