HP PROTECTTOOLS EMAIL RELEASE MANAGER

Business white paper

HP ProtectTools Email Release Manager provides enhancements to the Microsoft Exchange and Outlook clients. HP has developed HP ProtectTools Email Release Manager in the UK, building on the existing successful relationships with Microsoft and CESG (Communications - Electronics Security Group), the UK National Technical Authority for Information Security.

HP has integrated email security components with the Outlook mail client providing the user interface, integration, implementation and support services.

HP ProtectTools Email Release Manager fits with the highly desirable HP COTS (Commercial Off The Shelf) products philosophy, which is to provide off-the-shelf enhancements to standard Microsoft products.

Minimum Impact on Users
Proof of Content Origin (POC0)
Classification Labelling
Release Authority
Central Control of Security Policy
Enhancement to existing Exchange and Outlook Clients
Identity Based Encryption Drive RMS through policy
Virus Throttling

Minimum Impact on Users has been achieved by only making minimal changes to the standard user interface. These changes have been tightly integrated with the Outlook client. The enhancements are made through a published API to prevent restrictions on the use of different Exchange and Outlook client versions.

Proof of Content Origin involves electronically signing your message as you send it so that the person receiving it knows that it is definitely from you and that it has not been tampered with en route.

The Classification Label and the email addresses of the message drive the policy decisions. The user is only responsible for correctly labelling the email.

Confidentiality requires encryption of the message and attachments so that the email cannot be intercepted and read by anyone other than the intended recipients.

The Release Authority is an electronic gatekeeper performing policy compliance checking at the email domain boundary. All email released from the domain must pass through the Release Authority and will only be released if it has met the policy rules and carries an electronic signature applied by the client software.

Central Control of Policy provides system-wide email security policy. This automatically enforces the correct policy at the user's workstation.

User interface

HP ProtectTools Email Release Manager is designed to have a very low impact on users; changes to the 0utlook user interface are limited to:

- *Configuration items on a tab in the Tools Options dialogue*
- *Options on a tab in the Message Properties dialogue*
- *User prompts on sending and receiving mail*

Configuration

The system can be configured for general users so that they are only prompted when the policy requires it. This would normally be when the systems are configured to require message send confirmation or a policy exception occurs. The configuration options available from the Tools Options menu in the Outlook client can be centrally controlled to determine which options are available to particular users. Users may be allowed to set their own default message classification; alternatively their default can be set to a particular label or the network default. For example on a System High Confidential Network, the Network Default Classification would be set to Confidential. However, a user working only on restricted material may have their default classification set to Restricted. Then by default any mails they send would be marked Restricted, the classification label can still be modified for individual messages if required. The policy could be set to audit all messages sent below the default classification hence providing tracking of downgraded data.

Users may also be allowed to choose whether they want to be prompted for the message classification as they send each message. Alternatively this prompting can be set always on or off for a particular user.

Message Properties

The classification label for individual messages can be set through the message properties dialogue. This works well for users who typically work at a particular classification level and only occasionally need to modify the label[1]. A similar dialogue allows the user to view the classification of received mail.

Message Classification Prompt

Users who work on messages with a variety of classifications may find it more convenient to be prompted for the classification label as each message is sent. As they press the send button for each message a new dialogue can, optionally, be presented allowing them to choose a label from the available list.

1 The dialogue is available through a tool bar button

Message Send Dialogue

As a message is sent the policy rules may prevent this message from being sent or require that the user confirms that the message can be sent. The dialogue lists the first ten addressees of the message and the classification label. If the message cannot be sent the user is returned to editing the message to correct the addressee list. If confirmation is required the user may need to enter their password or simply press the confirm button depending on the policy defined.

Release Authority

The Release Authority provided in HP ProtectTools Email Release Manager acts as an electronic gatekeeper at the boundary of the email domain. All email bound out of the domain must pass through the Release Authority and will only be allowed through if the policy requirements have been met and the email carries an electronic signature. Electronic mail entering the domain can also be routed via the Release Authority; this allows the use of two network interfaces providing a separation of the email domain from the outside. The Release Authority is Windows 2000 based and acts as an SMTP router with flexible configuration options. It can be configured, for example, with two network interfaces, providing full separation of the network segments. It is designed to be extensible to include facilities such as dirty word checking and virus scanning.

The electronic signature required for the release of emails from the domain is applied by the HP ProtectTools Email Release Manager client extension and contains time and user-based parts designed to prevent signatures being reused in a replay style attack. Emails without this signature have not met the policy requirements and are not sent, a non-delivery message is generated. Audit facilities are flexible and can be configured to log all outgoing email, or rejections as required.

The Release Authority can also be used within an organisation without needing to have separate Exchange domains. The messages used by Exchange servers within a domain to synchronise directories and folders are passed by the Release Authority. Hence the Exchange infrastructure can be organisation-wide with all the features of replicated directories and folders but with the assurance of a division of information. This can be used, for example, to separate a project team working on sensitive data from a company's Intranet but still allowing them access to the company's Exchange infrastructure.

Alternatively, a Mailguard version of the Release Authority can be used which integrates with the Clearswift ES product. This allows additional decryption keys to be configured giving Clearswift the ability to content check encrypted mails.

Policy

The system-wide email security policy is centrally controlled and automatically enforced so it does not rely on users interpreting security policy manually. The Policy Manager (system administrator or security officer) can centrally configure policy that will determine when and how a mail can be sent to a particular destination.

The Policy Manager is able to configure the valid classification labels for the system, define rules for the handling of mail, define valid destinations and configure a matrix of destinations against labels choosing the rule for each case. The rules determine whether that mail should be labelled, whether an audit event should be created and when confirmation is required. The Policy Manager can change the policy at any time. Changes are replicated from a central server through any subordinate servers and out to the HP ProtectTools Email Release Manager clients. Alternatively, the policy can be stored in the Active Directory giving the policy distribution the same resiliency and fail over support as Active Directory. Policy is cached locally on the workstations minimising load on the server. Policy is implemented on the workstation as soon as it is received. The user certificates are distributed by the Microsoft certification server.

Users cannot change this policy which is enforced automatically in their Exchange client and Outlook client software. As the user sends a message they get immediate feedback if confirmation is required or the mail cannot be sent.

Labels

The available classification labels are defined centrally, allowing the Policy Manager to limit the labels that can be used on the system. These labels are then used along with the addressees to determine the processing of the message by the system. Labels are defined as text strings and may contain classifications, code words and caveats. Each label also has an integer value defining its precedence order, it would be sensible to define the label values at intervals to allow the insertion of new labels if required. Up to 128 labels can be defined each of up to 64 characters and these can be mixed case if required.

The default email label would typically match the system classification. For example, a System High

Confidential Network would have a default mail label of Confidential.

A 'Not Protectively Marked' label with a value of zero is provided in all configurations and cannot be deleted.

The label assigned to the email can be configured to become part of the subject either at the client end, which would affect all emails, or at the Release Authority just affecting emails leaving the domain. The label can also be displayed as a column in the explorer view of the Inbox giving users an immediate indication of the sensitivity of the email before they open it.

Destinations

*Up to 256 different destinations can be defined. For each destination, multiple destination addresses can be defined, up to a total of 4096 characters. The destinations can be defined in Exchange addressing, native SMTP format or X.400 format, with support for other Exchange Connections such as Fax Gateways. Destination addresses can be wildcarded, for example, a generic SMTP style address for HP would be *@hp.com, for any addressee at HP. Each component of the address can be wildcarded, so for example, *.bloggs@hp.com would be anyone with a surname Bloggs at HP.*

Wildcarding can be used in Exchange and X.400 style addresses to specify, for example, anyone in a particular organisation or organisational unit.

A destination name could be used to define, for example, a small group of users who are cleared to receive confidential information. All the addressees could be included individually as destinations within the destination name.

Users

Users of the HP ProtectTools Email Release Manager system are controlled centrally, with each Exchange User being either enabled or disabled for HP ProtectTools Email Release Manager. Users who are enabled have access to all the features of HP ProtectTools Email Release Manager, if a user is disabled they will not have access to these features and will not be able to release email from the domain via the Release Authority.

In addition, the Policy Manager may set the configuration options for the users, allowing the selection of default labels and classification prompt behaviour for a user.

Users may be allowed to set their own default message classification; alternatively their default can be set to a particular label or the network default. Users may also be allowed to choose whether they want to be prompted for the message classification as they send each message. Alternatively this prompting can be set always on or off for a particular user.

Rules

A rule is a way of naming the security options for a circumstance so that they can easily be referred to and reused. Up to 256 rules can be defined, for each rule the options are available for:

- *Package*
- *Facilities*
- *Audit*
- *Confirmation*

The Package and Facilities of that Package can be selected. In HP ProtectTools Email Release Manager, two options are available; Microsoft SMIME is supported providing Proof of Content Origin, Confidentiality or both. It protects the format of Exchange mail fonts, styles and position of text wrapping. It also allows OLE objects in a mail and preserves message properties allowing applications such as workflow to operate. Alternatively the mail can be sent with no package applied, i.e. sending the mail in clear.

Auditing of the messages can be enabled for failed sending, successful sending or both. When auditing is on the date and time, message subject, originator and recipients are recorded in the NT event log.

Should the server be unavailable for some reason the events are recorded locally. These event log entries are intended for auditing purposes only and do not contain any of the message text or attachments. Keeping copies of outgoing mail is referred to as journaling and can be achieved using Exchange server.

User confirmation can also be required. The available options are simple confirmation without password, or the NT password. Confirmation would normally be used to check that the user understands that they are, for example, releasing a document to the Internet; confirmation with a password provides a greater level of assurance that the user is actually present when sending the email.

The 'Default 'rule is provided as part of the standard set up and is used to fill the Policy Matrix where no other rule applies. This rule cannot be deleted but its properties may be changed. Initially the default rule does not allow mail to be sent and creates an audit record entry whenever the rule is applied.

Identity Based Encryption (IBE)

The use of certificates in email is ideal for many organisations as it provides the confidentiality and proof of content origin information which is essential in the environments in which these organisations operate. However the use of certificates could be considered to be cumbersome as it requires a Public Key Infrastructure which can be awkward and costly to manage.

Identity Based Encryption (IBE) provides a slick alternative to the use of certificates which uses a public key based on the recipient's name or identity. The recipient must go to an external entity, known as the trust authority, and request his/her private key. To access the key the recipient is required to submit some personal credentials such as their date of birth or mother's maiden name.

IBE can be configured to use Windows Authentication for in house email traffic further reducing administration.

The advantage of this method is that there is minimal impact on the user and it is much easier for the administrators to manage as the only information which needs to be set up is the credentials and roles.

Integration with Rights Management Server/Rights Management Services (RMS)

ProtectTools Email Release Manager is focused on providing central control of email activity with minimal impact on users. The product has now been fully integrated with Information Rights Management Services (RMS) to enhance this control and allow administrators to manage exactly what action users can take with mails that are received. The RMS template is selected through policy to prevent or allow users from printing, editing, extracting, forwarding and copying emails.

Virus Throttling

Email viruses and worms present a serious threat to an organisation's network performance and with this in mind ProtectTools Email Release Manager has now evolved to provide significant protection. The introduction of Virus Throttling, which has been developed by HP Labs, gives organisations the ability to control the number of emails which individuals can send within a specified period of time, dramatically reducing the propagation of unknown viruses and worms. The throttle identifies and restricts any harmful behaviour within seconds enabling networks to operate efficiently.

Virus throttling can be configured to suit the organisation's requirements with the ability to place ceilings on the number of emails sent together with restrictions on the timescales associated with the release of the mails.

Also mail calming helps to prevent users from sending messages to distribution lists by accident, and sending large messages.

Policy Matrix

The Policy Matrix brings together the destinations, labels and rules in an easily understood format. In the matrix the labels are shown across the top and destinations down the side. Each box in the grid specifies the rule that defines how the system will handle messages with a particular label to that destination. Each box on the grid has a drop down list from which the defined rules can be selected. As destinations or labels are defined the default rule is used for each new box in the grid.

This Policy Matrix is checked as each mail is sent, the label of the message and the addressees select the rules that must be applied. A single message to multiple destinations may match multiple rules, for example, allowing email within the organisation to move without intervention, but requiring an audited confirmation for email bound for a rival company.

Configuration Examples

Joe Smith Inc.

A fictional company, Joe Smith Inc., has a connection to a HP Secure Network for support purposes and through that connection to the Internet. The network is Company Confidential and also contains Commercial In Confidence and Unclassified material. HP can carry data up to Commercial In Confidence if encrypted, Company Confidential data on the HP network must be denied and only unclassified data can be released to the Internet. An example Policy configuration for this situation is shown below.

Table 1: Joe Smith Policy Matrix

	Unclassified	Commercial in confidence	Company Confidential
Local	*Allow*	*Sign*	*Sign plus no copy, forward & print template*
HP	*Allow*	*Encrypt*	*Deny*
Intranet	*Confirm*	*Deny*	*Deny*

The system default label for all messages would be Company Confidential and users would need to take positive action to 'downgrade 'messages below this level. When emails are sent with Company Confidential labels they need to be signed and the rights of the recipients are restricted through the implementation of RMS.

Table 2: Joe Smith Inc. Rules

Default	*Deny and create an audit event*
Deny	*Deny and create an audit event*
Confirm	*Require user confirmation and create an audit event*
Allow	*Label*
Sign	*Label and apply an SMIME electronic signature or IBE*
Encrypt	*Label, sign, encrypt with SMIME and create an audit record or IBE*
Sign & RMS	*Sign using SMIME or IBE and apply and RMS template disabling print, forward or copy*

Table 3: Joe Smith Inc. Destinations

Local	*EX:/o=hp/ou=joesmithinc/cn=*, SMTP: *@joesmithinc.com*
HP	*SMTP: *hp.com*
Intranet	*SMTP: *@**

All local email and any mail labelled Commercial In Confidence or below bound for HP is allowed without intervention. Company Confidential mail for HP is denied.

Any email released to the Internet must be labelled Unclassified, the user must confirm sending and an audit record is required.

Limiting emails to specific groups

The flexibility of the policy system allows the implementation of various labelling schemes, government or commercial. One of the particular strengths is to define a specific label with some kind of code word such as 'Company Confidential-Directors Only' or 'Top Secret - ProjectX'. Destination names can then be defined for 'Directors 'or 'ProjectX " though it is likely that Exchange Distribution lists already exist for these groups. The Policy Matrix can then be set to deny messages with these labels from being sent outside the defined group of addressees.

Tables 4 and 5 give an example where only cleared employees can send one another mail labelled 'Company Confidential'. Other local addressees can only be sent mail labelled 'Commercial In Confidence" or below.

Denying emails to particular addresses

Generally destinations will be defined to enable mail, meeting certain criteria, to be sent. However, it is possible to define a destination with addresses to which all mail will be denied. For example, a company could set up email policy preventing the general user population from sending email to a competitor.

Table 4: Specific Group Policy Matrix

	Unclassified	Commercial in confidence	Company Confidential
Cleared	*Allow*	*Allow*	*Allow*
Local	*Allow*	*Allow*	*Deny*
HP	*Allow*	*Allow*	*Deny*
Intranet	*Confirm*	*Deny*	*Deny*

Table 5: Specific Group Destinations

Cleared	*EX:/o=hp/ou=joesmithinc/cn=User1 EX:/o=hp=joesmithinc/cn=User2 etc.*
Local	*EX:/o=hp/ou=joesmithinc/cn=*, SMTP:*@joesmithinc.com*
HP	*SMTP: *hp.com*
Intranet	*SMTP: *@**

Product Road Map

The HP ProtectTools Email Release Manager system provides functionality to handle email based on label and destinations using a central systems policy. In addition, the Release Authority component provides boundary mailguard functionality. There are many enhancements planned to the system but the system can also be tailored to meet the requirements of particular customers.

Conclusion

The release of a sensitive email to an inappropriate person is a constant threat to any organisation. Email has become the easiest way of sending information around the world via the Internet and once it has been sent it has gone. HP ProtectTools Email Release Manager provides facilities to electronically sign, encrypt and audit emails to ensure your organisation is in control of email activity with minimal impact on users. The product has been enhanced further with the addition of Virus Throttling, IBE and the integration with RMS to provide a comprehensive email security solution.

For more information

If you would like to try this software for yourself please visit our Software Depot website (www.software.hp.com) where you can download free 60-day evaluations.

www.hp.com/hps/security/products

HP ProtectTools Security Team, 2005.

Call to action

www.hp.com/hps/security/products
email: ProtectTools@hp.com
Tel: 01925 841881.

4AA3-4640EEE, Created May 2011