TREND MICRO™

Trend Micro™ Encryption for Email Gateway5

Secured by Private Post™

Deployment Guide

Messaging Security

Document Part No. EEEM53704/80619

Release Date: January 2010

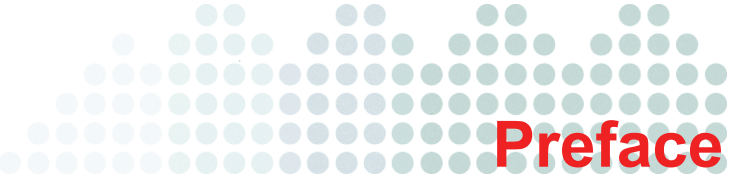
The user documentation of Encryption for Email Gateway is intended to introduce the main features of the software and installation instructions for your production environment. You should read through it prior to installing or using the software.

Detailed information about how to use specific features within the software are available in the Online Help file and the online Knowledge Base at Trend Micro's Web site.

Trend Micro is always seeking to improve its documentation. Your feedback is always welcome. Please evaluate this documentation on the following site:

http://www.trendmicro.com/download/documentation/rating.asp

Contents



Preface

Welcome to the *Encryption for Email Gateway Deployment Guide*. This guide contains information about product settings and service levels.

This preface discusses the following topics:

- *Trend Micro™ Encryption for Email Gateway Documentation*
- *Audience*
- *Document Conventions*

Trend Micro™ Encryption for Email Gateway Documentation

The Trend Micro™ Encryption for Email Gateway documentation consists of the following:

Trend Micro™ Encryption for Email Gateway Administrator's Guide — Helps you plan for deployment and configure all product settings.

Online Help — Helps you configure all features through the user interface. You can access the Online Help by opening the Web console and then clicking the **Help** icon ().

Trend Micro™ Encryption for Email Gateway Quick Installation Guide — Helps you plan for deployment and configure product settings.

Readme File — Contains late-breaking product information that might not be found in the other documentation. Topics include a description of features, installation tips, known issues, and product release history.

The readme is available at:

http://www.trendmicro.com/download

Audience

This document is intended to be used by new users of the Encryption for Email Gateway Administrator Console, including system administrators, operators, sensitive content contributors, information security staff, executives, and other users with other specific roles.

The audience should have a thorough understanding of the Encryption for Email Gateway system, including general operations and critical concepts. Familiarity with Web browsers and Web-based user interfaces are also required.

Document Conventions

To help you locate and interpret information easily, the Encryption for Email Gateway documentation uses the following conventions.

CONVENTION	DESCRIPTION
ALL CAPITALS	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, options, and ScanMail tasks
Italics	References to other documentation
`Monospace`	Examples, sample command lines, program code, Web URL, file name, and program output
Note:	Configuration notes
Tip:	Recommendations
WARNING!	Reminders on actions or configurations that should be avoided

Chapter 1

Deployment of Encryption for Email Gateway

This chapter introduces the *Encryption for Email Gateway Deployment Guide*.

Topics include the following:

Introduction

This deployment guide helps administrators deploy and manage Trend Micro™ Encryption for Email Gateway (Encryption for Email Gateway) in conjunction with an email gateway content filtering product such as:

- Trend Micro™ InterScan™ Messaging Security Suite (IMSS) 7.0
- Trend Micro™ InterScan™ Messaging Security Virtual Appliance (IMSVA) 7.0
- Any email gateway security offering that can route email messages based on policies and apply policies based on X-headers

When Encryption for Email Gateway is used with email content security products, it can help ensure that:

- End users do not use encryption to violate email policies.
- End users do not bypass content scanners and distribute encrypted emails contaminated with viruses and other malware.
- All outbound emails that contain sensitive information are encrypted.

For product information regarding Trend Micro Email Encryption, visit:

http://www.trendmicro.com/go/encryption

Mail Flow Setup

Administrators integrate Encryption for Email Gateway with email gateway content filtering products by defining policies or rules in these applications that pass messages to Encryption for Email Gateway whenever there is a need to encrypt or decrypt an email.

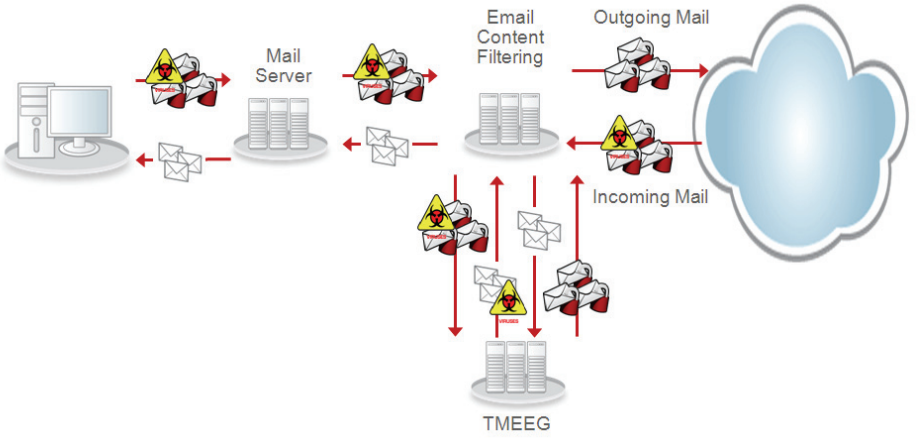
These rules minimize the need to change the flow of mail through the mail system, which in a typical Encryption for Email Gateway environment is as follows:

1. Identify encrypted messages.
2. Pass the encrypted messages to Encryption for Email Gateway for decryption.
3. Scan the encrypted message with the content filtering product.
4. (Optional) Pass the message back to Encryption for Email Gateway for re-encryption.
5. Deliver the message to the recipient.

The optional step of re-encrypting emails prior to delivery adds additional security as the email remains encrypted as it passes through the network and is stored on the internal email servers. Encrypted messages can be read using either Trend Micro™ Encryption for Email or a Web-based Zero Download reader. If messages are not re-encrypted, then Encryption for Email Gateway decrypts all messages for the user and delivers them as plain text. Administrators can also implement a mixture of both scenarios, if they wish.

For example, an administrator might decide that all emails are delivered unencrypted with the exception of emails to or from executives, which must be re-encrypted before delivery. This scenario appears in the following figure.

FIGURE 1-1 Typical Document Flow when Encryption for Email Gateway is Used at the Gateway



Configuring Encryption for Email Gateway

Use the following procedure as a guideline when integrating Encryption for Email Gateway with SMTP content filtering gateways such as Trend Micro InterScan Messaging Security Suite (IMSS) 7.0 or Trend Micro InterScan Messaging Security Virtual Appliance (IMSVA) 7.0.

Configuring SMTP

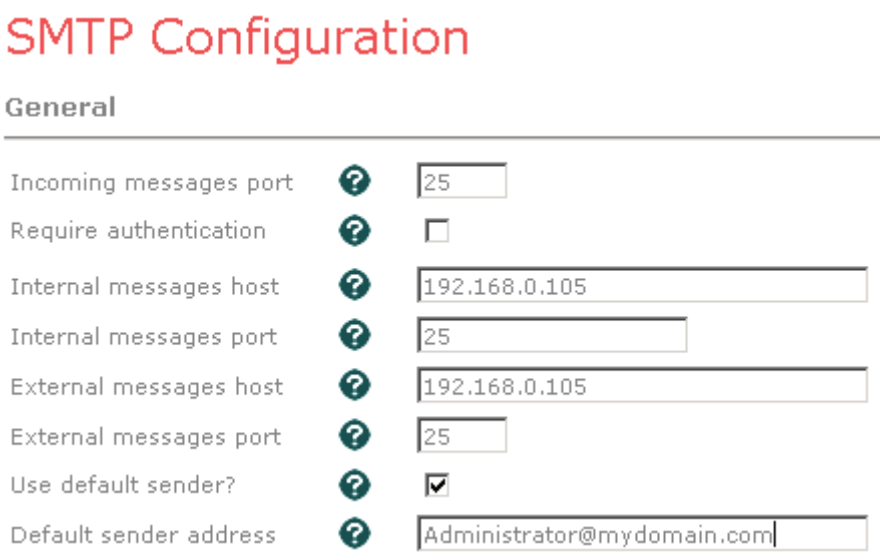
Before integrating Encryption for Email Gateway with a content filtering gateway such as IMSS, make sure that Encryption for Email Gateway is configured to listen to the assigned IP address and port number. Additionally, Encryption for Email Gateway should also be configured to accept email only from and deliver it to the gateway content filtering solution.

To configure the Encryption for Email Gateway SMTP feature:

1. Log in to the Encryption for Email Gateway Console as the administrator.
2. Navigate to **Configuration > SMTP**.
3. Configure the **Incoming Message Port** to the listening port assigned to Encryption for Email Gateway
4. Configure the **Internal message host** to point to the IP address of the content filtering gateway.
5. Configure the **Internal message port** to point to the correct port number on the content filtering gateway.
6. Configure the **External message host** to point to the IP address of the content filtering gateway.
7. Configure the **External message port** to point to the correct port number on the content filtering gateway.
8. Place a check mark beside the **Use default sender?** option.
9. Enter an email address whose domain you specified in the **Manage Domains** section's **Default sender address** field.

An example of a properly configured Encryption for Email Gateway SMTP interface appears in the following figure.

FIGURE 1-2 Example Encryption for Email Gateway SMTP Configuration Window Showing the Connection Settings for IMSS/IMSVA



Note: Encryption for Email Gateway uses the "Use default sender?" and "Default sender address" fields to sign emails in the event it cannot obtain the private key for the real sender. This setting is essential because it allows Encryption for Email Gateway to re-encrypt messages when the sender has an email address that is outside your internal domain.

Configuring MIMEBuilder

The Encryption for Email Gateway MIMEBuilder is responsible for encrypting and decrypting messages. The following configuration is needed to enable Encryption for Email Gateway to make encryption changes to the X-headers and to issue notifications for incoming encrypted messages.

1. Log in to the Encryption for Email Gateway Console as the administrator.
2. Navigate to **Configuration > MIMEBuilder**.
3. Place a check mark beside the **Add encryption X-Header** option to enable the feature.
4. In the **Encryption X-Header** field, specify the X-header field that Encryption for Email Gateway will add when a message is encrypted.
5. Place a check mark beside the **Add decryption X-Header** option to enable the feature.
6. In the **Decryption X-Header** field, specify the X-header that Encryption for Email Gateway will add when a message is decrypted.

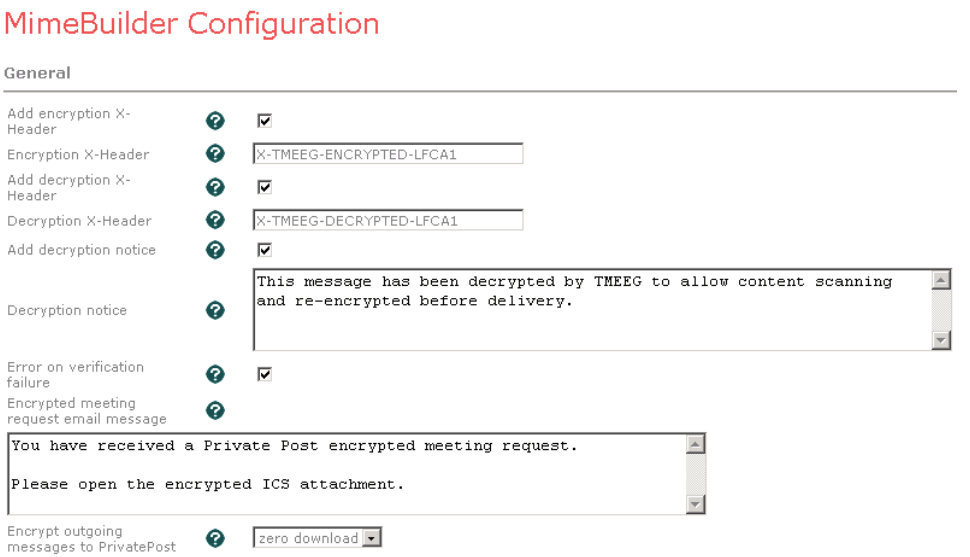
Note: The values you enter in the Encryption X-Header and Decryption X-Header fields must be unique. This a requirement for email gateway applications that do not parse custom X-headers.

---

7. Optional: Place a check mark beside the **Add decryption notice** option.
8. Optional: In the decryption notice, enter the notification text that Encryption for Email Gateway will use to alert the receiving party that the message was decrypted to allow content scanning.
9. Leave all other settings at the default and save the changes.

An example of a properly configured MIMEBuilder window appears in the following figure.

FIGURE 1-3 Encryption for Email Gateway MIMEBuilder Configuration Window with Correct Encryption and Decryption Settings



Choosing the Correct Runtime Configuration

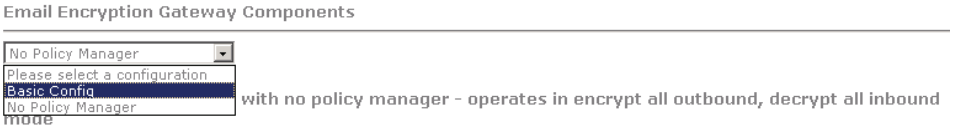
There are two configurations in which you can run Encryption for Email Gateway. Make sure you select the Basic Config option.

To select this mode:

1. Log in to the Encryption for Email Gateway Console as the administrator.

2. As shown in the following figure, navigate to the System Status area and use the **Encryption for Email Gateway Components** drop down to select the Basic Config option.

FIGURE 1-4 System Status, Encryption for Email Gateway, Basic Configuration Selection Drop Down



3. Enter your passphrase.
4. Click **Stop** to stop Encryption for Email Gateway so you can reconfigure it. The following figure shows what the status area of this window looks like after you complete this step.

FIGURE 1-5 System Status Showing All Components Stopped

Configuring Encryption for Email Gateway Encryption and Decryption Policies

Because IMSS, IMSVA, or another email content filtering product is being used to route messages to Encryption for Email Gateway, only two policies are needed: one to decrypt all messages, and another to encrypt all messages.

To configure these policies:

1. Log in to the Encryption for Email Gateway Console as the administrator.
2. Access the **Encryption for Email Gateway – New Policy** window.
3. Select **Configuration > Configure Policies > New Policy**.
4. Using the **Policy Details** drop down, select the *Decrypt message to* and *all recipients* option.
5. Do not add any conditions.

An example of the Policy Details drop down with the correct *Decrypt Messages to* settings appears in the following figure.

FIGURE 1-6 Encryption for Email Gateway – New Policy Window with the Correct "Decrypt Messages to" Settings

6. Click **Save**.
7. Click the **New Policy** option to create a new policy.
8. Using the **Policy Details** drop down, select the *Encrypt message to* and *all recipients* options. Use the default *TrendMicroEnvelope*.
9. Do not add any conditions.

An example of the Policy Details drop down with the correct *Encrypt Messages to* settings appears in the following figure.

FIGURE 1-7 Encryption for Email Gateway – New Policy Window with the Correct "Encrypt Messages to" Settings

10. Click **Save**. As shown in the following figure, the descriptions of your new polices appear in the **Policies** field.

FIGURE 1-8 Encryption for Email Gateway – Policies Window Showing the Selected Decryption and Encryption Policies

11. Click **Save**.
12. You must restart the Encryption for Email Gateway components for the new policies to take effect.

Integrating IMSS 7.0 or IMSVA 7.0 with Encryption for Email Gateway

Use the following IMSS 7.0 or IMSVA 7.0 functions to integrate the product with Encryption for Email Gateway:

- **IMSS Policies**: IMSS policies give administrators the option of isolating certain types of email based on keywords, attachments, or other mail properties, and to implement a message action (Quarantine, Delete, Hand-off, etc.). To integrate IMSS with Encryption for Email Gateway, IMSS must be able to identify an encrypted or decrypted mail based on its message headers.
- **Hand-Off Message Action**: One of the IMSS interception actions is "Hand-Off." This action allows IMSS to pass a message to another product, such as an MTA, for further processing. The scenarios in this document require that IMSS be able to "hand-off" messages to Encryption for Email Gateway for either encryption or decryption.
- **Downstream MTA**: The Downstream MTA is a component that allows IMSS/IMSVA to deliver mail directly to the receiving party and bypass any additional policies. All versions of IMSS listen on port 10026. Mail that has been processed by Encryption for Email Gateway and is ready for delivery and will be sent to this port to be delivered.

To integrate Encryption for Email Gateway with IMSS/IMSVA, create the following policies in the product. The sequence in which you implement these policies is important, and you should complete the steps that follow in the order in which they appear in this document.

Creating IMSS 7.0 and IMSVA 7.0 Policies

IMSS and IMSVA policies are used to determine if a message will be encrypted or decrypted. Create the following IMSS/IMSVA 7.0 policies to pass traffic to Encryption for Email Gateway.

Sending Scanned and Encrypted Outbound Mails

Complete the steps that follow to configure IMSS/IMSVA 7.0.

To send scanned and encrypted email:

1. In the IMSS or IMSVA 7.0 management console, navigate to **Policy > Policy List**.

Note: You must maintain the order in which you create the policies appearing as follows. Be sure to insert any new policies between the Global antivirus and Default spam policies.

---

2. Click **Add > Other**.
3. Click **Recipient** and select **Anyone**.
4. Click **Sender**.
5. Select the **Any of the selected addresses** option.
6. As shown in the following figure, create an entry with the "*" wildcard for all internal domains. For example, "`*@mydomain.com`".

FIGURE 1-9 Correct IMSS/IMSVA 7.0 Rule Settings for Sending Scanned and Encrypted Mails

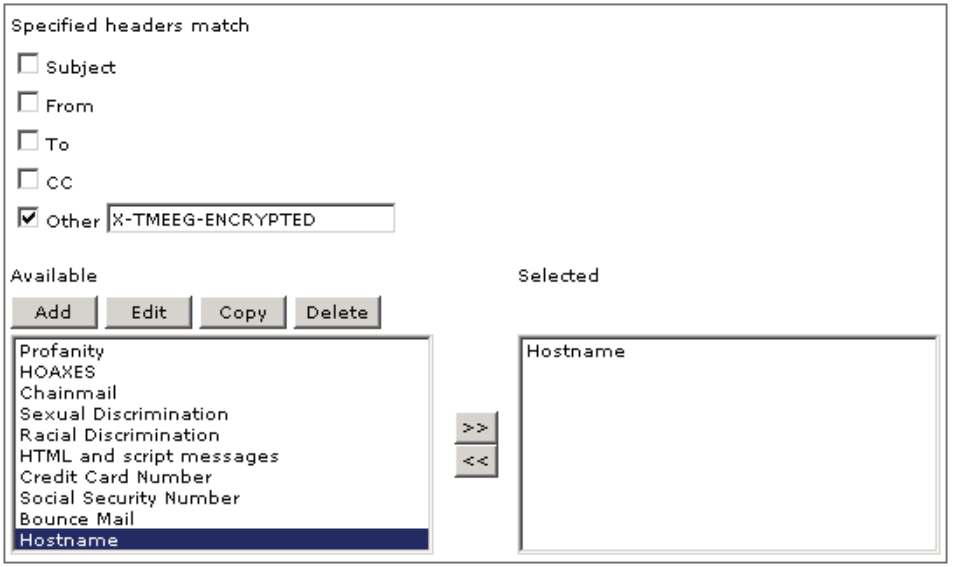
7. Click **Next**.
8. In the Content section of the window, place a check mark beside **Header keyword expressions**.
9. Click the **Header keyword expressions** link.
10. Place a check mark beside **Other**.
11. Enter the header specified in the **Encryption X-Header** field of the Encryption for Email Gateway console. See the section entitled *Configuring MIMEBuilder* for more information.
12. Click **Add**, enter a **List name** such as "Hostname," and add a keyword entry equivalent to the fully qualified domain name of the Encryption for Email Gateway server.

Your completed List name should resemble that of the following figure.

FIGURE 1-10 IMSS/IMSVA 7.0 Configuration Window Showing the Matches Selected for the "Hostname" List Name

13. As shown in the following figure, use the **>>** button to move the **Hostname** list item to the **Selected** box to indicate that Encryption for Email Gateway encrypted the message.

FIGURE 1-11 IMSS/IMSVA 7.0 Configuration Window with the Encrypted X-Header "Hostname" List Name Selected



14. Click **Save**.
15. Click **Next**.
16. In the *Intercept* section of the IMSS/IMSVA 7.0 configuration window, select the **Hand-off** option.
17. Specify the IP address and port number of the Downstream MTA. By default this value is equal to **127.0.0.1:10026**.
18. Click **Next**.
19. Use the **Rule Name** field to give the rule a name. Trend Micro recommends that you use the "Deliver Scanned and Encrypted Outbound Mails" option.
20. Set the **Order Number** equal to **2**.

Deliver Scanned and Encrypted Inbound Mails

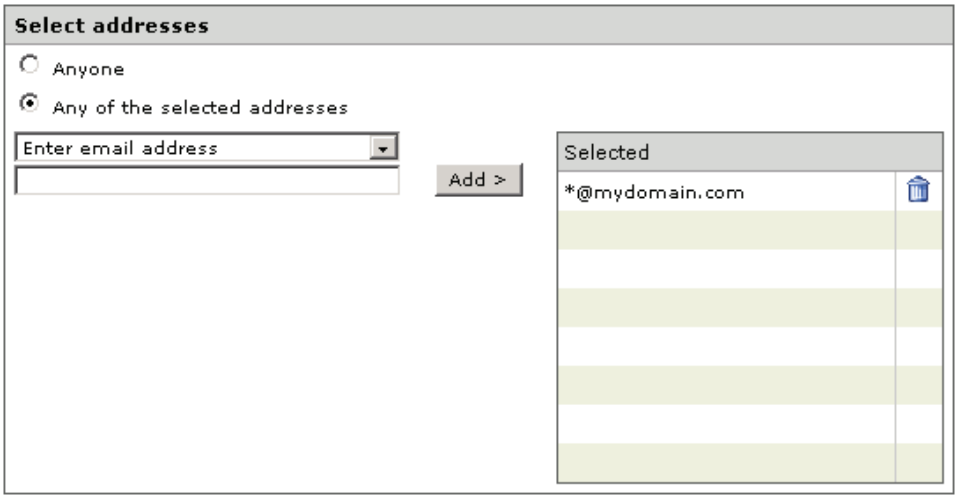
Complete the following steps to configure IMSS/IMSVA.

To scan and then deliver inbound encrypted emails:

1. In the IMSS or IMSVA management console, navigate to **Policy > Policy List**.
2. Click **Add > Other**.
3. Click **Recipient**.
4. Select the **Any of the selected addresses** option.

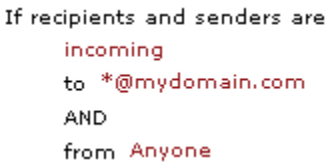
5. As shown in the following figure, create an entry with the "*" wildcard for all internal domains. For example "`*@mydomain.com`."

FIGURE 1-12 IMSS/IMSVA Select Addresses Window with "*@mydomain.com" Selected



6. Click **Sender**.
7. Select **Anyone**. The text of your rule appears in the following figure.

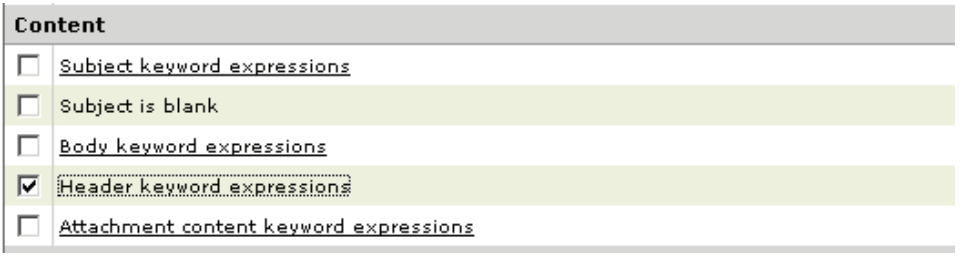
FIGURE 1-13 Correct Configuration Settings for Receiving Email at the "@mydomain.com" Address



8. Click **Next**.

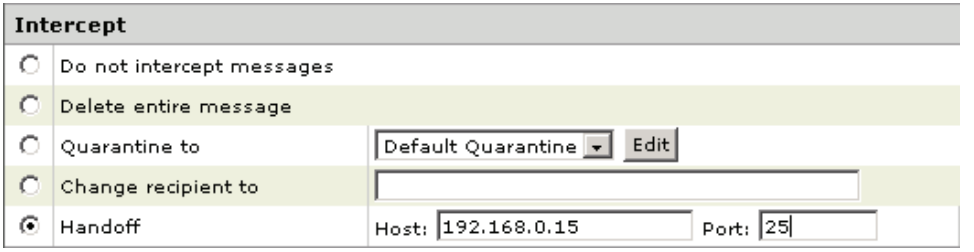
9. In the Content section of the window, as shown in the following figure, place a check mark beside the **Header Keyword expressions** option.

FIGURE 1-14 IMSS/IMSVA Content Area Showing the Header Keyword Expressions Link



10. Click the **Header keyword expressions** link.
11. Place a check mark beside **Other** and enter the Header specified in the **Encryption X-Header** field of the Encryption for Email Gateway console. See the section entitled Configuring MIMEBuilder for more information.
12. Use the **>>** button to move the **Hostname** list item to the **Selected** box to indicate that Encryption for Email Gateway has encrypted the message.
13. Click **Save**.
14. Click **Next**.
15. As shown in the following figure, in the *Intercept* section, select the **Hand-off** option. Then enter then IP address of the MTA in the **Host** field and the port number in the **Port** field.

FIGURE 1-15 IMSS/IMSVA Intercept Area with the IP and Port Number of the Handoff MTA Configured



16. Click **Next**.
17. Use the **Rule Name** field to give the rule a name. Trend Micro recommends that you use the **Deliver Scanned and Encrypted Inbound Mails** option.
18. Set the **Order Number** equal to **3**.
19. Click **Finish**.

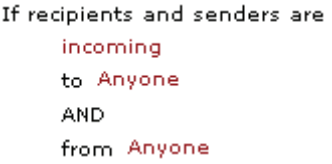
Re-encrypt Messages for Delivery

Complete the following steps to configure IMSS/IMSVA 7.0.

To scan and then re-encrypt incoming emails:

1. In the IMSS or IMSVA management console, navigate to **Policy > Policy List**.
2. Click **Add > Other**.
3. Click **Recipient** and select **Anyone**.
4. Click **Sender** and select **Anyone**. Your settings should look like those in the following figure.

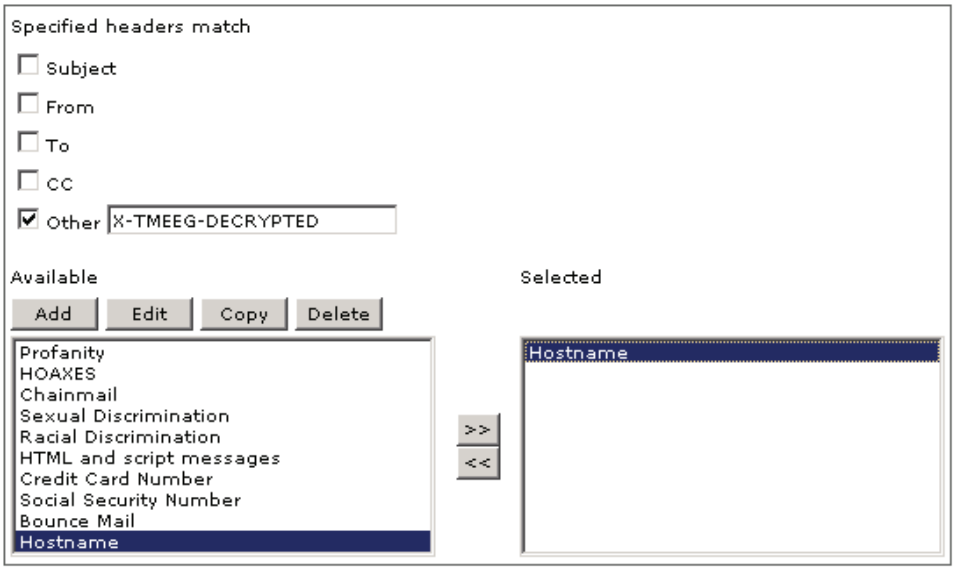
FIGURE 1-16 Correct IMSS/IMSVA 7.0 Rule Settings for Scanning and Re-encrypting Incoming Email



5. Click **Next**.
6. In the *Content* area, place a check mark beside the **Header Keyword expressions** option.
7. Click the link to **Header Keyword expressions**.
8. Place a check mark beside **Other** and enter the Header field specified in the **Decryption X-Header** field. See the section entitled Configuring MIMEBuilder for more information.

9. As shown in the following figure, use the **>>** button to move the **Hostname** list item to the **Selected** box to indicate that Encryption for Email Gateway decrypted the message.

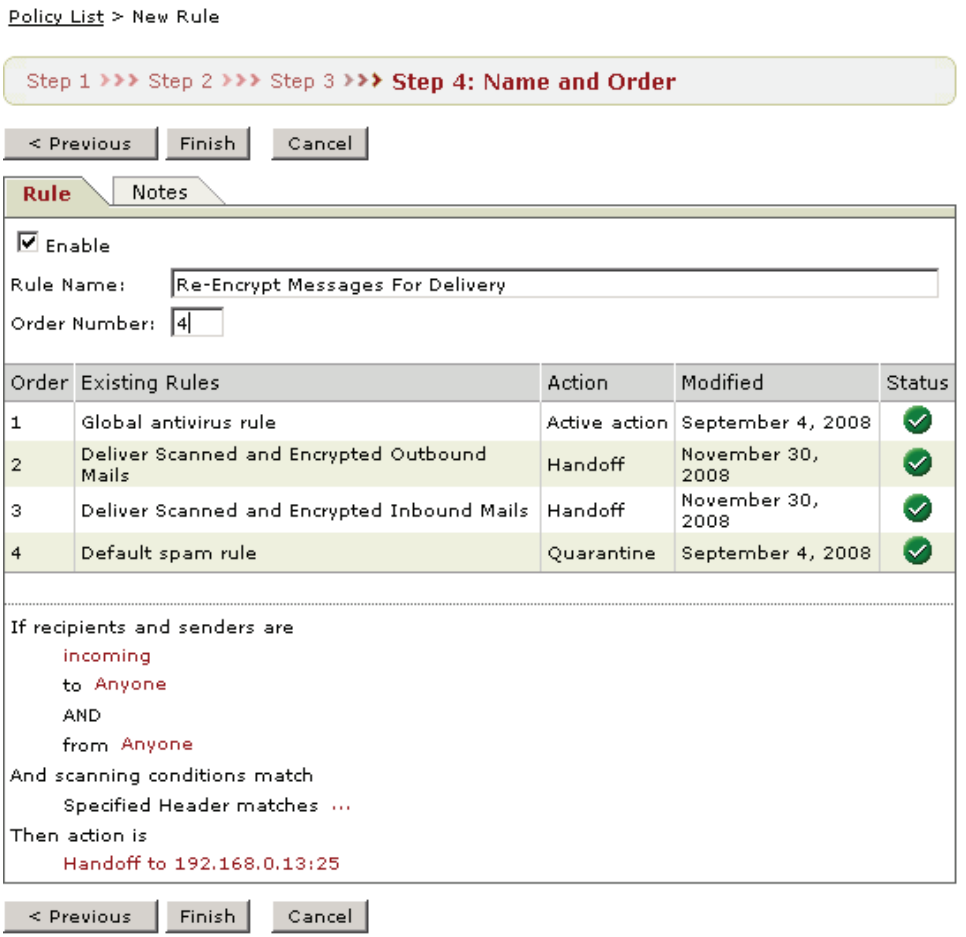
FIGURE 1-17 IMSS/IMSVA 7.0 Configuration Window with the Decrypted X-Header "Hostname" List Name Selected



10. Click **Save**.
11. Click **Next**.
12. In the *Intercept* section, select the **Hand-off** option.
13. Enter then IP address of the Encryption for Email Gateway server in the **Host** field and its port number in the **Port** field.
14. Click **Next**.
15. Use the **Rule Name** field to give the rule a name. Trend Micro recommends that you use "Re-encrypt Messages For Delivery."

16. Set the value in the **Order Number** field equal to **4**. The contents of your **Step 4: Name and Order** page should resemble that of the following figure.

FIGURE 1-18 Example Completed IMSS/IMSVA Re-Encrypt Messages for Delivery Rule



17. Click **Finish** to complete the rule.

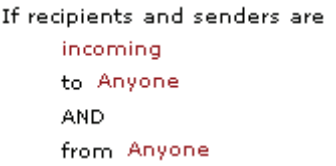
Decrypt Incoming Email

Complete the following steps to configure IMSS/IMSVA 7.0.

To decrypt and then deliver all incoming email:

1. In the IMSS or IMSVA 7.0 management console, navigate to **Policy > Policy List**.
2. Click **Add > Other**.
3. Click **Recipient** and select **Anyone**.
4. Click **Sender** and select **Anyone**. Your settings should look like those in the following figure.

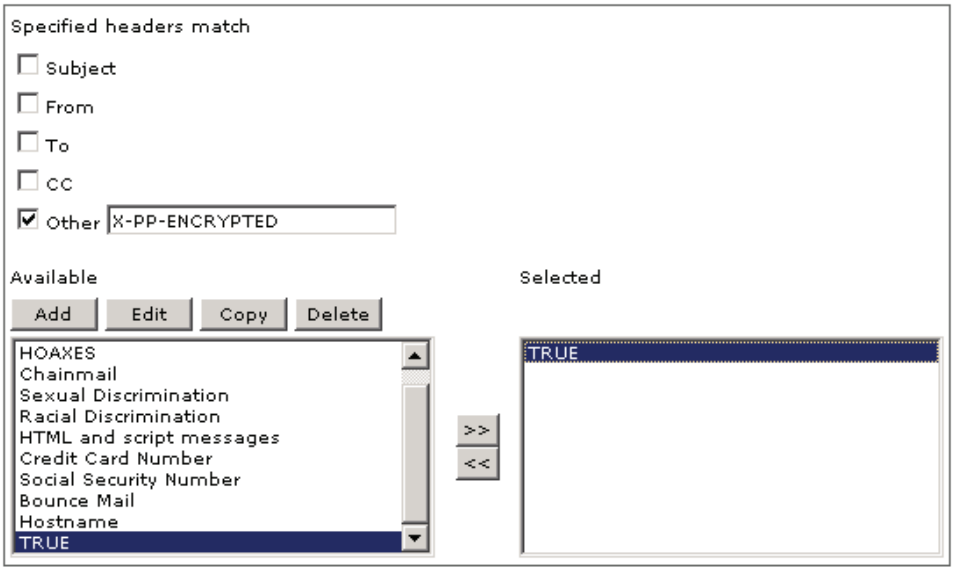
FIGURE 1-19 Correct IMSS/IMSVA 7.0 Rule Settings for Decrypting All Incoming Email"



5. Click **Next**.
6. Under *Content*, place a check mark beside **Header Keyword expressions**.
7. Click the link to **Header Keyword expressions.**
8. Place a check mark beside the **Other** option.
9. Enter the Header field: **X-PP-ENCRYPTED**.
10. Click **Add**.
11. Enter a list name (for example, **TRUE**), and add the **TRUE** keyword entry.

12. Use the **>>** button to move the **TRUE** list item to the **Selected** box to indicate that a Trend Micro Email Encryption Client encrypted the message.

FIGURE 1-20 IMSS/IMSVA Configuration Window with the Encrypted X-Header "Hostname" List Name Selected



13. Click **Save**.
14. Click **Next**.
15. In the *Intercept* section, select the **Hand-off** option.
16. Enter the **IP address** and **port number** of the Encryption for Email Gateway server.
17. Click **Next**.
18. Use the **Rule Name** field to give the rule a name. Trend Micro recommends that you use the **Decrypt Incoming Email** option.
19. Make the value of the **Order Number** equal to **5**.
20. Click **Finish**.

Optional: Encrypting Outgoing Email with Sensitive Information

The rules in the preceding sections handle passing encrypted emails between IMSS/IMSVA 7.0 and Encryption for Email Gateway for content scanning. After you have established these rules, you can create others to check for email that must be encrypted before sending. For example, you might want to create rules that check for messages containing credit card or social security numbers.

The steps in this section describe how to configure IMSS/IMSVA 7.0 to encrypt outgoing messages containing that type of sensitive information.

Note: This portion of the document describes how to define rules containing Regular Expressions. Both IMSS and IMSVA 7.0 support the use of these strings, which allow administrators to create their own pattern checks. For more information on using Regular Expressions, refer to the Trend Micro IMSS or IMSVA Administrator's Guide.

To create a rule to encrypt outgoing emails containing sensitive information:

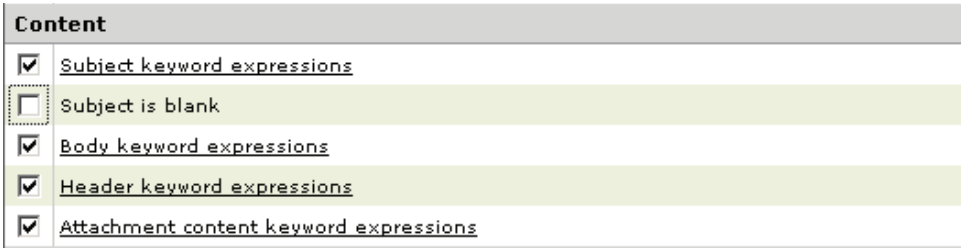
1. In the IMSS or IMSVA 7.0 management console, navigate to **Policy > Policy List**.
2. Click **Add > Other**.
3. Click **Recipient** and select the **Anyone** option.
4. Click **Sender** and select the **Any of the selected addresses** option.
5. As shown in the following figure, create an entry with the "*" wildcard for all internal domains. For example "`*@mydomain.com`".

FIGURE 1-21 Correct IMSS/IMSVA 7.0 Rule Settings for Encrypting Sensitive Outgoing Email

6. Click **Next**.

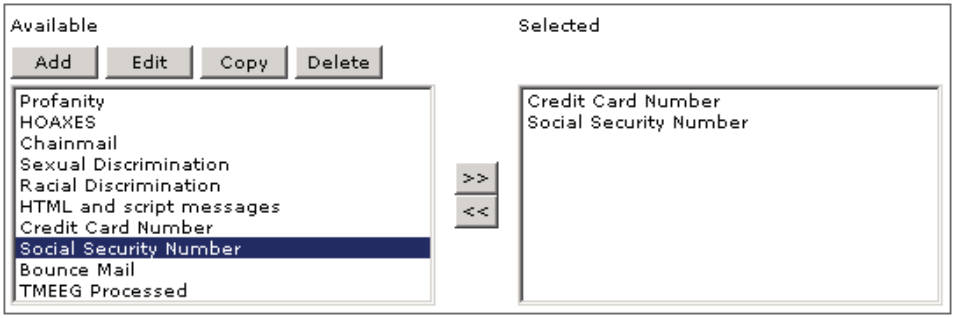
7. As shown in the following figure, in the Content area of the window, place a check mark beside any of the expressions that you want IMSS/IMSVA 7.0 to use to scan for sensitive information. You can select any or all of the following:
   a. Subject keyword expressions
   b. Body keyword expressions
   c. Header keyword expressions
   d. Attachment content keyword expressions

FIGURE 1-22 Available Email Content Expression Checks



8. Click the link for the selected *Content* item.
9. Create a **List Name** for keywords that are sensitive. Check lists for credit card and Social Security numbers are available by default.

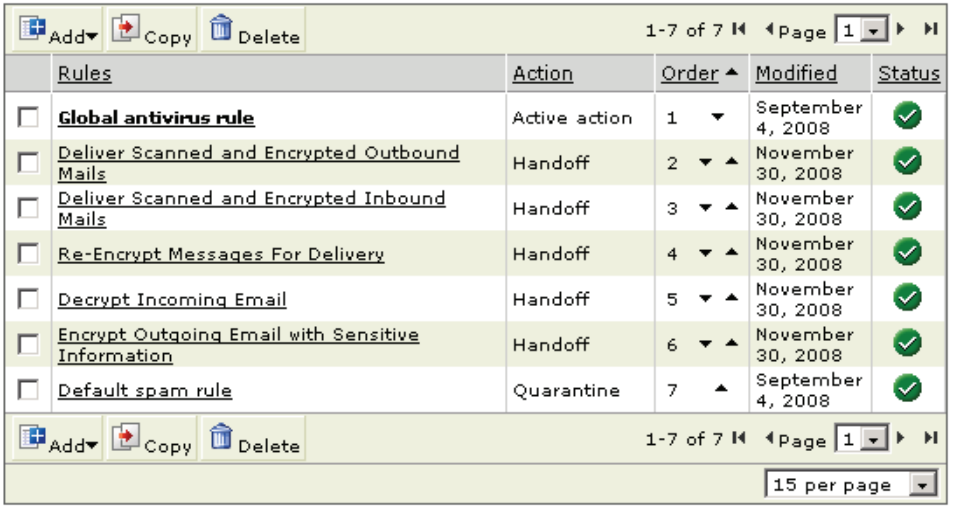
FIGURE 1-23 Selected Email Content Expressions



10. Click **Next**.

11. In the *Intercept* section, select the **Hand-off** option and enter the **IP address** and **port number** of the Encryption for Email Gateway server.
12. Click **Next**.
13. Use the **Rule Name** field to give the rule a name. Trend Micro recommends that you use the **Encrypt Outgoing Email with Sensitive Information** option.
14. Set the **Order Number** equal to **6**. Your new rule should appear at the indicated position in a list similar to the one shown in the following figure.

FIGURE 1-24 Complete List of the IMSS/IMSVA Rules Described in this Document



Note: If you need further information on configuring IMSS or IMSVA, refer to the Trend Micro InterScan Messaging Security Suite 7.0 or InterScan Messaging Security Virtual Appliance 7.0 Administrator's Guide.

Configuring Encryption for Email Gateway for Other Content Filtering Products

The previous sections detail the integration of Encryption for Email Gateway with Trend Micro InterScan Message Security products (IMSS/IMSVA 7.0). However, you can use Encryption for Email Gateway with any email content filtering product that supports these features:

- Applies policies to email based on X-headers
- Routes messages based on policies

The following are guidelines for the policies or rules you must create and a description of the actions these rules must take for any integration with a third-party product to be successful. The order in which you create these rules is important and you should follow them in numerical order (1 through 5).

1. **Deliver Scanned and Locally Encrypted Outbound Mails**

   This rule is used to forward all *outbound* emails that Encryption for Email Gateway encrypts. To determine if Encryption for Email Gateway has encrypted an email, the content filtering gateway should look for the X-header string specified in the Configuring MIMEBuilder section of this document. If the content filtering gateway finds a match, it should deliver the message to the *outbound* MTA.

2. **Deliver Scanned and Locally Encrypted Inbound Mails**

   This rule is used to forward all *inbound* emails that Encryption for Email Gateway encrypts. To determine if Encryption for Email Gateway has encrypted an email, the content filtering gateway should look for the X-header string specified in the Configuring MIMEBuilder section of this document. If the content filtering gateway finds a match, it should deliver the message to the *inbound* MTA.

3. **Re-Encrypt Messages For Delivery (Optional)**

   This rule is used to determine whether or not the local Encryption for Email Gateway has decrypted an email. The content filtering product can check for this by matching the message headers and X-header value specified in the Configuring MIMEBuilder section of this document. If the message matches the rule, the content filtering product should route it to Encryption for Email Gateway for re-encryption. This rule is optional and you should use it when you want to maintain encryption for desktop recipients.

4. **Decrypt Incoming Email**

   This rule is used to check for messages that have been encrypted by any Trend Micro Email Encryption product. The content filtering product can determine this by checking if an email's "**X-PP-ENCRYPTED**" X-header has a value of "**TRUE.**" If the message matches this rule, the content filtering product should route it to Encryption for Email Gateway for decryption.

5. **Additional Administrator Defined Rules**

   You can create additional rules to route messages to Encryption for Email Gateway for encryption. The only requirement is that you only add rules after you have configured the ones mentioned previously in this document.

About Trend Micro Incorporated

Trend Micro Incorporated, a global leader in Internet content security, focuses on securing the exchange of digital information for businesses and consumers. A pioneer and industry vanguard, Trend Micro is advancing integrated threat management technology to protect operational continuity, personal information, and property from malware, spam, data leaks, and the newest Web threats. Its flexible solutions, available in multiple form factors, are supported 24/7 by threat intelligence experts around the globe.

Founded in 1988, Trend Micro provides individuals and organizations of all sizes with award-winning security software, hardware, and services. With headquarters in Tokyo and operations in more than 30 countries, Trend Micro solutions are sold through corporate and value-added resellers and service providers worldwide. For additional information and evaluation copies of Trend Micro products and services, visit our Web site at http://www.trendmicro.com/.