TREND MICRO™

Trend Micro™ Encryption for Email Gateway 5

Secured by Private Post™

Administrator's Guide

Messaging Security

Trend Micro Incorporated reserves the right to make changes to this document and to the products described herein without notice. Before installing and using the software, please review the readme files, release notes, and the latest version of the applicable user documentation, which are available from the Trend Micro Web site at:

http://www.trendmicro.com/download

Document Part No. EEEM54296/100119

Release Date: January 2010

Protected by U.S. Patent No. not available. Patent pending.

The user documentation for the 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

Chapter 5: Scalability and Failover

Chapter 6: Administrative Options

Chapter 7: Exception Handling, Reporting, and Logging

Glossary

Preface

Preface

Welcome to the *Encryption for Email Gateway Administrator's 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 Branding*
- *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 Branding

This document, including the images displayed herein, as an example, have been branded for use by Trend Micro. The look and feel of your documentation and user interface will appear differently depending on your company's branding requirements.

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

Introduction

This chapter introduces Encryption for Email Gateway.

The topic includes the following:

- Terminology

Encryption for Email Gateway is a Linux-based software solution providing the ability to perform encryption and decryption of email at the corporate gateway. This provides the ability to encrypt and decrypt email regardless of the email client and platform from which it originated. The encryption and decryption of email on Encryption for Email Gateway is controlled by a Policy Manager that enables an administrator to configure policies based on various parameters, such as sender and recipient email addresses, keywords or where the email (or attachments) contain credit card numbers. Encryption for Email Gateway presents itself as a simple mail transfer protocol (SMTP) interface and delivers email out over SMTP to a configured outbound mail transport agent (MTA). This enables easy integration with other email server-based products, be them content scanners, mail servers or archiving solutions.

Note: The PCI Compliancy Helper and Credit Card checking component of the Policy Manager enables Encryption for Email Gateway to check for credit card numbers and (optionally) encrypt email based on the configured rules.

Terminology

The following list describes acronyms and definitions for terms used throughout this document:

TABLE 1-1. List of Terminology

TERM	DEFINITION
CORBA	Common Object Request Broker Architecture
DLP	Data Loss Prevention
IBE	Identity-Based Encryption
MTA	Mail Transport Agent
PCI	Payment Card Industry
SMTP	Simple Mail Transfer Protocol
VT	Virtualization Technology – for hardware assisted virtualization.

Chapter 2

System Architecture

The Encryption for Email Gateway system architecture is discussed in this chapter.

The topic includes the following:

- Core Components

Encryption for Email Gateway is heavily componentized and built on Common Object Request Broker Architecture (CORBA) infrastructure. This enables Encryption for Email Gateway to be scaled up and distributed across multiple machines. Given modern processor architectures the need to distribute the application across separate physical hardware is reduced. For more information refer to the Scalability and Failover section.

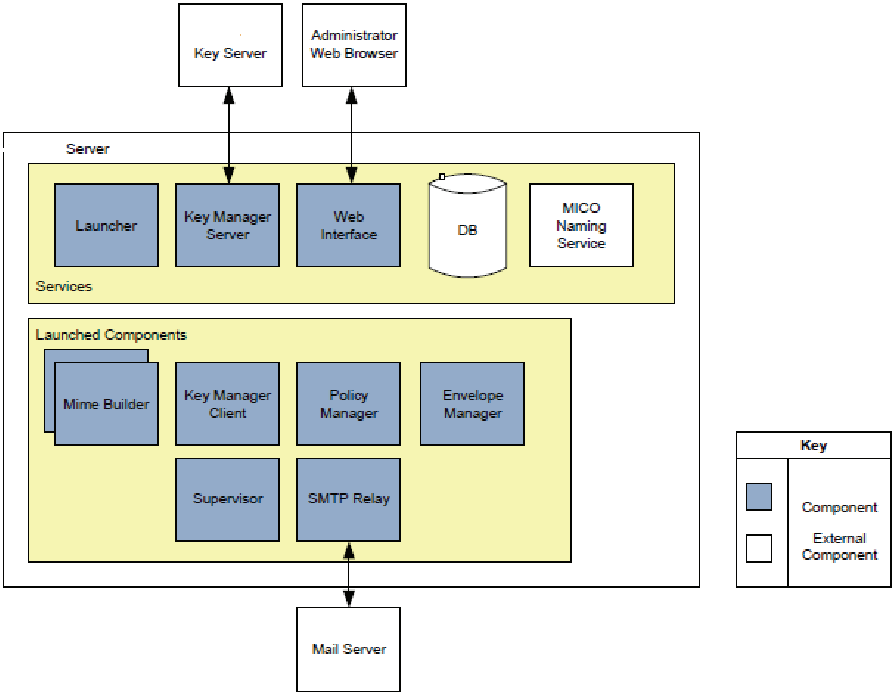


FIGURE 2-1 High-Level System Architecture

Core Components

The core components comprising the Encryption for Email Gateway server are the MIMEBuilder, Key Manager, Policy Manager, and the SMTP Relay. The CORBA infrastructure enables multiple named instances of components to be launched, and although this is possible for all components, it is not necessary.

MIMEBuilder

The MIMEBuilder is responsible for the actual encryption and decryption operations.

Key Manager

The key manager is responsible for obtaining and managing the private and public keys in the IBE system leveraged by Encryption for Email Gateway. With the core key infrastructure being located “in the cloud,” the Encryption for Email Gateway server requires outbound http access to the Key Server in order to obtain the keys as required. After the keys have been obtained they are stored encrypted in the database and cached in memory.

Policy Manager

The policy manager is responsible for identifying the action to be taken on email as it passes through Encryption for Email Gateway. Detailed information on the type of policies and rules that are configurable are discussed in the Policy and Rules Engine section.

SMTP Relay

The SMTP relay is the interface for receiving and sending emails through Encryption for Email Gateway. The corporate mail server must be configured to route outbound email through Encryption for Email Gateway and also receive inbound email from Encryption for Email Gateway.

Database

Although a supported and default configuration to run the database on the same physical hardware as Encryption for Email Gateway, it is also possible to use a separate database server which can service multiple Encryption for Email Gateway front ends. Currently Encryption for Email Gateway supports the Postgres database server.

Chapter 3

Modes of Operation

The Encryption for Email Gateway modes of operation are discussed in this chapter.

Topics include the following:

- Encryption for Email Gateway Deployment Scenarios
- Third-Party Integration

Encryption for Email Gateway can be deployed in several ways, that are all variations of an SMTP relay. Depending on the existing email infrastructure an organization might choose one or another. In the absence of content scanners (such as Antispam, Antivirus or Data Loss Prevention), it is recommended to use Encryption for Email Gateway in the standard SMTP relay configuration.

Encryption for Email Gateway Deployment Scenarios

The following sections provide sample deployment scenarios and options for Encryption for Email Gateway. Because of the highly configurable nature of email routing systems it is impossible to identify all modes of operation, however, they will essentially be variations on those described.

Standard SMTP Relay

The simplest mode of operation is to use Encryption for Email Gateway as an SMTP relay in the default email path. In this mode, all email passes through Encryption for Email Gateway, both inbound and outbound, with the Policy Manager (see the Policy and Rules Engine section) controlling whether to encrypt outbound emails and decrypt inbound emails.

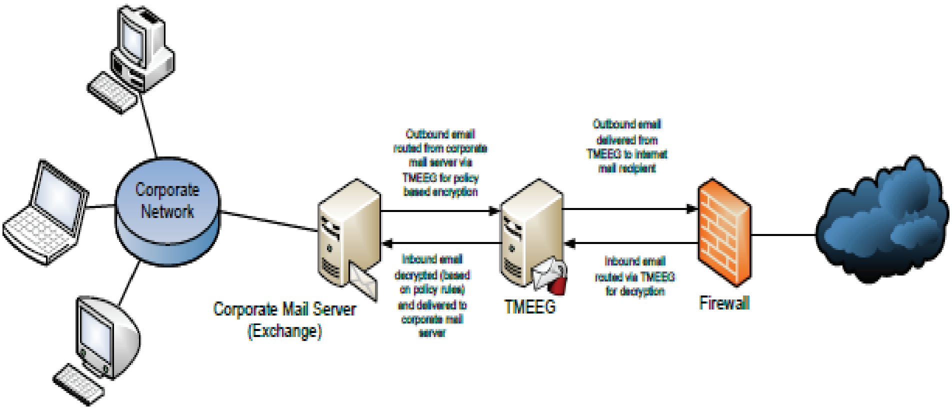

Corporate Network
Corporate Mail Server (Exchange)
Outbound email routed from corporate mail server via TMEEG for policy based encryption
Inbound email decrypted (based on policy rules) and delivered to corporate mail server
TMEEG
Outbound email delivered from TMEEG to internet mail recipient
Inbound email routed via TMEEG for decryption
Firewall

FIGURE 3-1 Simple SMTP Relay

In Figure 3-1, Encryption for Email Gateway is used in the default mail path. The Policy Manager encrypts outbound emails based on the policies configured on the system, and likewise decrypts the inbound emails based on policies.

To deploy Encryption for Email Gateway in this configuration, the corporate mail server must be configured to route all outbound email through Encryption for Email Gateway. Encryption for Email Gateway can be configured to then deliver outbound email directly to Internet recipients (using its own Mail Transport Agent (MTA) by default, but Postfix is pre-installed and can be used alternatively), or through another SMTP relay, for example the ISP.

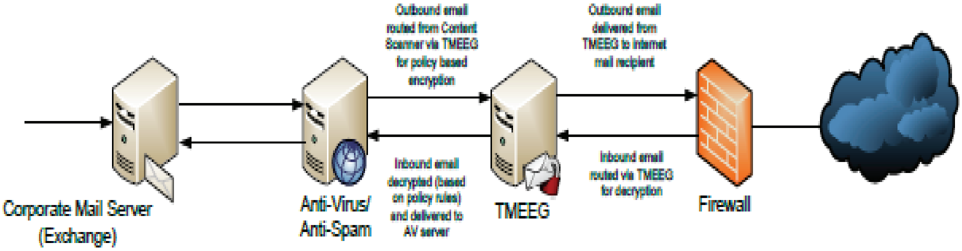

Outbound email routed from Content Scanner via TMEEG for policy based encryption
Outbound email delivered from TMEEG to Internet mail recipient
Corporate Mail Server (Exchange)
Anti-Virus/ Anti-Spam
Inbound email decrypted (based on policy rules) and delivered to AV server
TMEEG
Inbound email routed via TMEEG for decryption
Firewall

FIGURE 3-2 Encryption for Email Gateway with AV/AS Scanner

Figure 3-2 illustrates how Encryption for Email Gateway used in the default SMTP relay configuration can work with an antivirus or antispam server to perform content filtering after decryption of inbound emails and before encryption of outbound emails.

As is typical with the most common Encryption for Email Gateway deployment scenarios, email that is internal to the organization (that is email sent from an internal user to another internal user) will never be encrypted or decrypted by Encryption for Email Gateway. In order to provide internal email encryption the corporation would need to deploy the Encryption Client to the corporate desktops.

Encryption for Email Gateway as an Open Relay

It is worth noting that Encryption for Email Gateway has been intentionally designed as an open relay. This is both for simplicity and flexibility. In order to secure Encryption for Email Gateway and prevent it from being used by unauthorized persons, it is recommended to install an MTA that restricts relay hosts and domains in one of several places, including the firewall, the Encryption for Email Gateway server itself, or another machine in the mail path.

The Postfix MTA is pre-installed on the Encryption for Email Gateway virtual appliance to enable the edge of a network deployment of Encryption for Email Gateway in a secure, locked down manner.

There are three possible scenarios for Postfix usage as follows:

- Postfix up front (only)

  Here, Encryption for Email Gateway will be the downstream MTA from Postfix, which should be configured using the `relay_host` parameter of Postfix. As a minimum, `mynetworks`, `mynetworks_style` and `relay_domains` need to be configured in Postfix.
- Postfix behind Encryption for Email Gateway (only)

  Here the downstream MTA needs to be configured via `relay_host`. Encryption for Email Gateway will be configured to deliver to this Postfix for external message delivery. As a minimum, `mynetworks`, `mynetworks_style` and `relay_domains` need to be configured in Postfix. Optionally use of the `transport_maps` in Postfix could be made.
- Postfix before and after Encryption for Email Gateway

  In this scenario, Encryption for Email Gateway would be configured as a content filter, using the `content_filter` parameter and a second Postfix process will need to be configured in the Postfix master configuration.

Note: When using Postfix you must disable SELINUX, otherwise, it will block the inbound connection.

External Policy Management

When used with an external policy manager, Encryption for Email Gateway can easily be configured to use the default built-in policies, that is encrypt all clear text emails and decrypt all encrypted emails. This makes Encryption for Email Gateway a simple encryption or decryption application without the complexity and overhead of policy management.

This would also enable a third party DLP solution to control what content is encrypted and prevent users from using encryption as a way of circumventing such rules.

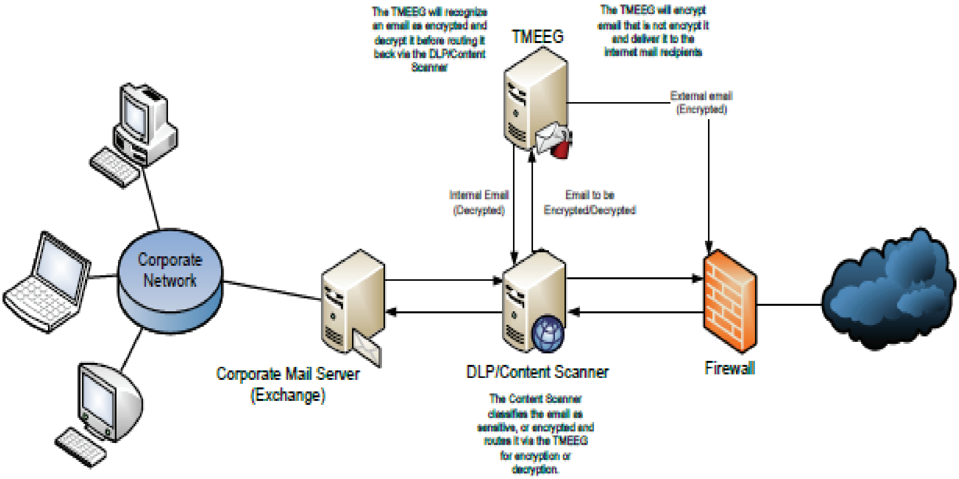

The TMEEG will recognize an email as encrypted and decrypt it before routing it back via the DLP/Content Scanner
TMEEG
The TMEEG will encrypt email that is not encrypt it and deliver it to the internet mail recipients
External email (Encrypted)
Internal Email (Decrypted)
Email to be Encrypted/Decrypted
Corporate Network
Corporate Mail Server (Exchange)
DLP/Content Scanner
Firewall
The Content Scanner classifies the email as sensitive, or encrypted and routes it via the TMEEG for encryption or decryption.

FIGURE 3-3 Encryption for Email Gateway with External Content/DLP Engine Managing Policies

Third-Party Integration

In a scenario where the enterprise requires the email to be encrypted all the way through the mail system, the content scanner can pass encrypted email to Encryption for Email Gateway for decryption prior to content scanning, before passing it back to Encryption for Email Gateway for re-encryption. When the email being scanned is from an external recipient (for example, is inbound) Encryption for Email Gateway will not be able to re-encrypt the message unless the “Use default sender” configuration is set. See the section Basic Configuration Options - Table 6-3.

As previously mentioned, Encryption for Email Gateway interface is SMTP enabling simple integration with other email filtering products, be them antivirus, antispam, DLP engines or archiving solutions. SMTP is the de facto standard for transmitting email over the Internet and most server based products providing additional email services support the SMTP interface.

It is impossible to search or scan the encrypted content of an email, and so Encryption for Email Gateway provides a mechanism for third-party applications to decrypt inbound email before it is scanned or archived enabling these applications to work seamlessly.

A common scenario is to have all emails archived in order to comply with government legislation regarding data retention and for data protection and backup. The problem is easy to recognize, in that archiving encrypted email makes it impossible to search the archive for a specific message. Email archives typically store their data encrypted so it is unnecessary to maintain the Private Post encryption.

To negate this problem, it is possible to place Encryption for Email Gateway in the path, enabling the email to be decrypted prior to delivery to the archive.

Chapter 4

Technical Requirements

The Encryption for Email Gateway technical requirements are discussed in this chapter.

Topics include the following:

- Operating System
- Encrypted Email Identification
- Limitations

The recommended deployment is to run Encryption for Email Gateway as a VMware virtual appliance on VMware ESX or ESXi virtualization platforms.

Operating System

When deployed as a virtual appliance, Encryption for Email Gateway runs on CentOS Linux 5.2 32-bit. This operating system is free from support costs and maintenance contracts and provides heavily tested and robust packages. After deployed, it is not necessary to constantly apply operating system updates unless they address a specific security concern applicable to Encryption for Email Gateway.

Internet Access

In order for Encryption for Email Gateway to operate correctly, a certain level of Internet access is required. This access enables Encryption for Email Gateway to register and obtain keys as required using HTTP. Encryption for Email Gateway can be configured to operate from behind an authenticating proxy server, if required.

The URLs and IP addresses Encryption for Email Gateway are required to access are listed in Table 4-1.

TABLE 4-1. Known URLs and IP Addresses to which Encryption for Email Gateway Requires Access

URL	IP ADDRESS	PROTOCOL/PORT
root.ibe-ta.com	213.129.92.130	TCP/80
public.ibe-ta.com	213.129.92.130	TCP/80
ppconfig.ibe-ta.com	213.129.92.130	TCP/80
www.myprivatepost.com	213.129.92.134	TCP/80; TCP/443
www.privatepost.net	216.104.20.128, 216.104.20.129	TCP/80; TCP/443
Downloads.privatepost.com	216.104.20.128, 216.104.20.129	TCP/80

Web Proxy Support

To configure Internet proxy support perform the following steps:

1. Log in to the Encryption for Email Gateway console using the username and password.
2. Edit the configuration file: `/etc/sysconfig/encryptiongateway.conf`:
   `vi /etc/sysconfig/encryptiongateway.conf`
3. Locate the “Proxy Settings” section in the file and set the following value:
   `useproxy="yes"`
4. Set the value of `proxyhost` and `proxyport` to the address and port of the proxy server.
5. Optionally, set `proxyuser` and `proxypasswd` to an appropriate value if authentication is required on the proxy server.

Encrypted Email Identification

In order to detect an email as Private Post encrypted, and therefore, route it through Encryption for Email Gateway for decryption, a basic understanding of the message format is required. Private Post emails are sent with the encrypted email body wrapped in an HTML attachment (see Table 4-2 for the attachment properties). In addition to the encrypted attachment, all emails encrypted using the Email Encryption products have the following X-Header set: X-PP-ENCRYPTED: TRUE

TABLE 4-2. Encrypted Attachment Properties

PROPERTY	VALUE
File Type	HTML File
Filename	Encrypted_Message.htm
Content Type	text/html

Limitations

As previously mentioned, Encryption for Email Gateway is a processor intensive rather than hard-disk or memory intensive application. By providing more processing power there will be a near proportional improvement in the system performance and throughput.

File Sizes

Encryption for Email Gateway provides no restriction on email sizes or attachments sizes as it is typically used in conjunctions with other MTAs that will limit this. By not including such limitations in Encryption for Email Gateway, it reduces the amount of configuration required by a system's administrator (as the attachment and email limit need only be configured in one place). If required, Encryption for Email Gateway processes attachments in excess of 100MB in size that are far in excess of the limits typically imposed by other MTAs.

Chapter 5

Scalability and Failover

Encryption for Email Gateway scalability and failover are discussed in this chapter.

Topics include the following:

- Database Clustering
- High Availability Deployment Scenarios

Database Clustering

A recommended configuration, as previously mentioned, is to use a dedicated database server or cluster to provide resilience and higher availability. This will also aid in the future addition of more front-end Encryption for Email Gateway servers, resulting in an Encryption for Email Gateway farm, as detailed in the Encryption for Email Gateway Farming section.

The database operations are largely read-only, however, when new keys are obtained, they will be written to the database. The statistics logging component that records the Encryption for Email Gateway usage also requires write access.

Given the complexities and resulting problems in multimaster database clustering, it is recommended to deploy Postgres with the Slony-I replication component providing a simple Master-Slave replication topology.

In this configuration, Encryption for Email Gateway is not able to automatically failover and use the slave database, however, it is a simple configuration change, and given the local caching of data in the Encryption for Email Gateway processes, the performance and availability or Encryption for Email Gateway will not be significantly impacted by a database failure.

High Availability Deployment Scenarios

There are several options available for deploying high-availability Encryption for Email Gateway systems. Typically they fall into two categories:

- Encryption for Email Gateway Multiple Independent Servers
- Encryption for Email Gateway Farming

These scenarios are discussed in the following section.

Encryption for Email Gateway Multiple Independent Servers

The nature of Encryption for Email Gateway provides it with the ability to operate on multiple independent servers, each with their own database server. After the initial deployment, each of the Encryption for Email Gateway servers will need to be registered so they are all able to get access to keys for the registered domains.

A limitation of this deployment scenario is the lack of an automated feature to manage the synchronization of configuration, registration and policies across multiple gateways, meaning any changes made to one of the Encryption for Email Gateways will need to be replicated on the others.

Figure 5-1 shows how such a deployment might look. For simplicity, only the outbound encrypted mail route is shown. In this example there are external content scanners responsible for classifying email to be encrypted.

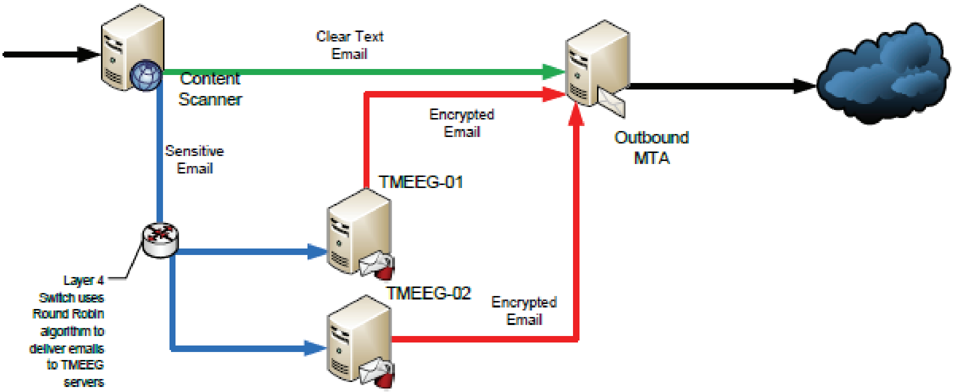


FIGURE 5-1 **Multiple Independent Encryption for Email Gateway Servers for High Availability**

Encryption for Email Gateway Farming

In environments requiring high availability and processing high-volumes of email traffic, Encryption for Email Gateway can be deployed in a farm sharing a single database, and therefore, rules and configuration. In a farmed configuration, multiple Encryption for Email Gateway servers each run their own SMTP relay interface, and it is the responsibility of the mail server routing to Encryption for Email Gateway to load balance the requests. This method is more efficient and reliable than clustering because all boxes are active to increase throughput and the Encryption for Email Gateway servers are all running independently, dramatically reducing the chances of an issue affecting multiple boxes.

An advanced and preferred configuration to achieve this is to use a Layer-4 managed switch configured to use the round-robin algorithm to balance traffic equally across the farmed Encryption for Email Gateway servers. Figure 5-2 shows how such a deployment might look. For simplicity, only the outbound encrypted mail route is shown. In this example there are external content scanners responsible for classifying email to be encrypted.

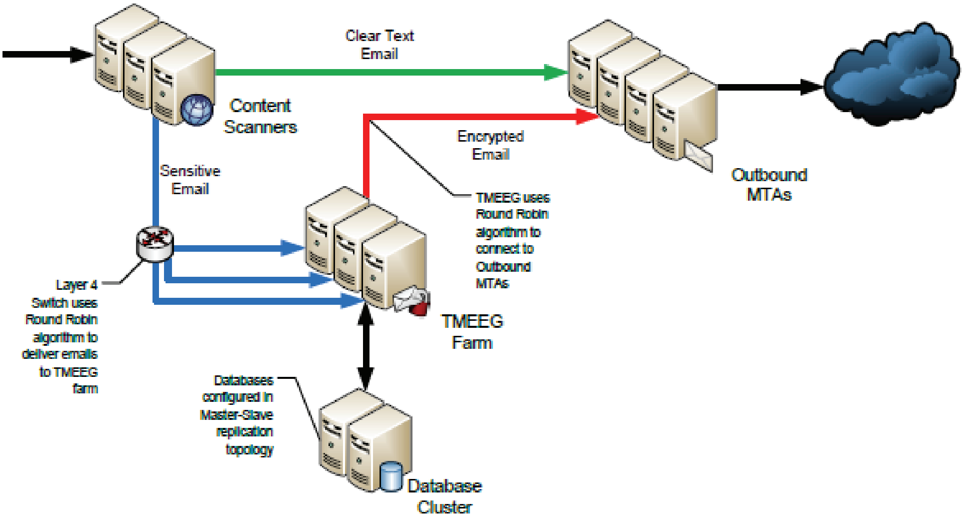

Clear Text Email
Content Scanners
Encrypted Email
Sensitive Email
TMEEG uses Round Robin algorithm to connect to Outbound MTAs
Outbound MTAs
Layer 4 Switch uses Round Robin algorithm to deliver emails to TMEEG farm
TMEEG Farm
Databases configured in Master-Slave replication topology
Database Cluster

FIGURE 5-2 Farmed Encryption for Email Gateway Deployment Showing only Outbound Encryption

Chapter 6

Administrative Options

The Encryption for Email Gateway administrative options are discussed in this chapter.

Topics include the following:

- Webmin
- Web Interface
- Runtime Configuration
- Basic Configuration Options
- Policy and Rules Engine
- Advanced Configuration Options

Many of the basic administration options can be configured through the Web interface application. This application is accessed by opening a Web browser and using the Gateway's host address. The configuration UI runs over HTTPS.

Note: The Certificate is self-signed and issued to *localhost.localdomain*. Additional configuration is required in order to upload and assign a correctly issued SSL certificate.

Webmin

Webmin is a Web-based interface for system administration for UNIX. Webmin removes the need to manually edit UNIX configuration files and lets you manage a system from the console or remotely using any modern Web browser. Webmin is configured to run over HTTPS on port 10000 of Encryption for Email Gateway.

To access Webmin on Encryption for Email Gateway, open a Web browser and enter the server address.

For example: `https://192.168.30.202:10000/`

Log in to Webmin using the root account on the Encryption for Email Gateway virtual appliance.

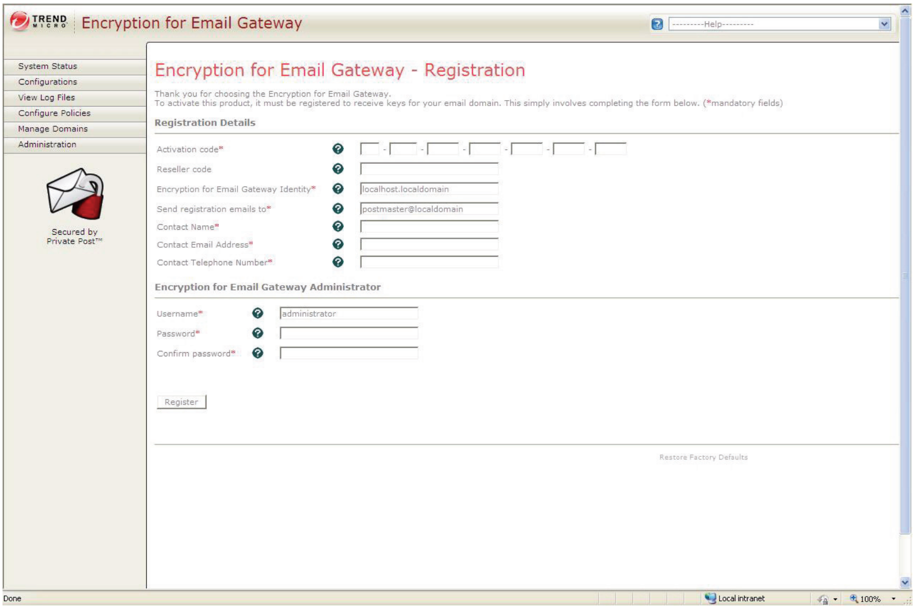
Web Interface

Encryption for Email Gateway provides an administrative Web interface for remote administration of Encryption for Email Gateway. In order to access the interface, a user name and password must be created during the initial configuration of the Encryption for Email Gateway server.

To access the Web interface on Encryption for Email Gateway, open a Web browser and enter the server address.

For example: `https://192.168.30.202/`

Figure 6-1 shows the initial Web interface screen on a new Encryption for Email Gateway installation. On this screen, the administrator is required to enter an activation code for the product as well as the registration information for Encryption for Email Gateway.



Encryption for Email Gateway - Registration

Thank you for choosing the Encryption for Email Gateway.
To activate this product, it must be registered to receive keys for your email domain. This simply involves completing the form below. (*mandatory fields)

Registration Details

Activation code* [ ] - [ ] - [ ] - [ ] - [ ] - [ ] - [ ]
Reseller code
Encryption for Email Gateway Identity* localhost.localdomain
Send registration emails to* postmaster@localdomain
Contact Name*
Contact Email Address*
Contact Telephone Number*

Encryption for Email Gateway Administrator

Username* administrator
Password*
Confirm password*

FIGURE 6-1 Encryption for Email Gateway Registration Screen

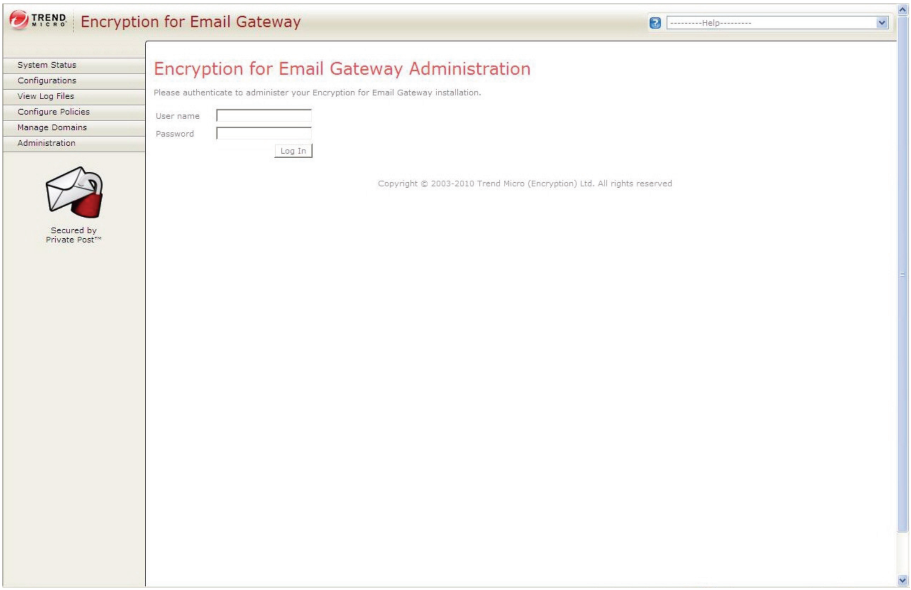
Note: Registration might take a considerable amount of time because of the security checks required to complete the process.

Figure 6-2 shows the main login screen displayed when connecting to the remote Web console.

To activate the Web UI Login screen:

1. Connect to the Encryption for Email Gateway Web Administration Console using a Web browser: `https://<eeg_address>/`
2. The Encryption for Email Gateway Administration screen appears.

After logging in, the user is presented with a series of tabbed sections, each of which are described in the following sections.



Encryption for Email Gateway Administration

Please authenticate to administer your Encryption for Email Gateway installation.

User name

Password

Copyright © 2003-2010 Trend Micro (Encryption) Ltd. All rights reserved

FIGURE 6-2 Encryption for Email Gateway Web UI Login Screen

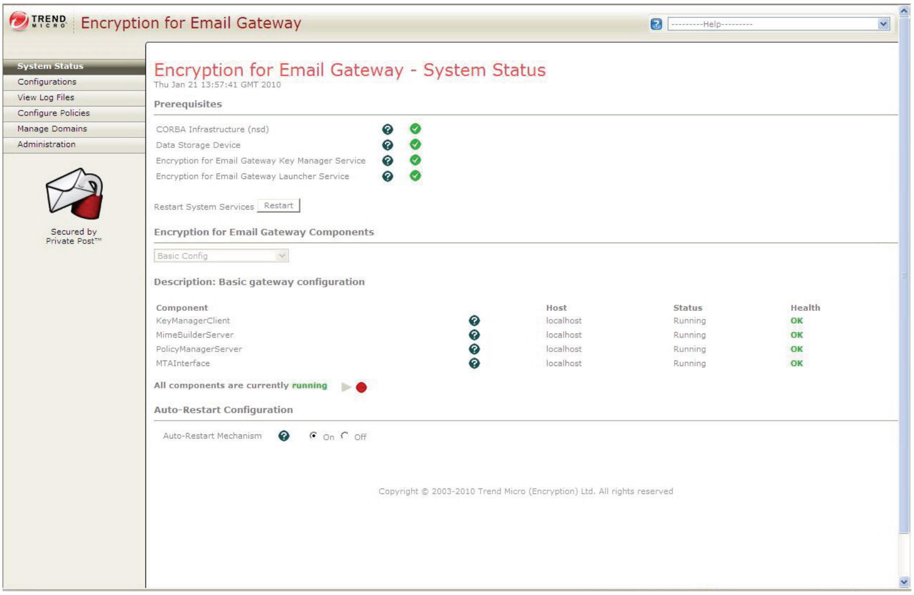
System Status

The System Status tab, as shown in Figure 6-3, provides a status overview of the Encryption for Email Gateway services and runtime components. From this screen it is possible to restart the system level services (listed under prerequisites), start and stop the runtime components (and therefore, Encryption for Email Gateway) and change the runtime configuration (see Runtime Configuration).

To access the Encryption for Email Gateway - System Status screen:

1. Select the **System Status** tab.

2. The System Status screen appears.



Encryption for Email Gateway - System Status

Thu Jan 21 13:57:41 GMT 2010

Prerequisites

CORBA Infrastructure (nsd) ✓

Data Storage Device ✓

Encryption for Email Gateway Key Manager Service ✓

Encryption for Email Gateway Launcher Service ✓

Restart System Services Restart

Encryption for Email Gateway Components

Basic Config

Description: Basic gateway configuration

Component	Host	Status	Health
KeyManagerClient	localhost	Running	OK
MimeBuilderServer	localhost	Running	OK
PolicyManagerServer	localhost	Running	OK
MTAInterface	localhost	Running	OK

All components are currently running ▶ ●

Auto-Restart Configuration

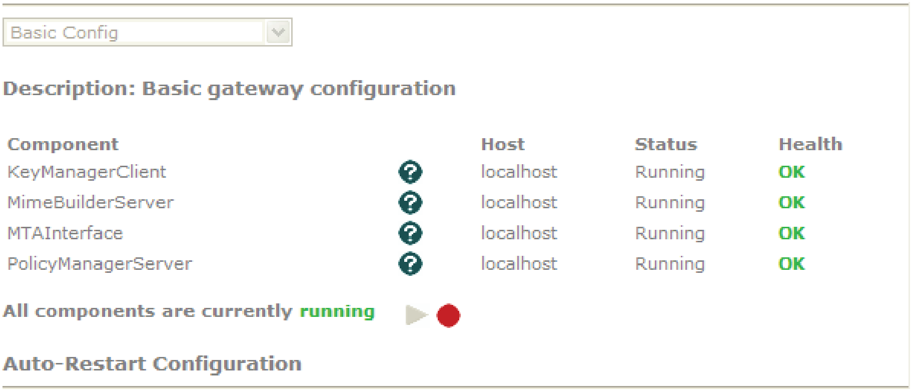
Auto-Restart Mechanism ● On ○ Off

Copyright © 2003-2010 Trend Micro (Encryption) Ltd. All rights reserved

FIGURE 6-3 Encryption for Email Gateway System Status screen

Auto-restart Configuration

After the initial startup of Encryption for Email Gateway (and each subsequent restart of the server) it is necessary to log into the Web console and start the runtime components. To do so, you must enter a password. This is a security measure that prevents the Encryption for Email Gateway box from being stolen and a malicious user gaining access to the keys. The passphrase is used to encrypt and decrypt the private keys in the database. Figure 6-4 shows the status as it should appear after the runtime components are started.



Basic Config

Description: Basic gateway configuration

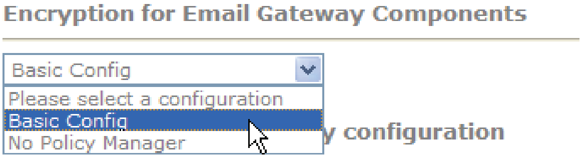
Component		Host	Status	Health
KeyManagerClient	?	localhost	Running	OK
MimeBuilderServer	?	localhost	Running	OK
MTAInterface	?	localhost	Running	OK
PolicyManagerServer	?	localhost	Running	OK

All components are currently running ▶ ●

Auto-Restart Configuration

FIGURE 6-4 Encryption for Email Gateway System Status with Runtime Components Launched

If multiple runtime configurations are enabled on the Encryption for Email Gateway server, the drop down list allows the administrator to select the desired configuration and launch it. After launched, the services must be stopped before the runtime configuration can be changed. Figure 6-5 illustrates the Encryption for Email Gateway server with multiple runtime configurations.



Encryption for Email Gateway Components

Basic Config

- Please select a configuration
- Basic Config
- No Policy Manager

y configuration

FIGURE 6-5 Encryption for Email Gateway System Status with Multiple Runtime Configurations

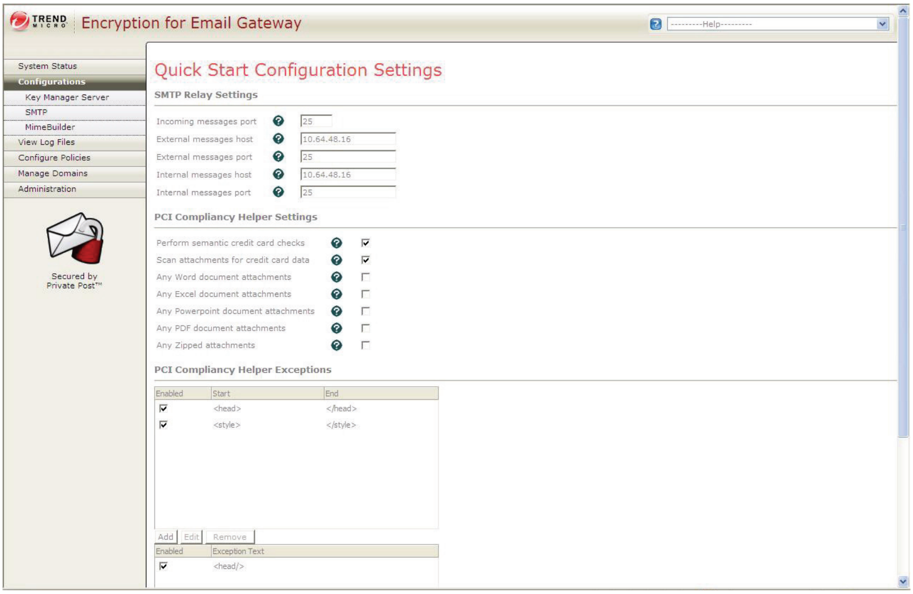
The auto-restart mechanism option enables the Encryption for Email Gateway runtime components to start automatically with the system services, for example after an upgrade or a reboot of the virtual appliance. By enabling this option, the passphrase is cached (in an encrypted state) on the Encryption for Email Gateway virtual appliance such that it can be automatically loaded as the system starts up.

The Restart System Services button invokes a restart of the components listed under the Prerequisites section.

Note: The Data Storage Device is not included in this restart.

Configuration

The Configuration tab provides the administrator with access to the basic system configuration options that are detailed in Basic Configuration Options. Figure 6-6 shows the Configurations Settings screen.



Quick Start Configuration Settings

SMTP Relay Settings

Incoming messages port	25
External messages host	10.64.48.16
External messages port	25
Internal messages host	10.64.48.16
Internal messages port	25

PCI Compliancy Helper Settings

Perform semantic credit card checks	☑
Scan attachments for credit card data	☑
Any Word document attachments	□
Any Excel document attachments	□
Any Powerpoint document attachments	□
Any PDF document attachments	□
Any Zipped attachments	□

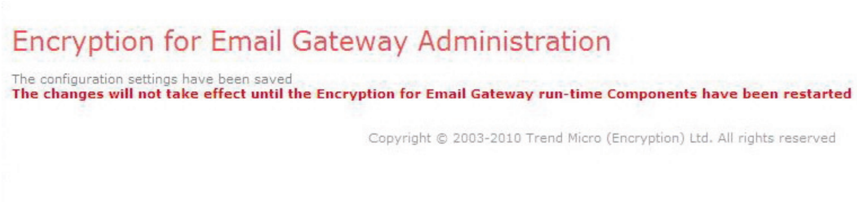
PCI Compliancy Helper Exceptions

Enabled	Start	End
☑	<head>	</head>
☑	<style>	</style>

Enabled	Exception Text
☑	<head/>

FIGURE 6-6 Encryption for Email Gateway Configuration Settings page

In order for configuration changes to take effect, the runtime components must be restarted through the System Status tab (see System Status). Figure 6-7 illustrates the Configuration screen after changes have been made and saved.



Encryption for Email Gateway Administration

The configuration settings have been saved

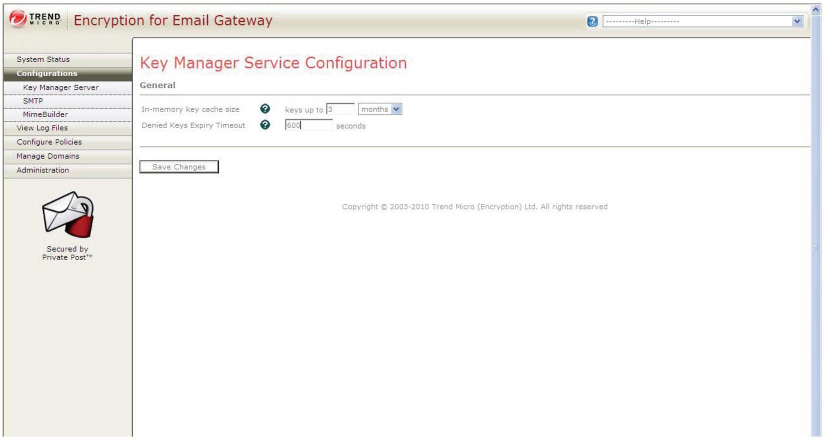
The changes will not take effect until the Encryption for Email Gateway run-time Components have been restarted

Copyright © 2003-2010 Trend Micro (Encryption) Ltd. All rights reserved

FIGURE 6-7 Encryption for Email Gateway Restart Runtime Components Notification

Key Manager Service Configuration

The Key Manager Service Configuration is accessible through the Key Manager Server menu item in the left Configurations menu. The default settings should be sufficient for the gateway to operate optimally. Figure 6-8 shows the Key Manager Service Configuration screen.



Key Manager Service Configuration

General

In-memory key cache size: keys up to 3 months

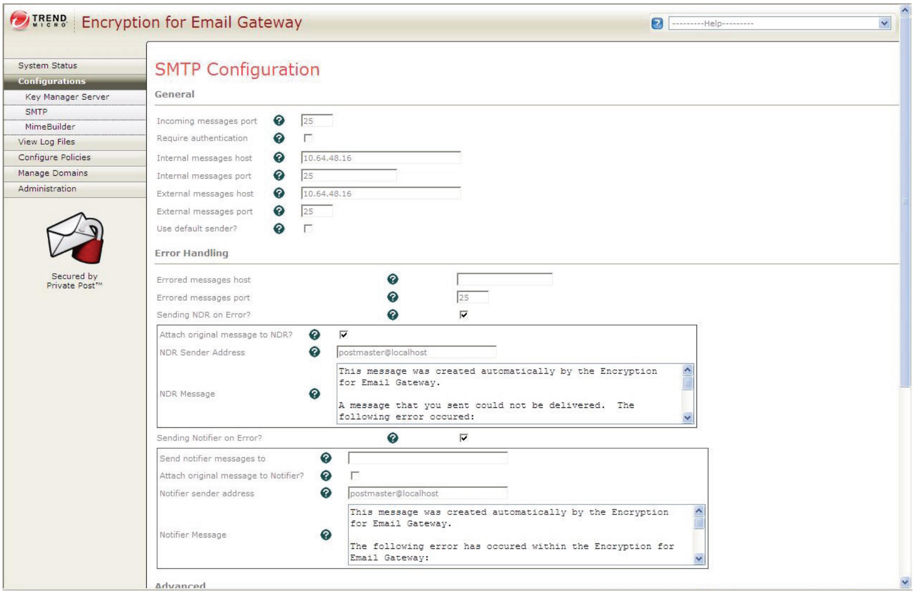
Denied Keys Expiry Timeout: 600 seconds

Copyright © 2003-2010 Trend Micro (Encryption) Ltd. All rights reserved

FIGURE 6-8 Key Manager Service Configuration

SMTP Configuration

The SMTP Configuration is accessible through the SMTP menu item in the left Configurations menu. Figure 6-9 shows the SMTP Configuration screen, and Figure 6-10 shows the advanced SMTP Configuration Settings (on the same screen as the basic settings).



SMTP Configuration

General

Incoming messages port: 25
Require authentication: ☐
Internal messages host: 10.64.48.16
Internal messages port: 25
External messages host: 10.64.48.16
External messages port: 25
Use default sender? ☐

Error Handling

Errored messages host:
Errored messages port: 25
Sending NDR on Error? ☑
Attach original message to NDR? ☑
NDR Sender Address: postmaster@localhost
NDR Message:

```
This message was created automatically by the Encryption
for Email Gateway.

A message that you sent could not be delivered.  The
following error occured:
```

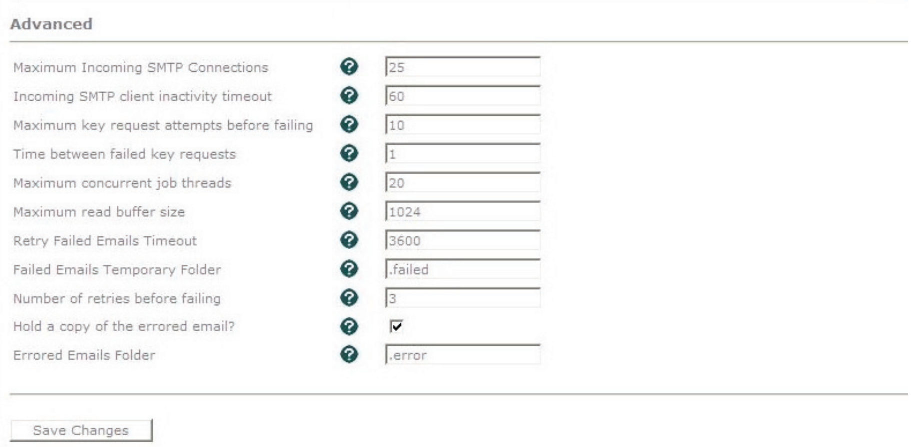
Sending Notifier on Error? ☑
Send notifier messages to:
Attach original message to Notifier? ☐
Notifier sender address: postmaster@localhost
Notifier Message:

```
This message was created automatically by the Encryption
for Email Gateway.

The following error has occured within the Encryption for
Email Gateway:
```

Advanced

FIGURE 6-9 Encryption for Email Gateway SMTP Configuration screen



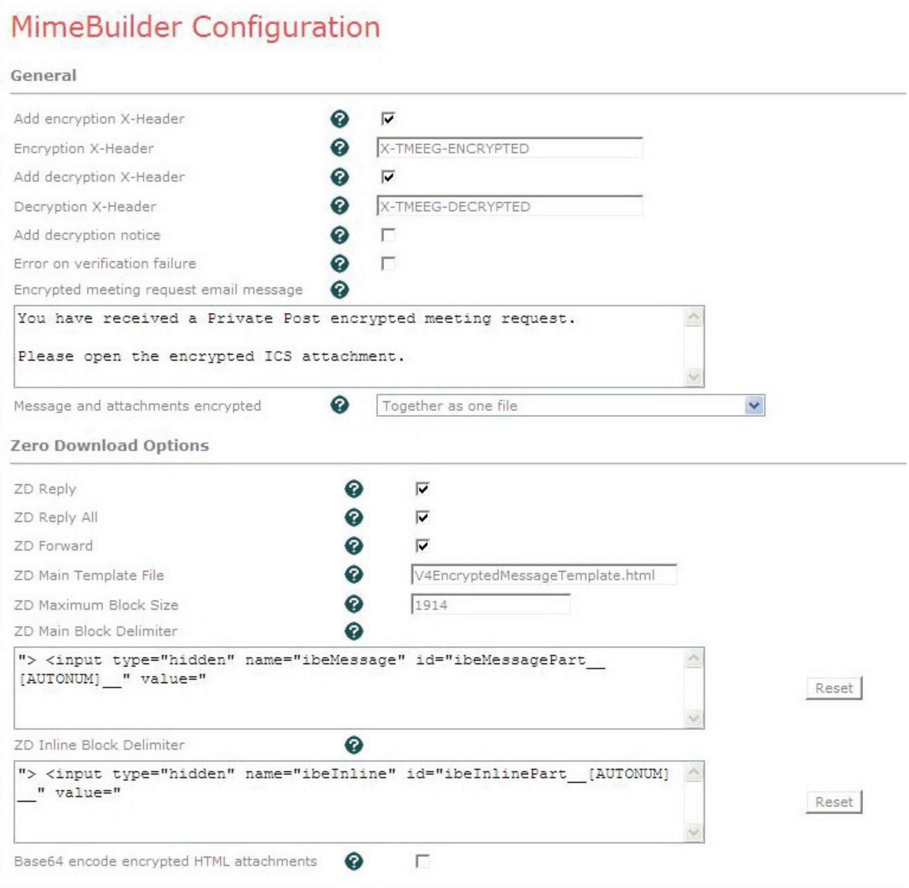
Advanced

Maximum Incoming SMTP Connections	25
Incoming SMTP client inactivity timeout	60
Maximum key request attempts before failing	10
Time between failed key requests	1
Maximum concurrent job threads	20
Maximum read buffer size	1024
Retry Failed Emails Timeout	3600
Failed Emails Temporary Folder	.failed
Number of retries before failing	3
Hold a copy of the errored email?	☑
Errored Emails Folder	.error

FIGURE 6-10 Encryption for Email Gateway Advanced SMTP Configuration

MIMEBuilder Configuration

The MIMEBuilder configuration is accessible through the MIMEbuilder link on the left menu. This enables the administrator to configure options regarding the MIME of emails which are encrypted or decrypted by Encryption for Email Gateway. Figure 6-11 shows the general MIMEBuilder options.



MimeBuilder Configuration

General

Add encryption X-Header ☑

Encryption X-Header: X-TMEEG-ENCRYPTED

Add decryption X-Header ☑

Decryption X-Header: X-TMEEG-DECRYPTED

Add decryption notice □

Error on verification failure □

Encrypted meeting request email message

```
You have received a Private Post encrypted meeting request.

Please open the encrypted ICS attachment.
```

Message and attachments encrypted: Together as one file

Zero Download Options

ZD Reply ☑

ZD Reply All ☑

ZD Forward ☑

ZD Main Template File: V4EncryptedMessageTemplate.html

ZD Maximum Block Size: 1914

ZD Main Block Delimiter

```
"> <input type="hidden" name="ibeMessage" id="ibeMessagePart__
[AUTONUM]__" value="
```

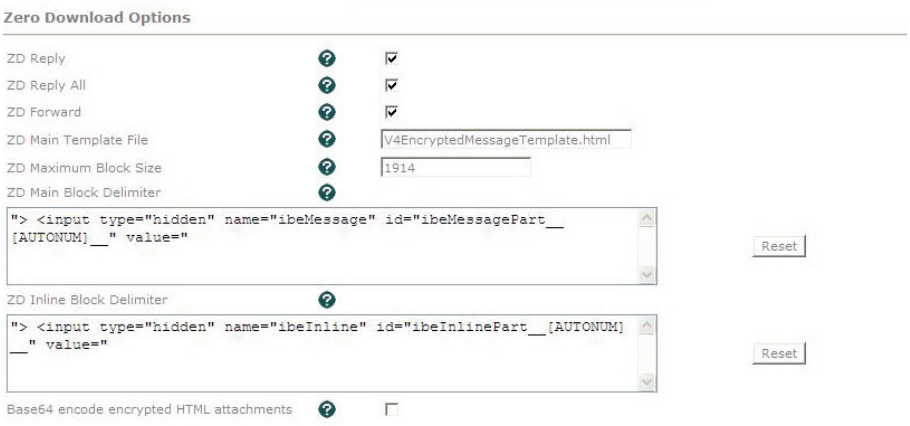
ZD Inline Block Delimiter

```
"> <input type="hidden" name="ibeInline" id="ibeInlinePart__[AUTONUM]
__" value="
```

Base64 encode encrypted HTML attachments □

FIGURE 6-11 General MIMEBuilder Configuration page

Depending on the outgoing encryption version setting, the Zero Download configuration options will be displayed, as in Figure 6-12.



Zero Download Options

ZD Reply ☑

ZD Reply All ☑

ZD Forward ☑

ZD Main Template File: V4EncryptedMessageTemplate.html

ZD Maximum Block Size: 1914

ZD Main Block Delimiter

```
"> <input type="hidden" name="ibeMessage" id="ibeMessagePart__
[AUTONUM]__" value="
```

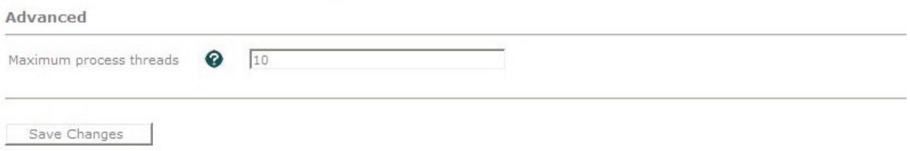
ZD Inline Block Delimiter

```
"> <input type="hidden" name="ibeInline" id="ibeInlinePart__[AUTONUM]
__" value="
```

Base64 encode encrypted HTML attachments ☐

FIGURE 6-12 Zero Download page

Figure 6-13 shows the advanced MIMEBuilder options which can be found at the bottom of the MIMEBuilder configuration page. Refer to the (MIMEBuilder Config table) for details on the configuration options available.



Advanced

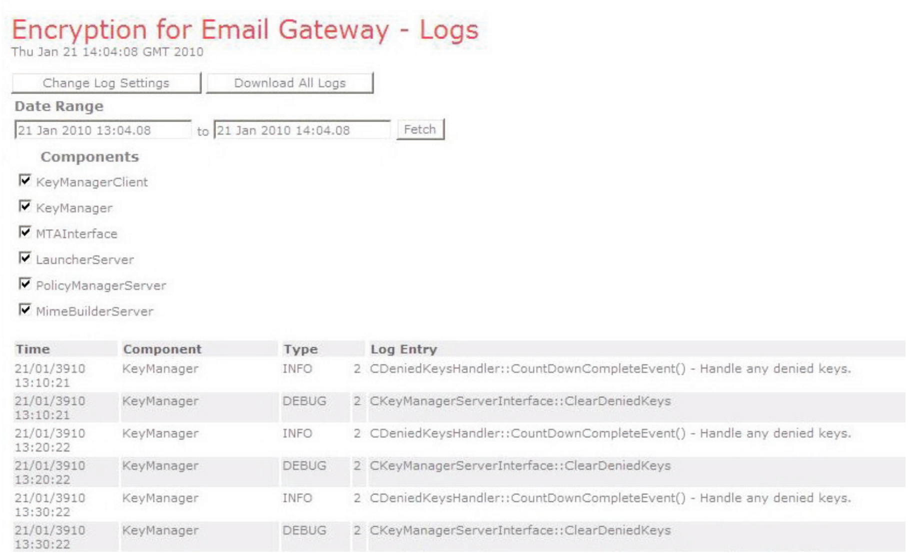
Maximum process threads: 10

FIGURE 6-13 MIMEBuilder Advanced page

View Log Files

The View Logs tab enables the administrator to configure log levels and settings, as well as view the system logs. To view the complete logs, they are (by default) stored in `/var/log/ppg/` and can be accessed by the root user on the Encryption for Email Gateway server console.

Figure 6-14 shows the View Logs tab. Figure 6-15 and Figure 6-16 show the Configure Log Options and Log View respectively. The “Download All Logs” button will download a compressed archive of all the Encryption for Email Gateway logs on the system.



Encryption for Email Gateway - Logs

Thu Jan 21 14:04:08 GMT 2010

Date Range

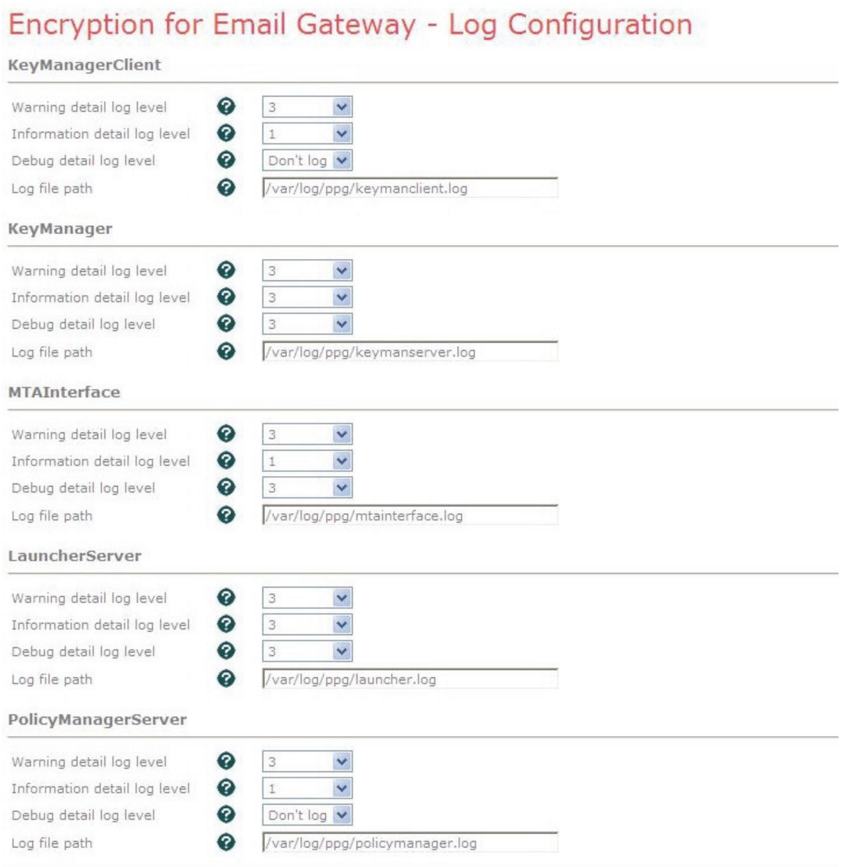
21 Jan 2010 13:04.08 to 21 Jan 2010 14:04.08

Components

☑ KeyManagerClient
☑ KeyManager
☑ MTAInterface
☑ LauncherServer
☑ PolicyManagerServer
☑ MimeBuilderServer

Time	Component	Type		Log Entry
21/01/3910 13:10:21	KeyManager	INFO	2	CDeniedKeysHandler::CountDownCompleteEvent() - Handle any denied keys.
21/01/3910 13:10:21	KeyManager	DEBUG	2	CKeyManagerServerInterface::ClearDeniedKeys
21/01/3910 13:20:22	KeyManager	INFO	2	CDeniedKeysHandler::CountDownCompleteEvent() - Handle any denied keys.
21/01/3910 13:20:22	KeyManager	DEBUG	2	CKeyManagerServerInterface::ClearDeniedKeys
21/01/3910 13:30:22	KeyManager	INFO	2	CDeniedKeysHandler::CountDownCompleteEvent() - Handle any denied keys.
21/01/3910 13:30:22	KeyManager	DEBUG	2	CKeyManagerServerInterface::ClearDeniedKeys

FIGURE 6-14 Encryption for Email Gateway View Log Files



Encryption for Email Gateway - Log Configuration

KeyManagerClient

Warning detail log level: 3
Information detail log level: 1
Debug detail log level: Don't log
Log file path: /var/log/ppg/keymanclient.log

KeyManager

Warning detail log level: 3
Information detail log level: 3
Debug detail log level: 3
Log file path: /var/log/ppg/keymanserver.log

MTAInterface

Warning detail log level: 3
Information detail log level: 1
Debug detail log level: 3
Log file path: /var/log/ppg/mtainterface.log

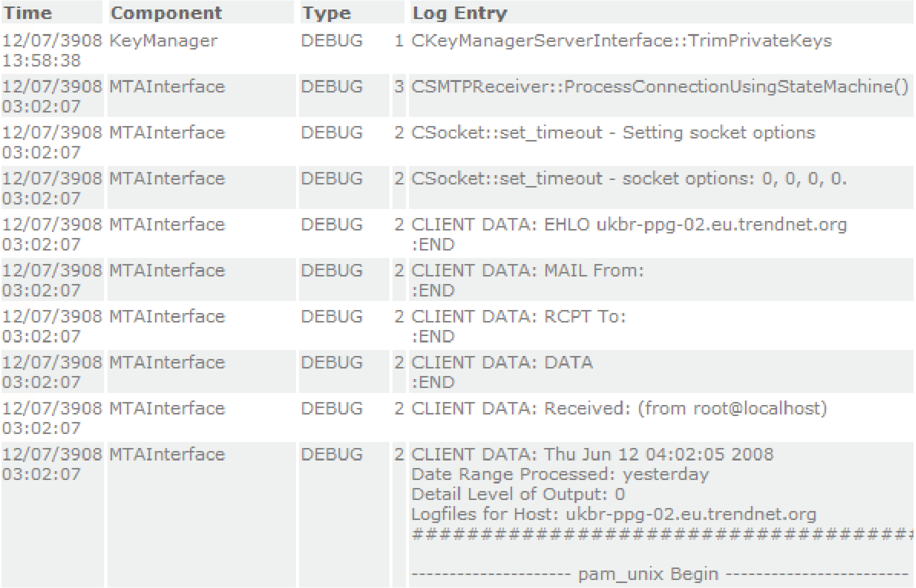
LauncherServer

Warning detail log level: 3
Information detail log level: 3
Debug detail log level: 3
Log file path: /var/log/ppg/launcher.log

PolicyManagerServer

Warning detail log level: 3
Information detail log level: 1
Debug detail log level: Don't log
Log file path: /var/log/ppg/policymanager.log

FIGURE 6-15 Encryption for Email Gateway Log Configuration screen

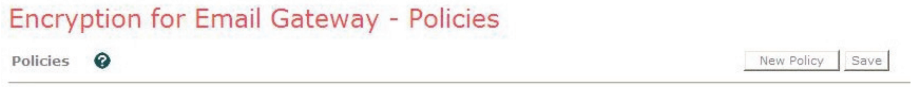


Time	Component	Type		Log Entry
12/07/3908 13:58:38	KeyManager	DEBUG	1	CKeyManagerServerInterface::TrimPrivateKeys
12/07/3908 03:02:07	MTAInterface	DEBUG	3	CSMTPReceiver::ProcessConnectionUsingStateMachine()
12/07/3908 03:02:07	MTAInterface	DEBUG	2	CSocket::set_timeout - Setting socket options
12/07/3908 03:02:07	MTAInterface	DEBUG	2	CSocket::set_timeout - socket options: 0, 0, 0, 0.
12/07/3908 03:02:07	MTAInterface	DEBUG	2	CLIENT DATA: EHLO ukbr-ppg-02.eu.trendnet.org :END
12/07/3908 03:02:07	MTAInterface	DEBUG	2	CLIENT DATA: MAIL From: :END
12/07/3908 03:02:07	MTAInterface	DEBUG	2	CLIENT DATA: RCPT To: :END
12/07/3908 03:02:07	MTAInterface	DEBUG	2	CLIENT DATA: DATA :END
12/07/3908 03:02:07	MTAInterface	DEBUG	2	CLIENT DATA: Received: (from root@localhost)
12/07/3908 03:02:07	MTAInterface	DEBUG	2	CLIENT DATA: Thu Jun 12 04:02:05 2008 Date Range Processed: yesterday Detail Level of Output: 0 Logfiles for Host: ukbr-ppg-02.eu.trendnet.org #################################### -------------------- pam_unix Begin -----------------------

FIGURE 6-16 Encryption for Email Gateway View Logs

Configure Policies

The Policy Management tab provides access to the rules engine for configuring the policies to apply to email; for example, "encrypt all outbound email with the word PRIVATE in the subject line." Through this interface, the administrator has complete control over the policy engine. Figure 6-17 shows the Policy tab as it is initially displayed (with no rules). For details on the types of rules that can be applied, see Basic Configuration Options and Policy and Rules Engine.



Encryption for Email Gateway - Policies

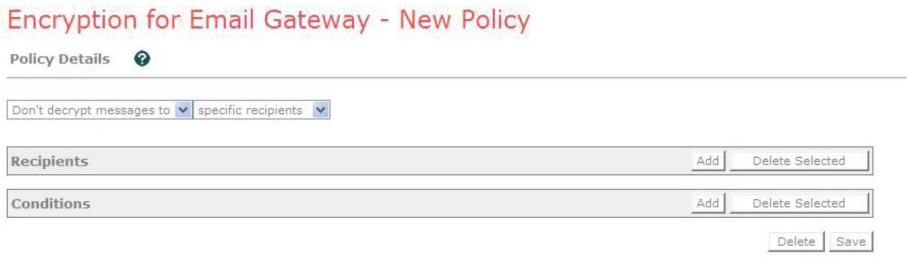
Policies

FIGURE 6-17 Encryption for Email Gateway Default Policy Screen

Duplicate policies will be merged. If a new policy is created and it matches an existing policy, the new policy will not be added to the database. If an existing policy is edited, and the modification resulted in duplicate policies, the edited policy will be removed from the database. For example, if after modifying policy P2, it becomes the same as P1, then P2 will be removed.

Adding Rules

To add new rules, click **New Policy** to take the administrator to the New Policy screen as show in Figure 6-18.



Encryption for Email Gateway - New Policy

Policy Details

Don't decrypt messages to | specific recipients

FIGURE 6-18 Encryption for Email Gateway New/Edit Policy

Editing Rules

To edit a rule, simply double-click it. This will take you to the New/Edit Policy page as shown in Figure 6-18.

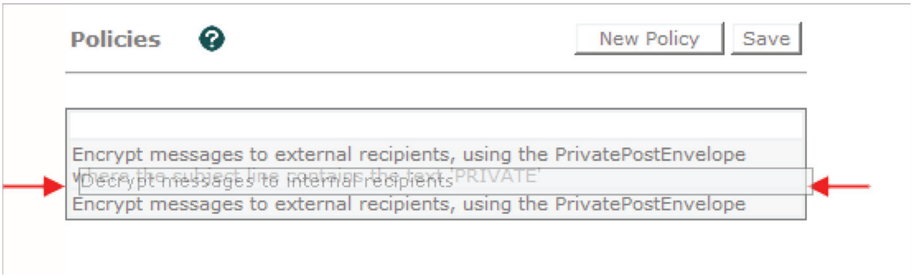
Deleting Rules

To delete a rule, simply double-click it to bring up the New/Edit Policy page and click **Delete** (see Figure 6-18).

Reordering Rules

Rules are logical or between one another and as soon as a match is found, that rule is applied. If no match is found, then the default built-in rules are applied (see Policy and Rules Engine).

To reorder policies, drag and drop them into the desired order as shown in Figure 6-19.



Encrypt messages to external recipients, using the PrivatePostEnvelope
Where the subject line contains the text 'PRIVATE'
Decrypt messages to internal recipients
Encrypt messages to external recipients, using the PrivatePostEnvelope

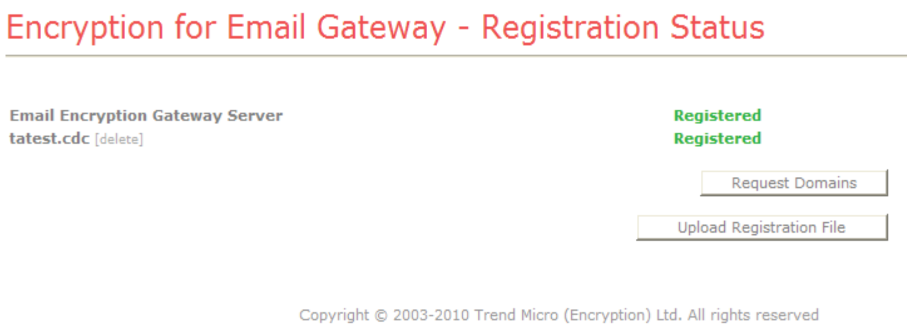
FIGURE 6-19 Figure 19 - Encryption for Email Gateway Reorder Policies

Manage Domains

The Manage Domains tab enables the administrator to register new domains for use with Encryption for Email Gateway. When a domain is registered with Encryption for Email Gateway, it is permitted to obtain private keys for email addresses on that domain, or any subdomain thereof. An example would be registering mycompany.org. After the registration is authorized and completed on Encryption for Email Gateway, Encryption for Email Gateway will be able to obtain private keys to decrypt email to user01@mycompany.org, user02@mycompany.org, and so on, as well as user01@admin.mycompany.org, user02@finance.mycompany.org. The security processes and checks to authorize an Encryption for Email Gateway domain registration, and will include checking publicly available information that might include contacting the domain registrant.

Note: For security reasons, the person who is the registered owner of the domain will be contacted by the registration team to validate the Encryption for Email Gateway registration. Therefore, to register a domain, you must be the owner of, or have the permission of the owner of the domain name.

It is possible to remove a domain registration from an Encryption for Email Gateway by selecting the [delete] link next to the domain. This removes the registration information from the Encryption for Email Gateway database and it will no longer be possible to obtain private keys for email addresses on this domain.



Encryption for Email Gateway - Registration Status

Email Encryption Gateway Server	Registered
tatest.cdc [delete]	Registered

Request Domains
Upload Registration File
Copyright © 2003-2010 Trend Micro (Encryption) Ltd. All rights reserved

FIGURE 6-20 Encryption for Email Gateway Registration Status

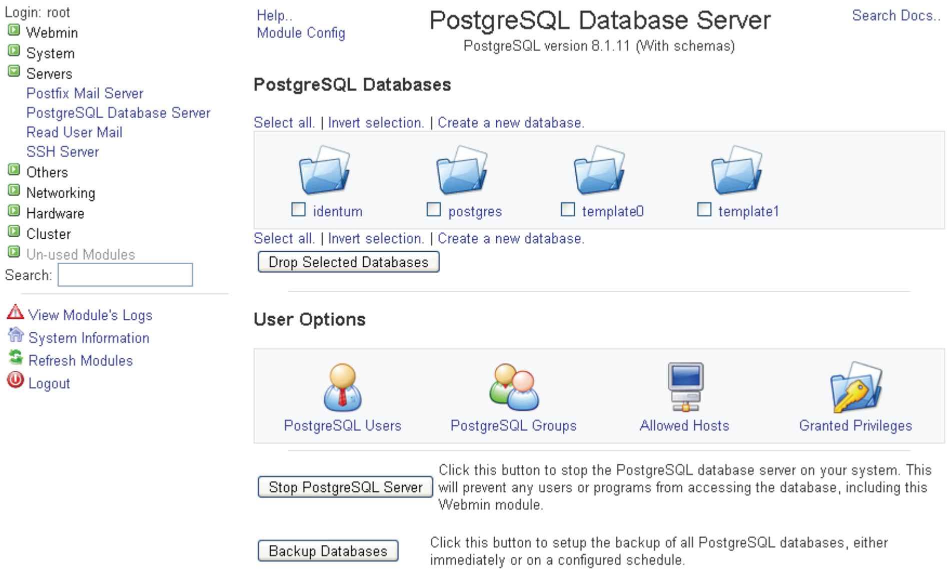
By design, after a domain is registered, it cannot be re-registered. If a domain has already been registered, subsequent re-registration results in a “domain already registered” error. This is enforced for the purpose of security. This also applies to the domain name used to register Encryption for Email Gateway. If there is a need to reinstall Encryption for Email Gateway, backup the database prior to re-installation, and restore it afterwards. This eliminates the need to re-register Encryption for Email Gateway and the same domains after re-installation.

However, if backing-up and restoring the database is not an option, submit a support request to remove the registration records from our internal database. Our registration management team will verify that you have the permission to remove these records, and then process the request. After the records have been removed, our support team will notify you to re-register. Because this is a time consuming process, only use this process as a last resort.

To backup the database:

1. Open the PostgreSQL Database server from Webmin.

2. The PostgreSQL Database Server page appears.

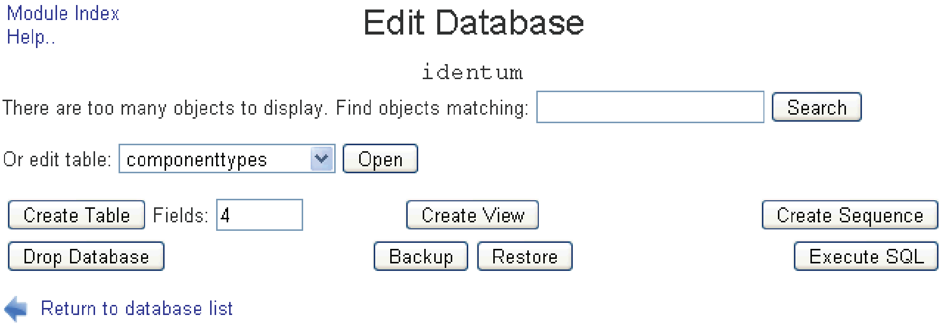


Click this button to stop the PostgreSQL database server on your system. This will prevent any users or programs from accessing the database, including this Webmin module.

Click this button to setup the backup of all PostgreSQL databases, either immediately or on a configured schedule.

FIGURE 6-21 PostgreSQL Database Server page

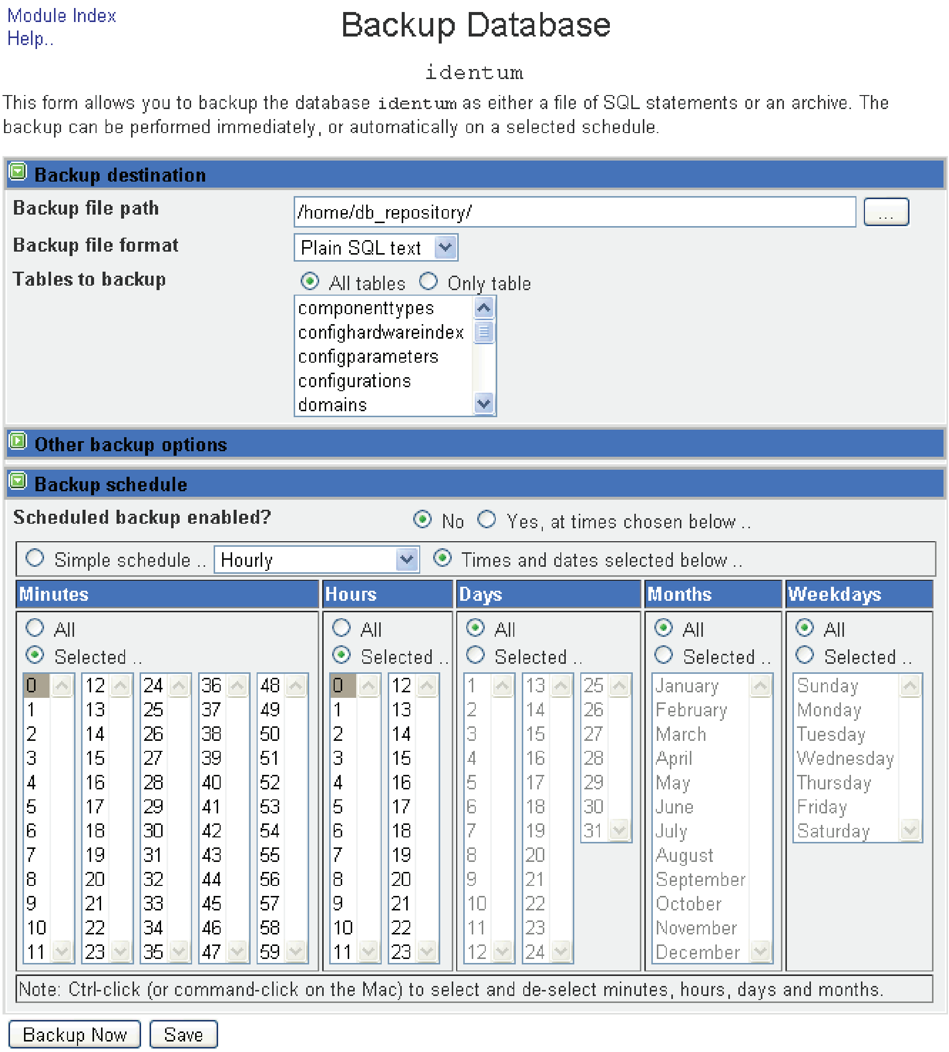
3. Click the identum icon.
4. The Edit Database page appears.



There are too many objects to display. Find objects matching:

FIGURE 6-22 Edit Database page

5. Click **Backup** in the Edit Database page.
6. The Backup Database page appears.



Module Index
Help..

Backup Database

identum

This form allows you to backup the database identum as either a file of SQL statements or an archive. The backup can be performed immediately, or automatically on a selected schedule.

Backup destination

Backup file path	/home/db_repository/ [...]
Backup file format	Plain SQL text
Tables to backup	● All tables ○ Only table componenttypes confighardwareindex configparameters configurations domains

Other backup options

Backup schedule

Scheduled backup enabled? ● No ○ Yes, at times chosen below ..

○ Simple schedule .. Hourly ● Times and dates selected below ..

Minutes: ○ All ● Selected ..
0 1 2 3 4 5 6 7 8 9 10 11 | 12 13 14 15 16 17 18 19 20 21 22 23 | 24 25 26 27 28 29 30 31 32 33 34 35 | 36 37 38 39 40 41 42 43 44 45 46 47 | 48 49 50 51 52 53 54 55 56 57 58 59

Hours: ○ All ● Selected ..
0 1 2 3 4 5 6 7 8 9 10 11 | 12 13 14 15 16 17 18 19 20 21 22 23

Days: ● All ○ Selected ..
1 2 3 4 5 6 7 8 9 10 11 12 | 13 14 15 16 17 18 19 20 21 22 23 24 | 25 26 27 28 29 30 31

Months: ● All ○ Selected ..
January February March April May June July August September October November December

Weekdays: ● All ○ Selected ..
Sunday Monday Tuesday Wednesday Thursday Friday Saturday

Note: Ctrl-click (or command-click on the Mac) to select and de-select minutes, hours, days and months.

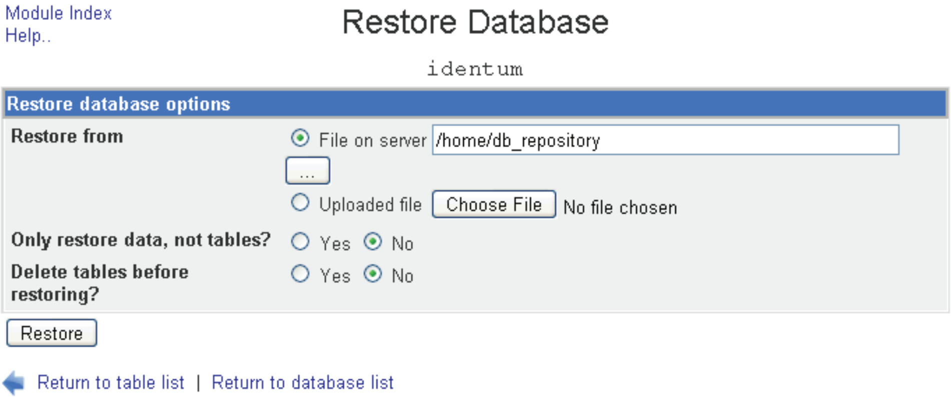
[Backup Now] [Save]

FIGURE 6-23 Backup Database page

7. Finally, edit the backup file path as needed in the Backup Database page, and then click **Backup Now**.

To restore the database:

1. Open the PostgreSQL Database server from Webmin.
2. Click the identum icon (see Figure 6-21).
3. Next, click **Restore** on the Edit Database page (see Figure 6-22).
4. Edit the restore from file path as needed in the Restore Database page, and then click **Restore** (see Figure 6-24).



Restore Database

identum

Restore database options	
Restore from	● File on server /home/db_repository ... ○ Uploaded file Choose File No file chosen
Only restore data, not tables?	○ Yes ● No
Delete tables before restoring?	○ Yes ● No

Restore

FIGURE 6-24 Restore Database page

Administration Screens

The Administration menu shown in Figure 6-25 provides access to features for upgrading and other administrative tasks. The following section provides an overview of these features.

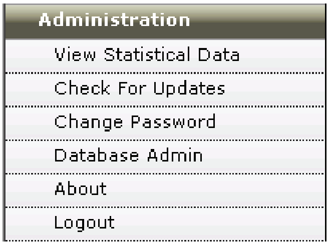


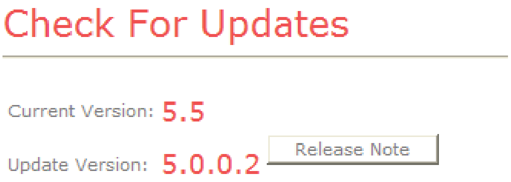
FIGURE 6-25 Encryption for Email Gateway Administration Menu Options

View Statistical Data

This displays graphical statistics data on the number of encryptions and decryptions performed by Encryption for Email Gateway over the specified period. Emails that are passed through Encryption for Email Gateway without being encrypted or decrypted are also recorded.

Check for Updates

Check for Updates enables online updating of the Encryption for Email Gateway software. Figure 6-26 through Figure 6-28 show the update process. When the update is complete the system auto-redirects the user to the System Status page (refer to System Status) so that the runtime components can be restarted.

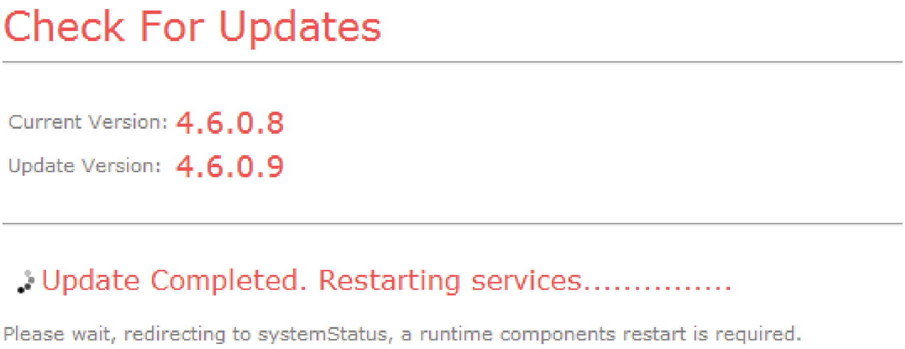


Check For Updates

Current Version: 5.5

Update Version: 5.0.0.2

FIGURE 6-26 Encryption for Email Gateway Check for Updates: updates available



Check For Updates

Current Version: 4.6.0.8

Update Version: 4.6.0.9

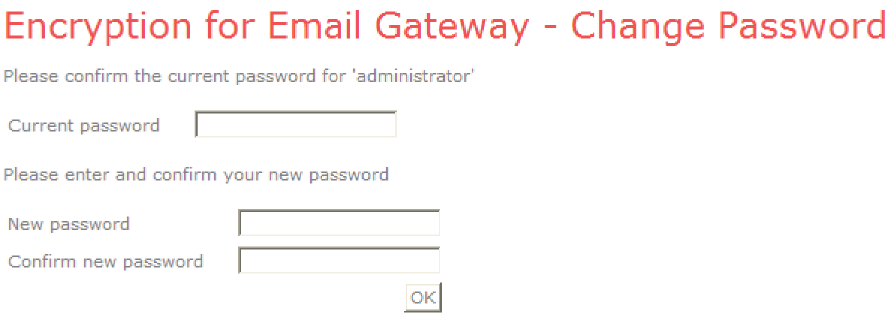
Update Completed. Restarting services...............

Please wait, redirecting to systemStatus, a runtime components restart is required.

FIGURE 6-27 Encryption for Email Gateway Check for Updates: latest version installed

Change Password

The Change Password option allows the current Web user to change the password used to access the Web interface. Note that this is different from the Passphrase used to start the runtime components. It is not possible to change the Passphrase used to start the runtime components. Figure 6-28 shows the Change Password screen.



Encryption for Email Gateway - Change Password

Please confirm the current password for 'administrator'

Current password

Please enter and confirm your new password

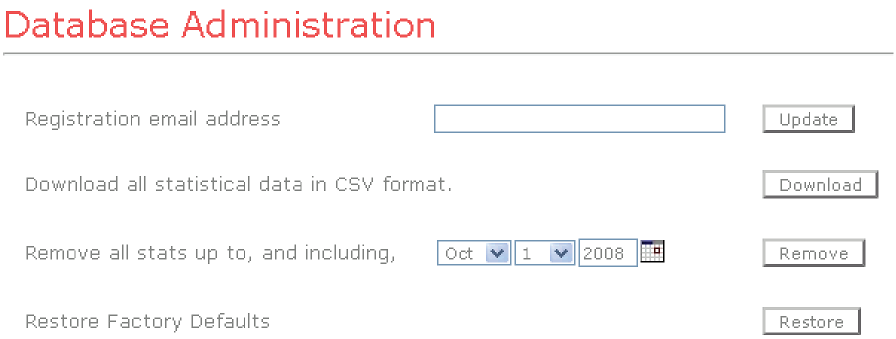
New password

Confirm new password

FIGURE 6-28 Encryption for Email Gateway Change Password screen

Database Administration

The Database Administration screen enables the administrator to reset the database to the factory default. This deletes all registration settings from Encryption for Email Gateway. Figure 6-29 shows the Database Administration screen.



Database Administration

Registration email address

Download all statistical data in CSV format.

Remove all stats up to, and including, Oct 1 2008

Restore Factory Defaults

FIGURE 6-29 Encryption for Email Gateway Database Administration screen

Registration Email Address

Changes the email address registration emails go to (this is initially entered during the Encryption for Email Gateway registration).

Download all statistical data in CSV format

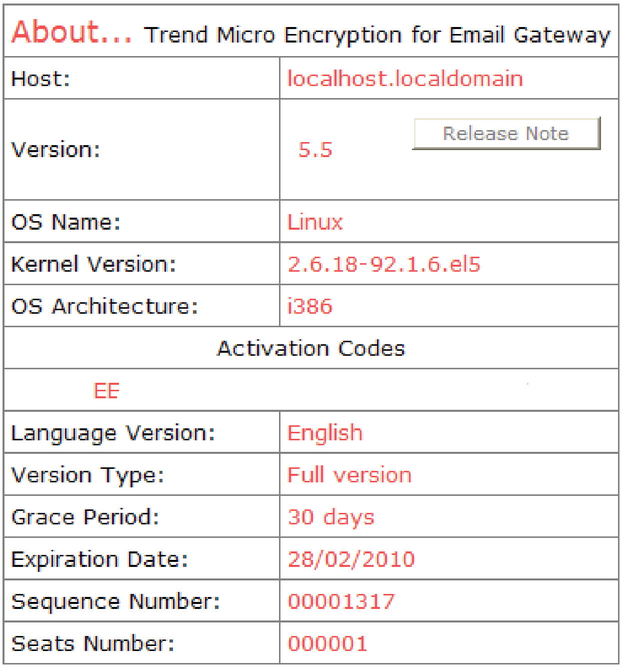
Downloads all statistical data in the CSV format.

Remove all stats up to and including <date>

Truncates the stats data to clear historical data as requested.

About...

The About screen displays the operating system and the Encryption for Email Gateway information that might be of use to the administrator, including the activation code and licensing information. Figure 6-30 shows the About… screen.



About... Trend Micro Encryption for Email Gateway	
Host:	localhost.localdomain
Version:	5.5
OS Name:	Linux
Kernel Version:	2.6.18-92.1.6.el5
OS Architecture:	i386
Activation Codes	
EE	
Language Version:	English
Version Type:	Full version
Grace Period:	30 days
Expiration Date:	28/02/2010
Sequence Number:	00001317
Seats Number:	000001

FIGURE 6-30 Encryption for Email Gateway About... screen

Runtime Configuration

Encryption for Email Gateway is preconfigured with two runtime configurations described as follows.

Basic Configuration

The Basic Configuration comprises of one instance of each of the MIMEBuilder, Key Manager Client, Policy Manager and MTA Interface. This configuration is the default setting and uses the Policy Manager for rules based encryption and decryption of messages as they pass through Encryption for Email Gateway.

No Policy Manager

This configuration comprises of one instance of each of the MIMEBuilder, Key Manager Client and MTA Interface, without a policy manager. This configuration causes Encryption for Email Gateway to use the default rules (see Policy and Rules Engine) that decrypts all inbound and encrypts all outbound messages. It is recommended that an external policy manager deployment scenario is used.

Basic Configuration Options

The Encryption for Email Gateway configuration is split into four categories:

1. Quick Start
2. Key Manager Server
3. SMTP
4. MIMEBuilder

Refer to the following tables for details of the configuration options for each configuration section.

Table 6-1 lists the configuration options accessible through the Web UI and their descriptions.

TABLE 6-1. Quick Start Configuration Settings

PARAMETER	DESCRIPTION
SMTP RELAY SETTINGS	
Incoming Messages Port	The port that Encryption for Email Gateway should listen on for incoming messages (default is 25).
External Messages Host	The hostname or IP address to send external emails to.
External messages port	The port on the External Messages Host to send external emails to.
Internal messages host	The hostname or IP address to send internal emails to.
Internal messages port	The port on the Internal Messages Host to send internal emails to.
PCI COMPLIANCY HELPER SETTINGS	
Perform semantic credit card checks	Enable PCI compliancy helper and credit card checking in the Policy Manager.
Scan attachments credit card data	Enable Credit Card check helper checking of attachments in the Policy Manager.
Any Word document attachments	Encrypt all emails with Word Attachments.
Any Excel document attachments	Encrypt all emails with Excel Attachments.

TABLE 6-1. Quick Start Configuration Settings (Continued)

Any PowerPoint document attachments	Encrypt all emails with PowerPoint Attachments.
Any PDF document attachments	Encrypt all emails with PDF Attachments.
Any Zipped attachments	Encrypt all emails with Zipped Attachments.
PCI Compliancy Helper Exceptions	Ignore anything between specific monikers in the message body.

TABLE 6-2. Key Manager Server Settings

PARAMETER	DESCRIPTION
GENERAL SETTINGS	
In-memory key cache size	Length of time to cache Private Keys in memory.
Denied Keys Expiry Timeout	Timeout between retrying to obtain keys after a “key Denied” error.

TABLE 6-3. SMTP Settings

PARAMETER	DESCRIPTION
GENERAL SETTINGS	
Incoming Messages Port	The port that Encryption for Email Gateway should listen on for incoming messages (default is 25).

TABLE 6-3. SMTP Settings (Continued)

Require Authentication	Should Encryption for Email Gateway force SMTP authentication on incoming connections (see Authentication settings below).
External Messages Host	The hostname or IP address to send external emails to.
External messages port	The port on the External Messages Host to send external emails to.
Internal messages host	The hostname or IP address to send internal emails to.
Internal messages port	The port on the Internal Messages Host to send internal emails to.
Use default sender?	Should a default sender address be used to sign encrypted emails in the event of not being able to get a private key for the real sender.
Default sender address	Email address to use if User Default Sender is enabled.
AUTHENTICATION SETTINGS	
Authentication username	Username required for authentication.
Authentication password	Password required for authentication.
ERROR HANDLING SETTINGS	
Errored messages host	The hostname or IP address to send error emails to.
Errored messages port	The port on the Errored Messages Host to send errored emails to.

TABLE 6-3. SMTP Settings (Continued)

Sending NDR on Error?	Send a NDR to the message sender if an error occurs processing their email (see NDR settings below).
Sending Notifier on Error?	Send a notification to configured mailboxes if an error occurs processing emails in Encryption for Email Gateway (see Notifier settings below).
NDR SETTINGS	
Attach original message to NDR?	Attach the original (errored) email to the NDR
NDR Sender Address	Email address to use as the FROM address in the NDR
NDR Message	Message body to display in the NDR (refer to Table 10).
NOTIFIER SETTINGS	
Send notifier messages to	Who should the notification emails be sent to as a comma separated list of email addresses.
Attach original message to Notifier?	Attach the original (errored) email to the notification
Notifier Sender Address	Email address to use as the FROM address in the notification
Notifier Message	Message body to display in the notification (refer to Table 10).
ADVANCED SETTINGS	
Maximum Incoming SMTP Connections	Maximum number of simultaneous inbound connects to the SMTP interface.

TABLE 6-3. SMTP Settings (Continued)

Incoming SMTP client inactivity timeout	Number of seconds of inactivity before timing out the SMTP session.
Maximum key request attempts before failing	Number of key request attempts before generating key request failure.
Time between failed key requests	Number of seconds to wait between key request attempts.
Maximum concurrent job threads	Number of SMTP processing threads.
Maximum read buffer size	SMTP interface incoming buffer size.
Retry Failed Emails Timeout	Number of seconds between retrying failed emails – used in conjunction with the Number of retries before failing value.
Failed Emails Temporary Folder	Folder to hold errored emails in, during the retry period.
Number of retries before failing	Number of attempts at processing an email before permanently failing it.
Hold a copy of the errored email?	Hold a copy of the errored email on permanent failure.
Errored Emails Folder	Folder to hold permanently failed emails in.

TABLE 6-4. MIMEBuilder Settings

PARAMETER	DESCRIPTION
GENERAL SETTINGS	
Add encryption X-Header	Add an X-Header to emails encrypted by Encryption for Email Gateway.
Encryption X-Header	The name of the X-Header to add. The value of the X-Header will be the Encryption for Email Gateway Identity as configured during initial registration.
Add decryption X-Header	Add an X-Header to emails decrypted by Encryption for Email Gateway.
Decryption X-Header	The name of the X-Header to add. The value of the X-Header will be the Encryption for Email Gateway Identity as configured during initial registration.
Add decryption notice	Add a notice to the bottom of emails decrypted by Encryption for Email Gateway.
Decryption notice	Decryption notice to add to emails decrypted by Encryption for Email Gateway.
Error on verification failure	Error an email if the digital signature verification fails on an email.
Encrypted meeting request email message	Body text to display if a meeting request is encrypted by Encryption for Email Gateway.

TABLE 6-4. MIMEBuilder Settings (Continued)

Encrypt outgoing messages to Private Post	Encrypted message format version to use. Version 3 and Version 4 are binary formats and do not allow for Web-based decrypting of email messages.
ZERO DOWNLOAD SETTINGS	
ZD Reply	Enable Zero Download „Reply? on encrypted emails.
ZD Reply All	Enable Zero Download „Reply to All? on encrypted emails.
ZD Forward	Enable Zero Download „Forward? on encrypted emails.
ZD Main Template File	Template file to use for the main message body of a Zero Download encrypted message.
ZD Attachment Template File	Template file to use for attachments of a Zero Download encrypted message.
ZD Attachment Contents Link File	File to use as the message body of an encrypted attachment on a Zero Download encrypted message.
ZD Maximum Block Size	Maximum size of blocks in a Zero Download message (should be left as is at 1914).
ZD Main Block Delimiter	Delimiter between data blocks in a Zero Download message (should be left as is).
ZD Inline Block Delimiter	Delimiter between data blocks in a Zero Download inline attachment (should be left as is).

TABLE 6-4. MIMEBuilder Settings (Continued)

Base64 encode encrypted HTML attachments	Use Base64 encoding on outbound encrypted emails (default is quoted-printable).
ADVANCED SETTINGS	
Maximum process threads	Maximum number of threads for processing MIME-data.

Monikers

NDR and Notification error messages contain monikers that are replaced on a per message basis. Table 6-5 lists the monikers available.

TABLE 6-5. Usable Monikers in NDR and Notification Messages

MONIKER	DESCRIPTION
__[EEG_ERROR_MESSAGE]__	Error message generated by Encryption for Email Gateway.
__[EEG_MESSAGE_ID]__	Message ID of the failed message.
__[EEG_SUBJECT]__	Subject of the failed message.
__[EEG_DATE]__	Date of the failed message.
__[EEG_SENDER]__	Sender address of the failed message.
__[EEG_JOB_ID]__	Internal EEG Job ID of the failed message.

Policy and Rules Engine

The Policy Manager is a runtime PPG component that provides a rules engine for decision making on when to cipher, or decipher, incoming and outgoing mail. The Web interface is utilized to add policy rules to the database. The BNF notation for the supported rules can be seen in Figure 6-31.

```
<RULES> ::= <RULES> OR <RULE> | <RULE>
<RULE> ::= <RULE> AND <SUBRULE> | <SUBRULE>
<SUBRULE> ::= FROM_RULE | RECIPIENT_RULE | SUBJECT_RULE |
              MSG_BODY_RULE | CREDIT_CARD_CHECK_RULE
```

FIGURE 6-31 BNF Notation for Supported Rules

An example of configured policy rules is illustrated in Table 6-6. In this example, all outbound email is encrypted, however, special policies take precedence, for example, email from the finance department to the bank will be encrypted, and any email (whether for internal or external recipients) will be encrypted if the word "Confidential" appears in the subject line. Similarly, all inbound email that is encrypted will be decrypted, unless it is destined for the CEO.

TABLE 6-6. Example Encryption for Email Gateway Policies and Rules

NUMBER	RULE
1	Encrypt email from finance@mycompany.org sent to *@mybank.com using the Finance Department envelope.
2	Encrypt email to all recipients where the subject contains the word "Confidential."
3	Encrypt email to external recipients.
4	Don't decrypt email sent to CEO@mycompany.org.
5	Decrypt email sent to internal recipients.

In the event of conflicting policies within the manager, the policies are prioritized from top to bottom within the Web configuration interface and the policy manager shall make a decision based on the highest priority policy rule.

If MIME data is received that does not have an associated policy, then the MTA Interface resorts to a set of hard-coded rules within the Private Post Gateway. These can be seen in Table 6-7.

TABLE 6-7. Encryption for Email Gateway Default Policy Table

MAIL TYPE	SENDER	RECIPIENTS	RESULT
Clear Text	Internal	External	Encrypt
Private Post	Internal	External	Nothing (Keep Private)
Clear Text	Internal	Internal + External	Nothing (Keep Clear)
Private Post	Internal	Internal +External	Decrypt
Clear Text	Internal	Internal	Nothing (Keep Clear)
Private Post	Internal	Internal	Decrypt
Any	External	External	Error
Clear Text	External	Internal	Nothing (Keep Clear)
Private Post	External	Internal	Decrypt
Clear Text	External	External + Internal	Nothing (Keep Clear)
Private Post	External	External + Internal	Decrypt

Wildcards

The example rules in Table 6-6 make use of a wildcard on the recipient email address (*@mybank.com). In this example, any email sent to the domain mybank.com will be encrypted. Wildcards are currently limited to the left side of the email address part and not in conjunction with any other characters (for example, *_doe@mycompany.org is not valid, however *@mycompany.org is).

Advanced Configuration Options

Advanced Configuration includes the ability to spawn multiple instances of launched components (such as the MIMEBuilder as discussed in Scalability and Failover). Because of the technical nature of such configurations there is no administrative user interface for them at this time, and as such they are beyond the scope of this document.

Chapter 7

Exception Handling, Reporting, and Logging

Encryption for Email Gateway exception handling, reporting, and logging are discussed in the paragraphs that follow.

Topics include:

- System Logging
- Encryption and Decryption
- Email Error Handling
- Exception Handling

There are various ways to monitor system health; primarily though the Web UI System Status and View Logs tabs (refer to System Status and View Log Files). In addition, more detailed logs can be accessed and there are measures in place to notify users and administrators of system failures.

System Logging

The system logs are configurable and can be accessed through the Web UI as described in View Log Files. The logs are stored in the file system, by default in the /var/log/ppg/ folder. There are three types of log, info, warning and debug, each has four levels, ranging from 0 (off) to 3 (verbose). To aid troubleshooting the log level can be set to full verbose on each of the three log types. By default the log levels are Warning 3, Info 1 and Debug 0. The logs can also be downloaded through the Web interface View Logs screen.

Encryption and Decryption

The statistics available through the Web interface provides information regarding the number of emails encrypted, decrypted and passed-through (no action) an Encryption for Email Gateway. This information can be downloaded as a CSV file through the Web interface.

Email Error Handling

In the event of an error occurring which would prevent the email from being encrypted or decrypted an appropriate SMTP error code is returned to the connecting MTA with a relevant error message. In addition, Encryption for Email Gateway can be configured to send a notification email to an administrative address, or addresses enabling support to be alerted as soon as an error occurs in Encryption for Email Gateway.

Exception Handling

In the event of a major system crash or internal failure within Encryption for Email Gateway the SMTP interface stops receiving incoming email and then attempts to restart the runtime components.

Glossary

This glossary describes special terms used in this document or the Online Help.

TERM	EXPLANATION
100BaseT	An alternate term for “fast Ethernet,” an upgraded standard for connecting computers into a local area network (LAN). 100BaseT Ethernet can transfer data at a peak rate of 100 Mbps. It is also more expensive and less common than 10BaseT. *Also see* 10BaseT.
10BaseT	The most common form of Ethernet is called 10BaseT, which denotes a peak transmission speed of 10 Mbps using copper twisted-pair cable. Ethernet is a standard for connecting computers into a local area network (LAN). The maximum cable distance is 100 meters (325 feet), the maximum devices per segment is 1, and the maximum devices per network are 1024. *Also see* 100BaseT.
access (verb)	To read data from or write data to a storage device, such as a computer or server.
access (noun)	Authorization to read or write data. Most operating systems allow you to define different levels of access, depending on job responsibilities.
action (*Also see* target and notification)	The operation to be performed when: - a virus has been detected - spam has been detected - a content violation has occurred - an attempt was made to access a blocked URL, or - file blocking has been triggered. Actions typically include clean and deliver, quarantine, delete, or deliver/transfer anyway. Delivering/transferring anyway is not recommended—delivering a virus-infected message or transferring a virus-infected file can compromise your network.

TERM	EXPLANATION
activate	To enable your software after completion of the registration process. Your products will not be operable until product activation is complete. Activate during installation or after installation (in the management console) on the Product License screen.
Activation Code	A 37-character code, including hyphens, that is used to activate your products. Here is an example of an Activation Code: SM-9UE7-HG5B3-8577B-TD5P4-Q2XT5-48PG4 *Also see* Registration Key.
active FTP	Configuration of FTP protocol that allows the client to initiate "handshaking" signals for the command session, but the host initiates the data session.
ActiveUpdate	ActiveUpdate is a function common to many products. Connected to the update Web site, ActiveUpdate provides up-to-date downloads of virus pattern files, scan engines, and program files through the Internet or the Total Solution CD.
ActiveX	A type of open software architecture that implements object linking and embedding, enabling some of the standard interfaces, such as downloading of Web pages.
ActiveX malicious code	An ActiveX control is a component object embedded in a Web page which runs automatically when the page is viewed. ActiveX controls allow Web developers to create interactive, dynamic Web pages with broad functionality such as HouseCall, a free online scanner. Hackers, virus writers, and others who want to cause mischief or worse may use ActiveX malicious code as a vehicle to attack the system. In many cases, the Web browser can be configured so that these ActiveX controls do not execute by changing the browser's security settings to "high."
ActiveUpdate	A utility that enables on-demand or background updates to the virus pattern file and scan engine, as well as the anti-spam rules database and anti-spam engine.

TERM	EXPLANATION
address	Refers to a networking address (*see* IP address) or an email address, which is the string of characters that specify the source or destination of an email message.
administrator	Refers to "system administrator" — the person in an organization who is responsible for activities such as setting up new hardware and software, allocating user names and passwords, monitoring disk space and other IT resources, performing backups, and managing network security.
administrator account	A user name and password that has administrator-level privileges.
administrator email address	The address used by the administrator of your product to manage notifications and alerts.
adware	Advertising-supported software in which advertising banners display while the program is running. Adware that installs a "backdoor"; tracking mechanism on the user's computer without the user's knowledge is called "spyware."
alert	A message intended to inform a system's users or administrators about a change in the operating conditions of that system or about some kind of error condition.
anti-relay	Mechanisms to prevent hosts from "piggybacking" through another host's network.
antivirus	Computer programs designed to detect and clean computer viruses.
archive	A single file containing one or (usually) more separate files plus information to allow them to be extracted (separated) by a suitable program, such as a .zip file.
attachment	A file attached to (sent with) an email message.
audio/video file	A file containing sounds, such as music, or video footage.

TERM	EXPLANATION
authentication	The verification of the identity of a person or a process. Authentication ensures that digital data transmissions are delivered to the intended receiver. Authentication also assures the receiver of the integrity of the message and its source (where or whom it came from). The simplest form of authentication requires a user name and password to gain access to a particular account. Authentication protocols can also be based on secret-key encryption, such as the Data Encryption Standard (DES) algorithm, or on public-key systems using digital signatures. *Also see* public-key encryption *and* digital signature.
binary	A number representation consisting of zeros and ones used by practically all computers because of its ease of implementation using digital electronics and Boolean algebra.
block	To prevent entry into your network.
bridge	A device that forwards traffic between network segments based on data link layer information. These segments have a common network layer address.
browser	A program which allows a person to read hypertext, such as Internet Explorer. The browser gives some means of viewing the contents of nodes (or "pages") and of navigating from one node to another. A browser acts as a client to a remote Web server.
cache	A small fast memory, holding recently accessed data, designed to speed up subsequent access to the same data. The term is most often applied to processor-memory access, but also applies to a local copy of data accessible over a network etc.
case-matching	Scanning for text that matches both words and case. For example, if "dog" is added to the content-filter, with case-matching enabled, messages containing "Dog" will pass through the filter; messages containing "dog" will not.

TERM	EXPLANATION
cause	The reason a protective action, such as URL-blocking or file-blocking, was triggered—this information appears in log files.
clean	To remove virus code from a file or message.
client	A computer system or process that requests a service of another computer system or process (a "server") using some kind of protocol and accepts the server's responses. A client is part of a client-server software architecture.
client-server environment	A common form of distributed system in which software is split between server tasks and client tasks. A client sends requests to a server, according to some protocol, asking for information or action, and the server responds.
compressed file	A single file containing one or more separate files plus information to allow them to be extracted by a suitable program, such as WinZip.
configuration	Selecting options for how your product will function, for example, selecting whether to quarantine or delete a virus-infected email message.
content filtering	Scanning email messages for content (words or phrases) prohibited by your organization’s Human Resources or IT messaging policies, such as hate mail, profanity, or pornography.
content violation	An event that has triggered the content filtering policy.
cookie	A mechanism for storing information about an Internet user, such as name, preferences, and interests, which is stored in your Web browser for later use. The next time you access a Web site for which your browser has a cookie, your browser sends the cookie to the Web server, which the Web server can then use to present you with customized Web pages. For example, you might enter a Web site that welcomes you by name.

TERM	EXPLANATION
daemon	A program that is not invoked explicitly, but lies dormant waiting for some condition(s) to occur. The perpetrator of the condition need not be aware that a daemon is lurking.
damage routine	The destructive portion of virus code, also called the payload.
default	A value that pre-populates a field in the management console interface. A default value represents a logical choice and is provided for convenience. Use default values as-is, or change them.
De-Militarized Zone (DMZ)	From the military term for an area between two opponents where fighting is prevented. DMZ Ethernets connect networks and computers controlled by different bodies. They may be external or internal. External DMZ Ethernets link regional networks with routers.
dialer	A type of Trojan that when executed, connects the user's system to a pay-per-call location in which the unsuspecting user is billed for the call without his or her knowledge.
digital signature	Extra data appended to a message which identifies and authenticates the sender and message data using a technique called public-key encryption. *Also see* public-key encryption *and* authentication.
directory	A node, which is part of the structure in a hierarchical computer file system. A directory typically contains other nodes, folders, or files. For example, *C:\Windows* is the Windows directory on the C drive.
directory path	The subsequent layers within a directory where a file can be found, for example, the directory path for the ISVW for SMB Quarantine directory is: *C:\Programs\<your company>\ISVW\Quarantine*
disclaimer	A statement appended to the beginning or end of an email message, that states certain terms of legality and confidentiality regarding the message, To see an example, click the online help for the **SMTP Configuration - Disclaimer** screen.

TERM	EXPLANATION
DNS	Domain Name System—A general-purpose data query service chiefly used on the Internet for translating host names into IP addresses.
DNS resolution	When a DNS client requests host name and address data from a DNS server, the process is called resolution. Basic DNS configuration results in a server that performs default resolution. For example, a remote server queries another server for data on a machine in the current zone. Client software on the remote server queries the resolver, which answers the request from its database files.
(administrative) domain	A group of computers sharing a common database and security policy.
domain name	The full name of a system, consisting of its local host name and its domain name, for example, tellsitall.com. A domain name should be sufficient to determine a unique Internet address for any host on the Internet. This process, called “name resolution”, uses the Domain Name System (DNS).
DoS (Denial of Service) attack	Group-addressed email messages with large attachments that clog your network resources to the point where messaging service is noticeably slow or even stopped.
DOS virus	Also referred to as “COM” and “EXE file infectors.” DOS viruses infect DOS executable programs- files that have the extensions *.COM or *.EXE. Unless they have overwritten or inadvertently destroyed part of the original program's code, most DOS viruses try to replicate and spread by infecting other host programs.
download (noun)	Data that has been downloaded, for example, from a Web site through HTTP.
download (verb)	To transfer data or code from one computer to another. Downloading often refers to transfer from a larger "host" system (especially a server or mainframe) to a smaller "client" system.
dropper	Droppers are programs that serve as delivery mechanisms to carry and drop viruses, Trojans, or worms into a system.

TERM	EXPLANATION
ELF	Executable and Linkable Format—An executable file format for UNIX and Linux platforms.
encryption	Encryption is the process of changing data into a form that can be read only by the intended receiver. To decipher the message, the receiver of the encrypted data must have the proper decryption key. In traditional encryption schemes, the sender and the receiver use the same key to encrypt and decrypt data. Public-key encryption schemes use two keys: a public key, which anyone may use, and a corresponding private key, which is possessed only by the person who created it. With this method, anyone may send a message encrypted with the owner's public key, but only the owner has the private key necessary to decrypt it. PGP (Pretty Good Privacy) and DES (Data Encryption Standard) are two of the most popular public-key encryption schemes.
End User License Agreement (EULA)	An End User License Agreement or EULA is a legal contract between a software publisher and the software user. It typically outlines restrictions on the side of the user, who can refuse to enter into the agreement by not clicking “I accept” during installation. Clicking “I do not accept” will, of course, end the installation of the software product. Many users inadvertently agree to the installation of spyware and adware into their computers when they click “I accept” on EULA prompts displayed during the installation of certain free software.
Ethernet	A local area network (LAN) technology invented at the Xerox Corporation, Palo Alto Research Center. Ethernet is a best-effort delivery system that uses CSMA/CD technology. Ethernet can be run over a variety of cable schemes, including thick coaxial, thin coaxial, twisted pair, and fiber optic cable. Ethernet is a standard for connecting computers into a local area network. The most common form of Ethernet is called 10BaseT, which denotes a peak transmission speed of 10 Mbps using copper twisted-pair cable.
executable file	A binary file containing a program in machine language which is ready to be executed (run).

TERM	EXPLANATION
EXE file infector	An executable program with a .exe file extension. *Also see* DOS virus.
exploit	An exploit is code that takes advantage of a software vulnerability or security hole. Exploits are able to propagate into and run intricate routines on vulnerable computers.
false positive	An email message that was "caught" by the spam filter and identified as spam, but is actually not spam.
FAQ	Frequently Asked Questions—A list of questions and answers about a specific topic.
file	An element of data, such as an email message or HTTP download.
file-infecting virus	File-infecting viruses infect executable programs (generally, files that have extensions of .com or .exe). Most such viruses simply try to replicate and spread by infecting other host programs, but some inadvertently destroy the program they infect by overwriting a portion of the original code. A minority of these viruses are very destructive and attempt to format the hard drive at a pre-determined time or perform some other malicious action. In many cases, a file-infecting virus can be successfully removed from the infected file. However, if the virus has overwritten part of the program's code, the original file will be unrecoverable
file type	The kind of data stored in a file. Most operating systems use the file name extension to determine the file type. The file type is used to choose an appropriate icon to represent the file in a user interface, and the correct application with which to view, edit, run, or print the file.
file name extension	The portion of a file name (such as .dll or .xml) which indicates the kind of data stored in the file. Apart from informing the user what type of content the file holds, file name extensions are typically used to decide which program to launch when a file is run.

TERM	EXPLANATION
filtering, dynamic	IP service that can be used within VPN tunnels. Filters are one way GateLock controls traffic from one network to another. When TCP/IP sends data packets to the firewall, the filtering function in the firewall looks at the header information in the packets and directs them accordingly. The filters operate on criteria such as IP source or destination address range, TCP ports, UDP, Internet Control Message Protocol (ICMP), or TCP responses. *Also see* tunneling and Virtual Private Network (VPN).
firewall	A gateway machine with special security precautions on it, used to service outside network (especially Internet) connections and dial-in lines.
FTP	A client-server protocol which allows a user on one computer to transfer files to and from another computer over a TCP/IP network. Also refers to the client program the user executes to transfer files.
gateway	An interface between an information source and a Web server.
grayware	A category of software that may be legitimate, unwanted, or malicious. Unlike threats such as viruses, worms, and Trojans, grayware does not infect, replicate, or destroy data, but it may violate your privacy. Examples of grayware include spyware, adware, and remote access tools.
group file type	Types of files that have a common theme, for example: - Audio/Video - Compressed - Executable - Images - Java - Microsoft Office
GUI	Graphical User Interface—The use of pictures rather than just words to represent the input and output of a program. This contrasts with a command line interface where communication is by exchange of strings of text.

TERM	EXPLANATION
hacking tool	Tools such as hardware and software that enables penetration testing of a computer system or network for the purpose of finding security vulnerabilities that can be exploited.
hard disk (or hard drive)	One or more rigid magnetic disks rotating about a central axle with associated read/write heads and electronics, used to read and write hard disks or floppy disks, and to store data. Most hard disks are permanently connected to the drive (fixed disks) though there are also removable disks.
header (networking definition)	Part of a data packet that contains transparent information about the file or the transmission.
heuristic rule-based scanning	Scanning network traffic, using a logical analysis of properties that reduces or limits the search for solutions.
HTTP	Hypertext Transfer Protocol—The client-server TCP/IP protocol used on the World Wide Web for the exchange of HTML documents. It conventionally uses port 80.
HTTPS	Hypertext Transfer Protocol Secure—A variant of HTTP used for handling secure transactions.
host	A computer connected to a network.
hub	This hardware is used to network computers together (usually over an Ethernet connection). It serves as a common wiring point so that information can flow through one central location to any other computer on the network thus enabling centralized management. A hub is a hardware device that repeats signals at the physical Ethernet layer. A hub retains the behavior of a standard bus type network (such as Thinnet), but produces a star topology with the hub at the center of the star. This configuration enables centralized management.

TERM	**EXPLANATION**
ICSA	ICSA Labs is an independent division of TruSecure Corporation. For over a decade, ICSA has been the security industry’s central authority for research, intelligence, and certification testing of products. ICSA Labs sets standards for information security products and certifies over 90% of the installed base of antivirus, firewall, IPSec, crytography, and PC firewall products in the world today.
image file	A file containing data representing a two-dimensional scene, in other words, a picture. Images are taken from the real world, for example, through a digital camera, or they may be generated by computer using graphics software.
incoming	Email messages or other data routed *into* your network.
installation script	The installation screens used to install UNIX versions of your products.
integrity checking	*See* checksumming.
IntelliScan	IntelliScan is a scanning technology that optimizes performance by examining file headers using true-file type recognition, and scanning only file types known to potentially harbor malicious code. True-file type recognition helps identify malicious code that can be disguised by a harmless extension name.
Internet	A client-server hypertext information retrieval system, based on a series of networks connected with routers. The Internet is a modern information system and a widely accepted medium for advertising, online sales, and services, as well as university and many other research networks. The World Wide Web is the most familiar aspect of the Internet.
Internet Protocol (IP)	An Internet standard protocol that defines a basic unit of data called a datagram. A datagram is used in a connectionless, best-effort, delivery system. The Internet protocol defines how information gets passed between systems across the Internet.

TERM	EXPLANATION
interrupt	An asynchronous event that suspends normal processing and temporarily diverts the flow of control through an "interrupt handler" routine.
“in the wild”	Describes known viruses that are actively circulating. *Also see* “in the zoo.”
“in the zoo”	Describes known viruses that are currently controlled by antivirus products. *Also see* “in the wild.”
intranet	Any network which provides similar services within an organization to those provided by the Internet outside it, but which is not necessarily connected to the Internet.
IP	Internet Protocol—*See* IP address.
IP address	Internet address for a device on a network, typically expressed using dot notation such as 123.123.123.123.
IP gateway	Also called a router, a gateway is a program or a special-purpose device that transfers IP datagrams from one network to another until the final destination is reached.
IT	Information technology, to include hardware, software, networking, telecommunications, and user support.
Java applets	Java applets are small, portable Java programs embedded in HTML pages that can run automatically when the pages are viewed. Java applets allow Web developers to create interactive, dynamic Web pages with broader functionality. Authors of malicious code have used Java applets as a vehicle for attack. Most Web browsers, however, can be configured so that these applets do not execute - sometimes by simply changing browser security settings to “high.”

TERM	EXPLANATION
Java file	Java is a general-purpose programming language developed by Sun Microsystems. A Java file contains Java code. Java supports programming for the Internet in the form of platform-independent Java "applets." (An applet is a program written in Java programming language that can be included in an HTML page. When you use a Java-technology enabled browser to view a page that contains an applet, the applet's code is transferred to your system and is executed by the browser's Java Virtual Machine.)
Java malicious code	Virus code written or embedded in Java. *Also see* Java file.
JavaScript virus	JavaScript is a simple programming language developed by Netscape that allows Web developers to add dynamic content to HTML pages displayed in a browser using scripts. Javascript shares some features of Sun Microsystems Java programming language, but was developed independently. A JavaScript virus is a virus that is targeted at these scripts in the HTML code. This enables the virus to reside in Web pages and download to a user's desktop through the user's browser. *Also see* VBscript virus.
joke program	An executable program that is annoying or causes users undue alarm. Unlike viruses, joke programs do not self-propagate and should simply be removed from your system.
KB	Kilobyte—1024 bytes of memory.
keylogger	Keyloggers are programs that catch and store all keyboard activity. There are legitimate keylogging programs that are used by corporations to monitor employees and by parents to monitor their children. However, criminals also use keystroke logs to sort for valuable information such as logon credentials and credit card numbers.
LAN (Local Area Network)	A data communications network which is geographically limited, allowing easy interconnection of computers within the same building.

TERM	EXPLANATION
LDAP (Lightweight Directory Access Protocol)	An Internet protocol that email programs use to locate contact information from a server. For example, suppose you want to locate all persons in Boston who have an email address containing the name “Bob.” An LDAP search would enable you to view the email addresses that meet this criteria.
license	Authorization by law to use a specific product.
license certificate	A document that proves you are an authorized user of a specific product.
link (also called hyperlink)	A reference from some point in one hypertext document to some point in another document or another place in the same document. Links are usually distinguished by a different color or style of text, such as underlined blue text. When you activate the link, for example, by clicking on it with a mouse, the browser displays the target of the link.
listening port	A port utilized for client connection requests for data exchange.
load balancing	Load balancing is the mapping (or re-mapping) of work to processors, with the intent of improving the efficiency of a concurrent computation.
local area network (LAN)	Any network technology that interconnects resources within an office environment, usually at high speeds, such as Ethernet. A local area network is a short-distance network used to link a group of computers together within a building. 10BaseT Ethernet is the most commonly used form of LAN. A hardware device called a hub serves as the common wiring point, enabling data to be sent from one machine to another over the network. LANs are typically limited to distances of less than 500 meters and provide low-cost, high-bandwidth networking capabilities within a small geographical area.
log storage directory	Directory on your server that stores log files.
logic bomb	Code surreptitiously inserted into an application or operating system that causes it to perform some destructive or security-compromising activity whenever specified conditions are met.

TERM	EXPLANATION
macro	A command used to automate certain functions within an application.
malware (malicious software)	Programming or files that are developed for the purpose of doing harm, such as viruses, worms, and Trojans.
management console	The user interface for your particular product.
Mbps	Millions of bits per second—a measure of bandwidth in data communications.
MB	Megabyte—1024 kilobytes of data.
Media Access Control (MAC) address	An address that uniquely identifies the network interface card, such as an Ethernet adapter. For Ethernet, the MAC address is a 6 octet address assigned by IEEE. On a LAN or other network, the MAC address is a computer's unique hardware number. (On an Ethernet LAN, it's the same as the Ethernet address.) When you're connected to the Internet from your computer (or host as the Internet protocol thinks of it), a correspondence table relates your IP address to your computer's physical (MAC) address on the LAN. The MAC address is used by the Media Access Control sublayer of the Data-Link Control (DLC) layer of telecommunication protocols. There is a different MAC sublayer for each physical device type.
Microsoft Office file	Files created with Microsoft Office tools such as Excel or Microsoft Word.
mixed threat attack	Complex attacks that take advantage of multiple entry points and vulnerabilities in enterprise networks, such as the “Nimda” or “Code Red” threats.
MTA (Mail Transfer Agent)	The program responsible for delivering email messages. *Also see* SMTP server.

TERM	EXPLANATION
network virus	A type of virus that uses network protocols, such as TCP, FTP, UDP, HTTP, and email protocols to replicate. Network viruses often do not alter system files or modify the boot sectors of hard disks. Instead, they infect the memory of client machines, forcing them to flood the network with traffic, which can cause slowdowns or even complete network failure.
notification (*Also see* action and target)	A message that is forwarded to one or more of the following: - system administrator - sender of a message - recipient of a message, file download, or file transfer The purpose of the notification is to communicate that a prohibited action has taken place, or was attempted, such as a virus being detected in an attempted HTTP file download.
offensive content	Words or phrases in messages or attachments that are considered offensive to others, for example, profanity, sexual harassment, racial harassment, or hate mail.
online help	Documentation that is bundled with the GUI.
open source	Programming code that is available to the general public for use or modification free of charge and without license restrictions.
operating system	The software which handles tasks such as the interface to peripheral hardware, scheduling tasks, and allocating storage. In this documentation, the term also refers to the software that presents a window system and graphical user interface.
outgoing	Email messages or other data *leaving* your network, routed out to the Internet.
parameter	A variable, such as a range of values (a number from 1 to 10).
partition	A logical portion of a disk. (*Also see* sector, which is a physical portion of a disk.)
passive FTP	Configuration of FTP protocol that allows clients within your local area network to initiate the file transfer, using random upper port numbers (1024 and above).

TERM	EXPLANATION
password cracker	An application program that is used to recover a lost or forgotten password. These applications can also be used by an intruder to gain unauthorized access to a computer or network resources.
pattern file (also known as Official Pattern Release)	The pattern file, as referred to as the Official Pattern Release (OPR), is the latest compilation of patterns for identified viruses. It is guaranteed to have passed a series of critical tests to ensure that you get optimum protection from the latest virus threats. This pattern file is most effective when used with the latest scan engine.
payload	Payload refers to an action that a virus performs on the infected computer. This can be something relatively harmless, such as displaying messages or ejecting the CD drive, or something destructive, such as deleting the entire hard drive.
policies	Policies provide the initial protection mechanism for the firewall, allowing you to determine what traffic passes across it based on IP session details. They protect the Trusted network from outsider attacks, such as the scanning of Trusted servers. Policies create an environment in which you set up security policies to monitor traffic attempting to cross your firewall.
port	A logical channel or channel endpoint in a communications system, used to distinguish between different logical channels on the same network interface on the same computer. Each application program has a unique port number associated with it.
protected network	A network protected by IWSA (InterScan Web Security Appliance).
proxy	A process providing a cache of items available on other servers which are presumably slower or more expensive to access.
proxy server	A World Wide Web server which accepts URLs with a special prefix, used to fetch documents from either a local cache or a remote server, then returns the URL to the requester.

TERM	EXPLANATION
public-key encryption	An encryption scheme where each person gets a pair of “keys,” called the public key and the private key. Each person's public key is published while the private key is kept secret. Messages are encrypted using the intended recipient's public key and can only be decrypted using his or her private key. *Also see* authentication *and* digital signature.
purge	To delete all, as in getting rid of old entries in the logs.
quarantine	To place infected data such as email messages, infected attachments, infected HTTP downloads, or infected FTP files in an isolated directory (the Quarantine Directory) on your server.
queue	A data structure used to sequence multiple demands for a resource when mail is being received faster than it can be processed. Messages are added at the end of the queue, and are taken from the beginning of the queue, using a FIFO (first-in, first-out) approach.
recipient	The person or entity to whom an email message is addressed.
registration	The process of identifying yourself as a company customer, using a product Registration Key, on the company Online Registration screen. *https://olr.trendmicro.com/registration*
Registration Key	A 22-character code, including hyphens, that is used to register in the customer database. Here is an example of a Registration Key: SM-27RT-UY4Z-39HB-MNW8 *Also see* Activation Code
relay	To convey by means of passing through various other points.
remote access tool (RAT)	Hardware and software that allow a legitimate system administrator to manage a network remotely. However, these same tools can also be used by intruders to attempt a breach of your system security.
removable drive	A removable hardware component or peripheral device of a computer, such as a zip drive.

TERM	EXPLANATION
replicate	To self-reproduce. As used in this documentation, the term refers to viruses or worms that can self-reproduce.
router	This hardware device routes data from a local area network (LAN) to a phone line's long distance line. Routers also act as traffic cops, allowing only authorized machines to transmit data into the local network so that private information can remain secure. In addition to supporting these dial-in and leased connections, routers also handle errors, keep network usage statistics, and handle security issues.
scan	To examine items in a file in sequence to find those that meet a particular criteria.
scan engine	The module that performs antivirus scanning and detection in the host product to which it is integrated.
script	A set of programming commands that, once invoked, can be executed together. Other terms used synonymously with "script" are "macro" or "batch file."
sector	A physical portion of a disk. (*Also see* partition, which is a logical portion of a disk.)
seat	A license for one person to use a particular product.
Secure Socket Layer (SSL)	Secure Socket Layer (SSL), is a protocol designed by Netscape for providing data security layered between application protocols (such as HTTP, Telnet, or FTP) and TCP/IP. This security protocol provides data encryption, server authentication, message integrity, and optional client authentication for a TCP/IP connection.
server	A program which provides some service to other (client) programs. The connection between client and server is normally by means of message passing, often over a network, and uses some protocol to encode the client's requests and the server's responses. The server may run continuously (as a daemon), waiting for requests to arrive, or it may be invoked by some higher-level daemon which controls a number of specific servers.

TERM	EXPLANATION
server farm	A server farm is a network where clients install their own computers to run Web servers, e-mail, or any other TCP/IP based services they require, making use of leased permanent Internet connections with 24-hour worldwide access. Instead of expensive dedicated-line connections to various offices, servers can be placed on server farm networks to have them connected to the Internet at high-speed for a fraction of the cost of a leased line.
shared drive	A computer peripheral device that is used by more than one person, thus increasing the risk of exposure to viruses.
signature	*See* virus signature.
signature-based spam detection	A method of determining whether an email message is spam by comparing the message contents to entries in a spam database. An exact match must be found for the message to be identified as spam. Signature-based spam detection has a nearly zero false positive rate, but does not detect “new” spam that isn’t an exact match for text in the spam signature file. *Also see* rule-based spam detection. *Also see* false positive.
SMTP	Simple Mail Transfer Protocol—A protocol used to transfer electronic mail between computers, usually over Ethernet. It is a server-to-server protocol, so other protocols are used to access the messages.
SMTP server	A server that relays email messages to their destinations.
SNMP	Simple Network Management Protocol—A protocol that supports monitoring of devices attached to a network for conditions that merit administrative attention.
SNMP trap	A trap is a programming mechanism that handles errors or other problems in a computer program. An SNMP trap handles errors related to network device monitoring. *See* SNMP.
spam	Unsolicited email messages meant to promote a product or service.

TERM	EXPLANATION
spyware	Advertising-supported software that typically installs tracking software on your system, capable of sending information about you to another party. The danger is that users cannot control what data is being collected, or how it is used.
subnet mask	In larger networks, the subnet mask lets you define subnetworks. For example, if you have a class B network, a subnet mask of 255.255.255.0 specifies that the first two portions of the decimal dot format are the network number, while the third portion is a subnet number. The fourth portion is the host number. If you do not want to have a subnet on a class B network, you would use a subnet mask of 255.255.0.0. A network can be subnetted into one or more physical networks which form a subset of the main network. The subnet mask is the part of the IP address which is used to represent a subnetwork within a network. Using subnet masks allows you to use network address space which is normally unavailable and ensures that network traffic does not get sent to the whole network unless intended. Subnet masks are a complex feature, so great care should be taken when using them. *Also see* IP address.
target (*Also see* action and notification)	The scope of activity to be monitored for a violating event, such as a virus being detected in an email message. For example, you could target virus scanning of all files passing into and out of your network, or just files with a certain file name extension.
TCP	Transmission Control Protocol—TCP is a networking protocol, most commonly use in combination with IP (Internet Protocol), to govern connection of computer systems to the Internet.
Telnet	The Internet standard protocol for remote login that runs on top of TCP/IP (Transmission Control Protocol/Internet Protocol). This term can also refer to networking software that acts as a terminal emulator for a remote login session.
top-level domain	The last and most significant component of an Internet fully qualified domain name, the part after the last ".". For example, host *wombat.doc.ic.ac.uk* is in top-level domain "uk" (for United Kingdom).

TERM	EXPLANATION
Total Solution CD	A CD containing the latest product versions and all the patches that have been applied during the previous quarter. The Total Solution CD is available to all Premium Support customers.
traffic	Data flowing between the Internet and your network, both incoming and outgoing.
Transmission Control Protocol/Internet Protocol (TCP/IP)	A communications protocol which allows computers with different operating systems to communicate with each other. Controls how data is transferred between computers on the Internet.
trigger	An event that causes an action to take place. For example, your product detects a virus in an email message. This may *trigger* the message to be placed in quarantine, and a notification to be sent to the system administrator, message sender, and message recipient.
Trojan Horse	A malicious program that is disguised as something benign. A Trojan is an executable program that does not replicate, but instead, resides on a system to perform malicious acts, such as opening a port for an intruder.
true-file type	Used by IntelliScan, a virus scanning technology, to identify the type of information in a file by examining the file headers, regardless of the file name extension (which could be misleading).
trusted domain	A domain from which your product will always accept messages, without considering whether the message is spam. For example, a company called Dominion, Inc. has a subsidiary called Dominion-Japan, Inc. Messages from dominion-japan.com are always accepted into the dominion.com network, without checking for spam, because the messages are from a known and trusted source.
trusted host	A server that is allowed to relay mail through your network because they are trusted to act appropriately and not, for example, relay spam through your network.

TERM	EXPLANATION
tunneling	A method of sending data that enables one network to send data through another network's connections. Tunnelling is used to get data between administrative domains which use a protocol that is not supported by the Internet connecting those domains. With VPN tunneling, a mobile professional dials into a local Internet Service Provider's Point of Presence (POP) instead of dialing directly into their corporate network. This means that no matter where mobile professionals are located, they can dial a local Internet Service Provider that supports VPN tunneling technology and gain access to their corporate network, incurring only the cost of a local telephone call. When remote users dial into their corporate network using an Internet Service Provider that supports VPN tunneling, the remote user as well as the organization knows that it is a secure connection. All remote dial-in users are authenticated by an authenticating server at the Internet Service Provider's site and then again by another authenticating server on the corporate network. This means that only authorized remote users can access their corporate network, and can access only the hosts that they are authorized to use.
tunnel interface	A tunnel interface is the opening, or doorway, through which traffic to or from a VPN tunnel passes. A tunnel interface can be numbered (that is, assigned an IP address) or unnumbered. A numbered tunnel interface can be in either a tunnel zone or security zone. An unnumbered tunnel interface can only be in a security zone that contains at least one security zone interface. The unnumbered tunnel interface borrows the IP address from the security zone interface. *Also see* Virtual Private Network (VPN).
tunnel zone	A tunnel zone is a logical segment that hosts one or more tunnel interfaces. A tunnel zone is associated with a security zone that acts as its carrier.

Term	Explanation
URL	Universal Resource Locator—A standard way of specifying the location of an object, typically a Web page, on the Internet, for example, *www.trendmicro.com*. The URL maps to an IP address using DNS.
VBscript virus	VBscript (Microsoft Visual Basic scripting language) is a simple programming language that allows Web developers to add interactive functionality to HTML pages displayed in a browser. For example, developers might use VBscript to add a “Click Here for More Information” button on a Web page. A VBscript virus is a virus that is targeted at these scripts in the HTML code. This enables the virus to reside in Web pages and download to a user’s desktop through the user’s browser. *Also see* JavaScript virus.
virtual IP address (VIP address)	A VIP address maps traffic received at one IP address to another address based on the destination port number in the packet header.
Virtual Local Area Network (VLAN)	A logical (rather than physical) grouping of devices that constitute a single broadcast domain. VLAN members are not identified by their location on a physical subnetwork but through the use of tags in the frame headers of their transmitted data. VLANs are described in the IEEE 802.1Q standard.
Virtual Private Network (VPN)	A VPN is an easy, cost-effective and secure way for corporations to provide telecommuters and mobile professionals local dial-up access to their corporate network or to another Internet Service Provider (ISP). Secure private connections over the Internet are more cost-effective than dedicated private lines. VPNs are possible because of technologies and standards such as tunneling and encryption.
virtual router	A virtual router is the component of Screen OS that performs routing functions. By default, your company’s GateLock supports two virtual routers: Untrust-VR and Trust-VR.

TERM	EXPLANATION
virtual system	A virtual system is a subdivision of the main system that appears to the user to be a stand-alone entity. Virtual systems reside separately from each other in the same GateLock remote appliance; each one can be managed by its own virtual system administrator.
virus	A computer virus is a program – a piece of executable code – that has the unique ability to infect. Like biological viruses, computer viruses can spread quickly and are often difficult to eradicate. In addition to replication, some computer viruses share another commonality: a damage routine that delivers the virus payload. While payloads may only display messages or images, they can also destroy files, reformat your hard drive, or cause other damage. Even if the virus does not contain a damage routine, it can cause trouble by consuming storage space and memory, and degrading the overall performance of your computer.
virus kit	A template of source code for building and executing a virus, available from the Internet.
virus signature	A virus signature is a unique string of bits that identifies a specific virus. Virus signatures are stored in the virus pattern file. The scan engine compares code in files, such as the body of an email message, or the content of an HTTP download, to the signatures in the pattern file. If a match is found, the virus is detected, and is acted upon (for example, cleaned, deleted, or quarantined) according to your security policy.
virus trap	Software that helps you capture a sample of virus code for analysis.
virus writer	Another name for a computer hacker, someone who writes virus code.
Web	The World Wide Web, also called the Web or the Internet.
Web server	A server process running at a Web site which sends out Web pages in response to HTTP requests from remote browsers.

TERM	EXPLANATION
wildcard	A term used in reference to content filtering, where an asterisk (*) represents any characters. For example, in the expression *ber, this expression can represent barber, number, plumber, timber, and so on. The term originates from card games, in which a specific card, identified as a “wildcard,” can be used for any number or suit in the card deck.
working directory	The destination directory in which the main application files are stored, such as `/etc/iscan/iwss`.
workstation (also known as client)	A general-purpose computer designed to be used by one person at a time and which offers higher performance than normally found in a personal computer, especially with respect to graphics, processing power and the ability to carry out several tasks at the same time.
worm	A self-contained program (or set of programs) that is able to spread functional copies of itself or its segments to other computer systems.
Zero Download	Technology enabling the decryption and reading of Private Post encrypted email messages using any modern Web browser.
zip file	A compressed archive (in other words, “zip file") from one or more files using an archiving program such as WinZip.
"Zip of Death"	A zip (or archive) file of a type that when decompressed, expands enormously (for example 1000%) or a zip file with thousands of attachments. Compressed files must be decompressed during scanning. Huge files can slow or stop your network.
zone	A zone can be a segment of network space to which security measures are applied (a security zone), a logical segment to which a VPN tunnel interface is bound (a tunnel zone), or a physical or logical entity that performs a specific function (a function zone).