Forcepoint

Email Security Gateway

v8.5.x

Administrator Help

Revision A

Published 26 March 2025

Contents

Chapter 1

Forcepoint Email Security Overview

Contents

Introduction

Welcome to Forcepoint Email Security, which provides maximum protection for email systems to prevent malicious threats from entering an organization's network. This email solution provides comprehensive on-premises email security hosted on a Forcepoint appliance or in the public cloud. Each message is processed by a robust set of antivirus and antispam analytics to prevent infected email from entering the network. Domain and IP address based message routing ensures reliable, accurate delivery of email.

Forcepoint Email Security may be deployed on a V or X Series appliance or as a virtual appliance. See the Forcepoint Appliances Getting Started Guide for details.

Starting in version 8.5, Forcepoint Email Security can be deployed in Microsoft Azure, which provides the same features and protections as with an Email Security deployment on an appliance, but with the flexibility of virtualization. See Installing Forcepoint Email Security in Microsoft Azure and v8.5 Release Notes for Forcepoint Email Security in Microsoft Azure.

Forcepoint Security Manager installed on a separate Windows machine is required for administration functions. An Email Security module administrator uses the manager to control email system configuration settings.

The Forcepoint Email Security Hybrid Module adds support for an email hybrid service pre-filtering capability in the cloud, which analyzes incoming email against a database of known malware. This feature can save network bandwidth and maintenance costs by dropping malicious email before it ever reaches an organization's network. The Hybrid Module also includes URL sandbox and phishing education capabilities.

Enhance your security by adding one of the following file sandbox capabilities to your product subscription:

- Forcepoint Advanced Malware Detection for Email - Cloud
- Forcepoint Advanced Malware Detection for Email - On-Premises

Forcepoint Advanced Malware Detection for Email - Cloud is a cloud-based file sandbox feature. Forcepoint Advanced Malware Detection for Email - On-Premises is an on-premises appliance that performs file sandbox functions. These advanced detection functions inspect email attachment file types that commonly contain security threats.

Integration with Forcepoint DLP provides valuable protection for an organization's most sensitive data and facilitates message encryption. Configure a data loss prevention policy in the Security Manager Data module

to enable message encryption options that are configured on the page **Settings** > **Inbound/Outbound** > **Encryption**.

If your network includes Forcepoint web protection, you can also use its URL analysis function. Your email protection software queries the Forcepoint URL category database and determines the risk level of a URL found in an email message. See *URL analysis*.

Logging and reporting capabilities allow a company to view system status and generate reports of system and email traffic activity.

A Personal Email Manager facility allows authorized end users to manage email messages that an email policy has blocked but that may be safe to deliver. End users can maintain individual Always Block and Always Permit lists of email addresses to simplify message delivery.

Related concepts
URL analysis on page 76

Administrator help overview

Administrator Help includes the following topics:

Topic	Title	Description
1	*Forcepoint Email Security Overview*	Includes a brief introduction to your email software, manager Help contents, and Technical Support contact information.
2	*Getting Started*	Provides an overview of the first-time Configuration Wizard, navigation descriptions and tips, dashboard customization, filtering database update information, and registration directions for Forcepoint Email Security Hybrid Module and Forcepoint DLP.
3	*Configuring System Settings*	Includes details for configuring administrator roles, user directories, domain and IP address groups, and appliance clusters, as well as backup and restore functions.
4	*Managing Messages*	Contains information for setting message properties and directory harvest attack and relay control options, creating message routes and queues, and handling exception messages and encryption.
5	*Working with Filters and Policies*	Provides descriptions of filters, filter actions, policies, and global Always Block and Always Permit lists.

Topic	Title	Description
6	*Working with Reports*	Includes an overview of reporting preference options, presentation report generation and management, and log database settings.
7	*Configuring Personal Email Manager End User Options*	Provides information about setting Personal Email Manager end-user options, including the contents of notification messages and whether an end user can manage personal block and permit lists; also contains details regarding end-user portal appearance.

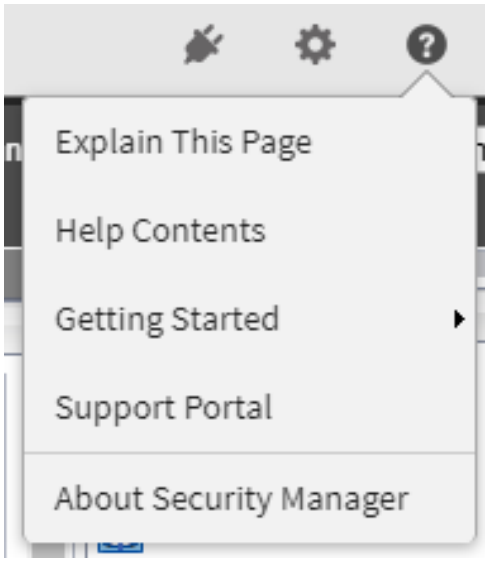
Related information

Forcepoint Email Security Overview on page 5
Getting Started on page 11
Configuring System Settings on page 81
Managing Messages on page 111
Working with Filters and Policies on page 171
Working with Reports on page 215
Configuring Personal Email Manager End User Options on page 239

Embedded help

Access embedded Administrator Help from the **Help** icon at the top right area of the screen, in the Security Manager banner.

Click **Help** > **Explain This Page** to open context-sensitive help for the active Email module page.



Important

Default Microsoft Internet Explorer settings may block operation of the Help system. If a security alert appears, select **Allow Blocked Content** to display Help.

If your organization's security standards permit, you can permanently disable the warning message on the Advanced tab of the **Tools** > **Internet Options** interface. (Under Security options, check **Allow active content to run in files on My Computer**.)

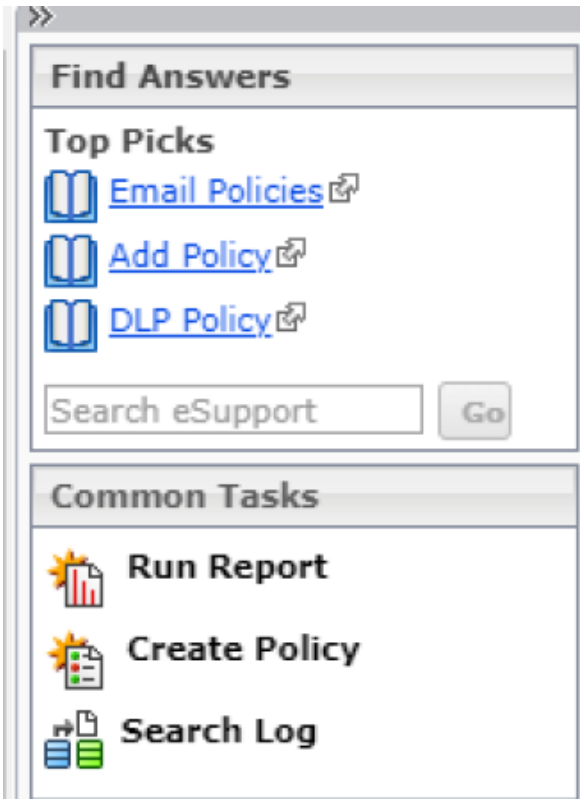
Click the **Previous page** and **Next page** icons to page through the Help topics, or click **Show the navigation pane** to display the complete embedded Administrator Help contents. To find a Help topic in the Help viewer, select one of the following tabs:

- **Contents**
  Click a book icon to expand that book's topics. Click a table of contents entry to display the corresponding topic.
- **Search**
  Enter a word or phrase and click Go! Click an entry of the results list to display the corresponding topic.

Find Answers portal

The right pane of the Security Manager Email module contains a Find Answers portal that may include the following components:

- A Top Picks section containing external links to information related to the screen content; and
- A Search field that you can use to find topics of interest in the Forcepoint eSupport site.
- A Common Tasks section containing internal links to related pages in the Forcepoint Security Manager.



Technical Support

Click **Help** > **Support Portal** in the Security Manager module tray to access the Forcepoint online Support site. Technical information about Forcepoint software and services is available 24 hours a day, including:

- the searchable knowledge base (Solution Center, product documentation, and customer forums),
- webinars and show-me videos,
- product documents and in-depth technical papers, and
- answers to frequently asked questions.

For additional questions, click the **Contact Support** tab at the top of the page.

The contact page includes information for finding solutions, opening an online support case, and calling Technical Support.

For faster phone response, please use your **Account ID**, which you can find in the Profile section on the My Account page.

For telephone requests, please have ready:

- Product subscription key
- Access to the Security Manager for your solutions
- Access to the machine running reporting tools and the database server (Microsoft SQL Server or SQL Server Express)
- Familiarity with the architecture of your network, or access to a specialist

Chapter 2

Getting Started

Contents

Using the First-time Configuration Wizard

The Configuration Wizard is available the first time you open your email product after installation. The wizard lets you quickly and easily enter some critical configuration settings before you open the Forcepoint Email Security module user interface.

Click the Email Security module in the Forcepoint Security Manager to display a pop-up box that allows you to enter your subscription key. You can enter your key

here, or skip this step and enter your subscription key later on the page **Settings** > **General** > **Subscription** (see *Entering and viewing subscription information*).

After you click **OK** in the subscription key pop-up box, a subsequent message box offers a choice of opening the Configuration Wizard or the email dashboard.

Note

If you open the dashboard instead of the wizard, you are presented with an option to open a document containing some helpful configuration settings information.

If you decide to skip the Configuration Wizard, you cannot access it later for this appliance.

You can enter the following information in the first-time Configuration Wizard:

- *Fully qualified domain name (FQDN)*
- *Domain-based route*
- *Trusted IP addresses for inbound mail*
- *Email Log Server information*
- *System notification email address*

To save your settings, review them in the Confirmation page of the Configuration Wizard and click **Complete**.

If you click **Cancel** at any time while you are in the Configuration Wizard, any settings you entered up to that point are lost.

A **Confirmation** page at the end of the wizard lets you review all your settings and modify any of them if desired.

- Click **Edit** next to the item you want to change. The appropriate wizard page displays.
- Make required changes and click **OK** on the edited page to return to the Confirmation page.

Click **Complete** when you are finished with your configuration settings to open the email dashboard.

Related concepts

Entering and viewing subscription information on page 14
Fully qualified domain name (FQDN) on page 12
Trusted IP addresses for inbound mail on page 13
Email Log Server information on page 13
System notification email address on page 14

Related tasks

Domain-based route on page 12

Fully qualified domain name (FQDN)

The FQDN page of the Configuration Wizard is used to specify the appliance fully qualified domain name (FQDN), as configured in your public DNS. This setting is used for the HELO/EHLO connection and is critical for proper email security software operation. An incorrect fully qualified domain name may cause disruptions in email traffic flow.

Enter the appliance FQDN in the field **Fully Qualified Domain Name**

FQDN format is mail.parentdomain.com.

This FQDN appears as the default entry on the page **Settings** > **General** > **System Settings**.

Domain-based route

The **Domain-based Route** page of the Configuration Wizard is used to identify a domain that you want protected and to designate the SMTP server to which mail to this domain should be sent.

You can add more protected domains on the page **Settings** > **Inbound/Outbound** > **Mail Routing**. See *Protected Domain group*.

Use the following steps in the wizard to designate a protected domain:

Steps

1) In the field **Route name**, enter a name for your route.
2) In the field **Protected Domain Name**, designate a protected domain.
3) In the appropriate fields, enter the SMTP server IP address or hostname and port number for the protected domain.
4) To enable email routing to use Transport Layer Security (TLS) to encrypt the transmission, mark the check box **Use Transport Layer Security**.
5) To force a user to enter username and password credentials, mark the check box **Require Authentication**.
6) In the appropriate fields, enter the username and password that must be used.

Related concepts
Protected Domain group on page 99

Trusted IP addresses for inbound mail

On the page Trusted Inbound Mail, you can create a list of trusted IP addresses for which some inbound email filtering is not performed. Trusted IP addresses may include your internal mail servers or a trusted partner mail server.

See *Managing domain and IP address groups* for detailed information about how trusted IP addresses are handled in the email system.

Enter an IP address in the **Trusted IP address** field, and then click the right arrow button to add it to the **Trusted IP address list**.

Delete an address from the Trusted IP addresses list by selecting the address and clicking **Remove**.

Related concepts
Managing domain and IP address groups on page 99

Email Log Server information

The Email Log Server receives records of system event and email analysis activity, which the Log Database uses to generate reports. Enter the Log Server IP address and port number on the page **Log Server**. Click **Check Status** to receive Log Server availability information.

System notification email address

Identify an email address to which you want system notification messages sent on the wizard page **Notifications**. Typically, this is an administrator address. Enter the desired address in the field **Notification email address**.

Entering and viewing subscription information

You should receive a subscription key when you purchase Forcepoint Email Security.

If you did not enter the subscription key the first time you opened the Email Security module, enter it on the page **Settings** > **General** > **Subscription**. This subscription key can be entered in one appliance and is applied to all the appliances controlled by the Email Security module.

Enter a new key any time you receive one to update your subscription. If your subscription includes the Forcepoint Email Security Hybrid Module, you must register with the email hybrid service every time you enter a new subscription key to establish the connection and synchronize email protection system functions. After you enter a valid subscription key, the expiration date and number of subscribed users are displayed. Purchased subscription features appear in the Subscribed Features list.

There are two different license modes: Forcepoint Email Security and Forcepoint DLP Email Gateway. Forcepoint DLP Email Gateway is an alternative to Forcepoint Email Security and provides capability to analyze inbound or outbound mail for data loss or theft. If you use Forcepoint DLP, you can add a subscription key to register Forcepoint DLP Email Gateway. It is not possible to deploy Forcepoint DLP Email Gateway concurrently with Forcepoint Email Security.

If you enter a new subscription key for a different license mode, the email protection system automatically reloads the configuration to provide access to the functionality available with the subscription. All menu options are available with a new installation of Forcepoint Email Security. If you register a new Forcepoint DLP Email Gateway license, the email protection system automatically updates to allow access to Forcepoint DLP Email Gateway menu options. See *Forcepoint Email Security versus Forcepoint DLP Email Gateway* for a comparison table of the menu options available in each product.

Related reference
Forcepoint Email Security versus Forcepoint DLP Email Gateway on page 15

Add subscription key

Steps

1) Navigate to the page **Settings** > **General** > **Subscription**.

2) In the field **Subscription key**, enter the subscription key.

3) Click **OK**.

If this is a changed subscription rather than a new installation, Forcepoint Email Security automatically reloads configuration. The dialog box Reload System Configuration displays with a countdown to the reload. After the system reloads, the menu options change according to the license mode.

A success message displays at the top of the Subscription page. The expiration date and number of subscribed users display below the subscription key.

Purchased subscription features display in the Subscribed Features list.

When a subscription key is added for Forcepoint DLP Email Gateway, DLP policies are applied by default to inbound and outbound traffic. See *Enabling data loss prevention policies*.

4) (*Optional*) Mark the check box **Block incoming email connections when subscription expires**.

Functionality blocks inbound email traffic when your subscription expires. Selecting this option also blocks inbound connections when your email protection system has not had a successful database download in two weeks. This function is disabled by default.

A valid subscription includes a grace period of two weeks in which to renew your product licenses after the subscription expires. Alerts are sent daily during the grace period as a reminder that the subscription has expired.

5) (*If your subscription key includes Forcepoint Email Security Hybrid Module*) Navigate to the page **Settings** > **Hybrid Service** > **Hybrid Configuration**.

Register with the email hybrid service to establish the connection and synchronize email protection system functions. See *Registering the Email Security Hybrid Module*.

Related concepts

Registering the Email Security Hybrid Module on page 63

Related tasks

Enabling data loss prevention policies on page 202

Forcepoint Email Security versus Forcepoint DLP Email Gateway

The following table details the menu options available in Forcepoint Email Security and Forcepoint DLP Email Gateway.

Menu	Email Security	DLP Email Gateway
Status	■ Dashboards ■ Alerts ■ Logs ■ Presentation Reports ■ Real-Time Monitor	N/A

Menu	Email Security	DLP Email Gateway
Message Management	■ Blocked Messages ■ Delayed Messages ■ Message Queues	N/A
Policy Management	■ Policies ■ Filters ■ Actions ■ Always Block/Permit	■ Policies ■ Filters (Disclaimer filter only)
General	■ Subscription ■ Email Appliances ■ Cluster Mode ■ System Settings ■ Backup/Restore ■ Database Downloads ■ Proxy Server ■ URL Analysis ■ Advanced File Analysis ■ Data Loss Prevention ■ SIEM Integration	■ Subscription ■ Email Appliances ■ System Settings ■ Data Loss Prevention
Administrators	■ Delegated Administrators ■ Roles	N/A
Users	■ User Directories ■ Domain Groups ■ User Authentication	■ Domain Groups

Menu	Email Security	DLP Email Gateway
Inbound/Outbound	■ Mail Routing ■ Connection Control ■ True Source IP ■ IP Groups ■ Relay Control ■ Message Control ■ DKIM Settings ■ DMARC Settings ■ Directory Attacks ■ Exceptions ■ Non-Delivery Options ■ Encryption ■ Enforced TLS Connections ■ TLS Certificate ■ Address Rewriting ■ URL Sandbox ■ Phishing Detection ■ Traffic Shaping	■ Mail Routing ■ IP Groups ■ Relay Control ■ Exceptions ■ Encryption
Hybrid Service	■ Hybrid Configuration ■ Hybrid Service Log Options	N/A
Personal Email	■ General Settings ■ Notification Message ■ User Accounts ■ End-User Portal ■ SSL Certificate	N/A
Alerts	■ Enable Alerts ■ Alert Events	■ Enable Alerts
Reporting	■ Log Database ■ Log Server ■ Preferences	■ Log Database

Navigating the Forcepoint Security Manager

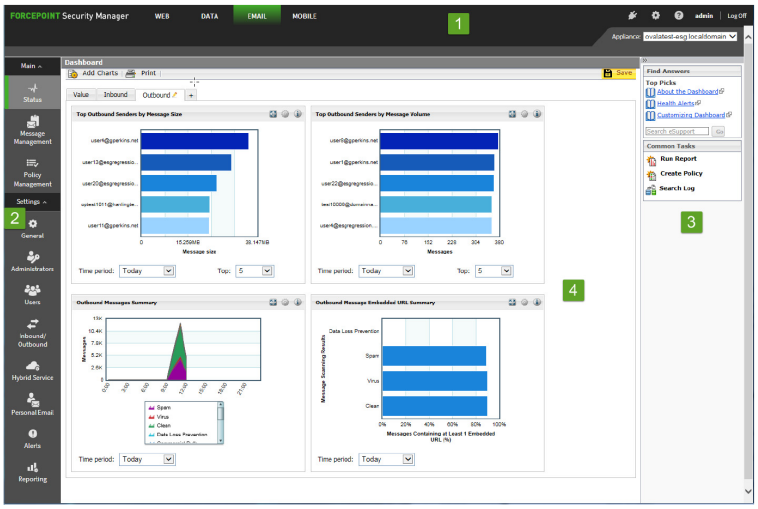
The Email Security module user interface can be divided into four main areas:

- The Security Manager toolbar
- The left navigation pane
- The right shortcut pane
- The context pane

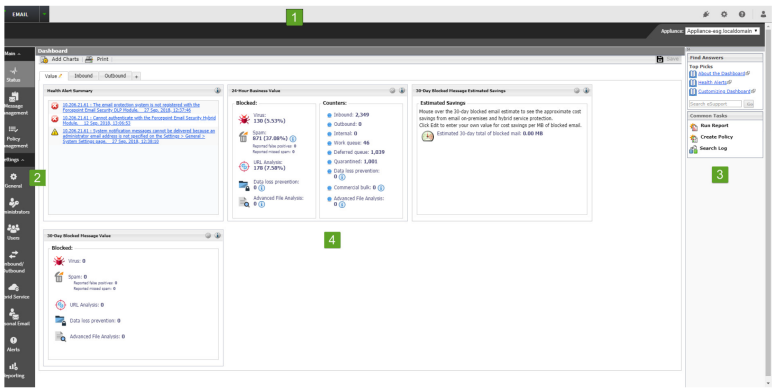
The content displayed in the Email Security module varies based on the privileges granted to the logged-on user. A user who is a reporting administrator, for example, does not see server configuration settings or policy administration tools.

This section describes the options available to users with Super Administrator privileges.

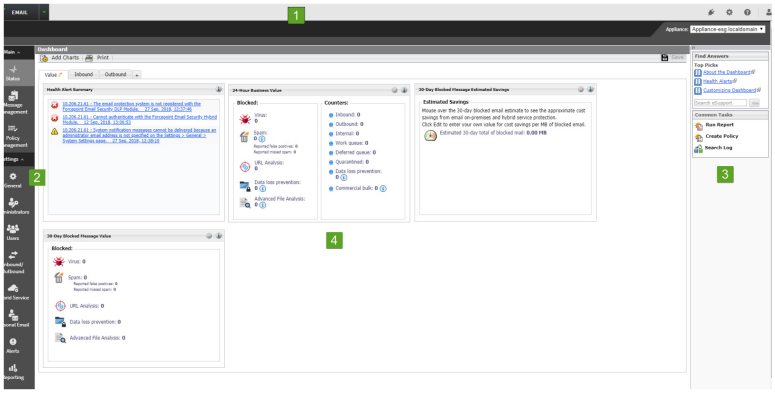
Certain menu options were changed in versions 8.5.3 and 8.5.4. The following image displays the user interface for Security Manager version 8.5:



The following image displays the user interface for Security Manager version 8.5.3:



The following image displays the user interface for Security Manager version 8.5.4:



1) Security Manager toolbar

2) Left navigation pane

3) Right shortcut pane

4) Content pane

Forcepoint Security Manager toolbar

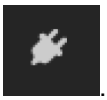
The Forcepoint Security Manager toolbar displays across the top of the Forcepoint Security Manager and provides:

- Access to the Security Manager product modules
- Icons to access the Manage Appliances and Global Settings pages
- An icon to access product Help information
- The status for your current logon account; i.e., Administrator or Super Administrator
- A Log Off button, for ending your administrative session

Manage appliances

The Manage Appliances page is used to register new appliances and access all Forcepoint appliances in your network.

Access the Manage Appliances page

From the Security Manager banner, click the icon **Appliances**  .

The Manage Appliances page displays. See Forcepoint Security Manager Help.

Global Settings

The Global Settings page is used to configure the following management settings for all Forcepoint Security Manager modules:

- Manage your administrator account.
- Add other Forcepoint Security Manager administrators and assign them appropriate permissions.
- Specify and configure the desired directory service for Security Manager administrators.
- Configure administrator account notification message details.
- Enable and configure two-factor authentication to the Security Manager.
- Audit administrator logon attempts and changes to Global Settings.

Access the Global Settings page

From the Security Manager banner, click the icon **Global Settings**  .

The Global Settings page displays. See Forcepoint Security Manager Help.

Help options

The Help icon provides access to Explain This Page context-sensitive Help, complete Help system contents, helpful initial configuration setting information, and the Forcepoint Support Portal.

Access Explain This Page

Steps

1) From the Security Manager banner, click the icon **Help**. The Help options display.

2) Click **Explain This page**.
   A new tab displays, showing the Help topic for the current page of the Forcepoint Security Manager.

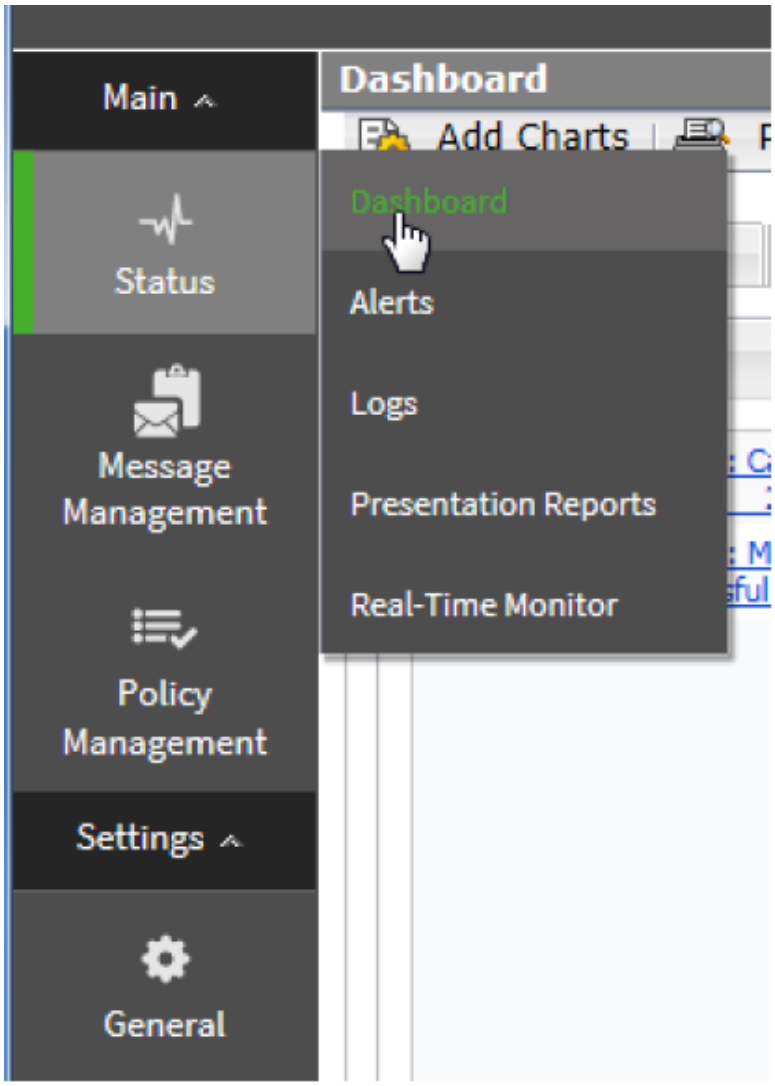
3) (*Optional*) From the Help topic, click **Open topic with navigation**. The complete Help system displays.

Left navigation pane

The left navigation pane, just under the module tray, provides access to two groups of menu items: Main and Settings.

The Main menu is used to access email software status, reporting, and policy management features and functions. The Settings menu is used to perform system

administration tasks. Individual configuration pages are accessed from the menu items. The toolbar also includes a pull-down menu of system appliances.



Right shortcut pane

The right shortcut pane contains a Find Answers portal that may include links to topics related to the active screen. The search function can be used to find relevant information in the Forcepoint Support Portal. The right pane also includes links to common administrative tasks.

Use Find Answers portal

Steps

1) From the Common Tasks section of the right shortcut pane, click a link. A new tab displays, showing the Help topic for the selected item.

2) (*Optional*) In the field **Search eSupport**, enter search terms and click **Go**.
   A new tab displays, showing the search results from the Forcepoint Support Portal.

Access common tasks

From the Common Tasks section of the right shortcut pane, click an item. The page on which the selected task performs displays.

Minimize the right shortcut pane

Steps

1) From the top of the right shortcut pane, click the double arrow icon (**>>**).
   The right shortcut pane minimizes.

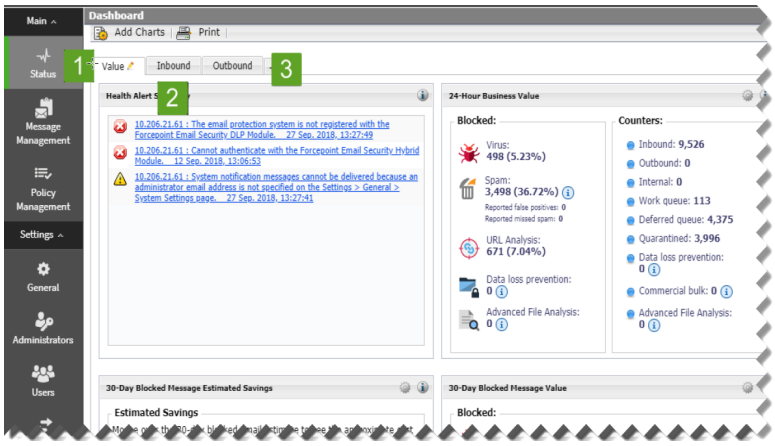
2) Reopen the right shortcut pane; click the double arrow icon (**<<**).
   The right shortcut pane opens.

The dashboard

The dashboard displays on initial login to the Email Security module of the Forcepoint Security Manager and provides access to charts detailing metrics for the Forcepoint Email Security product.

The dashboard includes three default tabs.

The following image displays the dashboard in version 8.5.3:



The following image displays the dashboard in version 8.5.4:

- The *Value dashboard tab* (1) displays on first login and shows information about the value of Forcepoint Email Security in the network, along with a summary of system health alerts.
- The *Inbound dashboard tab* (2) shows graphical charts that display top domains and message recipients for inbound email. Top domain and recipient information is sorted by message size or volume.
- The *Outbound dashboard tab* (3) shows graphical charts that display top senders for outbound email, sorted by message size or volume. Other default charts for this tab show an overall outbound message summary and a summary of outbound messages that contained embedded URLs.

Dashboard elements are visible to Super Administrators and those delegated administrators with permission to view reports on the email dashboard (see *Managing administrator accounts*). The type of information and level of detail shown depends on your subscription level. For example, the Forcepoint Email Security Hybrid Module is required to display information about the email hybrid service and how it safeguards your system. Forcepoint Advanced Malware Detection for Email - Cloud must be purchased to view metrics on advanced file analysis functions in the cloud; Forcepoint Advanced Malware Detection for Email - On-Premises must be purchased to view advanced file analysis appliance metrics. The following table details the options available on the dashboard.

Icon	Option	Description
Add Charts	Add Charts	Selection displays the Add Charts page to add elements to the Value, Inbound, Outbound, or any custom dashboard tab. See *Adding elements to a dashboard tab*.
Print	Print	Selection displays a secondary window with a printer-friendly version of the charts displayed on the tab. Browser options are used to print the page.
Save	Save	Selection saves dashboard changes, such as adding, moving, or editing charts. The Save button only activates when changes are made to the dashboard. Save any changes before navigating away from the dashboard.

Related concepts
Value dashboard tab on page 26
Inbound dashboard tab on page 29
Outbound dashboard tab on page 30
Managing administrator accounts on page 81
Adding elements to a dashboard tab on page 31

Adding and configuring dashboard charts

The default Value, Inbound, and Outbound dashboard tabs can each display up to 12 charts at a time. You can customize most dashboard charts to change their time period (for example, today, last 7 days, last 30 days) and their display format (for example, stacked column, stacked area, multi-series line). You can include multiple versions of the same chart on a tab (for example, showing different time periods). See *Available dashboard charts* for a list of charts for dashboard display.

- Most dashboard elements are updated every two minutes. The Health Alert Summary is updated every 30 seconds.
  All elements on a tab are also updated when any element on the tab is modified. For example, if the time period for one chart is changed, data is refreshed in all of the charts on the page.
- The available set of dashboard elements depends on your subscription type. Charts related to the email hybrid service, for example, are available only for deployments that include the Forcepoint Email Security Hybrid Module.
- Clicking a pie, bar, or line chart typically allows the display of drill-down data with more details. For example, clicking a chart element that represents data for a 24-hour period can display the same data in one-hour increments. These capabilities are available in the Edit, Enlarge, and Preview chart views.

Related concepts
Available dashboard charts on page 32

Add a chart to a dashboard tab

From the dashboard, click **Add Charts**.

The Add Charts window displays. See *Adding elements to a dashboard tab*.

Related concepts
Adding elements to a dashboard tab on page 31

Move a chart on a dashboard tab

Steps

1) Click the title bar of a chart.

2) Keeping the mouse button selected, drag the chart to a new location on the same tab.
A check mark icon displays when the chart can be placed in a new location.

3) Release the mouse button.
The chart displays in its new location on the dashboard tab.

4) From the dashboard, click **Save**.
The dashboard configuration is saved.

Remove a chart from a dashboard tab

Steps

1) On the title bar of a chart, click the icon **Options**. The chart options display.

2) Click **Remove**.
The Confirm Remove Chart dialog window displays.

3) Click **Remove**.
The chart is removed from the dashboard tab.

4) From the dashboard, click **Save**.
The dashboard configuration is saved.

Print a chart

Steps

1) On the title bar of a chart, click the icon **Options**. The chart options display.

2) Click **Print**.
A new tab displays with a printer-friendly version of the chart.

3) Click **Print**.
The chart prints.

Edit a chart

Steps

1) On the title bar of a chart, click the icon **Options**. The chart options display.

2) Click **Edit**.
   The Edit dialog box displays with editing options for the selected chart. Available options depend on the type of chart you selected. Change the following:
   - Chart name
   - Chart type
   - Time period
   - “Top” numerical designation (e.g., Top *N* Data Loss Prevention Violations)
   - Restore default chart settings
   - Copy chart (adds chart to the active tab with “(2)” at the end of the title; select **Edit** to change the chart name)

3) Click **OK**.
   The changes are saved.

4) From the dashboard, click **Save**.
   The dashboard configuration is saved.

View a larger version of a chart

Steps

1) On the title bar of a chart, click the icon **Enlarge**.
   The Enlarge dialog box displays with an enlarged view of the chart and configuration options.

2) From the section Chart Options, configure options for the selected chart.
   Example: chart type, time period, top numerical designation.

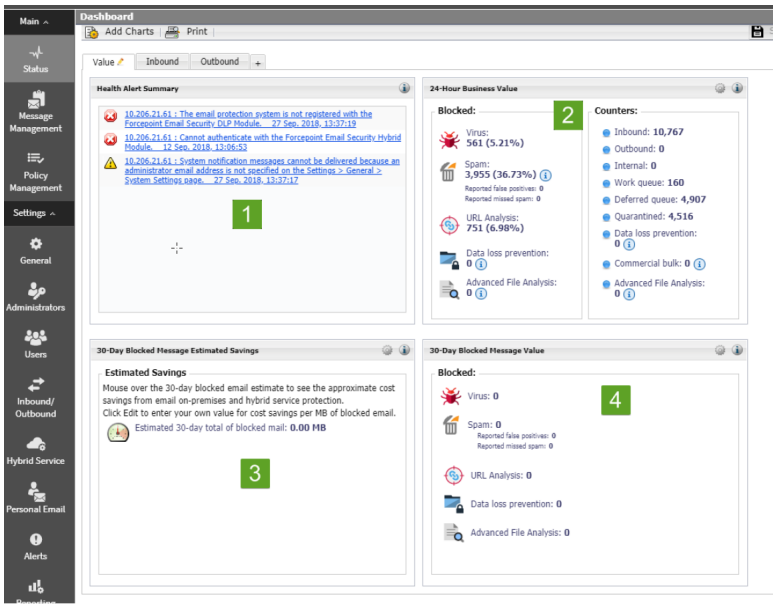
3) (*Optional*) Print the chart; select **Print Chart**.

4) When finished, click **Close**.

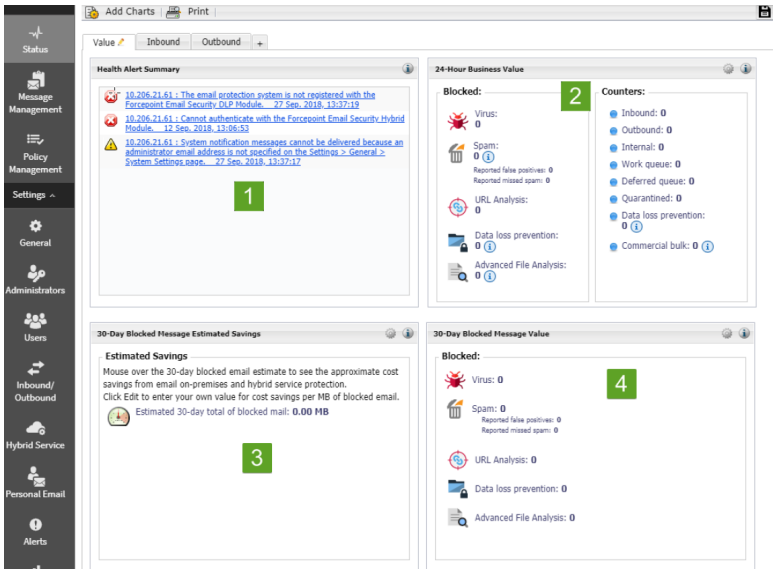
Value dashboard tab

The Value dashboard tab is a default tab that displays alert messages and graphical charts that show the current state of your email protection system, focusing on email traffic activity in your network.

The following image displays the default elements on the Value tab in version 8.5.3:



The following image displays the default elements on the Value tab in version 8.5.4:



- The **Health Alert Summary** (1) shows the status of your Forcepoint software. Selection of an error or warning alert message to open the Alerts page, where more detailed alert information is available (see *Viewing system alerts*).
- The **24-Hour Business Value** chart (2) displays statistics showing how your email security software has protected your network during the past 24 hours by blocking suspicious email traffic. Data includes total numbers of blocked connections and messages listed by analysis result, the numbers of false positive and missed spam results from email analysis, and the number totals for various types of messages handled by the email system.
- The **30-Day Blocked Message Estimated Savings** chart (3) provides an estimate of savings afforded by your email protection system, which can stop unwanted mail and threats (including at the connection level), protect network resources, and save an organization time and money. With the addition of the Forcepoint Email Security Hybrid Module, infected traffic is stopped before it enters the network, increasing the savings. Hover over the estimated savings item for the approximate cost savings from the email hybrid service and on-premises email analysis. Default value of cost per MB includes the estimated cost saving from preventing threats and unwanted mail, and the resulting bandwidth saved. Use the Options icon in the element's title bar to set the cost savings per MB of blocked mail.

- The **30-Day Blocked Message Value** chart (4) displays metrics similar to the 24-hour value chart demonstrating email system protection for the previous 30 days. This chart illustrates the total numbers and percentages of blocked connections and messages, including false positive and missed spam results from email analysis.

Related concepts
Viewing system alerts on page 34

Change the name of the Value dashboard tab

Steps

1) From the Value dashboard tab, click the icon **Edit**. The Edit Tab dialog box displays.

2) In the field **Tab name**, enter the new name for the Value tab.

3) Click **OK**.
The new name of the tab is saved. Default tabs, such as the Value tab, can be renamed but not removed.

Add a chart to the Value dashboard tab

From the dashboard, click **Add Charts**.

The Add Charts window displays. See *Adding elements to a dashboard tab*.

Related concepts
Adding elements to a dashboard tab on page 31

Remove a chart from the Value dashboard tab

Steps

1) On the title bar of a chart, click the icon **Options**. The chart options display.

2) Click **Remove**.
The Confirm Remove Chart dialog box displays.

3) Click **Remove**.
The chart is removed from the Value dashboard tab.

4) From the dashboard, click **Save**.
The dashboard configuration is saved.

Inbound dashboard tab

The Inbound dashboard tab is a default tab that provides summary data on inbound message traffic.

Default charts on the Inbound tab include the following:

- The **Top Inbound Domains by Message Size** chart displays the message domains that are the source of the majority of inbound messages, plotted by message size.
- The **Top Inbound Domains by Message Volume** chart shows the message domains that account for the majority of all inbound messages.
- The **Top Inbound Recipients by Message Size** chart displays the recipient addresses that receive the majority of inbound email, plotted by message size.
- The **Top Inbound Recipients by Message Volume** chart shows the recipient addresses that receive the majority of all inbound email.

Change the name of the Inbound dashboard tab

Steps

1) From the Inbound dashboard tab, click the icon **Edit**. The Edit Tab dialog box displays.

2) In the field **Tab name**, enter the new name for the Inbound tab.

3) Click **OK**.
   The new name of the tab is saved. Default tabs, such as the Inbound tab, can be renamed but not removed.

Add a chart to the Inbound dashboard tab

From the dashboard, click **Add Charts**.

The Add Charts window displays. See *Adding elements to a dashboard tab*.

Related concepts
Adding elements to a dashboard tab on page 31

Remove a chart from the Inbound dashboard tab

Steps

1) On the title bar of a chart, click the icon **Options**. The chart options display.

2) Click **Remove**.
   The Confirm Remove Chart dialog box displays.

3) Click **Remove**.
The chart is removed from the Inbound dashboard tab.

4) From the dashboard, click **Save**.
The dashboard configuration is saved.

Outbound dashboard tab

The Outbound dashboard tab is a default tab that provides summary data on outbound message traffic.

Default charts on the Outbound tab include the following:

- The **Top Outbound Senders by Message Size** chart displays the sender addresses that account for the majority of outbound email, plotted by message size.
- The **Top Outbound Senders by Message Volume** chart shows the sender addresses that represent the majority of all outbound messages.
- The **Outbound Messages Summary** chart displays the total number of outbound messages processed by your email protection software, sorted by message analysis result (clean, virus, spam, and so on).
- The **Outbound Message Embedded URL Summary** chart shows the percentage of analyzed outbound messages that contain at least one embedded URL, displayed by message analysis result. For example, if 50 outbound messages are determined to be spam, and 40 of those messages contain an embedded URL, then the percentage shown in this chart for the spam message type is 80% (40/50).

Change the name of the Outbound dashboard tab

Steps

1) From the Outbound dashboard tab, click the icon **Edit**. The Edit Tab dialog box displays.

2) In the field **Tab name**, enter the new name for the Outbound tab.

3) Click **OK**.
The new name of the tab is saved. Default tabs, such as the Outbound tab, can be renamed but not removed.

Add a chart to the Outbound dashboard tab

From the dashboard, click **Add Charts**.

The Add Charts window displays. See *Adding elements to a dashboard tab*.

Related concepts
Adding elements to a dashboard tab on page 31

Remove a chart from the Outbound dashboard tab

Steps

1) On the title bar of a chart, click the icon **Options**. The chart options display.

2) Click **Remove**.
The Confirm Remove Chart dialog box displays.

3) Click **Remove**.
The chart is removed from the Outbound dashboard tab.

4) From the dashboard, click **Save**.
The dashboard configuration is saved.

Adding elements to a dashboard tab

The page **Status** > **Dashboard** > **Add Charts** is used to add elements to the Value, Inbound, Outbound, or any custom dashboard tab. The following table details the options on the Add Charts page.

Option	Description
Available Tabs	Enables selection of any available tab to add charts. Selection of a tab updates the Preview pane. Functionality is also available to restore defaults for default dashboard tabs.
Dashboard Elements	Enables selection of charts to be added to the selected tab. See *Available dashboard charts* for a complete list of available elements.
Preview	Displays a preview of the selected chart and enables changes to be made to the chart name, chart type, time period, and top value.

Related concepts
Available dashboard charts on page 32

Add charts to a dashboard tab

Steps

1) In the section Available Tabs, from the pull-down menu **Add elements to tab**, select the desired dashboard tab.

2) (*Optional*) If a default tab is selected (i.e., Value, Inbound, or Outbound), click **Restore** Tab Defaults.
The default settings for the selected default tab are restored.

3) In the section Dashboard Elements, mark the check boxes next to the elements to be added to the tab.
Selection of an element displays a sample in the Preview pane.

   - You can add an element to any tab.
   - Each tab can show a maximum of 12 elements.
   - Elements currently displayed on the selected tab are marked by a blue circle icon.
   - You can add multiple copies of the same element to a tab (for example, each might show a different time period).

4) From the Preview pane, view and customize the selected chart as needed, such as changing the chart name.
The chart name may be up to 47 alphanumeric characters and include spaces and underscores.

   - **Chart type**: Many charts can be displayed as a multi-series bar, column, or line chart, or as a stacked area or column chart. Some can be displayed as bar, column, line, or pie charts. The types available depend on the data being displayed.
   - **Time period**: Most charts can display a variable time period: Today (the period since midnight of the current day), the last 7 days, or last 30 days.
   - **Top**: Charts displaying information about the top users, categories, URLs, and so on can display up to 5 values. Select whether to show the top five values, 6-10 values, 11-15 values, or 16-20 values.

5) (*Optional*) Start over with configuration, from the Preview pane, select **Restore Defaults**.
Changes made to the selected chart are reset the chart to is default time period, type, and top value (if any).

6) Complete all configuration changes and click **Add**.
The dashboard tab displays with the configured elements.

Available dashboard charts

Dashboard tabs can be customized by adding up to 12 charts per tab. The page **Status** > **Dashboard** > **Add Charts** is used to add charts to a tab. See *Adding elements to a dashboard tab*. The following table details the charts available to be added to all dashboard tabs.

Note

Some charts show potentially sensitive information, such as usernames or IP addresses. Ensure that the charts you select are appropriate for all of the administrators who may view them.

Chart Name	
30-Day Blocked Message Value	

Chart Name
30-Day Blocked Message Estimated Savings
24-Hour Business Value
Connections Summary
Inbound Messages Summary
Outbound Messages Summary
Average Message Volume in Work Queue
Data Loss Prevention Violations by Severity
Top Data Loss Prevention Violations
Top Outbound Senders by Message Size
Top Outbound Senders by Message Volume
Top Blocked Protected Domain Addresses
Top Inbound Domains by Message Size
Top Inbound Domains by Message Volume
Top Inbound Recipients by Message Size
Top Inbound Recipients by Message Volume
Inbound Message Embedded URL Summary
Outbound Message Embedded URL Summary
Inbound Message Embedded URL Categories
Outbound Message Embedded URL Categories
Top Inbound Targeted Phishing Attacks
Top Inbound Phishing Attack Victims
Inbound Message Throughput
Outbound Message Throughput
Outbound Encrypted Messages Summary
Message Volume by Direction
Top Inbound Senders
Inbound Spam Volume
Inbound Spam Percentage
Inbound Virus Volume
Inbound Virus Percentage
Inbound Commercial Bulk Volume
Inbound Commercial Bulk Percentage
Outbound Spam Volume

Chart Name
Outbound Spam Percentage
Outbound Virus Volume
Outbound Virus Percentage
Inbound Volume by Message Type
Outbound Volume by Message Type
Opportunistic TLS Usage Volume
Top Recipient Domains Via Mandatory TLS Channel
Top Mandatory TLS Usage Failures
Inbound Forcepoint Advanced Malware Detection for Email - Cloud Analysis Volume
Top Inbound Attachments Detected by Forcepoint Advanced Malware Detection for Email - Cloud
Top Attachments by File Type Detected by Forcepoint Advanced Malware Detection for Email - Cloud
Top Recipients Protected by Forcepoint Advanced Malware Detection for Email- Cloud
Inbound Analysis Volume for Forcepoint Advanced Malware Detection for Email - On-Premises
Top Malicious Attachments Detected by Forcepoint Advanced Malware Detection for Email - On-Premises
Top Recipients Protected by Forcepoint Advanced Malware Detection for Email- On-Premises
Attachment File Types Detected by Forcepoint Advanced Malware Detection for Email - On-Premises
Email Hybrid Service Message Size Summary (requires Forcepoint Email Security Hybrid Module)
Email Hybrid Service Message Volume Summary (requires Forcepoint Email Security Hybrid Module)

Related concepts
Adding elements to a dashboard tab on page 31

Viewing system alerts

The page **Status** > **Alerts** displays information about problems affecting the health of the email software, provides links to troubleshooting help, and documents the details of recent real-time analytic database updates.

The Alerts page can be accessed from the Status menu or from the Health Alert Summary chart on the Value tab of the dashboard, which shows the status of your email protection software.

Access Alerts from the left navigation pane

From the left navigation pane, select **Status** > **Alerts**. The Alerts page displays.

Access Alerts from the Health Alert Summary chart

From the Health Alert Summary chart on the Value dashboard tab, select an error or warning message.

The Alerts page displays.

Active Alerts

The Active Alerts list displays the status of monitored Forcepoint software components with functionality to view detailed information about which components are monitored.

View monitored components

- From Active Alerts, click **What is monitored?**
  A new tab displays with the Help topic for *System health alerts*.

Troubleshoot a problem

- From an error or warning message in Active Alerts, click **Solutions**.
  A new tab displays with the applicable Help topic for troubleshooting.

View details of an informational alert

- From an informational alert, click **Learn More**.

Related concepts
System health alerts on page 35

System health alerts

The Health Alert Summary lists any potential concerns encountered by monitored components of your software. Alerts are generated for the following conditions:

- Subscription expiration issues or subscription key problems
- Email services unavailable or not running
- Email software configuration problems
- Forcepoint URL Database server connection problems
- Filtering database engine and download problems
- URL analysis server problems
- Log Server unavailable, not running, or having performance problems
- Email module, Log Server, or Log Database version mismatches
- Log Database unavailable or having performance problems
- Low disk space problems
- Old system log or message queue files
- Unavailable system logs or message queues
- Third-party encryption application problems
- Appliance cluster connection and synchronization problems
- User directory server unavailable or not running
- Invalid user directory credentials

- SIEM server configuration problems
- Personal Email Manager server connection problems
- Undelivered email accumulation problems
- Work and exception queue capacity problems

If you have subscribed to the Forcepoint Email Security Hybrid Module, or if your subscription includes both email and data security components, your email protection software monitors interoperability components to provide alerts about the following conditions:

- Forcepoint Security Manager Data module registration, configuration, and connection status
- Hybrid Module registration, authentication, and email hybrid service connection status

See *Configuring system alerts* for information about system alert delivery options.

The icon next to the alert message indicates the potential impact of the related condition.

 The message is informational, and does not reflect a problem with your installation (for example, a successful database download or cluster synchronization).

 The alert condition has the potential to cause a problem, but does not immediately prevent filtering or reporting (for example, email hybrid service data is not available or the subscription key is about to expire).

 A Forcepoint software component is not functioning (has not been configured or is not running), which may impair email analysis or reporting, or your subscription has expired.

Selection of an alert message in the Health Alerts Summary displays the Alerts page, which provides additional information about current alert conditions. See *Viewing system alerts*.

Related concepts

Configuring system alerts on page 71
Viewing system alerts on page 34

Viewing and searching logs

The page **Main** > **Status** > **Logs** provides access to several logs for monitoring system and email message status. Logs are searchable by predefined or customized time periods. The Message Log additionally allows searches to be refined for messages, using search conditions like email address, message analysis result, or message status.

The search results for any log can be exported to a comma-separated value (CSV) or HTML file. The maximum number of log entries exported cannot be greater than 100,000. Starting in version 8.5.4, when logs are filtered and then exported, the exported file contains only the filtered logs.

The following logs are accessed from the Logs page:

Related concepts

Message Log on page 37
Connection Log on page 44
Audit Log on page 47
Personal Email Manager Audit Log on page 50
System Log on page 52
Console Log on page 54
Email Hybrid Service Log on page 57

Message Log

The Message Log records information about each email message (inbound, outbound, and internal) processed by the email system. Access the Message Log on the Message tab of the page **Main** > **Status** > **Logs**.

Message Log data

The following table details the Message Log data that is collected and displayed in the Message Log in table format.

Message data item	Description
Received Date/Time	The date and time a message was received.
Subject	The message subject.
Sender Address	The message sender email address.
Sender IP	The message sender IP address.
Recipient Address	Message recipient email address. If the message has multiple recipients, the first recipient address is displayed.
Analysis Result	Message analysis results or filter type (Clean, Virus, Spam, URL Analysis, Data Loss Prevention, Exception, Commercial Bulk, Block List, Phishing, Advanced Malware Detection - Cloud, Advanced Malware Detection - On-Premises, Email Attachment, Spoofed Email, or Custom Content). The Block List type applies to a message that is blocked by a Personal Email Manager Always Block List. When a data loss prevention (DLP) policy is indicated, a View Incident link in this column opens the incident details in the Security Manager Data Security module.

Message data item	Description
Message Status	Current message status (Delivered, Delayed, Dropped, Exception, Failed, Waiting for delivery, or Waiting for message analysis). A message with multiple recipients may have multiple status entries based on the policy applied.
From: Header	The message From: header.
Spam Score	The spam score of the message.
Message Size (KB)	The size of the message, in KB.

Message Log search options

The Message Log Search Options section includes search options such as date range or keyword, as well as filtering options to search messages by specific criteria, and the functionality to drag columns to resize them. The View from/To calendar controls are used to determine the date and time range for a search. The default value for the from and to fields is the date and time at which the log is opened. The calendar includes the following options:

- Back and Next arrows display around the month and year at the top of the calendar to change the date.
- The current date displays in the lower left corner of the calendar; selection sets the calendar to the current date.
- The Clean option is used to clear the current date/time calendar selection.
- The entry fields to the right of the calendar are used to set the time range in hours and minutes.

The search filter functionality is used to narrow the search by filtering results by criteria such as Subject, Spam Score, Recipient Address, or Appliance. Up to 10 filters can be added, with a relationship of “and” to further refine the search. The following table details the search filter options.

Option	Description
Filter	Pull-down menu functionality to select a message element on which to search: ■ Subject ■ Sender Address ■ Sender IP ■ Recipient Address ■ Analysis Result ■ Message Status ■ To: Header ■ From: Header ■ Spam Score ■ Message Size (KB) ■ Appliance

Option	Description
Condition	Pull-down menu functionality to select a condition for the selected filtering option. The available conditions depend on the selected filter; not all conditions are available for all filters. Conditions include: ■ Contains ■ Does not contain ■ Equals ■ Does not equal ■ Starts with ■ Does not start with ■ Ends with ■ Does not end with ■ Is ■ Is not ■ Is in this range **Note** If you select the filter Spam Score and the condition “is” or “is not,” the value of “null” can be input in the Value field. If you select the filter Sender Address or Recipient Address and the filter “is” or “is not,” multiple addresses can be entered in the Value field, separated by a semicolon.
Value	User-defined text field to enter a value for the filter and condition.
Add/Remove	Selection adds or removes a row of filtering options to further narrow the search.

Option	Description

Advanced Options	Selection displays additional sort conditions to refine the search:
	■ By Direction
	  ■ Inbound
	  ■ Outbound
	  ■ Internal
	  ■ Open Relay
	■ By Analysis Result
	  ■ Clean
	  ■ Virus
	  ■ Spam
	  ■ URL Analysis
	  ■ Commercial Bulk
	  ■ Data Loss Prevention
	  ■ Custom Content
	  ■ Exception
	  ■ Block List
	  ■ Advanced Malware Detection - Cloud
	  ■ Phishing
	  ■ Advanced Malware Detection - On-Premises
	  ■ Spoofed Email
	  ■ Email Attachment
	  ■ SMTP Authentication Fail
	  ■ RBL
	  ■ Reputation
	  ■ RDNS
	  ■ SPF
	  ■ DMARC
	■ By Message Status
	  ■ Delivered
	  ■ Delayed
	  ■ Dropped
	  ■ Exception
	  ■ Failed
	  ■ Expired
	  ■ Rejected

Search the Message Log

Steps

1) From the section Message Log Search Options, set the date and time to be searched in the fields **View from** and **To**.
   (*Optional*) Use the calendar functionality to specify a date to search.

2) From the pull-down menu **Filter**, select a message element on which to search.

3) From the pull-down menu **Condition**, select a filter condition on which to search.

4) In the field **Value**, enter a keyword on the filter and condition.
   Example: If you selected the filter **Sender Address** and the condition **Is**, enter at least one email address on which to search. Separate multiple addresses with a semicolon.

5) To add more search filters, click the **plus sign**. A second row of filtering options displays.
   Up to 10 filters can be added. The relationship between filters is “and,” which allows searches to be narrowly refined.

6) (*Optional*) To remove a search filter, click the **(-)** minus sign. The filter is removed.

7) To add more search options, click **Advanced Options**. The Advanced Options display.

8) From Advanced Options, mark the check boxes for the conditions on which to sort.

9) Click **Search**.
   The search results display in the Message Log table.

10) (*Optional*) Restore all search settings to the default; click **Set to Default**. Search settings are reset.

Configure display settings and navigate log entries

Steps

1) From the pull-down menu **Per page**, select the number of entries to display; **25**, **50**, **100**, or **200**.

2) Scroll through Message Log pages, select the arrows to go back and next, or to the first and last pages of Message Log entries.

3) Jump to a specific page; in the field **Page**, enter the page number and select **Go**.

Message Log export options

The length of time message records are saved in the database depends on the message volume and database partition capacity. The Export option is used to preserve message records by exporting log data; it is recommended to export data on a regular basis.

Exporting does not remove records from the Message Log; it copies log data to a CSV or HTML file.

Export Message Log data

Steps

1) From the Message Log, click **Export**. The Export Log dialog box displays.

2) From the pull-down menu **File type**, select the desired output file type; **CSV** or **HTML**.
   - Selection of CSV enables data to be opened or saved as a text file in comma-separated value format.
   - Selection of HTML enables data to be opened or saved as an HTML file.

3) From Page range, indicate the pages to export; **All**, **Current Page**, or **Pages**.

4) Click **OK**.
   The Export Log window closes and the selected data is exported.

Log Details

The Log Details page displays information about a selected message. The following table details the Message Log detail items that display on the Log Details page.

Detail Item	Description
Recipient Address	Message recipient email address. If the message has multiple recipients, this column has multiple entries.
Recipient IP	Message recipient IP address.
Direction	Message direction (Inbound, Outbound, or Internal). If the message has multiple recipients, this column may have multiple entries.
Delivered Date/Time	The date and time a message was delivered to a recipient.
Policy	Name of the policy applied to the message. If the message has multiple recipients, this column may have multiple entries.
Rule	Name of the policy rule applied to the message. If the message has multiple recipients, this column may have multiple entries for a single message. This item is blank for a message with an analysis result of Clean.

Detail Item	Description
Analysis Result	Message analysis results or filter type (Clean, Virus, Spam, URL Analysis, Data Loss Prevention, Exception, Commercial Bulk, Block List, Phishing, Advanced Malware Detection - Cloud, Advanced Malware Detection - On-Premises, Email Attachment, Spoofed Email, or Custom Content). The Block List type applies to a message that is blocked by a Personal Email Manager Always Block List.
Message Status	Current message status (Delivered, Delayed, Dropped, Exception, Failed).
Quarantined?	Indicator of whether message is quarantined (Yes or No). A **View** link appears for a message isolated by a DLP or advanced file analysis policy.

View message details

Steps

1) From the Message Log, click the subject of a message. The Log Details page displays.

2) (*Optional*) View additional log details, click **View Log Details**.
Additional details display in table format. See *Message Log details*.

3) Return to the Message Log, click **Back**.
The Message Log page displays.

Related concepts
Message Log details on page 44

View quarantined message details

Steps

1) From the Log Details page, in the column **Quarantined?**, click **View**. The Message Details page displays with options for quarantined message.

2) From the Message Details page, click an option for the message; **Deliver**, **Delete**, **Reprocess**, **Not Spam**, or an available option from the pull-down menu **More Actions**.

3) Return to the Log Details page, click **Back**.
The Log Details page displays.

Message Log details

The Log Details page includes an option at the bottom of the page to view additional log details. Message Log details appear in a table, with columns for the date and time of receipt, and the source of the message details. Detail sources can include message and connection control data, email policy data, and delivery data.

The log details appear in a third column, which can contain information about:

- Message size, sender, and recipients
- Connection type, sender IP address, and the email appliance that received the connection request
- Email policies and actions applied, including policy and rule names (filter and action), email direction (inbound, outbound, or internal), name of the virus or spam encountered, and the action taken as a result of filtering
- Email hybrid service analysis results, including a DKIM validation, if applicable
- Message delivery dispositions, including recipient email and IP address, and delivery status
- When advanced file analysis is performed, a list of the files that cannot be analyzed because the file type is not supported

View log details

Steps

1) From the Message Log, click the **subject** of a message. The Log Details page displays.

2) From the Log Details page, click View **Log Details**.
   Additional details display in table format.

3) Return to the Message Log, click **Back**.
   The Message Log displays.

Connection Log

The Connection Log is a record of incoming connection requests and the results of connection analysis. Access the Connection Log on the Connection tab of the page **Main** > **Status** > **Logs**.

Connection Log data

The following table details the connection data that is collected and displayed in the Connection Log in table format:

Connection Data Item	Description
Sender IP Address	The connection's sender IP address.
Date/Time	The date and time a connection was received.
Number of Messages	The number of messages in the connection.
Security Level	Encrypted or Not Encrypted.

Connection Data Item	Description
Connection Status	Current connection status (Accepted or Blocked). Status details are displayed in a hover-over pop-up box. Possible **Blocked** status details are as follows: ■ HELO/EHLO received before SMTP server greeting. ■ Connection from <*server address*> failed SPF check. ■ Reverse DNS lookup failed. ■ Simultaneous connections from <*server address*> exceeded limit. ■ Message volume exceeded limits. ■ Message size exceeded limit. Message was forwarded to <*queue id*> queue. ■ File size exceeded limit. Message was forwarded to <*queue id*> queue. ■ Data size per connection exceeded limit. Message was forwarded to <*queue id*> queue. ■ HELO command syntax error. ■ EHLO command syntax error. ■ Percentage of invalid recipients exceeded limit. ■ Connection attempt by <*server name*> failed global Always Block list check. ■ Connection attempt by <*server name*> failed recipient validation check. ■ Connection attempt by <*server name*> failed user authentication. ■ Open relay from <*sender name*> blocked. Possible **Accepted** status details are as follows: ■ Email Hybrid Service IP Group entry match. ■ Trusted IP group entry match. ■ Access list entry match. ■ Global Always Permit List entry match. ■ BATV bypass entry match. ■ True source IP address matched a Trusted IP group entry. ■ True source IP address matched an access list entry. ■ True source IP address matched an Email Hybrid Service IP Group entry. ■ True source IP address matched a global Always Permit List entry. ■ True source IP address matched a BATV bypass.

Connection Log search options

The Connection Log Search Options section includes search options such as date range or keyword. The View from/To calendar controls are used to determine the date and time range for a search. The default value for the from and to fields is the date and time at which the log is opened.

The calendar includes the following options:

- Back and Next arrows display around the month and year at the top of the calendar to change the month and the year.
- The current date displays in the lower left corner of the calendar; selection sets the calendar to the current date.
- The Clean option is used to clear the current date/time calendar selection.
- The Today option is used to set the calendar date to the current date.
- The entry fields to the right of the calendar are used to set the time range in hours and minutes.

Search the Connection Log

Steps

1) From the section Connection Log Search Options, set the date and time to be searched in the fields **View from** and **To**.

   (*Optional*) Use the calendar functionality to specify a date to search.

2) From the pull-down menu **Keyword search**, select a Connection Log element in which to search; **All**, **Sender IP address**, **Security level**, or **Connection status**.

3) In the text field, enter a search term.

   Alphanumeric characters are supported in the keyword search entry field. Wildcards and special characters are not supported in the keyword search for Sender IP address.

4) Click **Search**.

   The search results display.

5) (*Optional*) Restore all search settings to the default, click **Set to Default**. Search settings are reset.

Configure display settings and navigate log entries

Steps

1) From the pull-down menu **Per page**, select the number of entries to display; **25**, **50**, **100**, or **200**.

2) Scroll through Connection Log pages, select the arrows to go back and next, or to the first and last pages of Connection Log entries.

3) Jump to a specific page; in the field **Page**, enter the page number and select **Go**.

Connection Log export options

The length of time connection records are saved in the database depends on the connection volume and database partition capacity. The Export option is used to preserve connection records by exporting log data; it is recommended to export data on a regular basis. Exporting does not remove records from the Connection Log; it copies log data to a CSV or HTML file.

Export Connection Log data

Steps

1) From the Connection Log, click **Export**. The Export Log dialog box displays.

2) From the pull-down menu **File type**, select the desired output file type; **CSV** or **HTML**.
   - Selection of **CSV** enables data to be opened or saved as a text file in comma-separated value format.
   - Selection of **HTML** enables data to be opened or saved as an HTML file.

3) From **Page range**, indicate the pages to export; All, Current Page, or Pages.

4) Click **OK**.
   The Export Log window closes and the selected data is exported.

Connection Log details

Selection of an individual sender IP address link in the Connection Log displays the Log Details page with details about the message or messages associated with the selected connection. See *Log Details*.

Related reference
Log Details on page 42

Audit Log

The email protection system provides an Audit Log, which is an audit trail showing which administrators have accessed the Security Manager Email Security module and any changes made to policies and settings. The Audit Log additionally shows message actions taken by administrators, such as clearing a message queue or releasing, forwarding, or deleting email messages (added in version 8.5.3). Other actions shown in the audit log include changes made in the appliance CLI (added in version 8.5.3).

Monitoring administrator changes through the Audit Log enables you to ensure that system and message control is handled responsibly and in accordance with your organization's acceptable use policies. This information is available only to Super Administrators.

Access the Audit Log on the Audit tab of the page **Main** > **Status** > **Logs** to view the Audit Log and to export selected portions of it to a CSV or an HTML file, if desired.

Audit Log data

The following table details the system audit information that is collected and displayed in the Audit Log in table format:

Column	Description
Date	Date and time of the change, adjusted for time zones. To ensure consistent data in the Audit Log, ensure that all machines running Forcepoint components have their date and time settings synchronized.
User	Username of the administrator who made the change.
Server	IP address of the appliance affected by the change.
Client	IP address of the administrator machine that made the change.
Role	Administrator role (Super Administrator, Auditor, Quarantine Administrator, Reporting Administrator, Security Administrator, Policy Administrator, CLI Administrator, or Group Reporting Administrator).
Type	The location of the change in the module interface (for example, if you enter a new subscription key, this column displays **General** | **Subscription**).
Element	Identifier for the specific dynamic object changed, if any.
Action	Type of change made (for example, add, delete, update, import, export, move, auth, sync, reset, save, deliver, reprocess, or not spam).
Action Detail	A link that opens a Details message box with information about the change made. Starting in version 8.5.4, Action Detail includes information about specific changes between updates to the global Always Block and Always Permit lists.

Audit Log display options

The most recent records display when the Audit Log opens. The View from/To calendar controls are used to determine the date and time range to view. The calendar includes the following options:

- The pull-down menu View is used to select the range of log entries to display; All, One Day, One Week, One Month, or Custom.
- Back and Next arrows display around the month and year at the top of the calendar to change the month and the year.
- The current date displays in the lower left corner of the calendar; selection sets the calendar to the current date.
- The Clean option is used to clear the current date/time calendar selection.
- The Today option is used to set the calendar date to the current date.

- The entry fields to the right of the calendar are used to set the time range in hours and minutes.

View Audit Log records

Steps

1) From the pull-down menu **View**, select the range of log entries to display; **All**, **One Day**, **One Week**, **One Month**, or **Custom**.
   Selection of Custom enables the View from and To fields to specify the desired custom date and time range.

2) Use the icons **<** and **>** to specify the time range.

3) (*If Custom was selected*) Enter the desired date and time range in the fields, or use the calendar functionality.

4) Select the icon **>**.
   The Audit Log records for the selected time range display.

Configure display settings and navigate log entries

Steps

1) From the pull-down menu **Per page**, select the number of entries to display; **25**, **50**, **100**, or **200**.
   The default is 25.

2) Scroll through Audit Log pages, select the arrows to go back and next, or to the first and last pages of Audit Log entries.

3) Jump to a specific page; in the field **Page**, enter the page number and select **Go**.

Audit Log export options

Audit records are saved for 30 days. The Export option is used to preserve audit records longer than 30 days by exporting the log on a regular basis. Exporting does not remove records from the Audit Log; it transfers log data to a CSV or HTML file.

Export Audit Log records

Steps

1) From the pull-down menu **Export range**, select a time period; **Current page**, Last **24 hours**, **Last 7 days**, or **Last 30 days**.
   Selection of Last 30 days exports the entire Audit Log file. The Export Log dialog box displays.

2) From the pull-down menu **File type**, select the desired output file type; **CSV** or **HTML**.
   - Selection of CSV enables data to be opened or saved as a text file in comma-separated value format.
   - Selection of HTML enables data to be opened or saved as an HTML file.

3) Click **OK**.
   The Export Log window closes and the selected data is exported.

Personal Email Manager Audit Log

The Personal Email Manager Audit Log records end-user email management activities performed from either the Personal Email Manager notification message or the Quarantined Messages List. Access the Personal Email Manager Audit Log from the Personal Email Manager tab on the page **Main** > **Status** > **Logs**.

Personal Email Manager Audit Log data

The following table details the data that is collected and displayed in the Personal Email Manager Audit Log in table format:

Message Data Item	Description
Date	The date and time an action was performed on a message in Personal Email Manager.
User Name	The email address of the Personal Email Manager user who performed the message action.
End-user Action	The action performed on the message in Personal Email Manager (Deliver, Delete, or Clear All Messages; does not include the actions Add to Always Block list, Add to Always Permit list, Forward, or Download). If the action Clear All Messages was performed, all logs are deleted from Personal Email Manager and a separate log for each deletion is recorded in the Personal Email Manager Audit Log.
Message ID	A database-generated message identifier. The Message ID for a message with multiple recipients may appear multiple times in the log.
End-user Action Status	An indicator of whether the Personal Email Manager end-user action was completed successfully (Success or Failure).

Personal Email Manager Audit Log search options

The Personal Email Manager Audit Log can be searched using options such as date range or keyword. The View from/To calendar controls are used to determine the date and time range for a search. The default value for the from and to fields is the date and time at which the log is opened. The calendar includes the following options:

- The pull-down menu View is used to select the range of log entries to display; All, One Day, One Week, One Month, or Custom.
- Back and Next arrows display around the month and year at the top of the calendar to change the month and the year.
- The current date displays in the lower left corner of the calendar; selection sets the calendar to the current date.
- The Clean option is used to clear the current date/time calendar selection.
- The Today option is used to set the calendar date to the current date.
- The entry fields to the right of the calendar are used to set the time range in hours and minutes.

Search the Personal Email Manager Audit Log

Steps

1) From the pull-down menu **View**, select the range of log entries to display; **All**, **One Day**, **One Week**, **One Month**, or **Custom**.
   Selection of Custom enables the View from and To fields to specify the desired custom date and time range.

2) Use the icons **<** and **>** to specify the time range.

3) (*If Custom was selected*) Enter the desired date and time range in the fields, or use the calendar functionality.

4) From the pull-down menu **Keyword search**, select a Personal Email Manager Audit Log element in which to search; **Message ID** or **User Name**.

5) In the text field, enter a search term.
   Alphanumeric characters are supported in the keyword search entry field.

6) From the pull-down menu **Appliance**, select the appliance on which to perform the search.
   The default is the active appliance.

7) Click **Search**.
   The search results display.

8) (*Optional*) Restore all search settings to the default, click **Set to Default**.
   Search settings are reset.

Configure display settings and navigate log entries

Steps

1) From the pull-down menu **Per page**, select the number of entries to display; **25**, **50**, **100**, or **200**.

2) Scroll through Personal Email Manager Audit Log pages; select the arrows to go back and next, or to the first and last pages of Personal Email Manager Audit Log entries.

3) Jump to a specific page; in the field Page, enter the page number and select **Go**.

Personal Email Manager Audit Log export options

The Export option is used to preserve Personal Email Manager records by exporting log data. Exporting does not remove records from the Personal Email Manager Audit Log; it copies log data to a CSV or HTML file. It is recommended to export data on a regular basis.

Export Personal Email Manager Audit Log records

Steps

1) From the pull-down menu **Export range**, select a time period; **Current page**, **Last 24 hours**, **Last 7 days**, or **Last 30 days**.

   Selection of Last 30 days exports the entire Personal Email Manager Audit Log file.

   The Export Log dialog box displays.

2) From the pull-down menu **File type**, select the desired output file type; **CSV** or **HTML**.
   - Selection of CSV enables data to be opened or saved as a text file in comma-separated value format.
   - Selection of HTML enables data to be opened or saved as an HTML file.

3) Click **OK**.

   The Export Log window closes and the selected data is exported.

System Log

System Log records reflect the current state of the email system, along with any errors or warnings produced. Access the System Log from the System tab on the page **Main** > **Status** > **Logs**.

System Log data

The following table details the system information collected and displayed in the System Log in table format.

Column	Description
Date	Date and time of the system event, adjusted for time zones. To ensure consistent data in the System Log, ensure that all machines running Forcepoint components have their date and time settings synchronized.
Server	IP address of the machine affected by the system event.
Type	The type of system event (update, config exception, email hybrid service, cluster, log, quarantine, scan engine, data loss prevention, patch and hotfix, watchdog, system maintenance, or alert).
Message	A link that opens a Details message box with information about the system event.

System Log display options

The most recent records display when the System Log opens. The View from/To calendar controls are used to determine the date and time range to view. The calendar includes the following options:

- The pull-down menu View is used to select the range of log entries to display; All, One Day, One Week, One Month, or Custom.
- Back and Next arrows display around the month and year at the top of the calendar to change the month and the year.
- The current date displays in the lower left corner of the calendar; selection sets the calendar to the current date.
- The Clean option is used to clear the current date/time calendar selection.
- The Today option is used to set the calendar date to the current date.
- The entry fields to the right of the calendar are used to set the time range in hours and minutes.

View System Log records

Steps

1) From the pull-down menu **View**, select the range of log entries to display; **All**, **One Day**, **One Week**, **One Month**, or **Custom**.
   Selection of Custom enables the View from and To fields to specify the desired custom date and time range.

2) Use the icons **<** and **>** to specify the time range.

3) (*If Custom was selected*) Enter the desired date and time range in the fields, or use the calendar functionality.

4) From the pull-down menu **View by type**, select the type of system events to display.

5) Select the icon **>**.
   The System Log records for the selected time range display.

Configure display settings and navigate log entries

Steps

1) From the pull-down menu **Per page**, select the number of entries to display; **25**, **50**, **100**, or **200**.
   The default is 25.

2) Scroll through System Log pages, select the arrows to go back and next, or to the first and last pages of Audit Log entries.

3) Jump to a specific page; in the field **Page**, enter the page number and select **Go**.

System Log export options

System event records are saved for 30 days. The Export option is used to preserve system records longer than 30 days by exporting the log on a regular basis. Exporting does not remove records from the System Log; it transfers log data to a CSV or HTML file.

Export System Log records

Steps

1) From the pull-down menu **Export range**, select a time period; **Current page**, **Last 24 hours**, **Last 7 days**, or **Last 30 days**.
   Selection of Last 30 days exports the entire System Log file. The Export Log dialog box displays.

2) From the pull-down menu **File type**, select the desired output file type; **CSV** or **HTML**.
   - Selection of CSV enables data to be opened or saved as a text file in comma-separated value format.
   - Selection of HTML enables data to be opened or saved as an HTML file.

3) Click **OK**.
   The Export Log window closes and the selected data is exported.

Console Log

The Console Log is a record of any administrator activities or changes made to the Email Security module of the Forcepoint Security Manager. Access the Console Log from the Console tab on the page **Main** > **Status** > **Logs**.

Console Log data

The following table details the data that is collected and displayed in the Console Log in table format:

Column	Description
Date	Date and time of the change, adjusted for time zones. To ensure consistent data in the Console Log, ensure that all machines running Forcepoint components have their date and time settings synchronized.
User	Username of the administrator who made the change.
Client	IP address of administrator machine that made the change.
Role	Administrator role that made the change; in this case, Super Administrator.
Action	Type of change made (for example, entries indicating administrator login or logoff, an administrator role change, or the addition of a new user).
Action Detail	A link that opens a Details message box with information about the change made.

Console Log display options

The most recent records display when the Console Log opens. The View from/To calendar controls are used to determine the date and time range to view. The calendar includes the following options:

- The pull-down menu View is used to select the range of log entries to display; All, One Day, One Week, One Month, or Custom.
- Back and Next arrows display around the month and year at the top of the calendar to change the month and the year.
- The current date displays in the lower left corner of the calendar; selection sets the calendar to the current date.
- The Clean option is used to clear the current date/time calendar selection.
- The Today option is used to set the calendar date to the current date.
- The entry fields to the right of the calendar are used to set the time range in hours and minutes.

View Console Log records

Steps

1) From the pull-down menu **View**, select the range of log entries to display; **All**, **One Day**, **One Week**, **One Month**, or **Custom**.

   Selection of Custom enables the View from and To fields to specify the desired custom date and time range.

2) Use the icons **<** and **>** to specify the time range.

3) (*If Custom was selected*) Enter the desired date and time range in the fields, or use the calendar functionality.

4) Select the icon **>**.
   The Console Log records for the selected time range display.

Configure display settings and navigate log entries

Steps

1) From the pull-down menu **Per page**, select the number of entries to display; **25**, **50**, **100**, or **200**.
   The default is 25.

2) Scroll through Console Log pages, select the arrows to go back and next, or to the first and last pages of Console Log entries.

3) Jump to a specific page; in the field **Page**, enter the page number and select **Go**.

Console Log export options

The length of time connection records are saved in the database depends on the connection volume and database partition capacity. The Export option is used to preserve connection records by exporting log data. Exporting does not remove records from the Console Log; it copies log data to a CSV or HTML file. It is recommended to export data on a regular basis.

Export Console Log records

Steps

1) From the pull-down menu **Export range**, select a time period; **Current page**, **Last 24 hours**, **Last 7 days**, or **Last 30 days**.
   Selection of Last 30 days exports the entire Console Log file. The Export Log dialog box displays.

2) From the pull-down menu **File type**, select the desired output file type; **CSV** or **HTML**.
   - Selection of CSV enables data to be opened or saved as a text file in comma-separated value format.
   - Selection of HTML enables data to be opened or saved as an HTML file.

3) Click **OK**.
   The Export Log window closes and the selected data is exported.

Email Hybrid Service Log

The Email Hybrid Service Log contains records of email messages that are blocked by the email hybrid service before they reach the network. Functionality requires a valid subscription key for the Forcepoint Email Security Hybrid Module and successful registration with the module for the Email Hybrid Service Log to be available (see *Registering the Email Security Hybrid Module*).

Following successful registration with the email hybrid service, you can enable the Email Hybrid Service Log and set data delivery options on the page **Settings** > **Hybrid Service** > **Hybrid Service Log Options**. See *Configuring the Email Hybrid Service Log*. Access the Email Hybrid Service Log from the Email Hybrid Service tab of the page **Main** > **Status** > **Logs**.

Related concepts
Registering the Email Security Hybrid Module on page 63

Related tasks
Configuring the Email Hybrid Service Log on page 68

Email Hybrid Service Log data

The following table details the message data collected and displayed in the Email Hybrid Service Log in table format:

Message Data Item	Description
Hybrid Service Log ID	A database-generated message identifier.
Date/Time	The date and time a message was received.
Subject	The message subject.
Sender Address	Message sender email address.
Recipient Address	Message recipient email address. If the message has multiple recipients, the first recipient address is displayed.
Sender IP	Message sender IP address.
Message Status	Current message status (e.g., discarded or bounced).
Reason	Supplied by the email hybrid service, the analysis result that determines message disposition.

Email Hybrid Service Log search options

The Email Hybrid Service Log Search Options section includes search options such as date range or keyword. The View from/To calendar controls are used to determine the date and time range for a search. The default value for the from and to fields is the date and time at which the log is opened. The calendar includes the following options:

- Back and Next arrows display around the month and year at the top of the calendar to change the month and the year.

- The current date displays in the lower left corner of the calendar; selection sets the calendar to the current date.
- The Clean option is used to clear the current date/time calendar selection.
- The Today option is used to set the calendar date to the current date.
- The entry fields to the right of the calendar are used to set the time range in hours and minutes.

Search the Email Hybrid Service Log

Steps

1) From the section Email Hybrid Service Log Search Options, set the date and time to be searched in the fields View from and To.

   (*Optional*) Use the calendar functionality to specify a date to search.

2) From the pull-down menu **Keyword search**, select a Email Hybrid Service Log element in which to search; **Email Hybrid Service Log ID**, **Subject**, **Sender Address**, **Recipient Address**, **Sender IP**, or **Message Status**.

3) In the field, enter a search term.

   Alphanumeric characters are supported in the keyword search entry field.

4) Click **Search**.

   The search results display.

5) (*Optional*) Restore all search settings to the default, click **Set to Default**. Search settings are reset.

Configure display settings and navigate log entries

Steps

1) From the pull-down menu **Per page**, select the number of entries to display; **25**, **50**, **100**, or **200**.

2) Scroll through Email Hybrid Service Log pages, select the arrows to go back and next, or to the first and last pages of Email Hybrid Service Log entries.

3) Jump to a specific page; in the field **Page**, enter the page number and select **Go**.

Email Hybrid Service Log export options

The length of time Email Hybrid Service Log records are saved in the database depends on the message volume and database partition capacity. The Export option is used to preserve message records by exporting log data. Exporting does not remove records from the Email Hybrid Service Log; it copies log data to a CSV or HTML file. It is recommended to export data on a regular basis.

Export Email Hybrid Service Log data

Steps

1) From the Email Hybrid Service Log, click **Export**. The Export Log dialog box displays.

2) From the pull-down menu **File type**, select the desired output file type; **CSV** or **HTML**.
   - Selection of CSV enables data to be opened or saved as a text file in comma-separated value format.
   - Selection of HTML enables data to be opened or saved as an HTML file.

3) From **Page range**, indicate the pages to export; **All**, **Current Page**, or **Pages**.

4) Click **OK**.
   The Export Log window closes and the selected data is exported.

Real-time monitor

Real-time log information for email traffic is available on the page **Main** > **Status** > **Real-Time Monitor** for selected appliances. This information can be valuable for troubleshooting purposes. The following table details the Real-Time Monitor parameters.

Option	Description
	Selection temporarily halts the real-time log stream.
	Selection opens a running log of email traffic data for selected appliances.
Display log entries for	Check box functionality to select any or all of the available types of log information for display: ■ Message status This is the default selection. ■ Connection status ■ Message delivery status ■ Message analysis result
Search filter	User-defined text field to enter a keyword search term on which to search individual entries.
Advanced search	Selection enables advanced search filter options. Functionality enables searching of log entries and display records by message subject, IP address (source, destination, or both), or email address (sender, recipient, or both).
Appliance	Selection enables monitoring of appliances. The current appliance is monitored by default.

Option	Description
Real-Time logs	Displays the selected log entries or search results.

Display log entries

Steps

1) Pause the Real-Time Monitor, click the icon **Pause**.
   The Real-Time Monitor pauses and the display options enable for selection.

2) From **Display log entries for**, click the check boxes for one or multiple types of log entries to display; **Message status**, **Connection status**, **Message delivery status**, or **Message analysis result**.

3) Start the Real-Time Monitor, click the icon **Start**.
   The selected log entries display in the section Real-Time logs.

Search log entries

Steps

1) Pause the Real-Time Monitor, click the icon **Pause**.
   The Real-Time Monitor pauses and the display options enable for selection.

2) In the field **Search filter**, enter keywords on which to search.

3) (*Optional*) Click **Advanced search**.
   The advanced search filter options display.
   Configure advanced options to search on message subject, IP address (source, destination, or both), or email address (sender, recipient, or both).

4) Start the Real-Time Monitor, click the icon **Start**.
   The selected log entries display in the section Real-Time logs.

Monitor multiple appliances in cluster mode

Steps

1) Pause the Real-Time Monitor, click the icon **Pause**.
   The Real-Time Monitor pauses and the display options enable for selection.

2) From Appliance, click **Select**.
   The Select Appliance list displays.

3) Mark the appropriate check boxes for appliances. Ensure that the primary cluster appliance is selected.

4) Start the Real-Time Monitor, click the icon **Start**.
The selected log entries display in the section Real-Time logs.

Security Information and Event Management (SIEM) integration

Third-party security information and event management (SIEM) tools allow the logging and analysis of internal alerts generated by network devices and software. Integration with SIEM technology allows the transfer of message activity events to a SIEM server for analysis and reporting.

Third-party SIEM providers may not support FIPS 140-2 Level 1 certified cryptography. Contact your SIEM provider for more information about FIPS-certified cryptography.

Access SIEM integration settings on the page **Settings** > **General** > **SIEM Integration**.

Enable and configure SIEM integration

Steps

1) On the page SIEM Integration, mark the check box **Enable SIEM integration for all email appliances**.
SIEM configuration settings are enabled for editing.

2) In the entry field **IP address or hostname**, enter the IP address or hostname for the SIEM integration server.

3) In the entry field **Port**, enter the port number for the SIEM integration server. The default is 514.

4) From the section **Transport protocol**, select the protocol used for data transport; **UDP** or **TCP**.
User datagram protocol (UDP) is a transport layer protocol in the Internet protocol suite. UDP is stateless and therefore faster than transmission control protocol (TCP), but can be unreliable. Like UDP, TCP is a transport layer protocol, but provides reliable, ordered data delivery at the expense of transport speed.

Tip

When using TCP, it is recommended to end all logs with %<\n>.

5) From the pull-down menu **SIEM format**, select the format to be used in SIEM logs.
   The format determines the syntax of the string used to pass log data to the integration.
   - The available formats are syslog/CEF (ArcSight), syslog/key-value pairs (Splunk and others), syslog/LEEF (QRadar), and Custom.
   - The text boxes populate with CEF format when Custom is selected, and can be edited as needed. The maximum size for each format is 2048 characters. Logs are not saved to the SIEM server for any log fields left blank. Selection of a new template returns any edited custom format to the default.
   - Sample formats display for non-custom options.

6) Confirm that the SIEM product is properly configured and can receive messages from the email software; click **Send Test Message**.
   Check the SIEM Server log entries to verify that the test message is delivered.

7) From the bottom of the page SIEM Integration, click **OK**.
   The SIEM configuration settings are saved. See SIEM: Email Logs.

Email hybrid service configuration

Forcepoint Email Security combined with the Forcepoint Email Security Hybrid Module offers a flexible, comprehensive email security solution can combine on-premises and hybrid (in-the-cloud) analysis as needed to manage inbound and outbound email for your organization.

The email hybrid service provides an extra layer of email analysis, stopping spam, virus, phishing, and other malware attacks before they reach the network and considerably reducing email bandwidth and storage requirements. You can also use the email hybrid service to encrypt outbound email before delivery to its recipient (your subscription must also include the Forcepoint Email Security - Encryption Module for this feature).

You can create policies for on-premises and hybrid analysis in the same user interface—the Email Security module—and configuration, reporting, and management are centralized.

Before you can use the email hybrid service to examine email for your organization, you must enter a valid subscription key that includes the Forcepoint Email Security Hybrid Module and configure a number of settings in the Email Security module and in your Domain Name System (DNS). This creates a connection between the on-premises and cloud portions of your email protection system. See *Registering the Email Security Hybrid Module*.

The Email Hybrid Service Log contains records of the email messages that are blocked by the email hybrid service before they reach the network. See *Email Hybrid Service Log* for information about the contents of this log. See *Configuring the Email Hybrid Service Log* for details about enabling and scheduling Email Hybrid Service Log updates.

The flow of email through the hybrid service can vary, depending on the filters or rules you have configured. The following provides some general steps regarding the flow of inbound email:

1) An email message is received by Forcepoint Email Security Cloud and initially scanned for DKIM verification, spam, viruses, and malicious URLs.

2) An email message that triggers any of these options may be blocked, or may be sent to on-premises Forcepoint Email Security with related information (such as spam score, DKIM results, virus information, and URLs).

3) On-premises Forcepoint Email Security scans the message based on the rules and filters configured in your system settings. Information provided by Forcepoint Email Security Cloud is used when enforcing spam, virus, or anti-spoofing rules.

4) If not blocked by a filter or rule and Advanced File Analysis is enabled, the email message is sent to Advanced Malware Detection - Cloud for analysis.

For more information about mail flow through different types of Forcepoint Email Security deployments, see the Deployment & Installation Center.

Related concepts

Registering the Email Security Hybrid Module on page 63
Email Hybrid Service Log on page 57

Related tasks

Configuring the Email Hybrid Service Log on page 68

Registering the Email Security Hybrid Module

The Forcepoint Email Security Hybrid Module account is activated on the page **Settings** > **Hybrid Service** > **Hybrid Configuration**. Selection of **Register** initiates a registration wizard. Registration proceeds on the following pages of the wizard:

1) Enter customer information

2) Define delivery routes

3) Configure your DNS

4) Set up your firewall

5) Configure your MX records

6) Modifying email hybrid service configuration

Important

Multiple appliances controlled by a single email management server share the same email hybrid service configuration settings, regardless of appliance mode (cluster or standalone).

If you need to register more than one appliance with the email hybrid service from the same email management server, you should:

- Add all your appliances to the module (**Settings** > **General** > **Email Appliances**)
- Create an appliance cluster, if desired (**Settings** > **General** > **Cluster Mode**)
- Enter your subscription key (**Settings** > **General** > **Subscription**)
- Register the (**Settings** > **Hybrid Service** > **Hybrid Configuration**)

If your appliances are operating in standalone mode, register from the appliance on which you entered the subscription key.

You may need to add an appliance after you have registered with the email hybrid service (for example, after a new appliance purchase). In this situation, you should add the new appliance to the module, then register your existing appliance with the email hybrid service again without changing any configuration settings. Hybrid service configuration is synchronized across all appliances after you re-register.

Related concepts

Enter customer information on page 64
Define delivery routes on page 64
Configure your DNS on page 66
Set up your firewall on page 67
Configure your MX records on page 67
Modifying email hybrid service configuration on page 67

Enter customer information

Use the Basic Information page under **Settings** > **Hybrid Service** > **Hybrid Configuration** to provide the contact email address, phone number, and country for your Forcepoint filtering administrators.

The email address is typically an alias monitored by the group responsible for managing your email protection software. This very important email sent to your account should be acted upon promptly when it is received.

- Technical Support uses this address to send notifications about urgent issues affecting hybrid filtering.
- If there is a configuration problem with your account, failure to respond to an email message from Technical Support in a timely fashion could lead to service interruptions.
- Should certain rare problems occur, the email address is used to send information that allows Sync Service to resume contact with the hybrid service.
- This email address is **not** used to send marketing, sales, or other, general information.

The country you enter provides the system with time zone information.

Click **Next** to continue with hybrid configuration on the page *Define delivery routes*.

Related concepts

Define delivery routes on page 64

Define delivery routes

Use the Delivery Route page under **Settings** > **Hybrid Service** > **Hybrid Configuration** to define the domains for which email traffic will be routed to and from the email hybrid service, and the SMTP server addresses that receive mail from and send mail to the hybrid service. Each group of one or more domains and one or more SMTP server addresses comprises a delivery route.

Important

Email hybrid service checks the connection to your SMTP server by sending commands to a “postmaster” address. If your SMTP server does not have a postmaster or administrator address (for example, postmaster@mydomain.com) you should add it manually before completing this step.

Add a delivery route

Steps

1) On the page Delivery Route, click **Add**.

2) Enter a **Delivery route name**.

3) Add domains to your delivery route; under Protected Domains, click **Add**.

4) Enter the **Domain Address** (for example, mydomain.com).

5) Define whether the delivery route should apply to all subdomains in the domain.

6) To add another domain, repeat steps 3–5.

Note

Protected domains added here must already be entered in the Protected Domain group on the page **Settings** > **Users** > **Domain Groups**. See *Managing domain and IP address groups*.

7) Add inbound SMTP servers to your delivery route; under SMTP Inbound Server Addresses, click **Add**.

8) Enter the IP address or name of your email management server.
This must be the external IP address or name, visible from outside your network.

9) (*If needed*) Add more servers; click **Add**.
Each new server is given the next available ID number and added to the end of the list. The lowest ID number has the highest preference. Mail will always be received by the server with the highest preference; if that server fails, the server with the next highest preference for that delivery route is used.

10) (*Optional*) Change the preference order; check the box next to a server name, then click **Move up** or **Move down**.

11) Add outbound SMTP servers to your delivery route; under SMTP Outbound Server Addresses, click **Add**.
The email system uses these IP addresses to send email to the hybrid service for encryption. See *Forcepoint email encryption* for information about this encryption function.

12) Enter the IP address or name of your email management server.
This must be the external IP address or name, visible from outside your network.

13) (*If needed*) Add more servers; click **Add**.
Each new server is added to the end of the list. If an outbound server connection fails, email in this delivery route that needs to be encrypted is sent to a delayed messages queue for a later delivery attempt.

14) Click **OK**.

The delivery route appears in the Route List on the Delivery Route page.

Click **Next** to continue with hybrid configuration on the page *Configure your DNS*.

Related concepts

Managing domain and IP address groups on page 99
Forcepoint email encryption on page 164
Configure your DNS on page 66

Configure your DNS

Use the information on the CNAME Records page under **Settings** > **Hybrid Service** > **Hybrid Configuration** to configure your DNS.

Before a delivery route is accepted by the email hybrid service, it must be checked to ensure that the service can deliver mail for each protected domain to your mail server and that each domain belongs to your company.

CNAME records are used to assign an alias to an existing host name in DNS. Contact your DNS manager (usually your Internet service provider) and ask them to set up a CNAME record for each of your protected domains, using the alias and associated domain information on the DNS page.

A CNAME record has the following format:

```
abcdefgh.mydomain.com CNAME autodomain.mailcontrol.com.
```

Where:

- `abcdefgh` is the **Alias** displayed on the DNS page
- `mydomain.com` is the **Protected Domain**
- `CNAME` indicates that you are specifying a CNAME record
- `autodomain.mailcontrol.com` is the **Associated domain** displayed with the above alias and protected domain

Ensure that the trailing period is included in the associated domain name.

The above example indicates that the alias **abcdefgh.mydomain.com** is assigned to **autodomain.mailcontrol.com**. This enables the email hybrid service to confirm that you own **mydomain.com**.

After you have created your CNAME records, click **Check Status** to verify that your entries are correctly set in your DNS. Resolve any error situations if necessary. If the **Check Status** button does not appear on the page, click **Next** to continue.

Note

The validation performed by clicking **Check Status** occurs in your local system. Because the propagation of DNS changes across all Internet servers can take between a few minutes to several hours, the verification process for the email hybrid service may take longer.

Click **Next** to continue with hybrid configuration on the page *Set up your firewall*.

Related concepts

Set up your firewall on page 67

Set up your firewall

Use the information on the Network Access page under **Settings** > **Hybrid Service** > **Hybrid Configuration** to configure your firewall.

Because the email hybrid service is a managed service, Forcepoint is responsible for managing system capacity. For this reason, the route of your email may occasionally alter within the service. To enable this to happen seamlessly without requiring you to make further changes, you must allow SMTP access requests from all the IP ranges listed on the Network Access page to port 25.

Click **Next** to continue with hybrid configuration on the page *Configure your MX records*.

Related concepts

Configure your MX records on page 67

Configure your MX records

Use the information on the MX Records page under **Settings** > **Hybrid Service** > **Hybrid Configuration** to configure your Mail eXchange (MX) records.

An MX record is an entry in a DNS database that defines the host willing to accept mail for a given machine. Your MX records must route inbound email through the email hybrid service to your email protection system.

Your MX records, which end in **in.mailcontrol.com**, are listed on the MX Records page. Contact your DNS manager (usually your Internet service provider) and ask them to set up or replace your current MX records for each protected domain you have specified with the customer-specific records provided by the email hybrid service on the MX Records page. For example, they might change:

Change	From	To
MX Preference 1	mydomain.com. IN MX 50 mail.mydomain.com.	mydomain.com. IN MX 5 **cust0000-1.in.mailcontrol.com**.
MX Preference 2	mydomain.com. IN MX 51 mail.mydomain.com.	mydomain.com. IN MX 5 **cust0000-2.in.mailcontrol.com**.

Ensure that they include the trailing period, and ask them to set each of these records to an equal preference value.

Check the entries on your Internet service provider's DNS management site to ensure they match the MX records provided by the email hybrid service. After you validate your entries, click **Check Status** to verify that the update is successful.

It can take up to 24 hours to propagate changes to your MX records across the Internet. During this time, you should keep your previous mail routing active to ensure all your mail is delivered: while your MX records are changing over, some mail will be delivered using your old MX information, and some mail will be delivered using your new MX information.

Click **Finish** to complete your hybrid configuration.

Modifying email hybrid service configuration

After you complete the registration wizard, you can review and modify your email hybrid service configuration settings on the page **Settings** > **Hybrid Service** > **Hybrid Configuration**.

Note

The **Check Status** button may not appear in the CNAME records area if the hybrid service has already verified domain ownership.

Verify that email is properly routed through the hybrid service by sending email through your mail system from outside your protected domains.

Configuring the Email Hybrid Service Log

Email Hybrid Service Log options are set on the page **Settings** > **Hybrid Service** > **Hybrid Service Log Options**. Functionality is used to enable the Email Hybrid Service Log and determine the data transfer schedule for the log.

These options are available only if you have entered a subscription key that includes the Forcepoint Email Security Hybrid Module, and you have successfully registered the module. See *Registering the Email Security Hybrid Module*.

Configure Email Hybrid Service Log options

Steps

1) Enable the Email Hybrid Service Log; mark the check box **Enable the Email Hybrid Service Log**.

2) From the pull-down menu **Retrieve Email Hybrid Service Log data every**, specify the time interval for retrieving the most recent Email Hybrid Service Log information, from 15 minutes to 24 hours.
   The default is 15 minutes.

3) From the pull-down menu **Send the Email Hybrid Service Log data to the database every**, specify the time interval for sending Email Hybrid Service Log information to the log database, from 15 minutes to 24 hours.
   The default is 15 minutes.

4) Click **OK**.
   The settings are saved.

Related concepts
Registering the Email Security Hybrid Module on page 63

Registering the DLP Module

With the DLP module, your email can be analyzed for regulatory compliance and acceptable use and protect sensitive data loss via email by enabling DLP policies on the page **Main** > **Policy Management** > **Policies**. Data loss prevention policies are enabled by default.

See *Enabling data loss prevention policies* for more information about activating DLP policies.

Email DLP policy options are configured in the Security Manager Data Security module (**Main** > **Policy Management** > **DLP Policies** > **Manage Policies**). A new policy wizard provides the steps for creating a new email DLP policy. See Forcepoint DLP Administrator Help.

If you plan to use email encryption functions, you must configure an email DLP policy with an action plan that includes message encryption. See Forcepoint DLP Administrator Help.

You can also create filter actions for use in a DLP policy action plan. See *Creating and configuring a filter action* for information.

You must register email appliances with the Forcepoint Email Security DLP Module in order to take advantage of its acceptable use, data loss prevention, and message encryption features. Registration is automatic when you enter a valid subscription key. Subsequent appliances are registered when you add them to the Security Manager from the Email Security module.

If the Status field in the Email Security module **Settings** > **General** > **Data Loss Prevention** page displays **Unregistered**, you must manually register with the Forcepoint Email Security DLP Module. The following steps detail how to manually register a standalone appliance manually with the email DLP Module:

Related tasks

Enabling data loss prevention policies on page 202
Creating and configuring a filter action on page 195

Manually register the DLP module

Steps

1) Navigate to the page **Settings** > **General** > **Subscription**.

2) In the field **Subscription key**, enter a valid subscription key.

3) Click **OK**.
   The subscription is updated.

4) Navigate to the page **Settings** > **General** > **Data Loss Prevention**.

5) From the pull-down menu Communication IP address, specify the IP address used for communication with the email protection system.

   Note

   The appliance C interface IP address is selected by default. This setting is recommended for Forcepoint Email Security DLP Module registration.

   If you are running Forcepoint Email Security in Azure, you must use the C interface IP address, as Forcepoint Email Security in Azure only supports a single interface.

6) Select the registration method **Manual**. The Properties entry fields are enabled.

7) Specify the following data management server properties:
   - IP address
   - User name
   - Password

8) Click **Register**.

9) To complete the process, you must deploy DLP policies in the Data Security module; click the Data Security module and then click **Deploy**.

   Important

   Wait until DLP policies are completely deployed before you register another standalone appliance.

   Consider the following when deploying Forcepoint Email Security in an appliance cluster:

   - Register all the primary and secondary machines with the email DLP Module before you deploy any data loss prevention policies. If you deploy DLP policies on the primary appliance while you are registering a secondary machine, the registration process for the secondary machine may not complete.
   - Ensure that all machines in a cluster use the same physical appliance interface (the C, E1, or E2 IP address) to register with the email DLP Module.

Email filtering database updates

Regular updates to the email analytics database offer maximum protection from email-borne attacks. Manage database updates for antispam and antivirus filters on the page **Settings** > **General** > **Database Downloads**.

The Antivirus and Antispam filters tables list the set of analytics databases included in your product subscription. If the current appliance is a primary machine, these tables also include update information for any secondary appliances associated with the primary appliance. The update schedule for each database is shown in the Schedule column.

Reschedule updates for a filter

Steps

1) In the Schedule column, click **Edit**.
   The Reschedule Update dialog box displays.

2) Configure the following settings as needed:
   - **Frequency**
     How often the update should occur, from every five minutes to once per week.
   - **Day of week**
     The day on which the update should occur. This pull-down menu is enabled when the frequency **Every week** is selected.
   - **Time**
     The time of day at which the update should occur. These settings are enabled when the frequency **Every day** or **Every week** is selected.

3) Select **OK**.
   The dialog box closes and the Schedule column updates.

Update all databases

From the table Antivirus filters or Antispam filters, select **Update Now**. All Forcepoint databases are updated.

Configuring system alerts

In addition to displaying system alerts in the dashboard Health Alert Summary, your email protection system can use other methods to notify administrators that various system events have occurred. For example, notifications can be sent for updates to database download categories and subscription issues, as well as encryption and user directory issues.

Use the page **Settings** > **Alerts** > **Enable Alerts** to enable and configure the desired notification methods. Then, use the page **Settings** > **Alerts** > **Alert Events** to enable the types of alerts for which notifications should be sent.

Pop-up alerts are no longer supported. Use *Email alerts* or *SNMP alerts*.

Related tasks
Email alerts on page 72
SNMP alerts on page 72

Enabling system alerts

Determine how alerts are distributed by using one or more of the following delivery methods:

- To a specified individual via an email message
- To a specified community via an SNMP Trap system

Use the page **Settings** > **Alerts** > **Enable Alerts** to configure alert delivery methods.

Email alerts

Email alerts are distributed to specific individuals via a notification message.

Enable email alerts

Steps

1) From the Security Manager, navigate to the page **Settings** > **Alerts** > **Alert Events**.

2) From the section Email Alerts, mark the check box **Enable email alerts**. Selection indicates to deliver alerts and notifications to administrators by email.

3) In the text fields, configure the following settings:
   - **From email address**
     Email address to use as the sender for email alerts.
   - **Administrator email address (To)**
     Email address of the primary recipient of email alerts. Each address must be separated by a semicolon.
   - **Email addresses for completed report notification** E
     mail addresses for recipients of completed report notifications. Each address must be separated by a semicolon.

4) Click **OK**.
   Email alerts are enabled.

SNMP alerts

SNMP alert messages are delivered through an SNMP Trap system installed in your network.

The SNMP protocol does not support the use of FIPS 140-2 Level 1 certified cryptography. Use *Email alerts* if FIPS-certified cryptography is required.

Enable SNMP alerts

Steps

1) From the Security Manager, navigate to the page **Settings** > **Alerts** > **Alert Events**.

2) In the section SNMP Alerts, mark the check box **Enable SNMP alerts**.

3) In the text fields, provide the following information about your SNMP Trap system:
   - **Community name**
     Name of the trap community on your SNMP Trap system.
   - **Server IP or name**
     IP address or name of the SNMP Trap system.
   - **Port**
     Port number used by SNMP messages.

4) Click **Check Status**.
   A test message is sent to your SNMP server to verify that the specified port is open.

5) Click **OK**.
SNMP alerts are enabled.

Related tasks
Email alerts on page 72

Alert events

To ensure that administrators are notified of system events, like a database download failure or a subscription that is about to expire, you can configure system alerts to be distributed by email or through your SNMP Trap system.

Use the page **Settings** > **Alerts** > **Enable Alerts** to select the method used to send these alerts to Forcepoint Email Security administrators. See *Enabling system alerts*.

Use the page **Settings** > **Alerts** > **Alert Events** to select categories of alerts to be delivered and to indicate how you want the alerts delivered (email or SNMP). Each delivery method must be enabled on the Enable Alerts page in order to select the method for an event type.

Alerts in the following event categories can be sent:

- Subscription expiration
- Email system events
- Log Server and Log Database events
- Mail queue events
- Email analysis events
- Encryption and decryption events
- Appliance cluster configuration events
- User directory server events
- Email hybrid service operation events
- Signature update events
- SIEM server events
- Personal Email Manager server events

Related concepts
Enabling system alerts on page 71

Select alerts for event types

Steps

1) From the Security Manager, navigate to the page **Settings** > **Alerts** > **Alert Events**.

2) From the Alerts list, mark the check boxes for the desired delivery method for each event type.

   Example: For the event type Subscription event notifications, mark the check box **Email**.

   When the Email Security subscription is expiring, a notification email will be sent to the administrator(s) configured on the page Enable Alerts.

3) Enable one notification for all event types; mark the check box in the column heading.

   Example: From the column Email, mark the check box in the column heading. All notifications will be sent via email.

4) Click **OK**.

   Event alerts are saved.

Alert threshold values

In some cases, you can configure threshold values to trigger the delivery of an alert. Alerts are sent at 30-minute intervals when the configured threshold is exceeded.

These values can be set for the following alert events:

- Inbound undelivered email event notifications
- Work queue growth rate notifications
- Exception queue event notifications

Configure inbound undelivered email event notifications

You can set a frequency threshold for the inbound undelivered email events alert type. This setting triggers an alert notification after a specified number of inbound connection errors occurs on the mail server. Outbound traffic is not monitored for this alert.

Steps

1) From Inbound undelivered email event notifications in the list Events, click the link **Configure alert thresholds**.

   A configuration dialog box displays.

2) In the text field, enter the number of connection errors at which to trigger an alert notification.

   The default is 1. The notification is sent at 30-minute intervals after the connections threshold is exceeded.

3) Mark the check box **Configure backup destination address to send alerts when the mail server is down**.

4) In the text field, enter up to three email addresses as backup alert email destinations.

   The email addresses must be different from the mail server address. Separate multiple entries with semicolons.

5) Click **OK**.

   The dialog box closes.

6) From the page Alert Events, click **OK**.
Event alerts are saved.

Work queue growth rate notifications

The work queue includes the following message types:

- Incoming messages waiting for analysis
- Messages waiting for delivery
- Deferred messages waiting for subsequent delivery attempts

Use the following steps to set thresholds for sending alerts when the work queue growth rate threatens to exceed the queue size limit in a specified period of time:

Steps

1) From Work queue growth rate notifications in the list Events, click the link **Configure alert thresholds**.
A configuration dialog box displays.

2) From the pull-down menu **Alert sensitivity level**, select the alert sensitivity level, based on how much warning to provide regarding the queue growth rate and the probability of reaching the work queue size limit:
   - **High**. Work queue capacity reached in less than four days (default).
   - **Medium**. Work queue capacity reached in less than two days.
   - **Low**. Work queue capacity reached in less than one day.

3) Click **OK**.
The dialog box closes.

4) From the page Alert Events, click **OK**.
Event alerts are saved.

Exception queue event notifications

The exception queue includes any message that currently cannot be delivered because it encountered an exception during message analysis. Use the following steps to set thresholds for sending alerts when exception queue capacity reaches a specified percentage:

Steps

1) From Exception queue event notifications in the list Events, click the link **Configure alert thresholds**.
A configuration dialog box displays.

2) From the pull-down menu, select the percentage of queue capacity at which to be warned about exception queue size; 50% to 90%.
The default is 90%.

3) Click **OK**.
The dialog box closes.

4) From the page Alert Events, click **OK**.
Event alerts are saved.

URL analysis

URL analysis compares a URL embedded in email with a database of categorized URLs, providing category information to allow Forcepoint Email Security to properly handle the URL. Forcepoint Email Security provides the following options for accurate and efficient spam detection:

- Threat Intelligence Cloud Service
- Filtering Service
- Linking Service

Activate URL analysis by configuring and enabling a URL analysis filter on the page **Main** > **Policy Management** > **Filters** > **Add URL Analysis Filter**. See *URL analysis*.

Related concepts
URL analysis on page 179

Threat Intelligence Cloud Service

Threat Intelligence Cloud Service URL analysis uses the cloud-hosted Forcepoint URL

Database, which is the most current repository of classified URLs. This cloud database is used by many Forcepoint solutions to identify potentially dangerous or simply unwanted URLs. This URL analysis service does not require a Forcepoint web protection solution to be installed.

Enable Threat Intelligence Cloud Service

Steps

1) In the Security Manager, navigate to the page **Settings** > **General** > **URL Analysis**.

2) From the pull-down menu URL analysis service, select **Threat Intelligence Cloud Service**.

3) Verify the connection to the URL analysis service; click **Test Connection**.

4) Click the **refresh icon**.
The URL categories list is immediately updated.

5) Click **OK**.
The settings are saved.

Filtering Service

The Filtering Service requires the installation of a Forcepoint web protection solution.

The Web management server maintains an updated URL database from the product download server. The email protection system queries the URL category database and determines the risk level of a URL found in an email message.

The Web Security module version must be supported by the Email Security module for this function to be available.

Use the Filtering Service with a Forcepoint on-premises web security solution to access the local copy of the Forcepoint URL Database maintained by your web security product (Forcepoint Web Security or Forcepoint URL Filtering).

Filtering Service does not support the use of FIPS 140-2 Level 1 certified cryptography. Use *Threat Intelligence Cloud Service* or *Linking Service*if FIPS-certified cryptography is required.

Enable Filtering Service

Steps

1) In the Security Manager, navigate to the page **Settings** > **General** > **URL Analysis**.
2) From the pull-down menu URL analysis service, select **Filtering Service**.
3) In the field IP address or hostname, enter the location of the database.
4) Verify the connection to the URL analysis service; click **Test Connection**.
5) Click **OK**.
   The settings are saved.

Related tasks
Threat Intelligence Cloud Service on page 76
Linking Service on page 77

Linking Service

The Linking Service requires the installation of a Forcepoint web protection solution.

The Web management server maintains an updated URL database from the product download server. The email protection system queries the URL category database and determines the risk level of a URL found in an email message.

The Web Security module version must be supported by the Email Security module for this function to be available.

Use the Linking Service with a Forcepoint Web Security on-premises solution to access both the local copy of the URL Database as well as any custom categories you have created. This service also provides dynamic category mapping updates from the URL database. Because Linking Service is an optional web protection component, you must activate it in Forcepoint Web Security to use this option.

Enable Linking Service

Steps

1) In the Security Manager, navigate to the page **Settings** > **General** > **URL Analysis**.

2) From the pull-down menu URL analysis service, select **Linking Service**.

3) In the field IP address or hostname, enter the location of the database.

4) In the field Port, enter the port number for the Linking Service.

5) Verify the connection to the URL analysis service; click **Test Connection**.

6) Click the **refresh icon**.
   The URL categories list is immediately updated.

7) Click **OK**.
   The settings are saved.

Selecting advanced file analysis platform

Advanced file analysis is a cloud-hosted or on-premises sandbox for the inspection of email file attachments. The cloud function is available only if your subscription includes Forcepoint Advanced Malware Detection for Email - Cloud. The on-premises sandbox is available only if you have purchased a separate Forcepoint Advanced Malware Detection for Email - On-Premises system.

A cloud-hosted Advanced Malware Detection - Cloud sandbox examines the file types specified on the page **Main** > **Policy Management** > **Filters** > **Advanced File Analysis**. The on-premises Advanced Malware Detection - On-Premises file analysis system inspects a larger set of file types than the cloud sandbox, though not all file types may be supported.

See *Advanced file analysis* for details about configuring an advanced file analysis filter.

Configure the advanced file analysis platform

Steps

1) On the page **Settings** > **General** > **Advanced File Analysis**, from the pull-down menu **File analysis platform**, select a platform: **Advanced Malware Detection - Cloud** or **Advanced Malware Detection - On-Premises**).

2) If you selected Advanced Malware Detection - On-Premises: in the field Controller IP address, enter the Controller appliance IP address.

3) Verify the connection to the Controller appliance; click the button **Check Status**.

4) Click **OK**.
   The platform settings are saved.

Related concepts
Advanced file analysis on page 187

Using a proxy server

You can configure a proxy server for the following functions:

- Email filtering database updates
- Email traffic between the email hybrid service and the Internet
- Advanced file analysis
- Communication with Threat Intelligence Cloud Service URL analysis

The same proxy server can be used for all functions. Proxy server settings are configured on the page **Settings** > **General** > **Proxy Server**.

Note

The email software does not support the use of a Secure Sockets Layer (SSL) proxy for filtering database updates. An SSL server may be used as an email hybrid service proxy.

Configure a proxy server

Steps

1) On the page **Proxy Server**, mark the appropriate check box(es):
   - **Enable database update proxy server**
     The proxy is used for database updates.
   - **Enable email hybrid service proxy server**
     The proxy is used for email hybrid service communication.
   - **Enable advanced file analysis proxy server**
     The proxy is used for advanced file analysis purposes.
   - **Enable Threat Intelligence Cloud Service URL analysis proxy server**
     The proxy server is used for communication with the URL analysis service.
2) In the field Server IP address or hostname, enter the IP address or hostname of the proxy server.
3) In the text field Port, enter the port number of the proxy server.
4) In the text field Username, enter the username for the proxy server.
5) In the text field Password, enter the password for the proxy server.
6) Click **OK**.
   The settings are saved.

Using the Common Tasks pane

The right shortcut Common Tasks pane provides shortcuts to frequently performed administrative tasks like running a report, creating a policy, or searching a log.

To Use the Common Tasks pane: Click an item in the list. The page displays on which the task is performed.

Chapter 3

Configuring System Settings

Contents

Managing administrator accounts

Forcepoint Email Security module administrator accounts are created on the Global Settings page of the Forcepoint Security Manager. Only a Super Administrator can add, edit, or delete an administrator account.

A Super Administrator can create two types of accounts: local and network. A local account is stored in the local Security Manager database and contains a single user. A network account can contain a single user or a group of users and is stored on a network server. See Forcepoint Security Manager Help for details about managing Security Manager administrators on this page.

Administrator account settings and role assignments that are configured on one appliance are applied to all the appliances in your network.

Access administrator accounts

Steps

1) From the Security Manager, click **Global Settings**. The Global Settings page displays.

2) From the **General** menu, select **Administrators**. The Administrators page displays.

Administrator accounts

The page **Settings** > **Administrators** > **Delegated Administrators** lists all defined Email Security module administrators, their email address, account type, roles, and the administrator's current status (online or offline).

A new administrator is created with the role of Auditor. An Email Security module Super Administrator can assign a default role to a new administrator account or create a new role for that administrator. See *Administrator roles* for information about adding a new role and defining permissions.

The following table details the default roles available for selection:

Default Role	Description
Super Administrator	Administrators with this role have full access; they can add and remove administrators and edit the profiles and permissions of all other administrators.
Auditor	Administrators with this role can view all configuration settings but not change them.
Reporting Administrator	Administrators with this role can only edit, run, and schedule reports.
Security Administrator	Administrators with this role have access to all general settings and can add domains and set up routes and preferences. Permissions are identical to a Super Administrator, except they cannot manage other administrators.
Policy Administrator	Administrators with this role can create and manage policies only for the specific users or groups managed by this role. Permissions include reporting and quarantine management for these users and groups.
Quarantine Administrator	Administrators with this role can manage specific queues, troubleshoot from logs, and release messages to users from assigned queues.
Group Reporting Administrator	Administrators with this role can edit, run, and schedule reports only for users in specified groups.

Related concepts

Administrator roles on page 83

Assign administrator roles

Steps

1) From the page Delegated Administrators, click the name of an administrator. The Edit Administrator page displays.

2) From the pull-down menu **Role**, select a new default role.

3) Create a new role with different permissions; click **New Role**.

4) (*Optional*) View the administrator's current role and permissions; click **View Permission**.
The View Permission page displays.

5) Close the View Permission page; click **Cancel**.

6) Click **OK**.
The settings are saved.

Administrator roles

A Super Administrator can create several delegated administrators with a variety of roles and permissions on the page **Settings > Administrators > Roles**. When creating roles for delegated administrators, you specify the users or groups managed by the role along with the permissions associated with the role, before assigning an administrator to that role. An administrator may be assigned to only one role at a time.

Note

Managed users and user groups settings are used only for the following permissions:

- Policies
- Reports
- Queues and quarantined messages

A user's view of the Email Security module interface is different, depending on that user's specific administrator role. For example, a user with an Auditor role can view the entire Email Security module interface, but cannot modify any settings.

By default, a new Email Security module-specific administrator account is an Auditor account. A Super Administrator can use the following steps to change an administrator's role:

Note

Only one Super Administrator may access an email appliance at a time. Subsequent Super Administrators are assigned an Auditor (or read-only) role when they access the appliance.

Add new administrator role

Steps

1) From the page Roles, click **Add**. The Add Role page displays.

2) In the text field **Role Name**, enter a name for the new role.

3) In the text field **Description**, enter a brief, clear description of the role.

4) From the **Managed users and groups** table, define the users or user groups to be managed by this role:

   a) Under the Managed users and groups table, click **Add**.
   The Add Managed Users and Groups dialog box displays.

   b) Enter the email addresses of managed users or groups in one of the following ways:
   - From the field **User email address file**, click **Browse**.
     The Open window displays.
   - Browse to an email address file, a text file that contains one email address per line and is no larger than 10 MB, and click **Open**.
     The email address file is added.
   - In the field **User email addresses**, enter the desired email addresses, separated by semicolons.

   c) Click **OK**.
   The user and group settings are saved and the Add Role page displays.

Assigning an Administrator Role

In the section Permissions, define the permissions for this role by selecting the appropriate buttons in the Permissions table.

The following options are available:

Module	Permission Options
Policy	Read-only access to all policies Management Policies for users managed by this role All policies
System Settings and Status (includes access to the System Log, the Alerts page, the Message Queues page, and all Settings tab menu items except Administrators)	None Read-only access Management
Real-Time Monitor	None Read-only access
Message Logs (includes access to the Message, Connection, and Email Hybrid Service logs)	None Read-only access to all message logs Manage message logs for users managed by this role Manage all message logs
Audit and Console Logs (includes access to the Audit, Console, and Personal Email Manager logs)	None Access to logs
Always Block/Permit lists	None Read-only access Management
Administrators	None Read-only access Management

Module	Permission Options
Reports	None Reports for users managed by this role Access to all reports
Queues and quarantined messages	Queue access (None, Access to all queues, Access to selected queues) Manage all quarantined messages Manage messages for users managed by this role Read-only access to all quarantined messages

Steps

1) In the section Administrators, click **Assign Role**. The Assign Role dialog box displays.
2) Select the administrator to whom you want to assign this role. This role replaces the administrator's current role.
3) Click **OK**.
4) From the page Add Role, click **OK**. The new administrator role is saved.

Setting system preferences

The page **Settings** > **General** > **System Settings** is used to configure the following email system preferences:

Related concepts
Entering the fully qualified domain name on page 85

Related tasks
Setting the SMTP greeting message on page 86
Setting system notification email addresses on page 86
Configuring administrator console preferences on page 87

Entering the fully qualified domain name

The Fully Qualified Domain Name (FQDN) section of the System Settings page is used to define the FQDN. SMTP protocol requires the use of FQDNs for message

transfer. If you completed the First-Time Configuration Wizard, the FQDN you entered there appears on this page as the default entry.

If you did not complete the wizard, enter the appliance fully qualified domain name in the field **Fully Qualified Domain Name** (format is appliancehostname.parentdomain.com).

Important

This setting is important for proper email security system operation. You must replace the default fully qualified domain name entry with the correct appliance name.

An incorrect fully qualified domain name may cause disruptions in email traffic flow.

Setting the SMTP greeting message

The SMTP Greeting section of the System Settings page is used to define an SMTP greeting. The SMTP greeting message is the response to a connection attempt by a remote server. It can also be used to indicate that the system is working properly. For example, an SMTP greeting could be:

```
The email security service is ready.
```

Enter the SMTP greeting

Steps

1) In the text field **SMTP greeting**, enter a new start-up message.

2) Click **OK**
   The settings are saved.

Setting system notification email addresses

The System Notification Email Addresses section of the System Settings page is used to define default notification addresses. The email system can automatically send notifications of system events like a stopped service to a predefined address, often an administrator address. When this address is defined, notification messages can also be sent to or from an administrator email address for other events. For example, configuring a notification to be sent to or from an administrator address when a message triggers a filter (on the page **Main** > **Policy Management** > **Actions**) requires the administrator address to be defined on the page System Settings.

Define system notification email addresses

Steps

1) In the text field **Administrator email address**, enter the desired recipient address for notifications of system events.

2) In the text field **Default sender email address**, enter the desired sender address from which user notification messages should be sent.

3) Click **OK**.
   The settings are saved.

Configuring administrator console preferences

The Administrator Console Preferences section of the System Settings page is used to configure your desired character set encoding and console language.

Set console preferences

Steps

1) From the pull-down menu **Preferred character encoding**, select a character set for encoding messages.
   The selected character encoding setting is used to decode email attachments, including those for which no character encoding information is available.

2) From the pull-down menu **Administrator console language**, select the language that the appliance should use.

3) Click **OK**.
   The settings are saved.

Managing appliances

Before adding an appliance to the Email Security module, it is necessary to install and configure a Forcepoint appliance. Interface information includes IP address, subnet mask, default gateway, and up to three DNS server IP addresses. See the Forcepoint Appliances Getting Started Guide.

Forcepoint Email Security may be deployed as a virtual appliance. See the Forcepoint Appliances Getting Started Guide for complete information about deploying and configuring a virtual appliance.

Beginning with version 8.5, Forcepoint Email Security may be deployed on a virtual appliance in Microsoft Azure. See Installing Forcepoint Email Security in Microsoft Azure for more information.

Note

You can configure a primary, secondary, and tertiary DNS server, with the secondary and tertiary servers being optional entries.

When it starts, the email appliance polls each DNS server to determine which has the lowest latency level. That server is selected as the “primary” server for DNS queries, regardless of its designation. The other servers may be used for subsequent queries based on the network connection status of the primary server.

If you change either the appliance hostname or C interface IP address on the appliance, you must make the same change on the page **Settings** > **General** > **Email Appliances**. The Email Security module does not detect this change automatically.

Email traffic is usually routed through dedicated appliance interfaces (E1/E2). However, to route traffic through the C interface (for example, to transfer log data to a SIEM server), you need to define a route using the appliance CLI. It is necessary to stop and restart email security services on the appliance each time you add or delete a route on the appliance.

If you are running an Azure deployment, it is necessary to use the C interface for all email traffic.

Appliances overview

You can manage multiple email appliances from the page **Settings** > **General** > **Email Appliances** without having to log on to each machine separately. Managed appliances share a single Log Database, from which email log entries, presentation reports, and the dashboard statistics and charts are generated. The Email Security module and all appliances must share supported versions and subscription key for successful communication among the appliances.

An appliance may operate in standalone mode, which is the default mode when an appliance is added to the Email Security module. You can also create appliance clusters by designating an appliance as a primary machine or as a secondary machine associated with a primary machine. See *Designating a primary appliance in a cluster*.

The Email Appliances page lists all current system appliances in a table that displays information about the appliance and its status, with functionality to switch to a different appliance that is in standalone mode or to remove an unconnected primary

appliance from a cluster. The following table details the functionality on the Email Appliances page:

Option	Description
Hostname	Displays the hostname of the appliance. Selection displays the Edit Appliance page for editing the IP address.
Platform	Displays the appliance platform.
C/E1 interface IP address	Displays the appliance C/E1 interface IP address.
System Connection Status	Displays the appliance connection status.
Mode	Displays the appliance mode.
Action	Displays the actions available for the appliance; N/A, Launch, or Remove. Launch is used to switch to a different appliance; Remove is used to remove an unconnected primary appliance from a cluster. When a primary appliance is removed, all its secondary appliances change to standalone mode. The current and all secondary appliances display “N/A”.
Delete	Selection of the appliance and **Delete** removes the appliance from the Email Appliances page. An appliance that is being accessed by another user cannot be deleted. Once an appliance is removed from the list, you cannot manage it from the Email Appliances page.

Related tasks

Designating a primary appliance in a cluster on page 90

Add an appliance

Steps

1) From the page **Settings** > **General** > **Email Appliances**, click **Add**. The Add Appliance dialog box displays.

2) In the text field **C/E1 interface IP address**, enter the IP address used for communication with the Email Security module.

3) Click **OK**.
The dialog box closes and the appliance is added to the Email Appliances page.

Important

Changing the C interface IP address of an appliance terminates the appliance connection with the Email Security module. In order to re-establish the connection, the IP address must also be changed on the Email Security module page **Settings** > **General** > **Email Appliances**.

You should also change the address for the Personal Email Manager notification message (**Settings** > **Personal Email** > **Notification Message**).

For subscriptions that include the Forcepoint Email Security Hybrid Module, the email hybrid service must be re-registered after you change the IP address.

When you add an appliance, it is automatically registered with the Data Security module for data loss prevention (DLP). To complete the registration process and deploy DLP policies, click the Data Security module on the Security Manager toolbar and then click **Deploy**.

Editing appliance settings from the appliances list

The page Edit Appliance is used to edit the appliance C interface IP address. The system connection status and mode cannot be changed on this page.

Edit appliance settings

Steps

1) From the page **Settings** > **General** > **Email Appliances**, click the hostname of an appliance.
The Edit Appliance page displays.

2) In the text field **C/E1 interface IP address**, enter the new IP address.

3) Click **OK**.
The settings are saved.

Configuring an appliance cluster

An email appliance operates in standalone mode by default, but can be configured in a cluster of appliances to manage a large volume of email traffic. After you have added an appliance to the appliances list on the Email Appliances page, you can change its mode from the default standalone to either primary or secondary on the page **Settings > General > Cluster Mode**.

Some platform limitations apply to appliances in a cluster:

- A V10000 appliance cannot be configured in a cluster with a V5000 appliance.
- A virtual appliance may be clustered with other virtual appliances, but not with a physical appliance.
- Platform versions must match in a cluster.
- Appliances in a cluster should also have the same message queue configurations. Messages in a secondary appliance queue may be lost if that queue is not configured on the primary machine before the cluster is created.

Note

If you are deploying email protection in an appliance cluster and want to use DLP policies, be sure to register all the primary and secondary cluster machines with the Data Security module before you deploy DLP policies.

If you deploy DLP policies on the primary appliance while you are registering a secondary machine with the Data Security module, the registration process for the secondary machine may not complete.

Designating a primary appliance in a cluster

A primary appliance maintains and displays the configuration settings for all the appliances in its cluster.

Specify a primary appliance in a cluster

Steps

1) On the page **Settings** > **General** > **Cluster Mode**, select the appliance mode **Cluster (Primary)**.
   A Cluster Properties box opens with the primary appliance IP address displayed in the field **Cluster communication IP address**. Secondary appliances use this IP address for cluster communications.

Note

Use of the C appliance interface IP address for communication requires you to define a route in the appliance CLI.

You need to stop and restart email services on the appliance each time you add or delete a route on the appliance.

2) Click **Add**.
   The page Add Secondary Appliance displays, where you can designate the secondary appliances in this cluster.

3) From the list of standalone appliances on the left, select the secondary appliances to add to this cluster (up to seven appliances).
   (*Optional*) Add a new appliance that is not already on the list; click **Add New Appliance**.
   The Add Appliance page displays.

4) Click the arrow button to add the appliances to the Secondary Appliances list.

5) Click **OK**.
   The appliance is added to the Secondary Appliances list along with its status.

6) On the page Cluster Mode, click **OK**.
   The appliance is added to the cluster.

Next steps

View appliance details

From the Secondary Appliances list, click the appliance name.

The Appliance Properties dialog box displays with details about the appliance.

Remove a secondary appliance from a cluster

From the Secondary Appliances list, select the appliance and click **Remove**.

The appliance is removed from the cluster.

Managing user directories

A user directory is an important component of email traffic analysis when it is used to set sender/recipient conditions for a policy. It can also provide recipient validation capabilities and be the basis of user logon authentication settings. See *Managing user validation/authentication options*.

The page **Settings** > **Users** > **User Directories** is used to add a user directory. Available user directories display in table format with functionality to search by keyword or remove a user directory. The following table details the options on the User Directories page.

Option	Description
User Directory Name	Displays the name of the user directory. Selection displays the page Edit User Directory, with functionality to configure the user directory settings.
User Directory Type	Displays the user directory type; for example, Recipient List.
Cache Settings	Displays the user directory cache settings.
Cache Size	Displays the user directory cache size, with functionality to search entries listed in the user directory.
Status	Displays the user directory status.

Option	Description
Action	Displays available actions; for example, Delete.

Related concepts
Managing user validation/authentication options on page 103

Search a user directory by keyword

Steps

1) From the Cache Size column on the page **Settings** > **Users** > **User Directories**, click **View**.
   The User Directory Entries page displays.

2) In the text field, enter a keyword. Up to 100 characters can be entered.

3) Click **Submit**.
   The search results display in table format.

4) Empty the search field and display the complete user directory; click **Clear**.

Delete a user directory

A user directory may only be deleted if the directory is not currently being used by an email function. For example, if the directory is being used as part of a policy or as part of user authentication settings, it cannot be removed.

Select the user directory and click **Delete**. The user directory is deleted.

Adding and configuring a user directory

The Add User Directory page is used to add a new user directory. A newly added user directory displays a status of **Not referenced**, because it is not yet being used by an email function. User directory creation entries are different depending on the type of user directory being added.

Add a new user directory

Steps

1) On the page **Settings** > **Users** > **User Directories**, click **Add**. The Add User Directory page displays.

2) In the text field **User directory name**, enter a name for the user directory.

3) From the pull-down menu **User directory type**, select a type; **Microsoft Active Directory**, **IBM LDAP Server**, **Generic LDAP**, **Recipient List**, or **ESMTP**.
   The User Directory Properties section displays with configuration options for the selected user directory:
   - *Microsoft Active Directory*
   - *IBM LDAP Server Directory*
   - *Generic LDAP Server Directory*
   - *Recipient List*
   - *ESMTP Server Directory*

4) After configuring properties in the section User Directory Properties, click **OK**. The user directory is saved.

Related tasks
Microsoft Active Directory on page 93
IBM LDAP Server Directory on page 94
Generic LDAP Server Directory on page 95
Recipient List on page 96
ESMTP Server Directory on page 98

Microsoft Active Directory

Microsoft Active Directory provides user information management in a Windows environment.

If you plan to use Active Directory and your deployment includes Azure ExpressRoute, some additional configuration is needed in Azure. See the Microsoft article Azure Active Directory (AD) Domain Services for more information.

Configure a Microsoft Active Directory in the User Directory Properties section

Steps

1) On the page **Settings** > **Users** > **User Directories**, click **Add**. The Add User Directory page displays.

2) In the text field **User directory name**, enter a name for the user directory.

3) From the pull-down menu **User directory type**, select **Microsoft Active Directory**.
   User Directory Properties section displays with options for Microsoft Active Directory.

4) In the text field **Server IP address or hostname**, enter the IP address or hostname of your LDAP server.

5) In the text field **Port**, enter the port number. The default is 389.

6) (*Optional*) Enable secure LDAP, a nonstandard protocol also known as LDAP over SSL; mark the check box **Enable secure LDAP**.
   Marking this check box changes the default port number to 636.

7) In the text field **Username**, enter the username for this appliance.

The Username field can contain the user's username (such as admin), email address (such as admin@mycompany.com or distinguished name (such as cn=admin, dc=company, dc=com).

8) In the text field **Password**, enter the password for this appliance.

9) In the text field **Search domain**, enter the LDAP server's search domain name. This value is used when the search filter is applied.

10) Verify that the field **Search filter** contains a standard LDAP query that can use validation variables, for example:

(|(mail=%email%)(userPrincipalName=%email%)

(proxyAddresses=smtp:%email%))

11) From **Cache setting**, select either **Mirror** or **Cache address**.

- The **Mirror** setting means that valid addresses are cached all at once by synchronizing the cache with all the addresses stored on the LDAP server. You can manually synchronize the cache with the LDAP server any time after that by clicking **Synchronize** for this directory on the User Directories page.
- The **Cache address** setting means the cache is updated dynamically. A new, valid address is cached after it is verified with the LDAP server. Remove all addresses from the cache by clicking **Clear cache**.

12) In the text field **Cache timeout**, enter a value in minutes.

The timeout is the amount of time that a valid address remains in the memory cache. If an email message is sent from a previously validated address during this timeout period, the email is delivered without contacting the validation server.

However, if another message is sent from this address after the timeout has expired, the server will be contacted to validate the address. Default value is 60 minutes.

13) Click **OK**.

The settings are saved.

IBM LDAP Server Directory

An IBM LDAP Server Directory provides user information management on an IBM server.

Configure an IBM LDAP Server Directory in the User Directory Properties section

Steps

1) On the page **Settings** > **Users** > **User Directories**, click **Add**. The Add User Directory page displays.

2) In the text field **User directory name**, enter a name for the user directory.

3) From the pull-down menu **User directory type**, select **IBM LDAP Server**.

The User Directory Properties section displays with options for IBM LDAP Server Directory.

4) In the text field **Server IP address or hostname**, enter the IP address or hostname of your LDAP server.

5) In the text field **Port**, enter the port number. The default is 389.

6) (*Optional*) Enable secure LDAP, a nonstandard protocol also known as LDAP over SSL; mark the check box **Enable secure LDAP**.
Marking this check box changes the default port number to 636.

7) In the text field **Username**, enter the username for this appliance.
The Username field can contain the user's username (such as admin), email address (such as admin@mycompany.com or distinguished name (such as cn=admin, dc=company, dc=com).

8) In the text field **Password**, enter the password for this appliance.

9) From **Cache setting**, select either **Mirror** or **Cache address**.
- The **Mirror** setting means that valid addresses are cached all at once by synchronizing the cache with all the addresses stored on the LDAP server. You can manually synchronize the cache with the LDAP server any time after that by clicking **Synchronize** for this directory on the User Directories page.
- The **Cache address** setting means the cache is updated dynamically. A new, valid address is cached after it is verified with the LDAP server. Remove all addresses from the cache by clicking **Clear cache**.

10) In the text field **Cache timeout**, enter a value in minutes.
The timeout is the amount of time that a valid address remains in the memory cache. If an email message is sent from a previously validated address during this timeout period, the email is delivered without contacting the validation server.
However, if another message is sent from this address after the timeout has expired, the server will be contacted to validate the address. Default value is 60 minutes.

11) Click **OK**.
The settings are saved.

Generic LDAP Server Directory

A generic LDAP directory provides user information management that is supported on any LDAP server.

Configure a generic LDAP Server Directory in the User Directory Properties section

Steps

1) On the page **Settings** > **Users** > **User Directories**, click **Add**. The Add User Directory page displays.

2) In the text field **User directory name**, enter a name for the user directory.

3) From the pull-down menu **User directory type**, select **Generic LDAP**.
The User Directory Properties section displays with options for Generic LDAP Server Directory.

4) In the text field **Server IP address or hostname**, enter the IP address or hostname of your LDAP server.

5) In the text field **Port**, enter the port number. The default is 389.

6) (*Optional*) Enable secure LDAP, a nonstandard protocol also known as LDAP over SSL; mark the check box **Enable secure LDAP**.

   Marking this check box changes the default port number to 636.

7) In the text field **Username**, enter the username for this appliance.

   The Username field can contain the user's username (such as admin), email address (such as admin@mycompany.com or distinguished name (such as cn=admin, dc=company, dc=com).

8) In the text field **Password**, enter the password for this appliance.

9) In the text field **Search domain**, enter the LDAP server's search domain name. This value is used when the search filter is applied.

10) Verify that the field **Search filter** contains a standard LDAP query that can use validation variables; for example:

    (mail=%email%)

    (|(mail=%email%)(uid=%email%))

11) In the text field **Mail field**, enter any optional email addresses to import.

12) From **Cache setting**, select either **Mirror** or **Cache address**.

    - The **Mirror** setting means that valid addresses are cached all at once by synchronizing the cache with all the addresses stored on the LDAP server. You can manually synchronize the cache with the LDAP server any time after that by clicking **Synchronize** for this directory on the User Directories page.
    - The **Cache address** setting means the cache is updated dynamically. A new, valid address is cached after it is verified with the LDAP server. Remove all addresses from the cache by clicking **Clear cache**.

13) In the text field **Cache timeout**, enter a value in minutes.

    The timeout is the amount of time that a valid address remains in the memory cache. If an email message is sent from a previously validated address during this timeout period, the email is delivered without contacting the validation server.

    However, if another message is sent from this address after the timeout has expired, the server will be contacted to validate the address. Default value is 60 minutes.

14) Click **OK**.

    The settings are saved.

Recipient List

A recipient list is a text file that contains a list of email addresses and their associated passwords, one set per line. This file can be used for user recipient validation.

Configure a recipient list in the User Directory Properties section

Steps

1) On the page **Settings** > **Users** > **User Directories**, click **Add**. The Add User Directory page displays.

2) In the text field **User directory name**, enter a name for the user directory.

3) From the pull-down menu **User directory type**, select **Recipient List**.

4) The User Directory Properties section displays with options for Recipient List.

5) Enable a strong password policy; mark the check box **Enforce strong password policy**.
With this policy in force, a password must meet the following requirements:

   - Between 8 and 15 characters
   - At least one uppercase letter
   - At least one lowercase letter
   - At least one number
   - At least one special character; supported characters include:
     ! " # $ & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~

     If you have an existing recipient list and enable the strong password policy, the email protection system evaluates current passwords in the list against the policy. When this evaluation is complete, a Strength column appears in the Recipient List box, indicating any weak passwords that should be changed. A recipient list that contains weak passwords cannot be saved if the check box **Enforce strong password policy** is marked.

6) Add a predefined recipient list file; from the field Recipient information file, click **Browse** and navigate to the desired text file.
The file format should be one email address and password per line, up to a maximum of 1,000 entries.

Note

If you add a new recipient list file when you already have an active recipient list, the new file will overwrite the current file.

7) Manually create a recipient list; from the box **Enter Recipient Information**, enter an individual email address and associated password and click **>.**
The information is added to the Recipient List box on the right. Continue until all necessary recipients are added.

8) Click **OK**.
The settings are saved.

Search the recipient list

Steps

1) From the section Recipient List, enter a keyword in the text box and click **Search**.
Search results display in the Recipient List box.

2) View the entire recipient list; click **View All**.
The entire recipient list displays.

Export the recipient list

From the section Recipient List, click **Export**.

The recipient list is exported to your local drive as a text file.

Remove an entry from the recipient list

From the section Recipient List, select an individual entry and click **Delete**. The entry is removed.

ESMTP Server Directory

An ESMTP Server Directory provides user authentication and recipient validation using the features in extended SMTP.

Configure an ESMTP Server Directory in the User Directory Properties section

Steps

1) On the page **Settings** > **Users** > **User Directories**, click **Add**.
   The Add User Directory page displays.

2) In the text field **User directory name**, enter a name for the user directory.

3) From the pull-down menu **User directory type**, select **ESMTP**.
   The User Directory Properties section displays with options for ESMTP Server Directory.

4) Determine your desired email verification method; from Email verification method, select **Use the return status of the VRFY command** or **Use the return status of the RCPT command**:
   - Selection of Use the return status of the VRFY command verifies the email user name.
   - Selection of Use the return status of the RCPT command verifies the email recipient.

5) In the text field **Sender email address**, enter an email address for the user directory.

6) In the text field **Cache timeout**, enter a value in minutes.
   The cache timeout is the amount of time that a valid address remains in the memory cache. If an email message is sent from a previously validated address during this timeout period, the email is delivered without contacting the validation server. However, if another message is sent from this address after the timeout has expired, the server will be contacted to validate the address. Default value is 60 minutes.

   Remove all addresses from the cache by clicking **Clear cache**.

7) Click **OK**.
   The settings are saved.

Managing domain and IP address groups

A collection of domain names or IP addresses can be defined in a single group for use in email functions. For example, you can define a domain name group to establish domain-based delivery options, or you can define an IP address group for which Reputation Service, Real-time Blacklist (RBL), or directory attack prevention analysis is not performed. IP address groups can also be used for the email encryption functions. Domain groups are added and configured on the page **Settings** > **Users** > **Domain Groups**; IP groups are added and configured on the page **Settings** > **Inbound/Outbound** > **IP Groups**.

You can perform the following operations on domain or IP address groups:

- *Adding a domain group*
- *Editing a domain group*
- *Adding an IP address group*
- *Editing an IP address group*

There are two special default groups of domain or IP addresses:

- Protected Domain group
- Trusted IP Address group

See *Third-party encryption application* for information about using the Encryption Gateway default IP address group. Default groups cannot be deleted.

Related concepts
Third-party encryption application on page 165

Related tasks
Adding a domain group on page 101
Editing a domain group on page 101
Adding an IP address group on page 102
Editing an IP address group on page 103

Protected Domain group

The Protected Domain group should contain all the domains that an organization owns and needs the email system to protect. Message direction in the system is determined on the basis of an organization's protected domains:

- Inbound – The sender address is not from a protected domain and the recipient address is in a protected domain.
- Outbound – The sender address is from a protected domain and the recipient address is not in a protected domain.
- Internal – Both the sender and recipient addresses are in a protected domain.

An open relay results when both the sender and recipient addresses are not in a protected domain.

Unless you entered a protected domain name in the Domain-based Route page of the First-time Configuration Wizard, the default Protected Domain group is empty after product installation. Domains may be added to or deleted from the Protected Domain group, the Protected Domain group itself cannot be deleted.

Important

Ensure that the Protected Domain group contains all the domains you want your email system to protect.

An open relay is created when mail from an unprotected domain is sent to an unprotected domain within your organization. As a result, all mail from any domain that is not protected may be rejected. Mail from an external trusted IP address to an unprotected domain within your organization bypasses analysis and is delivered.

The email hybrid service uses the Protected Domain group during Forcepoint Email Security Hybrid Module registration to verify that the domains specified in its delivery routes are all from this group. The Protected Domain group should not be used to configure email delivery routes (on the page **Settings** > **Inbound/Outbound** > **Mail Routing**) if you need to define domain-based delivery routes via multiple SMTP servers. See *User directory-based routes*.

Related concepts

User directory-based routes on page 136

Trusted IP Address group

Like the Protected Domain group, the Trusted IP Addresses default group is empty after product installation. IP addresses may be added to or deleted from the Trusted IP Addresses group, but the Trusted IP Addresses group itself cannot be deleted. The Trusted IP Addresses group may include up to 1024 addresses.

Trusted IP addresses may include your internal mail servers or a trusted partner mail server.

Mail from an address in the Trusted IP Addresses group can bypass some inbound email analysis. Use of the Trusted IP Addresses group can result in improved email processing time.

Specifically, mail from trusted IP addresses bypasses the following email analysis:

- Global Always Block List (**Main** > **Policy Management** > **Always Block/Permit**)
- All message controls except message size, invalid recipient, and internal sender verification settings (**Settings** > **Inbound/Outbound** > **Message Control**)
- Recipient validation (**Settings** > **Users** > **User Authentication**)
- All connection controls except the connection control timeout (**Settings** > **Inbound/Outbound** > **Connection Control**)
- Directory harvest attack (**Settings** > **Inbound/Outbound** > **Directory Attacks**)
- Relay controls (**Settings** > **Inbound/Outbound** > **Relay Control**)
- Personal Email Manager Always Block List

Note

Mail from trusted IP addresses does not bypass policy and rule application, and is always subject to antispam and antivirus analysis.

Adding a domain group

The page Add Domain Group is used to add a new domain group.

Add new domain group

Steps

1) On the page **Settings** > **Users** > **Domain Groups**, click **Add**. The Add Domain Group page displays.

2) In the field **Domain Group Name**, enter a name for the new domain group. This field is required.

3) In the field **Description**, enter a brief description of the domain group.

4) In the section Domain Group Details, add a predefined domain group; from the field **Domain address file**, click **Browse** and navigate to the desired text file.
   The file format should be one domain address per line, and its maximum size is 10 MB. If a file contains any invalid entries, only valid entries are accepted. Invalid entries are rejected.

5) Manually add domain entries; in the field **Domain address**, enter an individual domain address and click **>**.
   The information is added to the Added Domains box on the right. Use wildcards to include subdomain entries (for example, *.domain.com).

6) Click **OK**.
   The settings are saved.

Export a domain group

From the section Added Domains, click **Export**.

The list of domain address entries in the group is exported to your local drive as a text file.

Remove an entry from the domain group

From the section Added Domains, select an individual entry and click **Delete**.

The entry is removed.

Editing a domain group

The page **Settings** > **Users** > **Domain Groups** is used to edit existing domain groups, including adding or removing individual domains or editing the domain group description.

If a domain is in use, you will be asked to confirm any changes that involve the domain.

Edit a domain group

Steps

1) From the page **Settings** > **Users** > **Domain Groups**, click the domain group name.
   The page Edit Domain Group displays.

2) Configure the settings.

3) Click **OK**.
   The settings are saved.

Adding an IP address group

The page **Settings** > **Inbound/Outbound** > **IP Groups** is used to view and add an IP address group.

Add a new IP address group

Steps

1) On the page **Settings** > **Inbound/Outbound** > **IP Groups**, click **Add**. The Add IP Group page displays.

2) In the field **IP Address Group Name**, enter a name for the new IP address group. This field is required.

3) In the field **Description**, enter a brief description of the IP address group.

4) In the section IP Address Group, add a predefined IP address group; from the field **IP address file**, click **Browse** and navigate to the desired text file.
   The file format should be one IP address per line, and its maximum size is 10 MB

   Note

   The default Encryption Gateway IP address group supports only the entry of individual IP addresses. Subnet address entries are considered invalid and are not accepted for this IP address group.

   Subnet addresses may be entered for other default and custom IP address groups.

5) Manually add IP address entries; in the field **IP address**, enter an individual IP address and click **>**.
   The information is added to the Added IP Addresses box on the right.

6) Click **OK**.
   The settings are saved.

Export an IP address group

From the section Added IP Addresses, click **Export**.

The list of IP address entries in the group is exported to your local drive as a text file.

Remove an entry from the IP address group

From the section Added IP Addresses, select an individual entry and click **Remove**.

The entry is removed.

Editing an IP address group

The page Edit IP Group is used to edit existing IP address groups, including adding or removing individual IP addresses and editing the IP address group description.

If an IP address is in use, you will be asked to confirm any changes that involve that address.

Steps

1) From the page **Settings** > **Inbound/Outbound** > **IP Groups**, click the IP address group name.
   The Edit IP Group page displays.

2) Configure the settings.

3) Click **OK**.
   The settings are saved.

Managing user validation/authentication options

After defining your domain groups, you can determine recipient validation and user authentication settings for users in the user directories you create. See *Managing domain and IP address groups*. User validation and authentication settings are configured on the page **Settings** > **Users** > **User Authentication**.

The following types of user validation/authentication are available:

- **Recipient validation**, in which a message recipient is validated before a message is received.
- **SMTP authentication**, in which a message sender is authenticated before a message is received.
- **Personal Email authentication**, in which a user is authenticated before accessing the Personal Email Manager facility for managing blocked email. See *Configuring Personal Email Manager End User Options*.
- **Distribution list validation**, in which individual members of an email distribution list are validated. If an individual recipient in the group is invalid, the message is rejected just for that individual. All valid recipients in the distribution list receive the message.

Include group email addresses in your user directories to use the distribution list validation option. A message to an invalid group alias is rejected for the entire group of recipients.

Users in a domain group are verified against the corresponding user directory, and specified authentication settings are applied.

Important

You may create multiple Personal Email Manager user authentication groups. However, any protected domain group (as defined in **Settings** > **Users** > **Domain Groups**) may be included in only one Personal Email Manager user authentication group.

Including a protected domain group in more than one Personal Email Manager user authentication group may result in the users of that domain group being denied access to the Personal Email Manager facility.

Add all the user directories that contain the users in this protected domain group to the associated Personal Email Manager authentication group.

The User Authentication List displays the configured user authentication settings. The Add and Delete buttons are used to add or remove recipient validation and authentication settings.

Related concepts

Managing domain and IP address groups on page 99

Related information

Configuring Personal Email Manager End User Options on page 239

Adding user authentication settings

The page **Settings** > **Users** > **User Authentication** is used to add new user validation/authentication settings for domain/user directory groups.

Add new user authentication and validation settings

Steps

1) From the page **Settings** > **Users** > **User Authentication**, click **Add**. The Add User Authentication page displays.

2) In the text field **Name**, enter a name for this set of authentication settings.

3) From Authentication options, mark the check box for the type of user validation/authentication settings to apply: **Recipient Validation**, **SMTP Authentication**, **Personal Email Authentication**, or **Distribution List Validation**.

   Multiple check boxes can be selected.

   - (*Optional*) If you specify recipient validation, you can mark the associated check box **If User Directory is not reachable for Recipient validation, continue to next user directory**.
     Selection allows the system to continue a recipient search in the next user directory listed in the User Directories section Recipients box if the current user directory cannot be accessed (e.g., server is down or not connected).
   - If you specify SMTP authentication, you must ensure that the option **Allow relays only for senders from trusted IP addresses** option is selected for both outbound and internal relays on the page **Settings** > **Inbound/Outbound** > **Relay Control**.

4) From the pull-down menu **Domain group**, select the domain group to target with your authentication settings.

5) (*Optional*) Add or remove domain names from your domain group; from Domains, click **Edit**.The Edit Domain Group page displays. Changes you make here are also reflected on the page **Settings** > **Users** > **Domain Groups**. See *Editing a domain group*.

6) From the box Current User Directories, select the corresponding user directories to which these authentication settings should apply; mark the check box next to the directory name and click **>**.
The user directory is added to the Recipients box.

7) (*Optional*) Create a new user directory for these authentication settings; click **Add user directory**.The Add User Directory page displays to create a new directory. See *Adding and configuring a user directory*.

8) In the Recipients box, move selected user directories up or down; select the buttons **Move up** and **Move down**.

9) (*Optional*) Delete a user directory reference from the Recipients box; select it and click **Delete**.This action removes the user directory from the Recipients list, but does not delete it from the page **Settings** > **Users** > **User Directories**.

10) Click **OK**.
The settings are saved.

Related tasks
Editing a domain group on page 101
Adding and configuring a user directory on page 92

Editing user authentication settings

The Edit User Authentication page is used to edit existing user authentication settings. Functionality is used to configure existing settings as well as add or remove user directories from user validation/authentication settings. User directory entries are modified on the page **Settings** > **Users** > **User Directories**. See *Adding user authentication settings*.

Edit authentication settings

Steps

1) From the page **Settings** > **Users** > **User Authentication**, click the name of the settings.
The Edit User Authentication Settings page displays.

2) Configure the settings.

3) Click **OK**.
The changes are saved.

Related tasks
Adding user authentication settings on page 104

Managing Transport Layer Security (TLS) certificates

Transport Layer Security (TLS) is a protocol that provides an extra layer of security for email communications. Use of this protocol helps prevent devices such as non-trusted routers from allowing a third party to monitor or alter the communications between a server and client. The email security system can receive messages transferred over TLS and can also send messages via this protocol to particular domains.

A default TLS certificate is supplied with Forcepoint Email Security for incoming connections. The email system presents this certificate during TLS communications.

After email product installation, default TLS certificate information appears on the page **Settings** > **Inbound/Outbound** > **TLS Certificate**, in the section TLS Certificate for Incoming Connection. Details include the certificate version, serial number, issuer, and expiration date.

Functionality on this page allows you to generate a new certificate when the default certificate expires. Generating a new certificate overwrites any certificate that currently exists. Additionally, certificates can be imported and exported on the TLS Certificate page.

The TLS Certificate page is additionally used to manage trusted Certificate Authority (CA) certificates for outgoing connections. Forcepoint Email Security uses CA-issued root and intermediate certificates (along with the default CA certificate bundle) to verify a server certificate presented by a third-party mail server during TLS communications.

The Trusted CA Certificate for Outgoing Connection table on the TLS Certificate page displays information about the certificate, including common name, issuer, and expiration date. Import functionality is used to browse to the location of a trusted certificate and add it to the Trusted CA Certificate for Outgoing Connection table. A search function is used to perform a keyword search of all your trusted CA certificates.

Generate a new TLS certificate

Steps

1) From the section TLS Certificate for Incoming Connection, click **Generate**. A prompt displays to indicate that the existing certificate will be overwritten.

2) Click **Yes**.
   TLS certificate generation continues.

Search trusted CA certificates by keyword

Steps

1) From the section Trusted CA Certificate for Outgoing Connection, enter a keyword in the text field **Search filter**.

2) Click **Search**.
   Search results display below the search bar.

3) Clear search results; click **Clear search filter**.
   All trusted CA certificates display below the search bar.

   See the following sections for details on importing and exporting TLS and CA certificates:

   - *Importing a TLS certificate*
   - *Exporting a TLS certificate*
   - *Importing a trusted CA certificate*

Related tasks
Importing a TLS certificate on page 107
Exporting a TLS certificate on page 108
Importing a trusted CA certificate on page 108

Importing a TLS certificate

Functionality is available on the page **Settings** > **Inbound/Outbound** > **TLS Certificate** to import a certificate from your network, rather than generate a new one. Importing a certificate overwrites any certificate that currently exists.

Import a certificate that is already located on your network

Steps

1) On the page **Settings** > **Inbound/Outbound** > **TLS Certificate**, click **Import**. A prompt displays to indicate that the existing certificate will be overwritten.

2) On the prompt, click **Yes**.
   An Import Certificate area appears below the Import button.

3) Click **Browse** and navigate to the certificate file.
   When you select a file, its filename appears in the **Certificate file** field. File format must be .p12 or .pfx.

4) In the text field **Password**, enter a password. Maximum length is 100 characters.

5) Click **OK**.
   The certificate is imported.

Exporting a TLS certificate

Functionality is available on the page **Settings** > **Inbound/Outbound** > **TLS Certificate** to export a TLS certificate to a location on your network.

Steps

1) On the page **Settings** > **Inbound/Outbound** > **TLS Certificate**, click **Export**. The Export TLS Certificate dialog box displays.

2) In the text field **Password**, create a password for the exported file.

3) In the text field **Confirm password**, re-enter the password.

4) Click **Yes**.
   A navigation window displays.

5) Browse to the location in your network where the certificate and password should be stored and click **Save**.
   The TLS certificate is saved to the specified location

Importing a trusted CA certificate

Functionality is available on the page **Settings** > **Inbound/Outbound** > **TLS Certificate** to import a trusted CA certificate from your network.

Steps

1) In the section Trusted CA Certificate for Outgoing Connection, click **Import**. The Import Trusted CA Certificate dialog box displays.

2) In the Import Trusted CA Certificate dialog box, enter the desired certificate file name or browse to its location in your network.

3) Click **OK**.
   The certificate is added to the trusted CA certificate table.

Delete a trusted CA certificate

From the section Trusted CA Certificate for Outgoing Connection, select a CA certificate and click **Delete**.

The CA certificate is deleted.

Backing up and restoring manager settings

The email management server maintains several important configuration setting files, including

- Database configuration
- Appliances list
- Administrator settings
- Presentation report templates and data

You may want to retain a backup copy of these settings to use if a system recovery operation is necessary. A backup and restore utility is included with the Email Security module. Backup and restore functions are available on the page **Settings** > **General** > **Backup/Restore**.

The Backup/Restore function includes a Backup and Restore Log, which displays time-stamped backup and restore activities for the manager.

Note

Because the Backup/Restore utility stops the Email Security module service, backup and restore activities are recorded only in the Backup and Restore log.

Backup and restore functions for an appliance cluster work properly only when cluster settings have not changed between the backup and restore operations. Unexpected results may occur if any of the following settings have been changed between the backup and restore:

- Appliance mode (cluster or standalone)
- IP address or hostname

You may need to rebuild a cluster if a restore operation encounters problems.

Note

If you specify your backup file location for a remote server, ensure that your restore operation is configured to restore configuration files from that remote server location.

Backing up settings

Backup functionality is available on the page **Settings** > **General** > **Backup/Restore**. Backup and restore settings on one appliance are applied to all the appliances in your network.

Note

- The version of the backed up settings must match the version of the currently installed product.
- Backup and restore settings must both use either local or remote file storage. You cannot restore a local file using remote settings.
- The backup settings file size may not exceed 10 MB.
- The following special characters are not supported in backup server entries: |, <, >, and &.

Steps

1) On the page **Settings** > **General** > **Backup/Restore**, from the section Backup Settings, click **Backup**.
   The utility activates and conducts a backup if settings have been defined.

2) Save your backup settings on the Log Database server, mark the check box **Save backup configuration settings files on a remote server**.
   The text fields in the section Remote Server Access are enabled; enter the following server information:

   - **Domain/Hostname**
     Enter the domain if a domain account is used; otherwise, enter the hostname of the SQL Server machine.
   - **User name**
     Enter a user with SQL Server log-in permission.
   - **Password**
     The password may not contain more than one double quotation mark.
   - **Backup/Restore file path**
     Enter the shared folder path on the remote SQL Server machine (for example, \\10.1.1.2\shared\).

3) Ensure that the remote log database server is accessible; click **Check Status**.
   The backup initiates when all configuration is complete. The Backup and Restore Log displays the time-stamped backup logs.

Restoring the settings

The Restore utility is used to return your settings to their original, backed up state on the Log Database server. The restore function retrieves the location of the backed up settings and applies them to the Email Security module configuration files. The Email Security module service restarts automatically after configuration settings are restored.

Steps

1) (*Optional*) On the page **Settings** > **General** > **Backup/Restore**, from the section Restore Settings, mark the check box **Use the backup files on the remote server to restore configuration settings**.
   From File location, click **Choose File** and navigate to the backup files on the remote server.

2) Click **Restore**.
   The Confirm Configuration Restore Operation dialog box displays.

3) Click **Yes**.
   The restore operation proceeds.

Chapter 4

Managing Messages

Contents

Configuring message properties

Email message control properties allow you to set message size and volume limits, and to determine how invalid recipients are handled. The following settings are configured on the page **Settings** > **Inbound/Outbound** > **Message Control**:

Related tasks

Setting size properties on page 112
Setting volume properties on page 112
Configuring invalid recipient settings on page 113
Enabling archive message options on page 113
Enabling message sender verification on page 114
Enabling bounce address tag validation (BATV) on page 114

Setting size properties

Use the Message Size Options to configure message size properties, such as setting a maximum message size or data size per connection.

Configure message size options

Steps

1) Navigate to the page **Settings** > **Inbound/Outbound** > **Message Control**.

2) From the section **Message Size Options**, mark the check box **Limit message size**.
   This is the default setting. Selection enables the corresponding text field Maximum message size.

3) In the text field **Maximum message size**, enter a maximum message size in KB, from 1–102400 KB.
   The default is 10,240. This setting can prevent very large messages from using valuable bandwidth.

4) Set a maximum message size per connection; mark the check box **Limit data size per connection**.
   Selection enables the corresponding text field Maximum data size.

5) In the text field **Maximum data size**, enter a maximum data size in KB, from 1–204800.
   The default is 20,480 KB. This setting can help limit the receipt of messages with very large attachments, which can take up valuable bandwidth.

6) Click **OK**.
   The settings are saved.

Setting volume properties

Use the Message Volume Options to configure message volume properties, such as limiting the number of messages per connection or recipients per message.

Configure message volume properties

Steps

1) Navigate to the page **Settings** > **Inbound/Outbound** > **Message Control**.

2) From the section Message Volume Options, mark the check box **Limit number of messages per connection**.
   Selection enables the corresponding text field Maximum number of messages.

3) In the text field **Maximum number of messages**, enter a maximum number of messages per connection, from 1–65535.
   The default is 30

4) Mark the check box **Limit number of recipients per message**.
   Selection enables the corresponding text field Maximum number of recipients.

5) In the text field **Maximum number of recipients**, enter a maximum number of recipients, from 1–4096.
   The default is 20. This can save bandwidth by preventing one message from being sent to hundreds of users.

6) Click **OK**.
   The settings are saved.

Configuring invalid recipient settings

Use the Invalid Recipient Options to configure invalid recipient settings, such as allowing invalid recipients.

Steps

1) Navigate to the page **Settings** > **Inbound/Outbound** > **Message Control**.

2) From the section Invalid Recipient Options, permit mail containing invalid recipients into your system; mark the check box **Allow invalid recipients**.
   This option is available only when the recipient validation is configured on the page **Settings** > **Users** > **User Authentication**. See *Managing user validation/authentication options*. Selection enables the corresponding text field and check box.

3) In the text field **Block message if the percentage of invalid recipients is at least**, enter a value for the percentage of invalid recipients that determines if a message is blocked.
   The default is 100%.

4) Enable the system to send a non-delivery report notification; mark the check box **Send non-delivery report (NDR) only if a message is not blocked**.

5) Click **OK**.
   The settings are saved.

Related concepts
Managing user validation/authentication options on page 103

Enabling archive message options

Use the Message Archive Queue settings to save all incoming messages to an archive message queue before they are scanned. Enabling this feature can impact storage capacity and system performance.

Enable message archive queue

Steps

1) Navigate to the page **Settings** > **Inbound/Outbound** > **Message Control**.

2) From the section Message Archive Queue, save incoming messages to an archive message queue; mark the check box **Enable archive queue storage**.
   This option is disabled by default.

3) Click **OK**.
   The settings are saved. View the archive queue by clicking **archive** in the queue list on the page **Main** > **Message Management** > **Message Queues**. See *Managing message queues*.

Related concepts
Managing message queues on page 147

Enabling message sender verification

Use the Internal Sender Verification settings to ensure that an internal email sender is an authenticated user. This operation performs a check to confirm that an email sender from an internal domain is also an authenticated user. For email to pass this check function, a mail sender's address must match the sender's login authentication entry.

Enable internal sender verification

Steps

1) Navigate to the page **Settings** > **Inbound/Outbound** > **Message Control**.

2) From the section Internal Sender Verification, mark the check box **Enable internal sender verification**.
   This option is disabled by default.

3) Click **OK**.
   The settings are saved.

Enabling bounce address tag validation (BATV)

Bounce address tag validation (BATV) is a method for determining whether a bounce message to an address in your protected domain is valid. This method helps to prevent backscatter spam, in which a bounce message to your organization contains a forged recipient address.

With BATV enabled, the sender address of outbound email is marked with a unique tag. A bounce message addressed to that sender is examined for the presence of that unique tag. If the tag is detected, the bounce message is cleared for delivery. A bounce message without the tag is blocked.

Steps

1) Navigate to the page **Settings** > **Inbound/Outbound** > **Message Control**.

2) From the section Bounce Address Tag Validation, mark the check box **Enable Bounce Address Tag Validation**.
   Selection enables the corresponding pull-down menus.

3) Define user and IP address groups to bypass the BATV function; select the groups from among the following pull-down menus:
   - Inbound IP address group
   - Inbound domain group
   - Outbound domain group
     A domain group selected for outbound bypass must also be selected for inbound bypass. The default setting for each group is **None**.

     Only user-defined domain and IP address groups are available in the pull-down menus. See *Managing domain and IP address groups* for information about creating domain and IP address groups.

4) Click **OK**.
   The settings are saved.

Related concepts
Managing domain and IP address groups on page 99

Managing connection options

The page **Settings** > **Inbound/Outbound** > **Connection Control** is used to configure connection settings, such as limiting the number of simultaneous connections per IP address and enabling real-time blacklist checking or reverse DNS verification.

The following settings can be configured on the page Connection Control:

- *Configuring simultaneous connections*
- *Using a real-time blacklist*
- *Using reverse DNS verification*
- *Using the reputation service*
- *Delaying the SMTP greeting*
- *Enabling the SMTP VRFY command*
- *Enabling SMTP authentication for email hybrid service*
- *Changing the SMTP port*
- *Using access lists*

To collect and view detailed information about some connections, allow connection control functions to save these details in the mail processing log, accessed via an appliance. When the function is activated, the log collects detailed data regardless of whether the connection control itself is enabled. This function is available for the following connection control options:

- Real-time blacklist (RBL)
- Reverse DNS lookup
- Reputation service
- SMTP greeting delay

Related concepts
Using access lists on page 121

Related tasks
Configuring simultaneous connections on page 116
Using a real-time blacklist on page 116
Using reverse DNS verification on page 117
Using the reputation service on page 118
Delaying the SMTP greeting on page 119
Enabling the SMTP VRFY command on page 119
Enabling SMTP authentication for email hybrid service on page 120
Changing the SMTP port on page 120

Configuring simultaneous connections

Limiting the number of simultaneous connections can improve system performance. The Connection Options section is used to limit these connections.

Limit simultaneous connections

Steps

1) Navigate to the page **Settings** > **Inbound/Outbound** > **Connection Control**.

2) From the section Connection Options, in the text field **Simultaneous connections per IP**, enter the maximum number of allowed simultaneous connections per IP address, from 1–500.
   The default is 10.

3) In the text field **Timeout**, specify the maximum number of seconds of inactivity allowed before a connection is dropped, from 1–43200.
   The default is 300.

4) Click **OK**.
   The settings are saved.

Using a real-time blacklist

A Real-Time Blacklist (RBL) is a third-party published list of IP addresses that are known sources of spam. When RBL checking is enabled, messages from a sender listed on an RBL are prevented from entering your system. The Email Security module supports the use of the Spamhaus Datafeed server or the entry of up to three third-party RBLs for RBL lookups. Functionality is configured from the section Real-time Blacklist Options on the page **Settings** > **Inbound/Outbound** > **Connection Control**.

Configure the RBL

Steps

1) Navigate to the page **Settings** > **Inbound/Outbound** > **Connection Control**.

2) From the section Real-time Blacklist Options, mark the check box **Perform RBL check**.
   This feature is enabled by default.

3) Save detailed connection information in the appliance mail processing log; mark the check box **Save connection details in the mail processing log**.
   If you enable this option without designating a third-party RBL, the email protection system still collects log information that email content filters can use for subsequent message analysis.

4) Under Spam RBL service, select one of the following RBL lookup methods:
   - **Spamhaus service**
     Use the Spamhaus server for RBL lookups.
   - **Domain address**
     Enter up to three domain addresses of the RBL services to use. Separate multiple addresses with a semicolon (;).

5) Click **OK**.
   The settings are saved.

Using reverse DNS verification

Reverse DNS lookup uses a pointer (PTR) record to determine the domain name that is associated with an individual sender IP address. The reverse DNS lookup function can determine whether email sent to your system is from a legitimate domain. Use of this option can enhance the detection of commercial bulk email. See *Commercial bulk email*.

However, if you enable Reverse DNS, server performance may be affected, or legitimate users may be rejected. This function is not enabled by default, but can be enabled from the section Reverse DNS Lookup Options on the page **Settings** > **Inbound/Outbound** > **Connection Control**.

Enable reverse DNS lookup

Steps

1) Navigate to the page **Settings** > **Inbound/Outbound** > **Connection Control**.

2) From the section Reverse DNS Lookup Options, mark the check box **Enable reverse DNS lookup**.
   Selection enables the corresponding check boxes.

3) Determine the response to a reverse DNS lookup by marking one or more of the following check boxes:
   - **Disconnect if the PTR record does not exist**
   - **Disconnect if the PTR record does not match the A record**
   - **Disconnect if a soft failure occurs during a reverse DNS lookup**
     If you select this option, a connection is terminated when the following events occur:
     - Named DNS lookup cache service is down.
     - Your DNS server is down.
     - A timeout occurs during a DNS lookup.
   - **Disconnect if the PTR record does not match the SMTP EHLO/HELO greeting**

4) Save detailed connection information in the appliance mail processing log; mark the check box **Save connection details in the mail processing log**.

5) Click **OK**.
   The settings are saved.

Related concepts
Commercial bulk email on page 186

Using the reputation service

The email protection system can check an email sender's IP address against the reputation service, which classifies email senders based on past behavior. With this function, the email system can block mail from known spam senders. The reputation service is enabled from the section Reputation Service Options on the page **Settings** > **Inbound/Outbound** > **Connection Control**.

Configure the reputation service

Steps

1) Navigate to the page **Settings** > **Inbound/Outbound** > **Connection Control**.

2) From the section Reputation Service Options, mark the check box **Enable Reputation Service**.
   This is the default setting. Selection enables the corresponding radio buttons.

3) Select one of the following analysis levels to specify the threshold for blocking mail:
   - **Conservative**
     Blocks mail from addresses that send spam 100% of the time.
   - **Medium**
     Blocks mail from addresses that send spam 99% of the time.
   - **Aggressive**
     Blocks mail from addresses that send spam 97% of the time. This is the default.
   - **Custom**
     Selection enables the corresponding text field in which to enter a custom spam percentage. The email system blocks mail from addresses that send spam the specified percentage of time.

4) Save detailed connection information in the appliance mail processing log; mark the check box Save connection details in the mail processing log.

5) Click **OK**.
The settings are saved.

Delaying the SMTP greeting

An SMTP greeting message can be delayed for a specified time interval, so that a connection from a client will be dropped if the client tries to send data during this time interval. This option can help prevent mail from spam-sending applications that send a high volume of messages very quickly. The connection is dropped as soon as a message is sent to the SMTP server before it is ready. This feature is not enabled by default, but can be enabled from the section SMTP Greeting Delay Options on the page **Settings** > **Inbound/Outbound** > **Connection Control**.

Configure the SMTP greeting delay

Steps

1) Navigate to the page **Settings** > **Inbound/Outbound** > **Connection Control**.

2) From the section SMTP Greeting Delay Options, mark the check box **Enable SMTP greeting delay**.
Selection enables the corresponding field.

3) In the text field Delay time, specify the delay time, in seconds, from 1–60. The default is 3 seconds.

4) Save detailed connection information in the appliance mail processing log; mark the check box **Save connection details in the mail processing log**.

5) Click **OK**.
The settings are saved.

Enabling the SMTP VRFY command

The SMTP VRFY command can be used to verify an email username. When asked to validate a username, a receiving mail server responds with the user's login name. The SMTP VRFY Command section on the page **Settings** > **Inbound/Outbound** > **Connection Control** is used to configure this option.

Important

Use this command with care. Although helpful in validating a user, this command can also create a network security issue if the user information is retrieved by someone with malicious intent.

Steps

1) Navigate to the page **Settings** > **Inbound/Outbound** > **Connection Control**.

2) From the section SMTP VRFY Command Option, mark the check box **Enable SMTP VRFY command**.

3) Click **OK**.
The settings are saved.

Enabling SMTP authentication for email hybrid service

By default, SMTP authentication is enabled for inbound messages that enter the system via the email hybrid service. This type of authentication provides additional authentication protection for email that is relayed to the email protection system from the hybrid service. The Email Hybrid Service SMTP Authentication section on the page **Settings** > **Inbound/Outbound** > **Connection Control** is used to enable or disable this option.

Disable SMTP authentication for Forcepoint Email Security Hybrid Module

Steps

1) Navigate to the page **Settings** > **Inbound/Outbound** > **Connection Control**.

2) From the section Email Hybrid Service SMTP Authentication Option, unmark the check box **Enable email hybrid service SMTP authentication**.
This option is available only when your subscription includes Forcepoint Email Security Hybrid Module and the hybrid service is registered and enabled.

3) Click **OK**.
The settings are saved.

Changing the SMTP port

The default SMTP port number is 25. Proper communication with the email hybrid service requires the use of port 25 for SMTP. However, the SMTP Port Option settings on the page **Settings** > **Inbound/Outbound** > **Connection Control** can be used to customize the port number.

Note

Changing this port setting causes module services to restart.

Steps

1) Navigate to the page **Settings** > **Inbound/Outbound** > **Connection Control**.

2) From the section SMTP Port Option, enter a valid port number in the text field **SMTP port**.
Valid values are from 25 to 5000.

3) Click **OK**.
The settings are saved. The Email Security module services are restarted.

Using access lists

An access list enables you to specify an IP address group for which certain email analysis is not performed. The Allow Access List Options on the page **Settings** > **Inbound/Outbound** > **Connection Control** are used to identify these IP addresses. Mail from these addresses bypasses the following email analysis:

- Connections per IP address
- RBL checks
- Reverse DNS lookup
- Reputation service
- SMTP greeting delay
- Directory harvest attack prevention
- Inbound relay control
- True Source IP detection

IP address groups are defined on the page **Settings** > **Inbound/Outbound** > **IP Groups**. The groups defined on that page appear for selection in the Connection Control Allow Access List Options section.

Create and modify an access list

Steps

1) Navigate to the page **Settings** > **Inbound/Outbound** > **Connection Control**.

2) From the section Allow Access List Options, select an IP group name from the pull-down menu **IP group**.
The IP addresses in the group display in the list of IP addresses list and the Edit button is enabled.

3) Click **Edit**.
The Edit IP Groups page displays to configure the IP addresses. See *Editing an IP address group*.

4) In the section IP Address Group, add a predefined IP address group; from the field **IP address file**, click **Browse** and navigate to the desired text file.
The file format should be one IP address per line, and its maximum size is 10 MB.

Because mail from the Trusted IP Addresses group bypasses additional email analysis, that group should not be entered in the Allow Access List. See *Managing domain and IP address groups*.

5) Manually add IP address entries; in the field **IP address**, enter an individual IP address and click **>**.
The information is added to the Added IP Addresses box on the right.

Note

Any changes made here to an IP address group are reflected on the page **Settings > Inbound/Outbound > IP Groups**.

6) Export the access list to a location in your network; click **Export**.

7) Delete an IP address from the Added IP Addresses list; select the IP address and click **Remove**.

8) Click **OK**.
The Connection Control page displays with the newly configured IP addresses.

9) Click **OK**.
The settings are saved.

Related concepts
Managing domain and IP address groups on page 99

Related tasks
Editing an IP address group on page 103

DomainKeys Identified Mail (DKIM) integration

The DomainKeys Identified Mail (DKIM) functionality provides an email authentication method to help ensure that a message is not modified while it is in transit from an organization's protected domains. The implementation depends on a set of keys (private and public), which a recipient domain can use to verify the sender domain. DKIM settings are configured on the page **Settings** > **Inbound/Outbound** > **DKIM Settings**.

A DKIM integration has the following components:

- Email signing
- Email verification

For the signing element, a private key resides in the mail transfer agent, providing a digital signature that is added to the header of each message sent from a protected domain. A public key is generated and published in the DNS as a text record that is used by a recipient mail system in the verification process.

A signing rule associates specified sender domains with a private and public key set.

Configuring a DKIM signing key

A signing key provides a digital signature for email sent from your protected domains. You may create a signing (private) key, import a key from a local directory, or export a key to a local directory.

The signing keys table includes the following information about each key:

Signing Key Item	Description
Key Name	Name of the signing key. Click the key name to open the Edit Signing Key page.

Signing Key Item	Description
Key Size (bits)	Number of bits in the signing key. The only option for key length is 1024 bits. See this Knowledge Base article to increase key length to 2048.
Rule Name	Name of the rule with which the signing key is associated.
Public Key	Link that opens a View Public Key box, which displays the public key text record.

Configure the number of entries per page

From the pull-down menu **Per page**, select the number of signing key entries per page, between 25 and 100.

Search entries by keyword

Steps

1) From the top right, enter a search term in the text field.

2) Click **Search**.
Search results display in the section DKIM Signing Keys.

3) Clear search results; click **Show all keys**.
The search field clears and all DKIM signing keys display.

Adding a key

Use the following steps to create a DKIM signing key on the page **Settings** > **Inbound/Outbound** > **DKIM Settings**:

Steps

1) From the section DKIM Signing Keys, click **Add**. The Add Signing Key page displays.

2) In the text field **Key name**, enter a name for your key.

3) Select one of the following options for creating your key:
   - **Generate key to create the private key**
     This is the default. The only option for key length is 1024 bits. See this Knowledge Base article to increase key length to 2048.
   - **Private key to enter a key you have already created**
     Paste the key in the entry box.

4) Click **OK**.
The key is saved and displays in the section DKIM Signing Keys.

Deleting a key

From the section DKIM Signing Keys, mark the check box for a key and select **Delete**.

The key is deleted. A key cannot be deleted if it is currently in use by a signing rule.

Editing a key

Steps

1) From the section DKIM Signing Keys, click the name of a key.
The Edit Signing Key page displays. The current private key displays in the text field.

2) Generate a new key; click the button **Generate Key**.
A new key is generated and displays in the text field. The only option for key length is 1024 bits. See this Knowledge Base article to increase key length to 2048.

3) Click **OK**.
The key is saved and displays in the section DKIM Signing Keys.

Importing or exporting a key

DKIM signing keys can be imported and exported on the page **Settings** > **Inbound/Outbound** > **DKIM Settings**.

Import a DKIM signing key

Steps

1) From the section DKIM Signing Keys, click **Import**. The Import Key dialog box displays.

2) Click **Browse** and navigate to the desired key file.

3) Click **Open**.
The Import Key dialog box displays.

4) On the Import Key dialog box, click **Import**.
The key is imported. Duplicate key files cannot be imported.

Export a DKIM signing key

Steps

1) From the section DKIM Signing Keys, mark the check box for the key and click **Export**.
   A dialog box displays.

2) Navigate to the desired directory location and click **Save**.
   The key is exported.

Creating a DKIM signing rule

A DKIM signing rule associates a private/public key pair with a set of domains and email addresses. Signing rule options let you determine which message headers to sign, how much of the message body to sign, and whether to attach additional signature tags for such items as signature date/time or expiration time. Signing rules are configured on the page **Settings** > **Inbound/Outbound** > **DKIM Settings**.

The signing rules table includes the following information about each rule:

Signing Rule Item	Description
Rule Name	Name of the signing rule. Click the rule name to open the Edit Signing Rule page.
Domain	Domain name to which the signing rule applies.
Selector	Name component in addition to the domain name used in the DNS query. A given domain may have multiple selectors (e.g., for location or organization division).
Signing Key Name	Name of the signing key associated with this rule.
DNS Text Record	Link that opens a Generate DNS Text Record dialog box. See *Generating a DNS text record (public key)*.
Test Rule	Link to test whether the signing rule is valid. A successful test must be performed before a rule can be enabled.
Status	Indicator of signing rule status (i.e., enabled or disabled). A rule must be enabled in order to take effect.

Configure the number of entries per page

From the pull-down menu **Per page**, select the number of signing rule entries per page, between 25 and 100.

Related concepts
Generating a DNS text record (public key) on page 128

Search entries by keyword

Steps

1) From the top right, enter a search term in the text field.

2) Click **Search**.
   Search results display in the section DKIM Signing Rules.

3) Clear search results; click **Show all rules**.
   The search field clears and all DKIM signing rules display.

Adding a signing rule

Use the following steps to create a DKIM signing rule on the page **Settings** > **Inbound/Outbound** > **DKIM Settings**:

Steps

1) From the section DKIM Signing Rules, click **Add**. The Add Signing Rule page displays.

2) In the text field **Rule name**, enter a name for your rule.

3) Enter the name of the domain to which this signing rule applies.

4) (*Optional*) Include the identity of the user or agent for whom the message is signed; mark the check box **Include user identifier**.

5) (*Optional*) In the text field **User identifier**, enter the user identifier.
   This field is not enabled if the check box **Include user identifier** is not marked.

6) In the text field **Selector**, enter the domain name selector.
   A selector is a name component provided in addition to the domain name used in the DNS public key query. A given domain may have multiple selectors.

7) From the pull-down menu **Signing key**, select the signing key to associate with this rule from the list of existing keys.

8) Click **Advanced Options**.

A box displays with additional optional rule settings:

- From the pull-down menu **Algorithm**, select an encryption algorithm. Options include RSA-SHA-1 or RSA-SHA-256. The default is RSA-SHA-1.
- In the section Canonicalization, specify a canonicalization method for message header and body. The canonicalization process prepares a message header and body before email is signed. Canonicalization is required because email processing may introduce minor changes to a message.

  The following header and body changes are made, based on the selection of **Simple** or **Relaxed**:

	Simple (default)	Relaxed
Message Header	No header changes made	■ Header names changed to lowercase ■ Header line breaks removed ■ Linear white spaces (including tabs and carriage returns) reduced to a single space ■ Leading and trailing spaces stripped
Message Body	Empty lines at end of body stripped	■ Empty lines at end of message body stripped ■ Linear white spaces (including tabs and carriage returns) reduced to a single space ■ Trailing spaces stripped

- From the list of standard headers, indicate the message headers to sign.
- In the field **Additional headers**, include other headers as a comma-separated list.
- Specify whether to sign the entire message body or only a portion.
  For the latter selection, enter the maximum number of Kbytes to be signed. The default is 1024.
- Select any optional signature tags for the signing rule:
  - **t** lets you add a signature creation timestamp.
  - **x** lets you specify a signature expiration time in seconds. The default is 3600 seconds.
  - **z** adds the list of signed header fields to the signature.

9) From the pull-down menu **Signing rule options**, select either **Sign email messages** or **Do not sign email messages**.

Next, create a list of email addresses to which this option applies.

- For example, if you select **Sign email messages**, then email from the addresses in the list is signed. Email from other addresses is not signed.
- If you select **Do not sign email messages**, then email from the addresses in the list is not signed, and email from all other users is signed.

Remove an email address from the list by selecting it and clicking **Remove**.

10) Click **OK**.
The settings are saved.

Importing or exporting a rule

DKIM signing rules can be imported or exported on the page **Settings** > **Inbound/Outbound** > **DKIM Settings**.

Import a DKIM signing rule

Steps

1) From the section DKIM Signing Rules, click **Import**. The Import Rule dialog box displays.

2) Click **Browse** and navigate to the desired key rule file.

3) Click **Open**.

4) On the Import Rule dialog box, click **Import**.
The key rule is imported. Duplicate key rule files cannot be imported.

Export a DKIM signing rule

Steps

1) From the section DKIM Signing Rules, mark the check box for the rule and click **Export**.
A dialog box displays.

2) Navigate to the desired directory location and click **Save**.
The rule is exported.

Generating a DNS text record (public key)

Generate a public key for a rule from the DKIM Signing Rules table by clicking the link for the desired rule in the DNS Text Record column. A Generate DNS Text Record box that contains the new public key appears.

View a public key by clicking **View** for a particular private key in the DKIM Signing Keys table Public Key column.

Testing a rule

Ensure that you have created a valid rule by clicking the **Test** link in the **Test Rule** column of the DKIM Signing Rules table for the desired signing rule. The test performs a DNS lookup query. You receive confirmation of success or failure when the test is complete.

You must have performed a successful rule test before a rule can be enabled.

Enabling DKIM verification

The DKIM validation method uses the message header digital signature to associate a domain name with the email. The DKIM signature verification function retrieves signer information, including the public key, from the DNS. This signer information is analyzed and verified to determine message legitimacy.

Enable DKIM verification on the page **Settings** > **Inbound/Outbound** > **DKIM Settings**, in the section DomainKeys Identified Mail (DKIM) Verification. Mark any or all of the following check boxes to activate DKIM verification:

- **Enable DomainKeys Identified Mail (DKIM) verification for inbound messages**
- **Enable DomainKeys Identified Mail (DKIM) verification for outbound messages**
- **Enable DomainKeys Identified Mail (DKIM) verification for internal messages**

By default, these check boxes are not marked.

Configure a custom content policy filter to scan for a DKIM signature in the message header, along with a filter action to take when a message header triggers the filter. See *Custom content*.

Related concepts
Custom content on page 190

Domain-based Message Authentication, Reporting and Conformance (DMARC) validation integration

Domain-based Message Authentication, Reporting and Conformance (DMARC) uses the results of its Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) validation processes, along with the sender domain's DMARC policy, to determine message disposition. Published in the sender's DNS record, a DMARC policy includes the sender's affirmation that its email is protected by SPF and DKIM validation, and provides instructions for handling mail that does not pass either of those checks on the recipient's end. A mechanism for reporting DMARC results is also provided.

SPF and DKIM analyses enabled and configured in the Email Security module are independent of DMARC verification. SPF checks are configured on the page **Settings** > **Inbound/Outbound** > **Relay Control**, whereas DKIM validation is configured on the page **Settings** > **Inbound/Outbound** > **DKIM Settings**. If either SPF or DKIM analysis is enabled in the Forcepoint Security Manager, DMARC can use the results in its own verification analysis.

Assuming a message is not dropped for failing either the SPF or DKIM check, DMARC validation comprises the following steps:

1) Extract the sender domain in the email header "From" field.

2) Query the DNS to determine if a DMARC policy exists for this domain.
   - If a policy is found, retrieve the policy and continue with step 3.
   - If a policy is not found, end the DMARC process.

3) Perform DKIM validation checks.

4) Perform SPF validation checks.

5) Perform DMARC identifier checks to determine if the sender information in the message aligns with what the recipient knows about that sender as a result of the SPF and DKIM analyses.

6) After completing the DMARC analysis, apply the DMARC policy to the message.

When you enable DMARC validation, a reporting mechanism is also included to provide the sender with information about the number of messages received from that sender domain and the results of the recipient's validation checks. Reports are sent to the email address specified in the sender domain's DNS text record via the RUA (reporting URL of aggregate reports) tag.

If SPF and DKIM are not enabled in the Email Security module, DMARC performs these checks. In this case, message disposition is determined only by the DMARC policy. A message is not rejected based on the individual SPF or DKIM analysis results.

For optimal protection, both SPF and DKIM validation settings should be configured and enabled on your email protection system, along with DMARC. See *Configuring relay control options* and *DomainKeys Identified Mail (DKIM) integration*.

Configure DMARC verification on the page **Settings** > **Inbound/Outbound** > **DKIM Settings**. Mark the check box for any or all of the following options:

- **Enable DMARC verification for inbound messages**
- **Enable DMARC verification for outbound messages**
- **Enable DMARC verification for internal messages**

Related concepts
DomainKeys Identified Mail (DKIM) integration on page 122

Related tasks
Configuring relay control options on page 134

True source IP detection

True Source IP detection uses message header information and the number of network hops to an email appliance to determine the IP address of the first sender outside the network perimeter. This feature allows Connection Control techniques (such as reverse DNS lookup and reputation checks) to be applied effectively to sender information, even when the appliance is downstream from a firewall or an internal mail relay.

Define direct relays and network edge locations to determine whether True Source IP detection is performed. A direct relay is the network device that connects directly to the email appliance. All mail from a direct relay device is subject to True Source IP Detection. A network edge is the network device that connects directly to the Internet (e.g., a firewall).

If your subscription includes Forcepoint Email Security Hybrid Module, you can use True Source IP detection with email hybrid service analysis. An Email Hybrid Service IP Group is created based on information entered during a successful email Hybrid Module registration. The IP group appears in the direct relay IP address list on the page **Settings** > **Inbound/Outbound** > **True Source IP**. Although this IP group cannot be edited directly,

its content is modified whenever you change an email hybrid service IP address (**Settings** > **Hybrid Service** > **Hybrid Configuration**).

Note

If registration is not successful, the Email Hybrid Service IP Group is empty.

Mark the check box **Use True Source IP Detection with email hybrid service analysis** to enable True Source IP detection with hybrid service and display the Email Hybrid Service IP Group in the direct relay IP address list. The Email Hybrid Service IP Group does not appear if the check box is not marked.

Configuring Direct Relay and Network Edge Devices for True Source IP Detection

Configure your direct relay and all network edge devices on the page **Settings** > **Inbound/Outbound** > **True Source IP** as follows:

Steps

1) Click **Add**.
   The Add Direct Relay IP Address/IP Group page displays.

2) Enter the IP address for the direct relay device to the email appliance, or specify the existing IP group to use for your direct relay.
   By default, the direct relay hop number is 1, because it is the closest network device to the email appliance.

   Important

   The IP address or group that you enter here must not already be defined in the Trusted IP Addresses group (**Settings** > **Inbound/Outbound** > **True Source IP**) or appear in the connection control Allow Access List (**Settings** > **Inbound/Outbound** > **Connection Control**).

3) In the field **Check for header**, enter header text to match for true source IP detection.
   If this field is empty, the message Received field is analyzed for the true source IP.

4) Add the network edge device IP address and hop number to the email appliance; click **Add Network Edge**.

5) Click **OK**.
   The settings are saved.

Enforced TLS connections

The page **Settings** > **Inbound/Outbound** > **Enforced TLS Connections** is used to specify that connections to or from a specific IP or domain group use mandatory

Transport Layer Security (TLS) and determine the security level used by that connection.

Functionality is used to define connection directions relative to the email SMTP server. Incoming connections are those from a protected or external domain or IP address group to the email protection system. Outgoing connections are those from the email system to a protected or external domain or IP address group.

After you define a group, you can change its order in the incoming or outgoing direction list. Select the group by marking its associated check box and use the **Move Up** or **Move Down** button to modify list order.

Delete a group by marking the check box and clicking **Delete**. You may configure up to 32 incoming or outgoing connections.

Add an incoming or outgoing connection for which to use TLS

Steps

1) Navigate to the page **Settings** > **Inbound/Outbound** > **Enforced TLS Connections**.

2) Click **Add**.
   The Add Incoming Connection page displays.

3) In the text field **Name**, enter a name for your enforced TLS connection.

4) From the pull-down menu **Priority order**, select a priority order for the connection.

5) Specify the security level for the connection. Security level options include the following:
   - **Encrypt**, the minimum enforcement level, used in all security levels This security level is the only option available for incoming connections.
   - **Encrypt and check CN**, validation of a certificate's common name
   - **Verify**, validation that the certificate is from a trusted CA
   - **Verify and check CN**, validation of the certificate's common name and that the certificate is from a trusted CA

   Important

   To use the two "verify" options, you must have imported a trusted CA certificate. See *Managing Transport Layer Security (TLS) certificates*.

6) Select one of the following connection encryption strength options:
   - Medium, which involves the use of cipher suites that use 128-bit encryption
   - High, which includes most cipher suites with key lengths larger than 128 bits

7) Define the IP address or domain group subject to forced TLS connection; select one of the following options:
   - **Any (for all connections)**
     This option applies to any connection, regardless of IP or domain address.
   - **IP address group**
     Select an existing IP address group in the pull-down menu or create a new group using **Add New IP Group**.
   - **Domain address group**
     Select an existing domain address group in the pull-down menu or create a new group using **Add New Domain Group**.

8) Click **OK**.
   The settings are saved.

Related concepts
Managing Transport Layer Security (TLS) certificates on page 106

Controlling directory harvest attacks

A directory harvest attack is used by questionable sources to gain access to an organization's internal email accounts. A directory attack not only consumes large amounts of system resource but also, through the acquisition of email accounts, creates spam problems for email end users. With directory attack prevention settings, you can limit the maximum number of messages and connections coming from an IP address over a given time period. These settings are configured on the page **Settings** > **Inbound/Outbound** > **Directory Attacks**.

Steps

1) Navigate to the page **Settings** > **Inbound/Outbound** > **Directory Attacks**.

2) Enable the directory harvest attack prevention function; mark the check box **Limit the number of messages/connections per IP every**.

3) From the pull-down menu, set the time period, from 1 second to 60 minutes. The default is 60 seconds.

4) Set the maximum number of messages allowed from an individual IP address during the specified time period.
   The default is 30.

5) Set the maximum number of connections allowed from an individual IP address during the specified time period.
   The default is 30.

6) If you have enabled the directory attack prevention option, you can also enable settings to block an IP address when a specific set of recipient conditions occurs; mark the check box **Block the IP address for** and enter the time interval during which to block an IP address.
   The default is 3 hours.

7) Enter the conditions for blocking the IP address:
   - Maximum number of message recipients. The default is 5.
   - Maximum percentage of invalid addresses among the recipients. The default is 50%.

   When these recipient limitations are exceeded, the connection is dropped automatically.

   This option is available only when the recipient validation option is used (see *Adding user authentication settings*).

8) Click **OK**.
   The settings are saved.

Related tasks
Adding user authentication settings on page 104

Configuring relay control options

Functionality on the page **Settings** > **Inbound/Outbound** > **Relay Control** is used to prevent the unauthorized use of your mail system as an open relay by limiting the domains and IP address groups for which your server is allowed to relay mail.

Protected domains are defined on the page **Settings** > **Users** > **Domain Groups**. Trusted IP address groups are defined on the page **Settings** > **Inbound/Outbound** > **IP Groups**.

Configure relay control settings on the page **Settings** > **Inbound/Outbound** > **Relay Control** as follows:

Steps

1) In the section Inbound Relay Options, enable Sender Policy Framework (SPF) checking by marking the check box **Enable SPF**.
   This option is enabled by default.

2) Mark the relevant check boxes to configure the SPF check function to reject mail for the following results:
   - **Fail**: The domain owner's SPF record does not authorize the sender host machine to send email for the domain.
   - **SoftFail**: The domain owner's SPF record allows the sender host machine to send email for this domain, even though the host is not explicitly authorized to do so.
   - **Neutral**: The domain owner's SPF record makes no statement as to whether the sender host machine is authorized to send email for the domain.
   - **None**: The lack of definitive SPF information prevents an SPF check (e.g., an SPF record does not exist).
   - **PermError**: A permanent error occurs (e.g., the SPF record has an invalid format).
   - **TempError**: A transient error occurs (e.g., a DNS timeout). These options are not marked by default.

3) In the Bypass SPF Option box, specify a sender domain group for which SPF settings are bypassed.
   a) Mark the check box **Bypass SPF validation for senders in the following domain group**
   b) Select a sender domain from the pull-down menu **Domain group**

4) In the section Outbound Relay Options, select the relay setting for senders in protected domains when SMTP authentication is not required; **Allow relays only for senders from trusted IP addresses** or **Allow all outbound relays**.
   The default setting is Allow relays only for senders from trusted IP addresses. Allowing all outbound relays may create a security vulnerability in your system.
   You must use the default setting if you use SMTP authentication.
   Mark the check boxes for the IP groups for which to allow relays.

5) In the section Internal Relay Options, select the relay setting for mail between protected domains when SMTP authentication is not required; **Allow relays only for senders from trusted IP addresses** or **Allow all internal relays**.
   The default setting is Allow relays only for senders from trusted IP addresses. Allowing all internal relays may create a security vulnerability in your system.
   The default setting is required if you use SMTP authentication.

6) Click **OK**.
   The settings are saved.

Configuring delivery routes

Configure delivery routes on the page **Settings** > **Inbound/Outbound** > **Mail Routing**. You can create the following types of message routes:

- *User directory-based routes*
- *Domain-based routes*

Change the order of a user directory- or domain-based route by marking its associated check box and using the **Move Up** or **Move Down** buttons.

Related concepts
User directory-based routes on page 136
Domain-based routes on page 138

Copying a route

Use the following steps to copy a route on the page **Settings** > **Inbound/Outbound** > **Mail Routing**:

Steps

1) Select a route in the route list by marking the check box next to its name.

2) Click **Copy**.
   A new route appears in the route list, using the original route name followed by a number in parentheses. The number added indicates the order that copies of the original route are created (1, 2, 3, etc.).

3) Click the new route name to edit route properties as desired.

Removing a route

To remove a route, select the route by marking the check box next to its name and click **Delete**.

The default domain-based route cannot be deleted.

User directory-based routes

Delivery routes based on user directory entries are examined first for a match with an email message recipient. Domain group entries are validated against the selected user directory to determine whether email will be delivered via a specified route.

Adding a user directory-based route

Use the following steps to add a user directory-based delivery route on the page **Settings** > **Inbound/Outbound** > **Mail Routing**:

Steps

1) Click **Add**.
   The Add User Directory-based Route page displays.

2) In the field **Name**, enter a name for your new route. Length must be between 4 and 50 characters.

3) From the pull-down menu **Route order**, select an order number to determine the scanning order of the route.

4) From the pre-defined domains in the pull-down menu **Domain group**, select a destination domain.
   The default is Protected Domain. Information about the domain group appears in the Domain details box.

   To edit your selected domain group, click **Edit** to open the Edit Domain Group page. See *Editing a domain group*.

5) In the section User Directories, select the user directories to use to define your route.

Select from the list of currently defined user directories and click the arrow button to move them to the Selected User Directories box.

ESMTP user directories are not included in the directory list. ESMTP user directories cannot be used for user directory-based routes.

- To add a new user directory, click **Add user directory**.
  The Add User Directory page displays. See *Adding and configuring a user directory*.
- To remove a user directory from the Recipients list, select it and click **Delete**.

6) In the section Delivery Method, select the delivery method:

- Based on the recipient's domain (using the Domain Name System [DNS]).
- Based on SMTP server IP address designation (using smart host). If you select this option, an SMTP Server List opens:

  a) Click **Add** to open the Add SMTP Server dialog box

  b) Enter the SMTP server IP address or hostname and port

  c) Mark the check box **Enable MX lookup** to enable the MX lookup function

  Important

  If you entered an IP address in the previous step, the MX lookup option is not available.

  If you entered a hostname in the previous step, this option is available.

  - Mark the **Enable MX lookup** check box for message delivery based on the hostname MX record.
  - If you do not mark this check box, message delivery is based on the hostname A record.

  d) Enter a preference number for this server, from 1–65535. The default value is 5.
  If a single route has multiple defined server addresses, mail is delivered in order of server preference. When multiple routes have the same preference, round robin delivery is used.

  You may enter no more than 16 addresses in the SMTP Server List.

7) In the section Delivery Options, select any desired security delivery options.

a) Ensure email traffic uses opportunistic TLS protocols; mark the check box **Use opportunistic Transport Layer Security (TLS)**.

b) Ensure that users supply credentials; mark the check box **Require authentication**
Enter the appropriate user name and password in the Authentication Information box. You must use the SMTP server IP address delivery method for users to authenticate.

8) Click **OK**.

The settings are saved and the new route displays under User Directory-based Routes.

Related tasks

Editing a domain group on page 101
Adding and configuring a user directory on page 92

Domain-based routes

Delivery routes based on domain groups are examined after defined user

directory-based routes for a match with an email message recipient. If a match is made with a user directory-based route, domain-based routes are not examined for matches.

Important

The Protected Domain group defined on the page **Settings** > **Users** > **Domain Groups** should not be used to configure delivery routes if you need to define domain-based delivery routes via multiple SMTP servers. Create domain groups that contain subsets of the Protected Domain group for mail routing purposes.

Adding a domain-based route

Use the following steps to add a domain-based delivery route on the page **Settings** > **Inbound/Outbound** > **Mail Routing**:

Steps

1) Click **Add**.
   The Add Domain-based Route page displays.

2) In the field **Name**, enter a name for your new route.

3) From the pull-down menu **Route order**, select an order number to determine the route's scanning order.

4) From the pre-defined domains in the pull-down menu **Domain group**, select a destination domain.
   Default is Protected Domain. Information about the domain group appears in the Domain details box.

   To edit your selected domain group, click **Edit** to open the Edit Domain Group page. See *Editing a domain group*.

5) Select the delivery method:
   - Based on the recipient's domain (using the Domain Name System [DNS])
   - Based on SMTP server IP address designation (using smart host) If you select this option, an SMTP Server List opens.
     a) Click **Add.**The Add SMTP Server dialog box displays.
     b) Enter the SMTP server IP address or hostname and port.
     c) Mark the check box **Enable MX lookup** to enable the MX lookup function.

Important

If you entered an IP address in the previous step, the MX lookup option is not available.

If you entered a hostname in the previous step, this option is available.

- Mark the check box **Enable MX lookup** for message delivery based on the hostname MX record.
- If you do not mark this check box, message delivery is based on the hostname A record.

     d) Enter a preference number for this server (from 1–65535; default value is 5).
     If a single route has multiple defined server addresses, mail is delivered in order of server preference. When multiple routes have the same preference, round robin delivery is used.

You may enter no more than 16 addresses in the SMTP Server List.

6) Select any desired security delivery options:
   a) Enable email traffic to use opportunistic TLS protocol; select **Use opportunistic Transport Layer Security (TLS)**.
   b) Ensure that users supply credentials; select **Require authentication**. Enter the appropriate user name and password in the Authentication Information box. You must use the SMTP server IP address delivery method for users to authenticate.

Related tasks

Editing a domain group on page 101

Rewriting email and domain addresses

An email envelope recipient address can be rewritten to redirect message delivery to a different address. Envelope sender and message header addresses can also be rewritten to mask address details from message recipients. Configure address rewriting for inbound, outbound, and internal email on the page **Settings** > **Inbound/Outbound** > **Address Rewriting**. Email or domain addresses in an address rewrite list can be added, exported, or deleted.

Adding recipient address rewrite entries

On the page **Settings** > **Inbound/Outbound** > **Address Rewriting**, use the Inbound Messages tab to specify recipient address rewrite entries for inbound messages and the Outbound and Internal Messages tab for outbound or internal message redirection.

The email envelope recipient address is rewritten based on the entries in the Envelope Recipient Address Rewrite List.

Steps

1) On the page **Settings** > **Inbound/Outbound** > **Address Rewriting**, click the **Inbound Messages** tab or the **Outbound and Internal Messages** tab to display the settings.

2) From the Envelope Recipient Address Rewrite List, click **Add**. The Add Recipient Email or Domain Address page displays.

3) Enter your addresses in one of two ways:

   - Mark the check box **Individual email address or domain rewrite entry** and enter the original recipient address and the rewrite address in the appropriate entry fields.
     An email address entry may have multiple rewrite entries, with each entry separated by a space. A domain address may have only one rewrite entry.
   - If you have an existing email or domain address rewrite entry file, mark the check box **Email address or domain rewrite entry file** and browse to the file File size may not exceed 10 MB.

4) Click **OK**.
   Your entries appear in the Envelope Recipient Address Rewrite List.

Adding message header address rewrite entries

On the page **Settings** > **Inbound/Outbound** > **Address Rewriting**, use the Inbound Messages tab to add message header address rewrite entries for inbound messages and the Outbound and Internal Messages tab for outbound or internal message address masking. The email envelope sender address and message header addresses are rewritten based on the entries in the Envelope Sender and Message Header Rewrite List.

Steps

1) On the page **Settings** > **Inbound/Outbound** > **Address Rewriting**, click the **Inbound Messages** tab or the **Outbound and Internal Messages** tab to display the settings.

2) From the Envelope Sender and Message Header Rewrite List, click **Add**. The Add Sender Email or Domain Address page displays.

3) Enter your addresses in one of two ways:
   - Mark the check box **Individual email address or domain rewrite entry** and enter the original sender address and the rewrite address in the appropriate entry fields.
     Each email or domain address entry may have only one rewrite entry.
   - If you have an existing email or domain address rewrite entry file, mark the check box Email address or domain rewrite entry file and browse to the file.
     File size may not exceed 10 MB.

4) Click **OK**.
   Your entries appear in the Envelope Sender and Message Header Rewrite List.

Exporting address rewrite entries

All email or domain addresses in an address rewrite list can be exported to a text file.

Steps

1) On the page **Settings** > **Inbound/Outbound** > **Address Rewriting**, click the **Inbound Messages** tab or the **Outbound and Internal Messages** tab to display the settings.

2) Mark the check box for the list to be exported and click **Export**.

3) From the Save As dialog box, select a directory to which to export the text file and click **Save**.
   The selected address rewrite list is exported. A success message displays at the top of the Address Rewriting page.

Deleting address rewrite entries

Email or domain addresses in an address rewrite list can be deleted individually or in bulk.

Steps

1) On the page **Settings** > **Inbound/Outbound** > **Address Rewriting**, click the **Inbound Messages** tab or the **Outbound and Internal Messages** tab to display the settings.

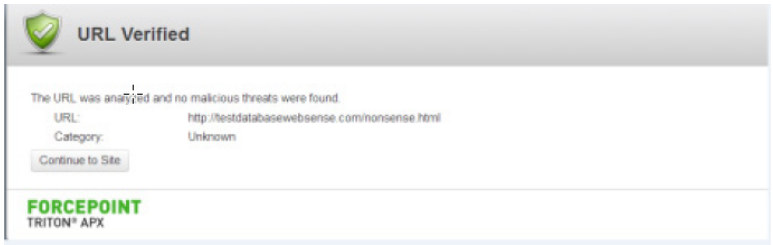
2) Mark the check boxes for any entries to be deleted and click **Delete**.
   The selected entries are deleted. A success message displays at the top of the Address Rewriting page.

URL Sandbox

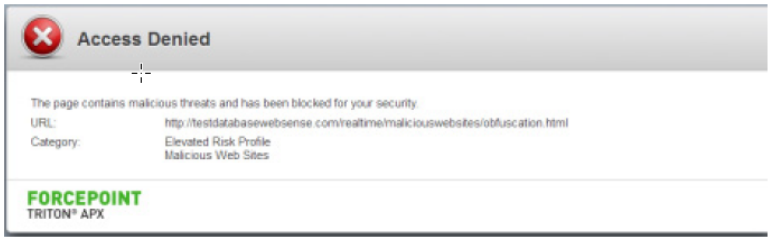
The URL sandbox function provides real-time analysis of uncategorized URLs that are embedded in inbound email. When a user clicks an uncategorized URL, a notification message prompts the user to initiate URL

analysis, because the link may not be safe. If the user chooses not to analyze the URL, the requested web page is not accessible.

If analysis determines that the link is not malicious, the user receives a notification that lists the URL and category or categories of the page, and clicks **Continue to site**.

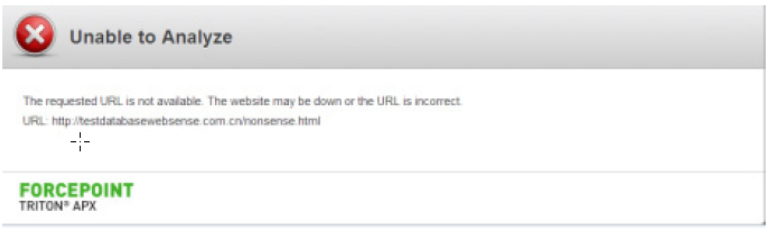


If the link is deemed malicious or if applicable policy does not allow a user to access uncategorized web pages, the user is notified that the site is blocked:



The user may also be notified in the following cases:

- If the function cannot access the requested page due to an inaccessible server or because the link is incorrect.
- If the protocol is not supported. Supported protocols are HTTP, HTTPS, and FTP. If you have selected the option **Allow the recipient to follow links with an unsupported protocol**, the user can proceed to view the page if desired; otherwise, the user cannot access the page.



Your subscription must include the Forcepoint Email Security Hybrid Module. URL sandbox capability is available only after the email hybrid service is successfully registered and enabled. See *Email hybrid service configuration*.

The URL sandbox configuration settings include three components:

- Default settings that apply to any recipient not covered by specific settings
- Recipient-specific settings that apply to an individual domain or email address
- List of domains to which sandbox settings do not apply

Related concepts

Email hybrid service configuration on page 62

Configuring URL Sandbox Settings in Forcepoint Email Security

Use the page **Settings** > **Inbound/Outbound** > **URL Sandbox** to configure the URL sandbox feature:

Steps

1) In the section Default Settings, specify the settings that apply to any recipient not covered by recipient-specific settings:
   a) Activate the URL sandbox function; mark the check box **Analyze suspicious URLs**.
   By default, the check box is not marked.
   b) If the URL sandbox is enabled, allow users to click unclassified URL links; mark the check box **Allow the recipient to follow links to unclassified URLs**.
   By default, the check box is not marked.
   c) Allow users to click a link that may redirect to a site with an unsupported protocol; mark the check box **Allow the recipient to follow links with an unsupported protocol**.
   d) Replace the original URL with other text; enter the string in the entry field below the check box.
   Leave this field blank to keep the original URL.
2) Use the section Recipient-specific Settings to add custom sandbox settings for individual domain or email addresses:
   a) Create sandbox settings for a particular group of addresses; click **Add**.
   b) In the Recipient Email/Domain Address List, enter comma-separated email or domain addresses to which the settings should apply.
   Wildcards are not permitted.
   c) Activate the URL sandbox function for these addresses; mark the check box **Analyze suspicious URLs**.
   By default, the check box is not marked.
   d) If the URL sandbox is enabled, allow the specified users to click unclassified URL links; mark the check box **Allow the recipient to follow links to unclassified URLs**.
   By default, the check box is not marked.
   e) Allow users to click a link that may redirect to a site with an unsupported protocol; mark the check box **Allow the recipient to follow links with an unsupported protocol**.
   f) Replace the original URL with other text; enter the string in the entry field below the check box.
   Leave this field blank to keep the original URL.

3) Enable the sandbox to examine URLs even if they appear in a message that contains the digital signature of a trusted sender; at the bottom of the section URL Sandbox, mark the check box **Analyze suspicious URLs that appear in digitally signed email**.

   By default, the check box is not marked.

4) In the entry field above the check box, enter the URL domains that should bypass the URL sandbox.

   Do not use wildcards, and separate multiple entries with a comma.

5) Click **OK**.

   The settings are saved.

   To delete a set of recipient-specific settings, mark the check box next to the address list and click **Delete**.

Phishing detection and education

Phishing involves an attempt to obtain personal information like passwords or credit card numbers via email while pretending to be a trusted entity. For example, an email message that purports to be from a known financial institution or popular web site may actually be an attempt to steal personal information.

The phishing detection and education function provides cloud-based analysis of an inbound message for phishing email characteristics. To use the phishing detection and education feature, your subscription must include the Forcepoint Email Security Hybrid Module. It is necessary to successfully register with the email hybrid service before you configure phishing detection and education capabilities. See *Email hybrid service configuration*.

Functionality requires rules to be defined that determine which sender domains are analyzed and how a suspected phishing email is handled. Suspect email may be treated the same as spam (blocked and saved to a spam queue) or be replaced by a message that educates the recipient about phishing attack email.

Dashboard charts and presentation reports can be configured to display suspected phishing attack data.

The page **Settings** > **Inbound/Outbound** > **Phishing Detection** includes the following tabs for configuring phishing detection:

- **Phishing Rules**, which contains a list of all your phishing rules. A default rule applies to domains that are not included in any other defined rule. See *Adding a phishing detection rule*
  The default rule cannot be deleted. Delete any other phishing rule from the list by marking its associated check box and clicking **Delete**, then clicking **Save to Cloud Service**.

  .
- **Phishing Education Pages**, which contains a list of all the education pages you have defined. A default page applies when a custom page is not specified for a phishing rule. See *Creating a phishing education page*. Delete any phishing education page (except the default page) from the list by marking its associated check box and clicking **Delete**. You may not delete a page that is being used by a phishing rule.

  Click **Save to Cloud Service** only if you receive an error message regarding a synchronization issue with the cloud service.

Related concepts

Email hybrid service configuration on page 62
Creating a phishing education page on page 146

Related tasks
Adding a phishing detection rule on page 145

Adding a phishing detection rule

Use the following steps to configure a phishing detection rule:

Steps

1) On the Phishing Rules tab, click **Add Rule**. The Add Rule page displays.

2) In the field **Phishing rule name**, enter a name for the rule.

3) In the field **Domain names**, specify the domains to which this rule applies. Separate multiple domains with a semicolon.

4) Select a phishing action option for this phishing rule:
   - **Treat as spam**:
     Selection quarantines the suspected phishing message.
   - **Educate**:
     Replace the URL with a link to the selected phishing education page and deliver the message.

5) Configure individual user exceptions to the phishing rule.
   For example, you may want to select a different action for a particular user or group or present a different phishing education page for that user or group.

   a) Click **Add User Exception**.
      The Add User Exception dialog box displays.

   b) In the text field **Description**, enter a brief description of this exception.

   c) In the text field **Email addresses**, specify the email addresses for the users or groups to whom this exception applies.

   d) Select a phishing action option for this user exception:
      - **Treat as spam**
        Selection quarantines the suspected phishing message.
      - **Educate**:
        Replace the URL with a link to the selected phishing education page and deliver the message.

   e) Click **Add**.

6) Click **OK**.
   The phishing rule is saved.

7) On the Phishing Rules tab, click **Save to Cloud Service**.
The phishing detection settings are sent to the email hybrid service.

Creating a phishing education page

Create a new phishing education page by copying an existing page and renaming it. You can also customize the default message template to suit your needs. A default page is used when a custom page is not specified for a phishing rule.

Copy an existing phishing education page

Steps

1) On the Phishing Education Pages tab, click **Copy Page**.

2) In the text field Page name, enter a name for the phishing education page copy.

3) Click **OK**.

Create a custom phishing education page

Steps

1) On the Phishing Education Pages tab, click **Add Page**. The Add Phishing Education Page screen displays.

2) Enter a name and description for the phishing education page.

3) In the text field **Page title**, specify a title for the page. This title appears as the browser window name.

4) In the Phishing Education Page Editor, specify the desired text and images.

5) Click **OK.**

Note

If you receive an error message regarding a synchronization problem with the cloud service, click **Save to Cloud Service** on the tab Phishing Education Pages to send your phishing education page settings to the email hybrid service.

Managing message queues

The page **Main** > **Message Management** > **Message Queues** is used to view, create, and configure message queues. You can also modify the following default queues:

- virus
- spam
- exception
- encryption-fail
- decryption-fail
- archive
- secure-encryption
- data-security
- url-analysis
- attachment

All blocked messages across all queues are accessed on the page **Main** > **Message Management** > **Blocked Messages** (see *Managing the blocked message queue*). Temporarily delayed messages can be viewed on the page **Main** > **Message Management** > **Delayed Messages** (see *Managing the delayed message queue*).

Related concepts

Managing the blocked message queue on page 152
Managing the delayed message queue on page 155

Message queues list

The following table details the information available in the Queue List on the Message Queues page.

Parameter	Description
Queue Name	Displays the name of the queue. Click a queue name in the Queue List to view and manage the messages in the queue. See *Viewing a message queue*.
Status	Indicates whether the queue is in use or not. From the Status column, click **Referenced** to display a list of the email functions that use the queue. During a queue move operation, an icon in this column indicates whether the move is in progress or has failed.
Message Volume	Indicates the total number of messages in the queue. The number of messages a delegated administrator sees may be less than the total displayed in this column, depending on the permissions granted to that administrator.

Parameter	Description
Size/Total	Indicates the queue's current size as a portion of its maximum configured size.
Storage Location	Displays the location of queue storage (Local, via Network File System [NFS], or via Samba). Icons in this column indicate storage status, such as low disk space or a lost connection.
Properties	Contains a link to a page displaying the queue's current settings. Click this **Edit** link to change any queue settings.

Remove a user-created queue by marking the check box next to the queue name in the Queue List and clicking **Delete**. You cannot delete a default queue.

Related concepts
Viewing a message queue on page 149

Creating a message queue

Use the following steps to create a new message queue on the page **Main** > **Message Management** > **Message Queues**:

Steps

1) Below the Queue List, click **Add**. The Add Queue page displays.

2) In the text field **Queue name**, enter a name for the new queue.

3) Select the storage location for this queue:
   - Store the queue locally; click **Local**.
   - Use the NFS protocol for file storage; click **Via Network File System (NFS)**. Enter the IP address or hostname of the storage location, along with its shared path.

     Note

     NFS version 3 or later is supported.
   - Use Samba to facilitate file storage; click **Via Samba**.
   - Enter the following information for Samba:
     - IP address or hostname of the storage location
     - Its shared path
     - Username
     - Password

4) Configure the maximum number of days a message is retained in the queue; in the field Maximum message retention, enter a number from 1 to 180 days.

   Default is 180 for default queues, 30 for administrator-created queues.

5) Configure the maximum queue size.
   Default is 1024 MB. The maximum queue size is dynamic and depends on the available space in the file storage location. Different types of appliances allow different maximum queue sizes.

6) For an appliance in a cluster, specify the maximum storage size (in MB) assigned to each cluster machine.

7) Click **OK**.
   The settings are saved.

Changing message queue properties

The Edit Queue page is used to change a message queue's properties.

Steps

1) In the Queue List, from the Properties column of the message queue to be edited, click **Edit**.
   The Edit Queue page displays.

2) Configure the settings and click **OK**.
   The settings are saved.

Viewing a message queue

The View Messages in a Queue page displays the messages in a message queue, with functionality to view by a specific time or date range, search messages, or perform actions such as Deliver, Delete, and Reprocess.

From the Queue List, click a queue name.

The View Messages in a Queue page displays.

View messages by date/time range

Use the **View from/to** fields to specify the desired date/time range for viewing entries. The calendar includes the following options:

- Change the month and year by using the back and next arrows around the month and year at the top of the calendar.
- Set the calendar to the current date by clicking the date in the lower left corner of the calendar.
- Click **Clean** to clear the current date/time calendar selection.
- Click **Today** to set the calendar date to today's date.

Set the time range in hours and minutes in the entry fields to the right of the calendar.

Click the arrow to the right of the **View** date/time range to display the desired queue items.

Search messages by keyword

Use the Search functionality to perform a keyword search of the message queue, and to refine a search by message IDs, senders, recipients, subjects, or policies applied. You can also search on the name of the

appliance that processed the messages (Processed By category). The Search functionality includes the following options:

Steps

1) In the text field, enter a keyword.

2) From the pull-down menu, click a category on which to search; **ID**, **Subject**, **Sender**, **Recipient**, **Policy/Rule**, **Processed By**, or **All**.

3) Click **Search**.
   The messages matching the search parameters display.

Configure the number of messages to display

Use the Per Page menu to configure how many messages to view on each page of the queue.

From the pull-down menu **per page**, select the number of messages to display on each page; **25**, **50**, or **100**.

The default is 25.

The following table details the information displayed in the list of messages.

Parameter	Description
Sender	Sender email address.
Recipient	Recipient email address.
Subject	Message subject. Click the link to display the View Message page for viewing message information and contents. See *Viewing a message in a queue*.
Size	Message size.
Date/Time	Date and time of message receipt.
Policy/Rule	Policy and rule applied to the message. If a data loss prevention (DLP) policy is applied to a message, this information displays as a clickable link. Click **View Incident** to open the DLP incident information in the Data module, where the message was processed. This column does not display in the archive queue.
Message Type	Type of message (for example, spam, virus, exception, commercial bulk, advanced malware detection - cloud, advanced malware detection - on-premises, spoofed email, URL analysis, encryption error, or decryption error).
Processed By	Name of the appliance that processed the message.

Parameter	Description
Quarantined Reason	Indicates why a message was sent to a quarantine queue: ■ Antivirus filter ■ Email hybrid service ■ URL analysis filter ■ Bounce address tag validation ■ Digital fingerprinting antispam tool ■ LexiRules antispam tool ■ Heuristics antispam tool ■ Commercial bulk email filter ■ Custom content filter ■ Block List (Personal Email Manager Always Block List entry) ■ Archive feature (a setting on the page **Settings** > **Inbound/Outbound** > **Message Control**) ■ Data loss prevention ■ Exception (message exception) ■ For a message attachment analyzed by Forcepoint Advanced Malware Detection for Email - Cloud, click **View report(s)** to open a pop-up box with links to an Advanced Malware Detection - Cloud report on each file examined.

Note

In high-traffic situations, a large number of virus filter and URL filter exceptions may occur, incorrectly sending many messages to the exception queue. After the situation is resolved, select the affected email and use the Reprocess action to restart email processing.

Select a message in the queue and perform the following actions:

Action	Description
Deliver	Deliver the message to its recipient(s).
Delete	Delete the message from the queue.
Reprocess	Delete the message from the queue and restart the email processing function as if the email system were receiving it for the first time. For the archive queue, this action is called **Process**.
Not Spam	Report that the message should not be classified as spam and release the message for delivery. This option is available only when spam messages are selected.
More Actions	Pull-down menu functionality to select additional actions to perform. See the following table for more information.

Action	Description
Refresh	Refresh the queue contents list to view up-to-date queue contents.

The pull-down menu **More Actions** includes the following operations:

Action	Description
Resume Processing	A message that has both spam and virus characteristics may be isolated by one type of filter before it has been processed by the other type. If the original quarantine is a false positive, use this action to make sure the message is processed by all relevant filters rather than delivered after only the first analysis.
Add to Always Block List	Add the message sender to the Always Block List.
Add to Always Permit List	Add the message sender to the Always Permit List.
Forward	Forward the message to one or more recipients. The forwarded message is added as an attachment to the forwarding message.
Download	Download the message in .eml format. Downloaded email is saved in a zip file.
Clear message queue	Delete all the messages in the queue.
Reprocess all messages	Reprocess messages in your search result. Only the first 5000 entries in your search result are reprocessed.
Delete all messages	Delete messages in your search result. Only the first 5000 entries in your search result are deleted.

Related concepts
Viewing a message in a queue on page 158

Managing the blocked message queue

The page **Main** > **Message Management** > **Blocked Messages** lists all blocked messages from most queues across all appliances together in a single table, with a column entry that indicates the name of the queue in which a message is stored. Messages in the archive and Delayed Messages queues are not included on this page.

View messages by date/time range

Use the **View from/to** fields to specify the desired date/time range for viewing entries. The calendar includes the following options:

- Change the month and year by using the back and next arrows around the month and year at the top of the calendar.
- Set the calendar to the current date by clicking the date in the lower left corner of the calendar.

- Click **Clean** to clear the current date/time calendar selection.
- Click **Today** to set the calendar date to today's date.

Set the time range in hours and minutes in the entry fields to the right of the calendar.

Click the arrow to the right of the **View** date/time range to display the desired queue items.

Search messages by keyword

Use the Search functionality to perform a keyword search of blocked messages, and to refine a search by message IDs, senders, recipients, subjects, or policies applied. You can also search on an individual queue or on the name of the appliance that processed the messages (Processed By category). The Search functionality includes the following options:

Steps

1) In the text field, enter a keyword.

2) From the pull-down menu, click a category on which to search; **ID**, **Subject**, **Sender**, **Recipient**, **Policy/Rule**, **Processed By**, or **All**.

3) Click **Search**.
   The messages matching the search parameters display.

Configure the number of messages to display

Use the Per Page menu to configure how many messages to view on each page of the queue.

From the pull-down menu **per page**, select the number of messages to display on each page; **25**, **50**, or **100**.

The default is 25.

The following table details the information displayed in the list of blocked messages.

Parameter	Description
Sender	Sender email address.
Recipient	Recipient email address.
Subject	Message subject. Click the link to display the View Message page for viewing message information and contents. See *Viewing a message in a queue*.
Size	Message size.
Date/Time	Date and time of message receipt.

Parameter	Description
Policy/Rule	Policy and rule applied to the message. If a data loss prevention (DLP) policy is applied to a message, this information displays as a clickable link. Click **View Incident** to open the DLP incident information in the Data module, where the message was processed. This column does not display in the archive queue.
Queue	Queue in which the message is stored (for example, spam, virus, exception, encryption-fail, or decryption-fail).
Message Type	Type of message (for example, spam, virus, exception, commercial bulk, advanced malware detection - cloud, advanced malware detection - on-premises, spoofed email, URL analysis, encryption error, or decryption error).
Processed By	Name of the appliance that processed the message.
Quarantined Reason	Indicates why a message was sent to a quarantine queue: ■ Antivirus filter ■ Email hybrid service ■ URL analysis filter ■ Bounce address tag validation ■ Digital fingerprinting antispam tool ■ LexiRules antispam tool ■ Heuristics antispam tool ■ Commercial bulk email filter ■ Custom content filter ■ Block List (Personal Email Manager Always Block List entry) ■ Archive feature (a setting on the page **Settings** > **Inbound/Outbound** > **Message Control**) ■ Data loss prevention ■ Exception (message exception) ■ For a message attachment analyzed by Forcepoint Advanced Malware Detection for Email - Cloud, click **View report(s)** to open a pop-up box with links to an Advanced Malware Detection - Cloud report on each file examined.

Select a message in the blocked messages queue and perform the following actions:

Action	Description
Deliver	Deliver the message to its recipient(s).
Delete	Delete the message from the queue.

Action	Description
Reprocess	Delete the message from the queue and restart the email processing function as if the email system were receiving it for the first time.
Not Spam	Report that the message should not be classified as spam and release the message for delivery. This option is available only when spam messages are selected.
Refresh	Refresh the queue contents list to view up-to-date queue contents.

The pull-down menu More Actions includes the following operations:

Action	Description
Resume Processing	A message that has both spam and virus characteristics may be isolated by one type of filter before it has been processed by the other type. If the original quarantine is a false positive, use this action to make sure the message is processed by all relevant filters rather than delivered after only the first analysis.
Add to Always Block List	Add the message sender to the Always Block List.
Add to Always Permit List	Add the message sender to the Always Permit List.
Forward	Forward the message to one or more recipients. The forwarded message is added as an attachment to the forwarding message.
Download	Download the message in .eml format. Downloaded email is saved in a zip file.
Reprocess all messages	Reprocess the messages in your search result. Only the first 5000 entries in your search result are reprocessed.
Delete all messages	Delete the messages in your search result. Only the first 5000 entries in your search result are deleted.

Related concepts

Viewing a message in a queue on page 158

Managing the delayed message queue

Email that is temporarily undeliverable as a result of various connection issues is sent to the delayed messages queue. Delayed messages may be automatically resent by the system. See *Handling undelivered messages* for information about setting the delayed messages delivery retry interval and configuring a notification message to be sent for undelivered email.

Delayed message delivery may also be scheduled for a future date using a custom content filter action. See *Custom content* for information about custom content filters and *Creating and configuring a filter action* for details about scheduling a delayed message delivery.

View the messages in this queue and manually perform necessary processing activities on the page **Main** > **Message Management** > **Delayed Messages**.

Related concepts
Custom content on page 190

Related tasks
Handling undelivered messages on page 160
Creating and configuring a filter action on page 195

View messages by date/time range

When the Delayed Messages page displays, the most recent messages are shown. Use the **View from/to** fields to specify the desired date/time range for viewing messages. The calendar includes the following options:

- Change the month and year by using the back and next arrows around the month and year at the top of the calendar.
- Set the calendar to the current date by clicking the date in the lower left corner of the calendar.
- Click **Clean** to clear the current date/time calendar selection.
- Click **Today** to set the calendar date to today's date.

Set the time range in hours and minutes in the entry fields to the right of the calendar.

Click the arrow to the right of the **View** date/time range to display the desired queue items.

Search messages by keyword

Use the Search functionality to perform a keyword search of delayed messages, and to refine a search by message IDs, senders, recipients, subjects, or reasons for delay. If appliances are configured in a cluster, you can also search on the name of the appliance that processed the messages (Processed By category). The Search functionality includes the following options:

Steps

1) In the text field, enter a keyword.

2) From the pull-down menu, click a category on which to search; **ID**, **Subject**, **Sender**, **Recipient**, **Processed By**, **Reason for Delay**, or **All**.

3) Click **Search**.
   The messages matching the search parameters display.

Configure the number of messages to display

Use the Per Page menu to configure how many messages to view on each page of the queue.

From the pull-down menu **per page**, select the number of messages to display on each page; **25**, **50**, or **100**.

The default is 25.

The following table details the information displayed in the list of delayed messages.

Parameter	Description
Sender	Sender email address.
Recipient	Recipient email address.
Subject	Message subject. Click the link to display the View Message page for viewing message information and contents. See *Viewing a message in a queue*.
Size	Message size.
Date/Time	Date and time of message receipt.
Policy/Rule	Policy and rule applied to the message. If a data loss prevention (DLP) policy is applied to a message, this information displays as a clickable link. Click **View Incident** to open the DLP incident information in the Data module, where the message was processed. This column does not display in the archive queue.
Next Scheduled Delivery Attempt	Date of the next scheduled message delivery attempt.
Reason for Delay	Reason a message is delayed. Entries in this column may be one of the following: ■ Temporary connection issue delay n. A temporary delay due to connection issues; n is the number of retry attempts remaining for the message. ■ Scheduled delay. An intentional delay that is scheduled via a custom content filter action (see *Creating and configuring a filter action* for information). ■ Advanced Malware Detection - Cloud or Advanced Malware Detection - On-Premises delay. A temporary delay due to in-progress advanced file analysis.
Processed By	Name of the appliance that processed the message.

Select a message in the queue and perform the following actions:

Action	Description
Release	Attempt the message delivery immediately.
Delete	Delete the message from the queue.
Refresh	Refresh the queue contents list to view up-to-date queue contents.

The pull-down menu **More Actions** includes the following operations:

Action	Description
Forward	Forward the message to one or more recipients. The forwarded message is added as an attachment to the forwarding message.
Download	Download the message in .eml format. Downloaded email is saved in a zip file.
Release all messages	Attempt to deliver all the messages in the queue.
Delete all messages	Delete the messages in your search result. Only the first 5000 entries in your search result are deleted.

Related concepts
Viewing a message in a queue on page 158

Viewing a message in a queue

Use the View Message page to view details about a message or the message contents from any message queue, including Blocked Messages, Delayed Messages, or any default or custom queue on the page Message Queues. Click the link for a message in the Subject column of a queue to open the View Message page.

The **Back** link at the top of the page returns you to the View Queue page. The **Previous** and **Next** links let you navigate to the previous or next message in the queue messages list.

The following information about a selected message is displayed on the View Message page:

Field Name	Description
Sender	Sender email address.
Recipient	Recipient email address.
From	Name of the sender.
To	Name of the recipient.
Date	Date the message was received.
Policy	Name of the policy applied to the message.
Message type	Message type, indicating message analysis result or filter type (Clean, Virus, Spam, Data Loss Prevention, Exception, Commercial Bulk, Phishing, Advanced Malware Detection - Cloud, Advanced Malware Detection - On-Premises, Spoofed Email, URL Analysis, Email Attachment, or Custom Content).
Processed by	Name of the appliance that processed the message.
Header	Click the link to view the message header.
Attachment	If the message contains an attachment, a link allows you to open it.
Subject	Message subject.

All message actions available ton any View Queue page are also available on the View Message page, except Clear All Messages or Release All Messages. See *Viewing a message queue*. You can also choose to view message contents in either text or HTML format or to **Clear message queue** from the pull-down menu More Actions.

Related concepts
Viewing a message queue on page 149

Configuring message exception settings

The page **Settings** > **Inbound/Outbound** > **Exceptions** specifies how to handle messages that cannot be processed for some reason. Configure message exception settings as follows:

Steps

1) Mark one or more check boxes to specify the action(s) to perform on a message that cannot be processed:
   - Deliver the message when an exception is caused by an antivirus filter.
   - Deliver the message when an exception is caused by an antispam filter (default setting).
   - Deliver the message when an exception is caused by the advanced file analysis filter.
   - Deliver the message when an exception is caused by the commercial bulk email filter.
   - Deliver the message when an exception is caused by a data loss prevention policy.
   - Deliver the message when an exception is caused by the URL analysis filter.
   - Deliver messages when an exception is caused by any other system operation.
   - Save exception messages to a queue (default setting).
     Select the desired folder from the pull-down menu (default is **exception**). The list includes all the default queue names and any administrator-created queues. To add a new queue, select **Add Folder** from the pull-down menu to open the Add Queue screen.

     Warning

     You must have the save option selected to save undelivered messages to a queue. If this option is not selected, messages may be dropped.

     Messages are saved to the queue regardless of whether the delivery option is selected for a specific filter.

2) Send a notification regarding the unprocessed message; mark the check box **Send notification** to enable the Notification Properties section.

3) Select the notification message sender from the following choices:
   - Original email sender
     This is the default.
   - Administrator
     If you use this option, you must configure a valid administrator email address on the page **Settings** > **General** > **System Settings** (see *Setting system notification email addresses*).
   - Custom
     Specify a single email address in this field.

4) Mark one or more check boxes to specify notification message recipients from among the following choices:
   - Original email sender
   - Original email recipient
   - Administrator
     This is the default. If you use this option, you must configure a valid administrator email address on the page **Settings** > **General** > **Settings** (see *Setting system notification email addresses*).
   - User specified; enter one or more email addresses, separated by semicolons, in this field

5) In the text field **Subject**, specify the subject line of your notification message.

6) In the text field **Content**, enter the body of your notification message.

7) Attach the original message to the notification message; mark the check box **Attach original message**.

8) Click **OK**.
   The settings are saved.

Related tasks
Setting system notification email addresses on page 86

Handling undelivered messages

Message delivery options help you control how undeliverable mail is handled. Options for these operations are configured on the page **Settings** > **Inbound/Outbound** > **Message Non-Delivery Options**.

Use the following steps to determine how to handle messages that are temporarily undeliverable due to error situations:

Steps

1) In the field **Retry interval**, enter the time for the message retry interval, in minutes.

Important

Message delivery retry intervals are calculated exponentially. For example, using the default entry of 15, retry attempts are made in 15, 30, 60, 120, 240, etc., minutes.

2) In the field **Maximum retry period**, enter the time for the maximum period for retrying message delivery, in minutes.
   The default is 1440.

3) In the field **Notification email address**, enter an email address to which to send notifications that a non-delivery report (NDR) cannot be delivered to the original sender at the end of the retry period.
   Mark the check box **Use Administrator email address** to send these messages to the administrator.
   You must configure the administrator address on the page **Settings** > **General** > **System Settings** (see *Setting system notification email addresses*).

4) Click **OK**.
The settings are saved.

Related tasks
Setting system notification email addresses on page 86

Traffic shaping options

The page **Settings** > **Inbound/Outbound** > **Traffic Shaping** is used to determine the rate of traffic delivery for a specified source or destination group based on domain group or user directory settings. For example, these settings allow you to send large volumes of email at a rate that prevents possible blacklisting of the domain.

Change the order of a traffic shaping group by marking its associated check box and using the **Move Up** and **Move Down** buttons. Copy an existing traffic shaping group by marking its associated check box and clicking **Copy**. Delete a traffic shaping group by marking its associated check box and clicking **Delete**.

In addition to specifying source and destination user groups, the following message delivery settings may be modified as part of traffic shaping:

- Maximum number of concurrent connections
- Maximum number of messages per connection within a designated time period
- Maximum number of recipients per message
- Use of the SMTP session cache, for which the maximum number of messages per session and the session duration are specified

The default traffic shaping group contains no traffic source or destination user groups.

Add message traffic shaping controls in your system

Steps

1) On the page Traffic Shaping, click **Add**.
The Add Traffic Shaping Group page displays.

2) In the text field **Traffic shaping group name**, enter a name.

3) From the pull-down menu **Order**, specify the location in which this group should appear in the traffic shaping group list.

4) Select the status of your traffic shaping group: **Active** or **Disabled**.

5) Configure an email source for the traffic shaping group, if desired. From **Source type**, designate one of the following source types:

- All sources
- Domain group
  This is the default. Select the domain group from the pull-down menu. Modify the selected domain group by clicking **Edit**.
- User directory
  Select a user directory from the list, or create a new user directory by clicking **Add user directory**.

6) Configure an email destination traffic shaping group, if desired.

From **Destination type**, designate one of the following destination types:

- All destinations
- Domain group
  This is the default. Select the domain group from the pull-down menu. Modify the selected domain group by clicking **Edit**.
- User directory
  Select a user directory from the list, or create a new user directory by clicking **Add user directory**.

7) In the field **Maximum number of concurrent connections**, enter the maximum number of simultaneous message deliveries to an individual routing address.

The range of values is 5–50; default value is 20.

8) In the field **Maximum number of messages per connection**, enter the maximum number of messages per connection within a defined time period.

The range of values for number of messages is 1–10000; default value is 10000. The time range is 60 seconds to 30 minutes; default value is 60 seconds.

9) In the field **Maximum number of recipients**, enter the maximum number of message recipients per message delivery.

The range of values is 5–100; default value is 50.

10) Use an SMTP session cache; mark the check box **Enable SMTP session cache**. This is the default.

a) Enter the maximum number of messages allowed per SMTP session.
Range of values is 5–100; default is 10. Enter zero (0) to specify an unlimited number of messages per session.

b) Enter the duration of the SMTP session, in seconds.
Range of values is 60–600 seconds; default value is 300 seconds.

11) Click **OK**.

The settings are saved. The new group displays on the page Traffic Shaping.

Handling encrypted messages

An email content policy configured in the Data Security module may specify that a message should be encrypted for delivery. To encrypt specific outbound messages, you must create an email DLP policy that includes an encryption action plan in the Data Security module (**Main** > **Policy Management** > **DLP Policies**).

Specify the type of encryption to use on the page **Settings** > **Inbound/Outbound** > **Encryption**.

The following types of message encryption are supported:

Related concepts

Mandatory Transport Layer Security encryption on page 163
Forcepoint email encryption on page 164
Third-party encryption application on page 165
Secure Message Delivery on page 167

Mandatory Transport Layer Security encryption

Transport Layer Security (TLS) is an Internet protocol that provides security for all email transmissions—inbound, outbound, and internal. The client and server negotiate a secure “handshake” connection for the transmission to occur, provided both the client and the server support the same version of TLS.

Enable TLS encryption with no backup method

In the Email Security module, if you select only TLS for message encryption and the client and server cannot negotiate a secure TLS connection, the message is sent to a delayed message queue for a later delivery attempt.

Steps

1) Navigate to the page **Settings** > **Inbound/Outbound** > **Encryption**.

2) From the pull-down menu **Encryption method**, select **Transport Layer Security (TLS)**.

3) Use only TLS for message encryption; from TLS Encryption Backup Options, select **Use TLS only (no backup encryption method; message is queued for later delivery attempt)**.

4) Click **OK**.
   The settings are saved.

Enable TLS encryption with a backup method

If you select TLS for message encryption, you can designate another encryption option as a backup method in case the TLS connection fails. Specifying a backup option allows you a second opportunity for message encryption in the event of an unsuccessful TLS connection. If both the TLS and backup connections fail, the message is sent to a delayed message queue for a later connection attempt.

Steps

1) Navigate to the page **Settings** > **Inbound/Outbound** > **Encryption**.

2) From the pull-down menu **Encryption method**, select **Transport Layer Security (TLS)**.

3) From TLS Encryption Backup Options, select one of the following options:
   - **Use Forcepoint Email Encryption as backup encryption method**
     This option is available only if your subscription includes the Forcepoint Email Security - Encryption Module.
   - **Use third-party application as backup encryption method**
   - **Use secure message delivery as backup encryption method**
     Additional options display according to your selection.

4) Configure the settings for the selected backup method.
   See *Third-party encryption application* and *Secure Message Delivery*.

5) Click **OK**.
   The settings are saved.

Related concepts
Third-party encryption application on page 165
Secure Message Delivery on page 167

Forcepoint email encryption

The Forcepoint Email Encryption option enables the email hybrid service to perform message encryption on outbound messages. Forcepoint email encryption is available only if your subscription includes the Forcepoint Email Security Hybrid Module and the Forcepoint Email Security - Encryption Module, and if the email hybrid service is registered and enabled.

You can also specify Forcepoint Email Encryption as a backup encryption method if mandatory TLS encryption is selected. See *Mandatory Transport Layer Security encryption*.

When an email DLP policy identifies an outbound message for encryption, the message is sent to the email hybrid service via a TLS connection. If the secure connection is not made, the message is placed in a delayed message queue for a later delivery attempt.

The SMTP server addresses used to route email to the email hybrid service for encryption are configured during the Forcepoint Email Security Hybrid Module registration process. Use the Delivery Route page under **Settings** > **Hybrid Service** > **Hybrid Configuration** to add outbound SMTP server addresses (see *Define delivery routes*).

If the email hybrid service detects spam or a virus in an encrypted outbound message, the mail is returned to the message sender.

The email hybrid service attempts to decrypt inbound encrypted mail and adds an x-header to the message to indicate whether the decryption operation succeeded. Message analysis is performed regardless of whether message decryption is successful.

The hybrid service does not encrypt inbound or internal mail. A DLP policy must be modified to designate only outbound messages for encryption when the email hybrid service is used.

See Forcepoint Email Security Message Encryption for more information.

Related concepts
Mandatory Transport Layer Security encryption on page 163
Define delivery routes on page 64

Enable Forcepoint email encryption

Steps

1) Navigate to the page **Settings** > **Inbound/Outbound** > **Encryption**.

2) From the pull-down menu **Encryption method**, select **Forcepoint Email Encryption**.

3) Click **OK**.
The settings are saved.

Third-party encryption application

The email protection system supports the use of third-party software for email encryption. The third-party application used must support the use of x-headers for communication with the email system.

You can also specify third-party application encryption as a backup encryption method if mandatory TLS encryption is selected. See *Mandatory Transport Layer Security encryption*.

The email protection system can be configured to add an x-header to a message that triggers a DLP encryption policy. Other x-headers indicate encryption success or failure. These x-headers facilitate communication between the email system and the encryption software. You must ensure that the x-header settings made on the Encryption page match the corresponding settings in the third-party software configuration.

Related concepts
Mandatory Transport Layer Security encryption on page 163

Configure third-party application encryption

Steps

1) Navigate to the page **Settings** > **Inbound/Outbound** > **Encryption**.

2) From the pull-down menu **Encryption method**, select **Third-party application**. Applicable configuration options display.

3) Add encryption servers (up to 32) to the Encryption Server List:

   a) Enter the IP address or hostname and port number of each server.

   b) Use the MX lookup feature; mark the check box **Enable MX lookup**.
   If you entered an IP address in the previous step, the MX lookup option is not available.

   c) Click the **arrow** to the right of the Add Encryption Server box to add the server to the Encryption Server List.

   Delete a server from the list; select it and click **Remove**.

4) In the pull-down menu **Encrypted IP address group**, specify an IP address group if decryption is enabled or if encrypted email is configured to route back to the email software.
   The default is Encryption Gateway.

5) Configure users to present credentials to view encrypted mail; mark the check box **Require authentication** and supply the desired user name and password in the appropriate fields.
   Authentication must be supported and configured on your encryption server to use this function.

6) In the field **Encryption X-Header**, specify an x-header to be added to a message that should be encrypted.
   This x-header value must also be set and enabled on your encryption server.

7) In the field **Encryption Success X-Header**, specify an x-header to be added to a message that has been successfully encrypted.
   This x-header value must also be set and enabled on your encryption server.

8) In the field **Encryption Failure X-Header**, specify an x-header to be added to a message for which encryption has failed.
   This x-header value must also be set and enabled on your encryption server.

9) Select any desired encryption failure options:

   - Mark the check box **Send messages to queue**.
     Select a queue for these messages from the pull-down menu. The default is the virus queue.
   - Mark the check box **Send notification to original sender**.
   - In the section Notification Details, enter the notification message subject and content in the appropriate fields.
   - Include the original message as an attachment to the notification message; mark the check box **Attach original message**.
   - Deliver the message that failed the encryption operation; select **Deliver message**.
     This is the default.
   - Do not deliver the message that failed the encryption operation; select **Drop message**.

10) Decrypt encrypted messages; mark the check box **Enable decryption**

11) Select any desired decryption options:

- In the field **Content type**, enter the message content types to decrypt, separated by semicolons. Maximum length is 49 characters. Default entries include multipart/signed, multipart/encrypted, and application/pkcs7-mime.
- In the field **X-Header**, specify a message x-header that identifies a message to decrypt.
  This x-header value must also be set and enabled on your encryption server.
- In the field **Decryption X-Header**, specify an x-header to be added to a message that should be decrypted.
  This x-header value must also be set and enabled on your encryption server.
- In the field **Decryption Success X-Header**, specify an x-header to be added to a message that has been successfully decrypted.
  This x-header value must also be set and enabled on your encryption server.
- In the field **Decryption Failure X-Header**, specify an x-header to be added to a message for which decryption has failed.
  This x-header value must also be set and enabled on your encryption server.
- Forward a message that has failed decryption to a specific queue; mark the check box **On decryption failure** and select a queue for these messages from the pull-down menu.
  The default is the virus queue.

12) Click **OK**.
The settings are saved.

Secure Message Delivery

Secure Message Delivery is an on-premises encryption method used to configure delivery options for a secure portal in which recipients of your organization's email may view, send, and manage encrypted email. For example, you may wish to include sensitive personal financial information in a message to a client. The portal provides a secure location for the transmission of this data.

Users within your organization who send and receive secure messages handle these messages via their local email clients, not the secure portal.

Secure messages are stored in a default secure-encryption queue (**Main** > **Message Management** > **Message Queues**). Search for and delete messages in the

secure-encryption queue view. Message details may not be viewed. The maximum queue size and number of days a message is retained are configured on the Edit Queue page. See *Managing message queues*.

You can also specify Secure Message Delivery as a backup encryption method for outbound email if mandatory TLS encryption is selected. See *Mandatory Transport Layer Security encryption*.

The Secure Message portal can be displayed in one of nine languages, which the end user selects during the registration process. The Forcepoint Secure Messaging User Help is available in Forcepoint Documentation, also in nine languages. It describes the user registration process and how to use the secure message portal.

Note

When advanced file analysis is enabled (see *Selecting advanced file analysis platform*), and the advanced file analysis filter is configured in Enforce mode with the option to send an enforcement notification (see *Advanced file analysis*), replies to messages from the Secure Message Delivery portal will include a plain text file, or only the filename, until analysis is complete.

Related concepts

Mandatory Transport Layer Security encryption on page 163
Managing message queues on page 147
Advanced file analysis on page 187

Related tasks

Selecting advanced file analysis platform on page 78

Configure Secure Message Delivery encryption

Steps

1) Navigate to the page **Settings** > **Inbound/Outbound** > **Encryption**.

2) From the pull-down menu **Encryption method**, select **Secure Message Delivery**.

3) Enter the IP address or hostname for the appliance that hosts the secure message delivery portal.
The maximum length for the hostname is 64 characters.

Entering a hostname rather than an IP address is recommended, to avoid potential Microsoft Outlook warning messages generated in an end user's inbox by the notification message.

Important

The entry in this field should be mapped to the E1 interface (for a V10000 appliance) or the P1 interface (for a V5000 appliance). Ensure that the interface you use is visible from outside your internal network.

If you have an appliance cluster, enter the IP address or hostname for one cluster appliance (primary or secondary). The cluster load balancing function directs traffic appropriately.

Note

Secure messaging uses the same port configured for the Personal Email Manager portal (**Settings** > **Personal Email** > **Notification Message**).

4) Specify the actions that your users are allowed to perform in the secure portal, along with the types of recipients to whom these users can send secure messages:

- **Enforce strong password policy**
  With this policy in force, an end-user password must meet the following requirements:
  - Between eight and 15 characters
  - At least one uppercase letter
  - At least one lowercase letter
  - At least one number
  - At least one special character; supported characters include:
    ! " # $ & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~

  End users are prompted to create strong passwords in the Secure Message portal.
- **Display images within messages viewed in the Secure Message Portal**
  Use this option to determine whether to allow images to display in secure messages viewed in the Secure Message portal. For security, this option is disabled by default.

  Warning

  Enabling this feature is not recommended, because a malicious script hosted remotely could be disguised in the email as an image, allowing the attacker to compromise your system.
- **Maximum message size**
  End-user message size includes any attachments. The default value is 50 MB; maximum value is 100 MB.
- **Reply all to secure messages received in the portal**
  An end user may reply to all message recipients. However, if the option **Internal domain email addresses only** is selected for Allowed Recipients, the user may reply only to recipients inside your organization.

  The recipient list cannot be modified for this type of message.
- **Forward secure messages received in the portal**
  An end user may forward any secure message received to allowed recipients.
- **Compose new secure messages within the portal**
  An end user may compose and send a new secure message to allowed recipients.
- **Attach files to secure messages sent from the portal**
  An end user may send an attachment in a secure message These options are all selected by default.

The Allowed Recipients box offers options for the types of recipients to whom your customer may reply, forward, or send new secure messages. For security purposes, the recipient list must include at least one email address within your organization.

- **Internal domain email addresses only**. Only email addresses within your organization's protected domains may be specified as recipients.
  Internal and external domain email addresses (at least one internal email address required). Email addresses outside your organization's protected domains may be specified as recipients, but at least one address within your domains must be entered (default selection).

  See *Protected Domain group* for more information about determining your protected domains.

5) From the Secure Email End-User Notification section, configure the notification email that users receive when secure messages sent to them have been delivered to the portal for viewing.

   - Use the default message or customize it to suit your needs.
     The URL field must be included in your notification because it creates the link the end user clicks to access the secure email portal.
   - In the field **Sender**, enter one sender address for the notification.
     The sender address must belong to your internal protected domain. Because you do not want responses to the notification, ensure that the sender address is configured to drop any direct replies to the notification.
   - In the field **Subject**, enter an email subject.

   Any customizations you make to the notification email template are lost when upgrading to a new version of Forcepoint Email Security. After upgrade, you will need to reconfigure your customized templates.

6) After you have configured your notification message, click **Preview Message** to view it.

7) Click **OK**.
   The settings are saved.

Related concepts
Protected Domain group on page 99

Chapter 5

Working with Filters and Policies

Contents

Managing filters

Create and configure filters on the page **Main** > **Policy Management** > **Filters**. A filter in use by a policy can be copied; a filter not in use by a policy can be copied or deleted. Default filters cannot be copied or deleted. See *Creating and configuring a filter*.

The following predefined default filter types can be used in email analysis:

- The virus filter analyzes an email message and its attachments for the presence of viruses and other threats. See *Antivirus*.
- The spoofed email filter can help reduce instances of email sender impersonation. See *Spoofed email*.
- The email attachment filter examines email attachment content to determine the attachment's true file type. The filter can also detect individual file attachment extensions configured by an administrator. See *Email attachment*.
- The URL analysis filter examines email content for embedded URLs and classifies them according to a database of known spam URLs. URLs classified by the filter can be removed or modified. See *URL analysis*.
- The spam filter analyzes email content and compares it against a database of known spam characteristics. A variety of antispam tools are available, including digital fingerprinting, LexiRules, and heuristics analysis tools. See *Antispam*.
- The commercial bulk email filter analyzes a message to determine whether it was sent from a business for advertising purposes. See *Commercial bulk email*.
- The advanced file analysis filter inspects email attachment file types that commonly contain security threats. See *Advanced file analysis*.
- The disclaimer filter is used to add text at the beginning or end of a message. See *Disclaimer*.
- A custom content filter can be added to examine a message based on configured message component conditions. The Forcepoint Email Security module does not provide a default custom content filter. See *Custom content*.

Related concepts
Creating and configuring a filter on page 173
Antivirus on page 174
Email attachment on page 178
URL analysis on page 179
Antispam on page 185
Commercial bulk email on page 186
Advanced file analysis on page 187
Custom content on page 190
Spoofed email on page 175

Related tasks
Disclaimer on page 193

Copying a filter

Copy an existing filter to modify and use the existing filter settings. A filter can be copied whether or not it is in use by a policy; however, default filters cannot be copied.

Steps

1) On the page **Main** > **Policy Management** > **Filters**, mark the check box to the left of the filter name.

2) Click **Copy**.
The Copy Filter dialog box displays.

3) In the field **Filter Name**, enter a new name for the filter.

4) Click **OK**.
The new filter displays in the Filters list. See *Creating and configuring a filter*.

Related concepts
Creating and configuring a filter on page 173

Deleting a filter

A filter can be deleted as long as it is not in use by a policy. Default filters cannot be deleted.

Steps

1) On the page **Main** > **Policy Management** > **Filters**, mark the check box to the left of the filter name.

2) Click **Delete**.
The Confirm Filter Delete dialog box displays.

3) Click **Yes**.
The filter is deleted.

Creating and configuring a filter

Create new filters on the page **Main** > **Policy Management** > **Filters**. The selected filter type determines the filter settings you can configure. Select from the following types:

Related concepts
Antivirus on page 174
Spoofed email on page 175
Email attachment on page 178
URL analysis on page 179
Antispam on page 185
Commercial bulk email on page 186
Advanced file analysis on page 187
Custom content on page 190

Related tasks
Disclaimer on page 193

Create a new filter

Steps

1) On the page **Main** > **Policy Management** > **Filters**, select **Add**. The Add Filter page displays.

2) In the text field **Filter Name**, enter a name for the filter.

3) In the text field **Description**, enter a description of the filter.

4) From the pull-down menu **Filter Type**, select a filter type.
The section Filter Properties displays with the available options for the selected filter.

5) Configure the filter properties and select **OK**.
The filter is saved.

Antivirus

Antivirus analysis checks email and any attachments for the presence of email-borne viruses and threats. Configure the antivirus filter on the page **Main** > **Policy Management** > **Filters** > **Add (or Edit) Filter**.

If your subscription includes the Forcepoint Email Security Hybrid Module, the email hybrid service analysis score can be used in addition to the on-premises email security system antivirus analysis.

The antivirus filter can be configured to specify the type and sensitivity of analysis, as well as the response of the filter.

Configure antivirus filter analysis

Steps

1) From the section Filter Properties, mark the check box for one or both options under **Filter analysis**:
   - **Treat errors as infected**
     If antivirus analysis encounters errors, the email is handled as if is infected. This setting is enabled by default.
   - **Analyze message body for viruses**
     The message content is analyzed for embedded malicious scripts or attachments that cannot be examined properly. If message format problems cause attachments to be viewed as part of the message body, the attachments are analyzed and viruses are detected. This setting is disabled by default.

2) From the section Filter Properties, select one or both of the options under **Tools**:
   - **Standard analysis**
     Performs standard email content and attachment analysis for virus threats.
   - **Advanced analysis**
     Performs email attachment analysis for Microsoft Office documents and macros.

     Either one or both types of analysis can be selected, along with the sensitivity level of each analysis type. If you select both types of analysis, standard analysis is performed first, then advanced analysis. The higher the sensitivity level, the larger the volume of email that is designated as virus. Enabling the advanced antivirus engine may affect system performance.

3) From the section Sensitivity Level, select **Low**, **Medium**, or **High**.

4) From the section Filter Properties, select one option under **Filter response**:
   - **Remove infected attachments**
     Deletes the attachment that triggers the antivirus filter.
   - **Take no action**
     This is the default action. The attachment and virus are stored in a predefined location (see *Creating and configuring a filter action*). If required, a message may be sent to the administrator stating that a virus has been found.

5) From the bottom of the section Filter Properties, click **Advanced**.
   The Advanced settings display. These settings are used to add a notification to a suspected virus email, to alert the recipient that the message may be infected.

6) Mark the check box **Notify recipient that the delivered email message may contain a virus**.

7) In the text box, enter the desired notification text.
   The maximum length is 8192 characters total, up to 990 characters per line; a line break is two characters.

8) Select where the notification should appear; **Insert notification at top of message** or **Insert notification at bottom of message**.
   The default location is at the top of the message.

9) Configure additional filter settings and click **OK**.
   The antivirus filter settings are saved.

Related tasks
Creating and configuring a filter action on page 195

Spoofed email

The spoofed email filter can help determine the validity of message senders and reduce instances of sender impersonation via a set of header sender comparisons and SPF, DKIM, and Sender ID analysis results.

Spoofed email filter message header comparisons involve the **From**, **envelope Sender**, and **Reply-To** fields.

- The **From** field indicates the entity (for example, person or mailbox) that is responsible for authoring the message.
- The envelope **Sender** field contains information about the entity responsible for the actual transmission of the message (for example, someone who sends a message on behalf of another person).
- If present, the **Reply-To** field specifies the address to which a message reply should be sent. If **Reply-To** is not present, a reply is sent to the From: address.

Note

The spoofed email filter provides SPF analysis in addition to the inbound relay SPF email rejection options on the page **Settings** > **Inbound/Outbound** > **Relay Controls**. The following should be considered regarding the use of these two SPF-based analyses:

- When a message triggers a mail routing SPF connection rejection option and is dropped, it will not be processed by the spoofed email filter and email content is not analyzed.
- When a message triggers a mail routing SPF connection rejection option but is not dropped, the SPF score from this analysis is stored for use by the spoofed email filter.

The spoofed email filter can be configured to use one or more header comparisons and to enable authentication analysis. Configure the spoofed email filter on the page **Main** > **Policy Management** > **Filters** > **Add (or Edit) Filter**.

Configure spoofed email filter analysis

The spoofed email filter is triggered if any selected address comparison fails, and the message sender is presumed to be forged.

Steps

1) From the section Filter Properties, mark the check box **Sender address comparison**.
   Selection is enabled by default.

2) Mark the check box for one or more sender address conditions:
   - **Verify that the From: address matches the envelope sender address**
     This setting is enabled by default.
   - **Verify that the From: address matches the Reply-To: address**
   - **Verify that the envelope sender address matches the Reply-To: address**
     This setting is enabled by default.

   Note

   When an envelope sender has been changed as a result of an address rewriting rule (**Settings** > **Inbound/ Outbound** > **Address Rewriting**), the spoofed email filter uses the original envelope sender address rather than the rewritten address for SPF analysis.

   For other checks like header comparison and bypass conditions, the rewritten envelope sender is used.

3) From the bottom of the section Filter Properties, click **Advanced**.
   The Advanced settings display. Advanced options for sender authentication analysis allow the configuration of filter conditions using combinations of SPF, DKIM, and SIDF analysis results.

4) Mark the check box **Sender authentication analysis**.
   Selection enables the use of one or more filter conditions.

5) Mark the check boxes for one or more conditions: **Default Condition 1** or **Default Condition 2**.
Default condition sets include the following (operator between SPF and SKIM results is **AND**):

Condition Name	SPF Result	DKIM Result	Sender ID Validation
Default Condition 1	Fail **or** SoftFail	Fail **or** Invalid **or** TempError	Enabled
Default Condition 2	PermError **or** TempError **or** None **or** Neutral	Fail	Enabled

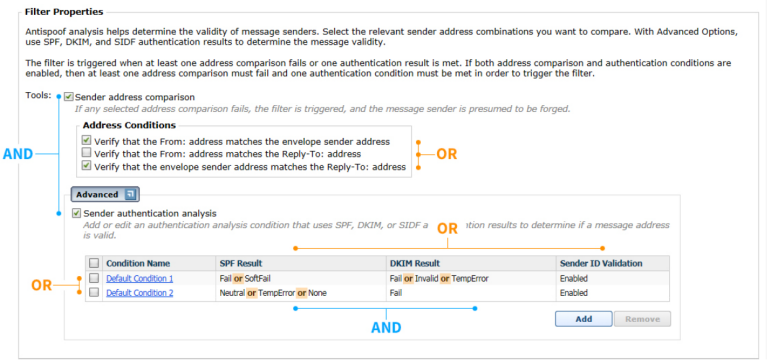
For Default Condition 1, the filter is triggered if:

- The SPF result is either Fail **or** SoftFail **AND** the DKIM result is Fail, Invalid, **or** TempError. The operator between SPF results and sender ID validation is **OR**.

For Default Condition 2, the filter is triggered if:

- The SPF result is PermError, TempError, None, **or** Neutral **AND** the DKIM result is Fail. The operator between SPF results and sender ID validation is **OR**.
  The SPF results are defined as follows:
  - **Fail**: The domain owner's SPF record does not authorize the sender host machine to send email for the domain.
  - **SoftFail**: The domain owner's SPF record allows the sender host machine to send email for this domain, even though the host is not explicitly authorized to do so.
  - **Neutral**: The domain owner's SPF record makes no statement as to whether the sender host machine is authorized to send email for the domain.
  - **None**: The lack of definitive SPF information prevents an SPF check (e.g., an SPF record does not exist).
  - **PermError**: A permanent error occurs (e.g., the SPF record has an invalid format).
  - **TempError**: A transient error occurs (e.g., a DNS timeout).

The following graphic summarizes the relationships among the spoofed email filter options:



If both sender address comparison and sender authentication condition tools are enabled, then at least one address comparison must fail *and* one authentication condition must be met to trigger the filter.

6) (*Optional*) Select a condition name to edit an existing condition, or select **Add** to create a new set of conditions.

7) Configure additional filter settings and click **OK**.
The spoofed email filter settings are saved.

Add or edit a spoofed email condition

Steps

1) From the section Advanced, select a condition name to edit an existing condition, or select **Add** to create a new set of conditions.
   The dialog box Add (or Edit) Condition displays.

2) If adding a new condition, enter a name in the field **Condition Name**.
   For an edit operation, this field is prefilled with the existing condition name.

3) From the section **SPF Result**, mark the check boxes next to the SPF results, if any, that the filter should detect.
   The operator between multiple SPF result selections is "**or**."

4) From the section **DKIM Result**, mark the check boxes next to the DKIM results, if any, that the filter should detect.
   The operator between multiple DKIM result selections is "**or**."

   Important
   The operator that joins selected SPF and DKIM results in a condition rule is "**and**."

5) Enable additional sender authentication; mark the check box **Validate Sender ID**. Selected SPF results are also used if the Sender ID option is selected.
   At least one SPF result must be selected in order to use the sender ID validation function.
   The operator between these two options is "**or**."
   For example, when both SPF and sender ID options are selected, if a message passes the SPF check but fails sender ID validation, the condition is considered failed. If only SPF options are selected, that same message passes the SPF check, and the condition is considered passed.

6) Select **OK**.
   The spoofed email condition is saved.

Email attachment

An email attachment policy filter allows Forcepoint Email Security to examine email attachment content and determine an attachment's true file type. The filter is triggered when a specified true file type is detected. Configure the email attachment filter on the page **Main** > **Policy Management** > **Filters** > **Add (or Edit) Filter**.

An additional option is available to designate an individual file attachment extension or filename allows the filter to detect the specified extension or filename. However, attachment content is not inspected for true file type when this option is enabled.

Configure email attachment filter analysis

Steps

1) From the section Filter Properties, mark the check boxes for the true file types that the filter should detect.
   Expand top-level categories; click the **plus sign**.
   Select all file types in a category; mark the check box for the top-level file type.
   Select all categories; at the top of the URL Categories list, mark the check box **All file types**.

2) (*Optional*) In the field **Find file type**, enter a file type category or extension to search the list of file types.

3) Allow the filter to examine the contents of archive files; mark the check box **Analyze archive files**.
   This option is enabled by default.

4) In the field **Custom filenames and extensions**, enter a comma-separated list of any custom filenames or file extensions that the filter should detect.
   Wildcard entries (*) are not supported.

5) From Filter response, select the desired filter response:
   - **Remove specified file attachments**
   - **Take no action**
     This is the default.

6) From the bottom of the section Filter Properties, click **Advanced**. The Advanced settings display.

7) Send a notification email when an email message triggers the filter; mark the check box **Notify recipient that the delivered email message contained a file attachment that triggered a filter**.

8) In the text box, keep the default notification text or enter a custom message.

9) Select the location for the notification text:
   - **Insert notification at top of message**
   - **Insert notification at bottom of message**

10) Configure additional filter settings and click **OK**. The email attachment filter is saved.

URL analysis

URL analysis examines email content for embedded URLs and classifies them according to a Forcepoint database of known spam URLs. When the filter detects a URL in a message from a selected category, it applies any configured filter response, such as removing the URL or modifying the URL to neutralize it. Configure the URL analysis filter on the page **Main** > **Policy Management** > **Filters** > **Add (or Edit) Filter**.

This filter uses one of the following services to perform URL analysis:

- Threat Intelligence Cloud Service, the cloud-hosted Forcepoint URL Database of classified URLs.
- Filtering Service, used to access the local copy of the Forcepoint URL Database maintained by your web security product (Forcepoint Web Security or Forcepoint URL Filtering).

- Linking Service, used with a Forcepoint Web Security on-premises solution to access the local copy of the URL Database as well as any custom categories you have created. This service also provides dynamic category mapping updates from the database.

The Filtering Service URL analysis performance can be more efficient than the Linking Service because the Filtering Service can perform bulk URL queries, whereas the Linking Service cannot. See *URL analysis* for more information about selecting a URL analysis service and integrating with Forcepoint Web Security solutions.

Dashboard charts summarize the instances of embedded URLs detected by the filter. A URL Analysis message type appears in the message type or message analysis result fields in presentation reports and dashboard charts. See *Available dashboard charts*.

When the URL analysis filter triggers, the default action is to drop the message and save it to the spam queue, where it may be released and delivered by a Personal Email Manager user. As a result, a message that contains a malicious link may be delivered to an inbox in your network.

Multiple URL analysis policy rules can be configured to detect and contain malicious URLs so that they cannot be released by a Personal Email Manager end user. When you configure a URL Analysis filter for this case, ensure that all **Security** URL categories are selected in the URL Categories list. See *Managing filter actions* to create a URL analysis filter action for handling email that may contain a malicious URL.

Note

A filter action option of “Resume message analysis” is also available so that message analysis can continue after a URL match is detected. See *Creating and configuring a filter action*.

Related concepts

URL analysis on page 76
Available dashboard charts on page 32
Managing filter actions on page 193

Related tasks

Creating and configuring a filter action on page 195

Configure URL analysis filter

Steps

1) From the section Filter Properties, in the list URL Categories, mark the check boxes for each URL category that the filter should detect.

   Expand top-level categories; click the **plus sign**.

   Select all sub-categories in a top-level category; when the category is expanded, click **select all**.

   Deselect all sub-categories in a top-level category; click **unselect all**.

   Select all categories; at the top of the URL Categories list, click **All Categories**.

   Note

   You can configure URL analysis policy rules to detect and contain malicious URLs so that they cannot be released by a Personal Email Manager end user. Configuration requires all URL categories under **Security** to be selected.

   See *Managing filter actions* for information about creating a URL analysis filter action for handling email that may contain a malicious URL.

2) From Filter response, mark the check box for one or both of the following filter responses; **Modify matching URLs** and **Bypass URL analysis if message size exceeds**.

   - Modify matching URLs
     Selection displays options for modifying and neutralizing URLs. Select the desired response and notification options when a malicious URL is detected:

     - **Remove matching URLs from message subject and body.** Neutralize URLs by rewriting the scheme and bracketing the last dot of the URL domain.
       Selection changes a malicious URL as follows:

       Before neutralization: http://www.malicious.com.ca/index.html.

       After neutralization: hXXp://www.malicious.com[.]ca/index.html.
     - **Rewrite URLs and link text labels with custom settings.**
       Enter the rewritten URL in the text field Rewritten URL or leave the field blank to remove URLs.

       Enter the rewritten link text label in the text field **Rewritten link text label** or leave the field blank to remove link text labels.
     - (*Optional*) From the section Options, mark the check box **Notify recipient when an email contains a modified URL**.
       In the text box, enter the desired notification text.

       Maximum length of 8192 characters total, up to 990 characters per line; a line break is two characters. The %CATEGORY% variable can be used in the notification message to inform the recipient about the specific categories triggered by the filter.

       Select where the notification should appear; **Insert notification at top of message** or **Insert notification at bottom of message**.

       The default location is at the top of the message.
   - **Bypass URL analysis if message size exceeds**
     In the text field, enter a message size in KB (default is 3072).

     Selection indicates to use message size to determine whether URL analysis is bypassed.

3) Configure additional filter settings and click **OK**.
   The URL analysis filter is saved.

Related concepts
Managing filter actions on page 193

Custom URLs and link text labels

The following variables can be used to rewrite URLs and link text labels with custom settings:

- %NURI%: neutralized URL
- %URI%: original URL
- Using this variable may leave potentially malicious URLs exposed.
- %LINKTEXT%: original link text label
- Only available for HTML links.
- %HOST%: domain name
- %CATEGORY%: Forcepoint URL category name

The following table details examples of HTML links, HTML text, and plain text rewritten using the available variables.

Sample Link	Variable	Rewritten Link
HTML link: here	%URI%	http://www.malicious.com/index.php
	%NURI%	hXXp://www.malicious[.]com/index.php
	%HOST%	www.malicious.com
	%CATEGORY%	Adult Material
	%LINKTEXT%	here
HTML text only: http://www.malicious.com/index.php	%URI%	http://www.malicious.com/index.php
	%NURI%	hXXp://www.malicious[.]com/index.php
	%HOST%	www.malicious.com
	%CATEGORY%	Adult Material
Plain text: http://www.malicious.com/index.php	%URI%	http://www.malicious.com/index.php
	%NURI%	hXXp://www.malicious[.]com/index.php
	%HOST%	www.malicious.com
	%CATEGORY%	Adult Material

Remove URL and neutralize URL

The following table details examples of removed and neutralized HTML links, HTML text, and plain text using the available variables.

Sample Link	Remove URL	Neutralize URL

HTML link: here	here	here
HTML text only: http://www.malicious.com/index.php		hXXp://www.malicious[.] com/index.php
Plain text: http://www.malicious.com/index.php		hXXp://www.malicious[.] com/index.php

Customize URL and customize link text

The following tables detail examples of customized HTML links, HTML text, and plain text using the variables %URI% or %LINKTEXT%. URLs and link text labels are removed when the text fields Rewritten URL or Rewritten link text label are left blank.

Keep original URL and keep link text

Sample Link	Customized URL	Customized Link Text	Result
HTML link: here	%URI%	%LINKTEXT%	here
HTML text only: http://www.malicious.com/index.php	%URI%	%LINKTEXT%	http://www.malicious.com/index.php
Plain text: http://www.malicious.com/index.php	%URI%	%LINKTEXT%	http://www.malicious.com/index.php

Neutralize URL and keep link text

Sample Link	Customized URL	Customized Link Text	Result
HTML link: here	%NURI%	%LINKTEXT%	here
HTML text only: http://www.malicious.com/index.php	%NURI%	%LINKTEXT%	hXXp://www.malicious[.]com/index.php
Plain text: http://www.malicious.com/index.php	N%URI%	%LINKTEXT%	hXXp://www.malicious[.]com/index.php

Customize URL and customize link text

Sample Link	Customized URL	Customized Link Text	Result
HTML link: here	http://www.urlEducation.com/index.php	Original link belonging to %CATEGORY% is malicious	<a href- ="http://www.urlEducation.com/index.php"> original link belonging to Adult Material is malicious</ a>
HTML text only: http://www.malicious.com/index.php	http://www.urlEducation.com/index.php	Original link belonging to %CATEGORY% is malicious	http://www.urlEducation.com/index.php
Plain text: http://www.malicious.com/index.php	http://www.urlEducation.com/index.php	Original link belonging to %CATEGORY% is malicious	http://www.urlEducation.com/index.php

Remove URL and keep link text

Sample Link	Customized Link Text	Result
HTML link: here	%LINKTEXT%	 here
HTML text only: http://www.malicious.com/index.php	%LINKTEXT%	
Plain text: http://www.malicious.com/index.php	%LINKTEXT%	

Customize URL and keep link text

Sample Link	Customized URL	Customized Link Text	Result
HTML link: here	http://www.urlEducation.com/index.php	%LINKTEXT%	here
HTML text only: http://www.malicious.com/index.php	http://www.urlEducation.com/index.php	%LINKTEXT%	http://www.urlEducation.com/index.php

Sample Link	Customized URL	Customized Link Text	Result
Plain text: http://www.malicious.com/index.php	http://www.urlEducation.com/index.php	%LINKTEXT%	http://www.urlEducation.com/index.php

Remove URL and customize link text

Sample Link	Customized Link Text	Result
HTML link: here	original %URI% is malicious and was cleared, please be careful with this link	original http://www.malicious.com/index.php is malicious and was cleared, please be careful with this link
HTML text only: http://www.malicious.com/index.php	original %URI% is malicious and was cleared, please be careful with this link	
Plain text: http://www.malicious.com/index.php	original %URI% is malicious and was cleared, please be careful with this link	

Analysis of URLs in file attachments

URLs in supported attachments can be scanned and classified by the on-premises Email Security system according to the configured filter options. Classifiable URLs in attachments triggered by the filter settings are handled like any other email content by the URL analysis filter action. A file attachment that triggers the URL filter is classified as a URL analysis message. Only the first 50KB of content in the email attachment is scanned. Functionality is not available for the Email Security Hybrid module. URLs can be extracted and analyzed from within the following file types:

- .doc
- .docm
- .docx
- .pdf
- .ppt
- .pptx
- .rtf
- .txt
- .xls
- .xlsm
- .xlsx

Antispam

The antispam analysis function checks email for various characteristics of spam. If the email hybrid service is enabled and configured, it performs antispam analysis as well (Email Security Hybrid module is required). If email hybrid service is not configured or available, a combination of other on-premises tools is used for effective

antispam analysis. Configure the antispam filter on the page **Main** > **Policy Management** > **Filters** > **Add (or Edit) Filter**.

The email hybrid service analyzes incoming email and blocks any message that it recognizes as spam. Mail that the hybrid service allows into the system for processing includes a header that contains an analysis result score. The email system uses this score to determine how to handle the message. If that score exceeds a specified spam threshold, the email system treats the message as spam and handles it according to applicable policy. In this case, the on-premises email security software does not perform its own, separate antispam analysis.

Configure antispam filter analysis

Steps

1) (*If applicable*) Enable hybrid service spam scoring; in the box Email Hybrid Service analysis, mark the check box **Use email hybrid service analysis with a threshold score for spam of**.

   Select a spam score from the pull-down menu (floating point number between 0 and 20; default is 6).

   This option only displays when the Email Security Hybrid module is configured and running.

2) From the section Tools, mark the check boxes for one or all of the following tools:

   a) **Digital Fingerprinting analysis**
   When enabled, digital fingerprint analysis checks message content for any digital fingerprint of known spam.

   b) **LexiRules analysis**
   When enabled, the LexiRules tool analyzes message content for word patterns commonly found in spam.

   c) **Heuristics analysis**
   When enabled, heuristics analysis checks the message header or content for spam characteristics.

   The on-premises software performs a complete antispam examination using the selected tools when the Email Security Hybrid module is not enabled.

3) From the section Heuristics Analysis, set the heuristics analysis sensitivity level, from Lowest to Highest.
   The default is Medium.

4) (*Optional*) Mark the check box **Bypass antispam analysis if message size exceeds**.
   In the text field, enter a message size in KB (default is 3072).

   Selection indicates to use message size to determine whether antispam analysis is bypassed.

5) Configure additional filter settings and click **OK**.
   The antispam filter settings are saved.

Commercial bulk email

Unlike spam email, commercial bulk email is often solicited by its recipients, sometimes inadvertently. For example, a user might neglect to clear a check box to “Share my personal information with selected partners” on a typical “opt out” privacy rights form. The commercial bulk email filter can analyze a message to determine

whether it was sent from a third-party bulk email management company or directly from a business. Configure the commercial bulk email filter on the page **Main** > **Policy Management** > **Filters** > **Add (or Edit) Filter**.

If your subscription includes the Email Security Hybrid module, you can activate commercial bulk email analysis as part of the email hybrid service pre-filtering process. The results of pre-filtering are added to the message header passed to on- premises email protection software, which uses the hybrid service score to determine how the message is processed.

Configure commercial bulk email filter analysis

Steps

1) (*If applicable*) Mark the check box **Use the results of the email hybrid service analysis for on-premises commercial bulk email analysis**.

   This option only displays when the Email Security Hybrid module is configured and running.

2) From the section Filter Properties, select the sensitivity level for the filter:

   - **Normal: Analyze email source**
     Use this option to set the filter to detect email only from indirect (third-party) sources of bulk email.
   - **High: Analyze email source and content**
     Use this option to set the filter to detect both direct and indirect sources of bulk email. This is the default.

3) (*Optional*) Mark the check box **Bypass antispam analysis if message size exceeds**.

   In the text field, enter a message size in KB (default is 3072). Selection indicates to use message size to determine whether antispam analysis is bypassed.

4) Configure additional filter settings and click **OK**. The commercial bulk email filter settings are saved.

   A commercial bulk default filter action can be used along with this filter. See *Managing filter actions*.

Related concepts
Managing filter actions on page 193

Advanced file analysis

Advanced file analysis is a cloud-hosted or on-premises sandbox for deep content inspection of types of files that are common threat vectors (for example, document, executable, data, or archive files). Use the advanced file analysis filter to configure file type analysis for your network.

The cloud sandbox capability is available only if your subscription includes Forcepoint Advanced Malware Detection for Email - Cloud. For on-premises analysis, you need to deploy a separate Forcepoint Advanced Malware Detection for Email - On-Premises.

Configure the advanced file analysis platform on the page **Settings** > **General** > **Advanced File Analysis**. You may select only one platform for advanced file analysis. See *Selecting advanced file analysis platform*. When you configure an advanced file analysis filter, the platform selected on the Advanced File Analysis page is reflected on the Add/Edit Filter page. Available filter settings depend on the platform used.

The filter can be used in either monitor or enforce mode, with an option for sending a notification message when the enforce mode is active, when the filter is triggered, and when the attachment is sent to advanced file analysis. You can define conditions that, when met, allow a message to bypass the advanced file analysis filter.

Related tasks

Selecting advanced file analysis platform on page 78

Configure advanced file analysis filter

Steps

1) From the section Modes, select one of the following operational modes for the filter:

   - **Monitor**
     Message is delivered to its recipient and a copy is sent to advanced file analysis. If analysis determines that the attachment is clean, no report is returned. If analysis determines that the attachment is malicious, the message is copied to a specified queue. A notification email can be sent regarding the analysis result. This is the default.

     Configure the corresponding filter action to ensure that the email message that triggered the filter is delivered to its recipient along with the attachment (Main > Policy Management > Actions). The default queue is the virus queue. See Managing filter actions, page 189.
   - **Enforce**
     Message is held in a queue until advanced file analysis is performed. If analysis determines that the attachment is clean, message processing is resumed. If analysis determines that the attachment is malicious, the email is quarantined. A notification email can be sent regarding the analysis result.

     Configure the corresponding filter action to ensure that the email message that triggered the filter is dropped and saved to a specified queue (**Main** > **Policy Management** > **Actions**). The default queue is the virus queue. See *Managing filter actions*.

     a) (*Only applicable if* ***Enforce*** *is selected in step 1*) Notify the recipient when analysis is underway, mark the check box **Send enforcement notification**.
     Selection displays the Notification Properties section with functionality to configure the notification email, which contains the original message as an attachment. The message attachment is handled as follows:

        - Some file types are converted to plain text (for example, .pdf, .doc/.docx, .xls/.xlsx, and .ppt/.pptx).
        - Files of other types are removed and only the filename appears in the message (for example, .exe and archive files).

     b) From the section Notification Properties, configure the email notification:
     From Sender, click the radio button for identifying the notification message sender; **Administrator** or **Custom**.

        The default is Administrator. If you select this option, you must configure a valid administrator email address on the page **Settings** > **General** > **System Settings** (see *Setting system notification email addresses*).

        Selection of Custom enables a text field to enter the sender address. If you choose this option, you can designate only one sender address.

     c) From Recipient, mark the check box for one or more message recipients: **Original email recipient**, **Administrator**, or **Custom**.
     The default is Administrator. If you select this option, you must configure a valid administrator email address on the page **Settings** > **General** > **System Settings** (see *Setting system notification email addresses*).

        - Selection of Custom enables a text field to enter the recipient addresses. If you choose this option, you can designate one or more recipient addresses, separated by semicolons.
        - In the text field **Subject**, enter the subject to be displayed when the notification is received.
        - In the text field **Content**, enter the text to be displayed in the notification message body.
        - From Attachment, specify whether to include the original message as an attachment to the notification message; **Do not attach message** or **Attach analyzed message**.
          The default is Do not attach message.

2) From the section File Types, mark the check boxes for the file types that cloud- hosted Advanced Malware Detection - Cloud should find and analyze.

   Expand top-level categories; click the **plus sign**.

   Select all file types in a category; mark the check box for the top-level file type.

   Select all categories; at the top of the File Types list, mark the check box **All file types**.

   This option is not available for the Advanced Malware Detection - On-Premises platform.

3) Configure bypass options for messages that should be excluded from advanced file analysis; from the section Advanced file analysis bypass conditions, select an existing condition name or add a new condition by clicking **Add**.

   The Add Bypass Condition dialog box displays to configure the following settings:

   - In the text field **Condition name**, enter a name for each set of bypass conditions.
   - In the text field **Sender email address/domain**, enter an individual email address or domain.
     Use an asterisk (*) for wildcard entries and separate multiple entries with a semicolon (;).
   - In the text field **Attachment filename keyword**, enter a character string that is included in the attachment filename.
     Use an asterisk (*) for wildcard entries.
   - Click **OK**.
     The settings are saved and the new condition displays in the list of bypass conditions.

4) (*Optional*) Mark the check box **Bypass advanced file analysis if message size exceeds**.

   In the text field, enter a message size in MB for the cloud-hosted file sandbox (default is 32), or enter a value that equals the maximum file size accepted by that appliance for Advanced Malware Detection - On-Premises.

   Selection indicates to use message size to determine whether advanced file analysis is bypassed.

5) Configure additional filter settings and click **OK**.

   The advanced file analysis filter settings are saved. See *Creating and configuring a filter action* for information about configuring an action for the advanced file analysis filter.

Related concepts

Managing filter actions on page 193

Related tasks

Setting system notification email addresses on page 86
Creating and configuring a filter action on page 195

Custom content

Use a custom content filter to allow message analysis based on conditions you configure. The Email module does not provide a default custom content filter.

Note

You can use the Add (or Edit) Rule page to add a rule for a custom content filter. You must have already defined a custom content filter before you attempt to add a custom content rule. See *Adding a rule*.

Custom content filter options are configured on the page **Main** > **Policy Management** > **Filters** > **Add (or Edit) Filter**.

Related concepts

Adding a rule on page 205

Configure custom content filter

Steps

1) Configure whether to trigger the filter on the match of a single condition or on all defined conditions; from the section Filter Properties, click the radio button **Match all conditions** or **Match any condition**.

2) Specify the conditions; from the section Filter Conditions, click **Add**. The Add Condition dialog box displays.

3) In the Add Condition dialog box, select the message attributes and operators to configure the custom filter.

The following table displays all available message attributes and operators. All message attributes except DKIM verification include the user-configurable entry field Filtering criteria.

Message Attribute	Operator Options	Additional Options
Sender IP address	Is, Is not	None
Envelope sender	Contains, Does not contain, Matches regular expression, Does not match regular expression	None
Envelope recipient	Contains, Does not contain, Matches regular expression, Does not match regular expression	None
Number of envelope recipients	Equals, Does not equal, Is less than, Is greater than	None
From field address	Contains, Does not contain, Matches regular expression, Does not match regular expression	None
To field address	Contains, Does not contain, Matches regular expression, Does not match regular expression	None
Cc field address	Contains, Does not contain, Matches regular expression, Does not match regular expression	None
Message subject	Contains, Does not contain, Matches regular expression, Does not match regular expression	Match case
Message header: partial	Contains, Does not contain, Matches regular expression, Does not match regular expression	Message attribute text (user configured), Match case
Message header: complete	Contains, Does not contain, Matches regular expression, Does not match regular expression	Match case
Message body text	Contains, Does not contain, Matches regular expression, Does not match regular expression	Match case
Message size	Equals, Does not equal, Is less than, Is greater than	Filtering criteria is in KB
DKIM verification result	DKIM verification is successful, DKIM verification failed	None
True Source IP	Is, Is not	None
Digital Fingerprinting analysis result	Is spam, Is clean	None
LexiRules analysis result	Is spam, Is clean	None
Heuristics analysis result	Equals, Is less than, Is greater than	Enter a floating-point value from 0–25. For example, the value 6 corresponds to a heuristics analysis level of Medium.
Email hybrid service analysis result (available only when your	Equals, Is less than, Is greater than	Enter a floating-point value from 0–25. For example, the email

4) Click **OK**.
   The Add Condition dialog box closes and the conditions are added to the Filter Conditions list.

5) Change the order of filter conditions; mark the check box next to the filter in the Filter Conditions list and click **Move Up** or **Move Down**.

6) Delete a set of filter conditions; mark the check box next to the filter in the Filter Conditions list and click **Remove**.

7) Configure additional filter settings and click **OK**.
   The custom content filter settings are saved.

Disclaimer

The disclaimer filter automatically adds defined text to the beginning or end of a message. Disclaimer filter options are configured on the page **Main** > **Policy Management** > **Filters** > **Add (or Edit) Filter**.

Configure a disclaimer filter

Steps

1) From the section Filter Properties, in the text field **Primary disclaimer**, enter the text for the primary disclaimer.
   A primary disclaimer may be written in any language, as long as the email message supports the same character set. The disclaimer text may be between four and 8192 characters in length. A line break uses two characters.

2) In the text field **Secondary disclaimer**, enter the text for the secondary disclaimer.
   The secondary disclaimer must be written in English, to be used when the email does not support the primary disclaimer character set.

3) From Disclaimer position, click the radio button to specify where the disclaimer should appear in the email, **Beginning of message** or **End of message**.

4) Allow message recipients to report a message as spam; mark the check box **Enable Report Spam feature**.
   Text boxes are enabled to configure either a rich text or plain text version of the Report Spam disclaimer. The link in the rich text disclaimer sends the recipient to the Personal Email Manager, where the message is automatically reported to Forcepoint as spam. The plain text disclaimer provides a default message with instructions for reporting spam to Forcepoint.

5) Configure additional disclaimer filter settings and click **OK**.
   The disclaimer filter settings are saved.

Managing filter actions

A filter action determines the final disposition of a message. The email security software analyzes messages and their attachments, then performs an action based on applicable policy settings. Actions are created on the page

Main > **Policy Management** > **Actions**. You can add a defined action to a policy rule when you configure your email policies.

In addition to defining an action used in an email policy, you can create an action for use in an email DLP action plan in the Data Security module. See Forcepoint DLP Administrator Help for information about DLP action plans.

For most network configurations (i.e., single standalone appliance or single appliance cluster), the property settings available for creating an action for an email DLP policy are the same as those for a policy action configured for the email security software.

However, if your network includes multiple standalone appliances or multiple clusters, limited DLP policy action settings are available when an action is initially created. Unless otherwise noted, the procedures for creating and configuring a filter action apply to both email and DLP policy actions.

The following default actions are available on the page **Main** > **Policy Management** > **Actions**:

- **Virus**: Drop the filtered message and save the original message to the **virus** queue. Allow a Personal Email Manager end user to view and manage the message.
- **Spoof**: Deliver the analyzed message and add “POSSIBLY SPOOFED:” to the message subject. Allow a Personal Email Manager end user to view and manage the message.
- **Email Attachment**: Drop the filtered message and save the original message to the **attachment** queue. Do not allow a Personal Email Manager end user to view and manage the message.
- **URL Analysis**: Drop the analyzed message and save the original message to the spam queue. Allow a Personal Email Manager end user to view and manage the message.
  You can configure multiple URL analysis rules if you are concerned that a Personal Email Manager end user may inadvertently release email that contains a malicious URL. In that case, you can set the following characteristics for your action:
  1) Set the action taken to **Drop Message**.
  2) In the section Drop Message Options, set the **Save the original, unanalyzed message to a queue** pull-down menu to the **url-analysis** default queue.
  3) Select **Do not display** for the Personal Email Manager end-user portal option, to prevent an end user from controlling message delivery.
  4) Click **OK** to save the new action.
- **Spam**: Drop the analyzed message and save the original message to the spam queue. Allow a Personal Email Manager end user to view and manage the message.
- **Commercial Bulk**: Deliver the analyzed message and add “COMMERCIAL:” to the message subject. Allow a Personal Email Manager end user to view and manage the message.
- **Advanced File Analysis**: Drop the analyzed message and save the original message to the virus queue. Send a notification message without attaching the original email to the original email sender.

Remove a filter action

You can delete a filter action only if its current status is **Not referenced**, which means that the action is not currently used in a policy rule or action plan. A filter action that is currently referenced by a filter or action plan does not have a check box for selection. You cannot remove a default email filter action.

1) Mark the check box to the left of the filter action name and click **Delete**.
   The Confirm Action Delete dialog box displays.

2) In the dialog box, click **Yes**. The filter action is deleted.

Add a new filter action

Click **Add**.

The Add Action page displays. See *Creating and configuring a filter action*.

Related tasks

Creating and configuring a filter action on page 195

Editing an existing filter action

Edit an existing filter action by clicking the action name on the page **Main** > **Policy Management** > **Actions**. The Edit Action page opens, displaying the current action properties. Modify any of the options listed in *Creating and configuring a filter action*.

You can also use this operation to change any default property configured when you created a data action. See *Deliver message* for default setting details.

Related tasks

Creating and configuring a filter action on page 195
Deliver message on page 196

Creating and configuring a filter action

Add a filter action and configure its properties on the page **Main** > **Policy Management** > **Actions**.

Add a new filter action

Steps

1) Click **Add**.
   The Add Action page displays.

2) In the text field **Action Name**, enter a name for the action.

3) From the pull-down menu **Used by**, select the policy type for which this action can be used: **Email** or **Data**.
Your selection determines which action properties are available when you create the action.

Email policy action options include:

- *Deliver message*
  This is the default.
- *Resume processing*
- *Drop message*

DLP policy action options include:

- *Deliver message*
  This is the default.
- *Drop message*

Related tasks
Deliver message on page 196
Resume processing on page 199
Drop message on page 199

Deliver message

The Deliver Message option includes the same action properties for both email and DLP policy actions. However, in some cases, the behavior for an email policy action and a DLP policy action in a single appliance/single cluster network is different from that for a DLP policy action that is created in a multiple appliance/multiple cluster environment.

Configure message delivery options

Steps

1) Click **Add**.
The Add Action page displays.

2) In the text field **Action Name**, enter a name for the action.

3) From the pull-down menu **Used by**, select the policy type for which this action can be used: **Email** or **Data**.

4) From the pull-down menu **Action taken when a message triggers a filter**, select **Deliver Message**.
Selection indicates to deliver an email message to its intended recipient. This option is the default selection for both an email policy action and a DLP policy action.

5) Define the following message delivery options:

1) - **Enable header modification.** Mark this check box to open a set of header modification condition entry fields. Options include the following:

Condition	Parameters
Add or rewrite header value	Header name, To value

Condition	Parameters
Remove header	Header name
Remove header if condition matches	Header name, If header contains the value
Find and replace header value	Header name, Find, Replace with
Add or append to header value	Header name, Add/append value
Add or prepend to header value	Header name, Add/prepend value

Click the icons at the end of each condition line to delete the current header modification condition or to add a new condition below the current condition.

- **Bcc the original unanalyzed message to**: Enter at least one email address to which to send a blind copy of the unanalyzed message; for example, the email system administrator. Separate multiple email addresses with a semicolon.
- **Delay message delivery until**: Specify a day and time for a delayed message delivery. You may select this option to delay the delivery of a message for some reason, for example, to send a large volume of marketing email at a time of low corporate email activity. This action option is recommended for use with a Custom Content filter in a policy rule. See *Custom content*.
- **Use IP address**: Specify an appliance IP address from the pull-down menu for message delivery. Only standalone appliances are included in the IP address list.

  Note

  This option is available for a DLP action being created in a multiple standalone appliance environment. The default setting is the appliance E1 or P1 interface.

  This setting may be customized for each standalone appliance.

  The IP addresses in the list are configured in the Forcepoint appliance. (See the Forcepoint Appliances Getting Started Guide or Forcepoint Appliances Command Line Interface (CLI) Guide for information.)

  This feature is useful for routing a large volume of outbound email. This action option is recommended for use with a Custom Content filter in a policy rule. See *Custom content*.
- **Deliver email messages based on domain-based route**: Specify message delivery via a defined domain-based route. Select the desired route from the pull-down menu. You can also modify the selected route by clicking **Edit Route**.

  Note

  This option is available for a DLP action being created in a multiple appliance/multiple cluster environment. The default setting is the domain-based route (**Settings** > **Inbound/Outbound** > **Mail Routing**). Change the default setting by selecting **Add Domain Based Route** in the pull- down menu.

  This setting may be customized for each appliance.
- **Save the original, unanalyzed message to a queue**: Send the message to a specified message queue for further processing. Select the **Add Queue** option to add a new queue for this filter action.

  Note

  This option is available for a DLP action being created in a multiple appliance/multiple cluster environment. The default setting is **data-security**. Change the default setting by selecting **Add Queue**.

  This setting may be customized for each appliance.

- **Personal Email Manager portal options**: This option is enabled only when the option **Save the original message to a queue** is marked. Specify how the queued message is handled in the Personal Email Manager end-user portal by selecting one of the following:
  - **View and manage messages**: Allow the end user to view the message and perform any action available in the Personal Email Manager end-user tool.
  - **Do not display**: Ensure the message does not appear in the Personal Email Manager end-user portal.
  - **Message log only**: Pertinent information about the message appears in the Personal Email Manager end-user portal, but the end user has only limited access. The user cannot view message content; deliver, download, or forward the message; or add the address to the personal Always Block or Always Permit lists.

6) (*DLP only*) Mark the check box **Drop attachment**.
   Select this option to remove an attachment from an email message as part of the policy action. Only available for DLP policy actions.

7) (*Optional*) Mark the check box **Send notification**.
   Use this option to configure a notification message to be sent regarding the delivered email.

8) Configure the following notification message settings:
   - **Sender**: Identify the notification message sender, from among the following options:
     - Original email sender.
     - Administrator (default). If you use this option, you must configure a valid administrator email address on the page **Settings** > **General** > **System Settings** (see *Setting system notification email addresses*).
     - Custom. If you choose this option, you can designate only one sender address.
   - **Recipient**: Identify the notification message recipient from among the following options:
     - Original email sender.
     - Original email recipient.
     - Administrator. If you use this option, you must configure a valid administrator email address on the page **Settings** > **General** > **System Settings** (see *Setting system notification email addresses*).
     - Custom. If you choose this option, you can designate one or more recipient addresses, separated by semicolons.
   - **Subject**: Enter the subject to be displayed when the notification is received.
   - **Content**: Enter the text to be displayed in the notification message body.
   - **Attachment**: Specify whether to include the original message as an attachment to the notification message. Select from among the following:
     - Do not attach message (default)
     - Attach original unanalyzed message
     - Attach analyzed message

9) Click **OK**.
   The settings are saved.

Related concepts
Custom content on page 190

Related tasks
Setting system notification email addresses on page 86

Resume processing

Use the Resume Processing option when you want to continue message analysis using the next filter in sequence if the current filter is triggered (for example, after a URL match is detected in a message). If this option is the final triggered filter's action, the message is delivered.

Additional message action options are the same as for message delivery.

Configure message processing options

Steps

1) Click **Add**.
   The Add Action page displays.

2) In the text field **Action Name**, enter a name for the action.

3) From the pull-down menu **Used by**, select the policy type for which this action can be used: **Email** or **Data**.

4) From the pull-down menu **Action taken when a message triggers a filter**, select **Resume Processing**.
   Selection indicates to deliver an email message to its intended recipient. This option is the default selection for both an email policy action and a DLP policy action.

5) Additional message action options are the same as for *Deliver message*; configure the options as needed.

6) Click **OK**.
   The settings are saved.

Drop message

Use the Drop Message option to delete a message without delivering it to its intended recipient. This option is available for both email and DLP policy actions.

Configure dropped message actions

Steps

1) Click **Add**.
   The Add Action page displays.

2) In the text field **Action Name**, enter a name for the action.

3) From the pull-down menu **Used by**, select the policy type for which this action can be used: **Email** or **Data**.

4) From the pull-down menu **Action taken when a message triggers a filter**, select **Drop Message**.
Selection indicates to delete a message without delivering it to the intended recipient.

5) Forward the dropped message; mark the check box **Forward to** and enter at least one email address in the text field.

6) Send the dropped message to a queue for further processing; mark the check box **Save the original, unanalyzed message to a queue** and select the desired queue from the pull-down menu.
Marking this check box enables the **Personal Email Manager portal options**. Specify how the dropped message is handled in the Personal Email Manager end- user portal by selecting one of the following:

- **View and manage messages**: Allow the end user to view the message and perform any action available in the Personal Email Manager end-user tool.
- **Do not display**: Ensure the message does not appear in the Personal Email Manager end-user portal.
- **Message log only**: Pertinent information about the message appears in the Personal Email Manager end-user portal, but the end user has only limited access. The user cannot view message content; deliver, download, or forward the message; or add the address to the personal Always Block or Always Permit lists.

Note

This option is available for a DLP action being created in a multiple appliance/multiple cluster environment. The default setting is **data-security**. Change the default setting by selecting **Add Queue**.

This setting may be customized for each appliance.

7) (*Optional*) Mark the check box **Send notification**.
Use this option to configure a notification message to be sent regarding the delivered email.

8) Configure the following notification message settings:
   - **Sender**: Identify the notification message sender, from among the following options:
     - Original email sender.
     - Administrator (default). If you use this option, you must configure a valid administrator email address on the page **Settings** > **General** > **System Settings** (see *Setting system notification email addresses*).
     - Custom. If you choose this option, you can designate only one sender address.
   - **Recipient**: Identify the notification message recipient from among the following options:
     - Original email sender.
     - Original email recipient.
     - Administrator. If you use this option, you must configure a valid administrator email address on the page **Settings** > **General** > **System Settings** (see *Setting system notification email addresses*).
     - Custom. If you choose this option, you can designate one or more recipient addresses, separated by semicolons.
   - **Subject**: Enter the subject to be displayed when the notification is received.
   - **Content**: Enter the text to be displayed in the notification message body.
   - **Attachment**: Specify whether to include the original message as an attachment to the notification message. Select from among the following:
     - Do not attach message (default)
     - Attach original unanalyzed message
     - Attach analyzed message

9) Click **OK**.
   The settings are saved.

Related tasks
Setting system notification email addresses on page 86

Managing policies

An email policy is applied based on defined sender/recipient conditions and the direction of the email. You can apply a different policy to different groups of senders and recipients. For example, you might apply one policy to a marketing department group in your organization and a different policy to a human resources group. After you define a set of senders and recipients in a policy, you can add the policy rules to apply when the sender/recipient conditions of the email match the policy.

Policy rules comprise the filters and filter actions that determine how a message that matches a policy's sender/recipient conditions is handled. Filters provide the basis for email analysis, and filter actions determine the final disposition of a message when it triggers a particular filter. After you have created and configured filters and filter actions, they are available for inclusion in your policies. See *Managing filters* and *Managing filter actions* for information about configuring filters and filter actions.

Three types of policies are available, depending on the direction of the message— inbound, outbound, or internal. Message direction is determined on the basis of an organization's protected domain addresses:

- Inbound—The sender address is not from a protected domain, and the recipient address is in a protected domain.
- Outbound—The sender address is from a protected domain, and the recipient address is not in a protected domain.
- Internal—Both the sender and recipient addresses are in a protected domain.

One predefined default policy is available for each email direction, along with a default data loss prevention (DLP) policy for each direction.

Data loss prevention policies may be applied to email in any direction. These policies are configured in the Data Security module of the Forcepoint Security Manager and are enabled or disabled in the Email Security module. You need to register the Email Security module with the Data Security module and click **Deploy** in the Data Security module for the policies to be active. See *Enabling data loss prevention policies*.

Changing policy order

After you add a policy, select it and use the **Move Up** and **Move Down** buttons to move it up or down in the policy list in order to specify when the policy is applied. When message conditions match a policy, subsequent policies in the list are not applied.

You cannot change the order of default policies. They are applied last when a message matches no other policy.

Deleting a policy

Remove a policy by marking the check box next to the policy name on the Policies page and clicking **Delete**. A default policy cannot be deleted.

Related concepts

Managing filters on page 171
Managing filter actions on page 193

Related tasks

Enabling data loss prevention policies on page 202

Enabling data loss prevention policies

In addition to creating and enabling policies that protect your email system from email threats, you can enable DLP policies that can detect the presence of sensitive data in your organization's email and execute appropriate actions to prevent data loss. You can use DLP policies for inbound, outbound, and internal email.

Configure email DLP policies in the Data Security module of the Forcepoint Security Manager (**Main** > **Policy Management** > **DLP Policies** > **Manage Policies**). A new policy wizard provides the steps for creating a new email DLP policy. See Forcepoint DLP Administrator Help for detailed information.

It is recommended to create a DLP policy in the Data Security module to use message encryption. Ensure that the policy has an action plan of "encrypt." See *Handling encrypted messages* for information about email encryption options.

You can also create filter actions for use in a DLP action plan. See *Creating and configuring a filter action* for information about configuring a DLP filter action.

Data loss prevention policies are enabled by default in the Email Security module. However, the Email Security module must be registered with the Data Security module before the policies are applied to email. See *Registering the DLP Module* for instructions on how to register with the Data Security module.

Steps

1) From the section Inbound, Outbound, or Internal on the page **Main** > **Policy Management** > **Policies**, click **Data Loss Protection**.
   The Edit Policy page displays.

2) On the page Edit Policy, set the following options:
   - **Status**: Enabled or Disabled. Enable or disable the DLP policy. Data loss prevention policies are enabled by default.
   - **Mode**: Monitor or Enforce. Select **Monitor** to enable the data loss prevention function to simply monitor your email, and select **Enforce** to apply DLP policies to your email.
   - **Notification**: Add a notification to a message when an email attachment to that message has been dropped as a result of a DLP policy.
     a) Enable notifications; mark the check box **Send notification when a message attachment is dropped**.
     b) In the text field, enter the notification message text.
     c) Select whether the notification text appears above or below the message body of the mail whose attachment was dropped.

     Note
     A message that triggers a DLP policy whose action is Quarantine is isolated in the Data Security module quarantine queue, not in an Email Security module queue. The message can be released for delivery by the Data Security module.

3) Click **OK**.
   The settings are saved.

Related concepts
Handling encrypted messages on page 163
Registering the DLP Module on page 68

Related tasks
Creating and configuring a filter action on page 195

Adding or editing a policy

Use the page **Main** > **Policy Management** > **Policies** to create a new inbound, outbound, or internal policy.

Steps

1) From the section Inbound, Outbound, or Internal on the page **Main** > **Policy Management** > **Policies**, click **Add**.
   The Add Policy page displays.

2) In the text field **Policy name**, enter a unique policy name.
   The policy name must be between 4 and 50 characters long. Use of the following special characters in the policy name is not recommended:
   * < > { } ~ ! $ % & @ # . " | \ & + = ? / ; : ,
   Policy names can include spaces, dashes, and apostrophes.

3) In the text field **Description**, enter a clear and concise description of the policy.
   The special character recommendations that apply to policy names also apply to descriptions.

4) From **Status**, select a status of **Enabled** or **Disabled** for your policy.

5) From the pull-down menu **Order**, define the order in which this policy is applied.
   By default, the new policy is placed at the top of the list. You cannot have multiple policies with the same order number. If you select a number that is already in use,
   the policy that currently has that number and all those below it move down one place in the list.

6) From the section **Sender/Recipient Conditions**, define the sender/recipient conditions.
   By default, each new policy contains a sender/recipient condition that applies the policy to all email senders and recipients. To add more conditions, click **Add**, and then see *Adding Sender/Recipient Conditions*.

   Note
   You must define at least one sender/recipient condition. A policy that does not contain a sender/recipient condition will not be applied.

7) From the section **Rules**, edit the available rules to tailor the filters and actions to this policy.
   Click a rule name, and then see *Editing rules*.

8) Click **OK**.
   The policy settings are saved.

Related tasks
Adding Sender/Recipient Conditions on page 204
Editing rules on page 207

Adding Sender/Recipient Conditions

While creating a policy on the page **Main** > **Policy Management** > **Policies** > **Add Policy**, use the page **Add Policy** > **Add Sender/Recipient Condition** to specify the senders and recipients to which a policy applies. You can make the policy as wide- ranging as required; for example, applying it to all users, or all users receiving mail in a particular domain, or specific email addresses only.

Steps

1) From the section **Sender/Recipient Conditions** on the page Add Policy, click **Add**.
   The Add Sender/Recipient Condition page displays.

2) For each sender/recipient condition, select a **Sender Source** and **Recipient Source**:
   - **Local Address**: If you select Local Address, enter the sender or recipient email addresses to use with the policy. You can use the asterisk wildcard to specify combinations, for example:
     - *.mycompany.com applies the policy to all users with a mycompany.com email address.
     - *sales@mycompany.com applies the policy to a subset of all email addresses in mycompany.com, such as us_sales@mycompany.com and uk_sales@mycompany.com.
     - john.doe@mycompany.com applies the policy to a specific user. To apply the policy to all email addresses, enter an asterisk (*).
   - **User directory**: If you select User directory, select the directory source from the pull-down menu. You must set up a user directory to connect to before selecting this option. From the pull-down menu, select **Add User Directory** to create a new directory source.
   - **Domain group**: If you select Domain group, select the domain source from the pull-down menu of existing domain groups or add a new domain group by selecting **Add Domain Group**.

3) Click **OK**.
   The Add or Edit Policy page displays to finish editing or creating a policy. See *Adding or editing a policy*.

Related tasks
Adding or editing a policy on page 203

Deleting Sender/Recipient Conditions

A policy should contain at least one sender/recipient condition.

From the section Sender/Recipient Conditions on the page **Add** or **Edit Policy**, mark the check box next to the condition ID and click **Delete**.

The sender/recipient condition is deleted. See *Adding or editing a policy*.

Related tasks
Adding or editing a policy on page 203

Adding a rule

A policy rule comprises the filter applied to a message that matches a policy's sender/ recipient conditions and the action taken when that message triggers the filter. The following default rules are available:

- **Antivirus** rule uses the default virus filter and virus default filter action.
- **Email Attachment** rule uses the default email attachment filter and email attachment default filter action.
- **Antispoof** rule uses the default spoofed email filter and spoof default filter action.
- **URL Analysis** rule uses the default URL analysis filter and URL analysis default filter action.

You can configure multiple URL Analysis rules to use settings other than the defaults. See *URL analysis* and *Managing filter actions*.

- **Antispam** rule uses the default spam filter and spam default filter action.
- **Commercial Bulk** rule uses the default commercial bulk email filter and commercial bulk default filter action.
- **Advanced File Analysis** rule uses the default advanced file analysis filter and advanced file analysis default filter action.
- **Disclaimer** rule uses the default disclaimer filter.

You may create a new rule in combination with the following filter types:

- URL analysis
- Spoofed email
- Email attachment
- Custom content

Related concepts
Managing filter actions on page 193
URL analysis on page 179

Add a policy rule

Steps

1) From the section Rules on the page **Add** or **Edit Policy**, click **Add**. The Add Rule page displays.

2) In the field **Rule Name**, enter a name for the rule.

3) From **Status**, select the desired policy status, **Enabled** or **Disabled**. The default is Enabled.

4) From the pull-down menu **Order**, select the order in which the rule should apply.
   By default, a new rule is created in the first position. The Disclaimer rule is always applied last.

5) In the section Filter, from the pull-down menu **Filter name**, select a predefined filter type or click **Add filter**.
   If you select Add filter, the Add Filter page displays to define a new filter. See *Creating and configuring a filter*.

6) In the section Action, from the pull-down menu **Action name**, select a default filter action or click **Add action**.
   If you select Add action, the Add Action page displays to define a new action. See *Creating and configuring a filter action*.

7) (*Optional*) From the section Action, click **Edit**. The Edit Action page displays.

8) (*Optional*) In the section Filter Bypass Condition, click **Add**.

   The Add Filter Bypass Conditions page displays. Create filter bypass entries in the Sender Email Addresses, Recipient Email Addresses, and IP Address Groups sections in one of the following ways:

   - Add a predefined email address list; click **Browse** next to the Email Address File field and navigate to the desired text file. The file format should be one email address per line, up to a maximum of eight addresses.
   - Enter an individual email address in the **Email address** field. Click the right arrow button to add the individual entry to the **Email Address List** on the right.
   - Select the IP address groups you want to bypass analysis, and click the **arrow button** to add them to the Added IP Address Groups box. You can also define a new IP address group on this page if desired. Use an asterisk (*) in an address as a wildcard.
   - Delete an entry in an Email Address List; select it and click **Remove**.
   - Export and save an address list as a text file; click **Export All**.
   - Click **OK** to save your bypass entries.
     You cannot use these settings to bypass a custom content filter.

9) Click **OK**.

   The rule is saved and displays in the Rules section of the Edit Inbound Policy page.

   Use the buttons **Move Up** and **Move Down** to adjust rule order.

Related concepts

Creating and configuring a filter on page 173

Related tasks

Creating and configuring a filter action on page 195

Editing rules

Use the page **Add** (or **Edit**) **Policy** > **Edit Rule** to define what happens to an email message that matches the sender/recipient conditions and triggers the policy. This page contains the filter and filter action that currently define the rule that you clicked. You can also define message sender/recipient conditions that, when met, allow a message to bypass the filter.

Steps

1) From the section Rules on the page **Add** or **Edit Policy**, click a rule name. The Edit Rule page displays.

2) On the Edit Rule page, configure the following options:
   - Status: Enabled or disabled.
   - Filter properties. Click **Edit** to open the Edit Filter page. See *Creating and configuring a filter*.
   - Action options. Click **Edit** to open the Edit Action page. See *Creating and configuring a filter action*.

   Note

   Any change you make to existing rule components will be reflected in the filter and action definitions you configured on the pages **Main** > **Policy Management** > **Filters** and **Main** > **Policy Management** > **Actions**. The changes are not unique to the individual policy.

   - Filter bypass conditions. See *Adding a rule*.

3) Click **OK**.
   The changes are saved.

Related concepts
Creating and configuring a filter on page 173
Adding a rule on page 205

Related tasks
Creating and configuring a filter action on page 195

Editing an existing policy

Edit an existing policy by clicking its name on the Policies page to open the Edit Policy page. Edit the Description, Status, Sender/Recipient Conditions, and Rules as described in *Adding or editing a policy*. You cannot edit the policy name.

You can edit policy order only for a policy you have created. You cannot edit policy order for a default policy.

Related tasks
Adding or editing a policy on page 203

Managing global Always Block and Always Permit lists

Maintaining lists of IP and email addresses that are either always blocked or always permitted can contribute to the efficiency of your email security system. Bandwidth and time can be saved when trusted mail can bypass some analysis features (including antispam, commercial bulk, and URL analysis).

Note

Mail from addresses in the global Always Permit list is subject to other email analysis, including antivirus analysis, message control, connection control, directory harvest attack, and relay control.

Managing the Always Block List

Add an IP or email address directly into the Always Block List from the page **Main** > **Policy Management** > **Always Block/Permit**. On this page, you can also add a predefined IP or email address list, remove individual entries from a list, export a list to your desktop as a text file, and search a list.

Messages from an email address that appears in both the Always Block and Always Permit lists will be permitted. Messages from an IP address that appears in both lists will be blocked.

Export IP or email address list

1) From the section IP Address List or Email Address List, click **Export All**.

2) Select a save location.
The list is exported as a text file.

Remove an individual entry

From the section IP Address List or Email Address List, select an individual entry and click **Remove**.

The selected address is removed.

Search a list

From the section IP Address List or Email Address List, enter a keyword in the text field and click **Search**.

Search results display in the list.

Adding an IP address to the Always Block List

Use the following procedures to add IP addresses to the Always Block list:

Steps

1) From the page **Main** > **Policy Management** > **Always Block/Permit**, click the **Always Block** tab.

2) In the section IP Address Block List, add a predefined IP address list; click **Browse** and navigate to the desired text file.
The file format should be one IP address per line, and its maximum size is 10 MB.

3) You can also enter an individual IP/subnet address in the field **IP/Subnet address** field. Click the right arrow button to add the individual entry to the **IP Address List** on the right.

4) Click **OK**.

Adding an email address to the Always Block List

Use the following procedures to add email addresses to the Always Block list:

Steps

1) From the page **Main** > **Policy Management** > **Always Block/Permit**, click the **Always Block** tab.

2) In the section Email Address Block List, add a predefined email address list; click **Browse** and navigate to the desired text file.
   The file format should be one email address per line, and its maximum size is 10 MB.

3) You can also enter an individual email address in the field **Email address**. Click the right arrow button to add the individual entry to the **Email Address List** on the right.

4) Click **OK**.

Related tasks
Enabling the Dynamic Always Permit List on page 212

Managing the Always Permit List

Add an IP or email address directly into the Always Permit List from the page **Main** > **Policy Management** > **Always Block/Permit**. On this page, you can also add a predefined IP or email address list, remove individual entries from a list, export a list to your desktop as a text file, and search a list.

Email from an address that appears in both the Always Block and Always Permit lists will be permitted. Messages from an IP address that appears in both lists will be blocked.

Export IP or email address list

1) From the section IP Address List or Email Address List, click **Export All**.

2) Select a save location.
   The list is exported as a text file.

Remove an individual entry

From the section IP Address List or Email Address List, select an individual entry and click **Remove**.

The selected address is removed.

Search a list

From the section IP Address List or Email Address List, enter a keyword in the text field and click **Search**.

Search results display in the list.

Adding an IP address to the Always Permit List

Use the following procedures to add IP addresses to the Always Permit List:

Steps

1) From the page **Main** > **Policy Management** > **Always Block/Permit**, click the **Always Permit** tab.

2) In the section IP Address Permit List, add a predefined IP address list; click **Browse** and navigate to the desired text file.
   The file format should be one IP address per line, and its maximum size is 10 MB.

3) You can also enter an individual IP/subnet address in the field **IP/Subnet address**. Click the right arrow button to add the individual entry to the **IP Address List** on the right.

4) Click **OK**.

Adding an email address to the Always Permit List

Use the following procedures to add email addresses to the Always Permit list:

Steps

1) From the page **Main** > **Policy Management** > **Always Block/Permit**, click the **Always Permit** tab.

2) In the section Email Address Permit List, add a predefined email address list; click **Browse** and navigate to the desired text file.
   The file format should be one email address per line, and its maximum size is 10 MB.

3) You can also enter an individual email address in the **Email address** field. Click the right arrow button to add the individual entry to the **Email Address List** on the right.

4) (*Optional*) Configure the Dynamic Always Permit List. See *Enabling the Dynamic Always Permit List*.

5) Click **OK**.

Related tasks
Enabling the Dynamic Always Permit List on page 212

Enabling the Dynamic Always Permit List

Enabling the Dynamic Always Permit List function allows some mail exchanged between a sender/recipient address pair to bypass antispam filtering. When mail between a sender to a recipient does not trigger an antispam filter a specified number of times, that sender/recipient address pair is added to the Dynamic Always Permit List. Antispam analysis is not performed on mail between this sender/recipient address pair. When a specified timeout period has elapsed, the address pair is removed from the list.

Steps

1) From the section Dynamic Always Permit List on the Always Permit tab, mark the check box **Enable Dynamic Always Permit List**.
   Functionality is enabled by default.

2) In the field **Occurrence**, enter the number of spam-free email exchanges (from 1 to 5) required before a sender/recipient pair is added to the list.
   The default is 1.

3) In the field **Timeout**, enter a value for the timeout interval in hours (from 1 to 720).
   The default is 720.

4) (*Optional*) Clear the list manually; click the button **Clear Dynamic Always Permit List**.
   If you disable this function, the list is automatically cleared.

Order of precedence

A specific order of precedence is applied for cases in which IP addresses or email addresses appear in multiple Always Block and Always Permit lists.

Duplicate email addresses or IP addresses are allowed on both the global Always Block and Always Permit lists, including mixtures of IP and email addresses. A warning displays when a duplicate entry is added.

Duplicate email addresses are not allowed on the Personal Email Manager Always Block or Always Permit lists. A warning displays when a duplicate entry is added. If you continue to add the email address, only the current list to which the email address is added will contain the email address. For any duplicates that existed in previous versions of Personal Email Manager prior to this behavior being changed, an automatic mechanism cleans up duplicates, leaving the particular entry only in the Block List.

In the case of email addresses or IP addresses included in multiple Always Block and Always Permit lists, the order of precedence is below:

1) Global Always Block IP List

2) Global Always Permit Email Address

3) Global Always Block Email Address

4) Global Always Permit Email IP List

5) Personal Email Manager Block/Permit Email Address Lists

6) Dynamic Permit List

Chapter 6

Working with Reports

Contents

Configuring Log Database options

The Log Database stores the records of email traffic activity and the associated email analysis on that traffic. These data records are used to generate presentation reports of email activity, including size and volume of email messages and identification of senders and recipients. They are also used to generate the status charts on the dashboard.

Administering the Log Database involves controlling many aspects of database operations, including the timing of maintenance tasks, the conditions for creating new database partitions, and which partitions are available for reporting. Manage Log Database operations on the page **Settings** > **Reporting** > **Log Database**.

Making changes to Log Database settings on one appliance applies those changes to all the appliances in your network.

The Log Database page is divided into six sections, as detailed in the following table. After making changes in any of these sections of the Log Database page, click the **OK** button within the section to save and implement the changes in that section.

Parameter	Description
Log Database Location	Provides options to configure the IP address/instance or hostname/instance of your Log Database server. By default, the Log Database created at installation is entered. See *Configuring the Log Database location*.
Database Rollover Options	Provides options to specify when you want the Log Database to create a new database partition, a process called a rollover.
Maintenance Configuration	Provides options to configure aspects of database processing, such as the time for running the database maintenance job, some of the maintenance tasks performed, and deletion of database partitions and error logs. See *Configuring maintenance options*.
Database Partition Creation	Provides options to define characteristics for new database partitions, such as location and size options. This area also lets you create a new partition right away, rather than waiting for a planned rollover. See *Creating database partitions*.

Parameter	Description
Available Partitions	Lists all database partitions available for reporting. The list shows the dates covered by the partition, as well as the size and name of each partition. Use this list to control what database partitions are included in reports, and to select individual partitions to be deleted.
Log Activity	Displays log activity to review database maintenance status and event and error messages recorded during the jobs run on the Log Database. See *Viewing log activity*.

Related concepts

Configuring the Log Database location on page 216
Viewing log activity on page 220

Related tasks

Configuring maintenance options on page 217
Creating database partitions on page 218

Configuring the Log Database location

Use the section Log Database Location on the page **Settings** > **Reporting** > **Log Database** to enter the IP address\instance or hostname\instance of your Log Database server. By default, the Log Database created at installation is entered. If you chose to encrypt the database connection at product installation, the **Encrypt connection** check box is marked. If you did not select the encryption option during installation, you can encrypt the database connection by marking the check box here.

Important

You must have imported a trusted SSL certificate to the Log Server machine in order to use SSL for the encryption option. See your database documentation for information about importing a trusted certificate.

Other settings created at installation and displayed here include the designated authentication method (Windows or SQL Server), user name, and password.

Determine the availability of the server

From the section Log Database Location, click **Check Status**.

Configuring database rollover options

The top of the Log Database Options section displays the name of the active Log Database and a Refresh link. Click **Refresh** to update the information shown on the Log Database page. Be sure you save your settings before you click **Refresh**, because any unsaved changes on the page will be cleared.

Use the Database Rollover Options section of the page **Settings** > **Reporting** > **Log Database** to specify when you want the Log Database to create a new database partition, a process called a rollover.

Use the **Roll over every** option to indicate whether database partitions should roll over based on size (MB) or date (weeks or months).

- For size-based rollovers, select MB and specify the number of megabytes the database must reach for the rollover to begin, from 100–10240 MB (default is 5120).
- For date-based rollovers, select either weeks or months as the unit of measure, and specify how many full calendar weeks (from 1–52) or months (from 1–12) to keep in a database partition before a new one is created.

Note

If the rollover begins during a busy part of the day, performance may slow during the rollover process.

To avoid this possibility, some environments choose to set the automatic rollover to a long time period or large maximum size. Then, they perform regular manual rollovers to prevent the automatic rollover from occurring.

See *Creating database partitions* for information on manual rollovers.

Extremely large individual partitions are not recommended. Reporting performance can slow if data is not divided into multiple, smaller partitions.

When a new database partition is created, reporting is automatically enabled for the partition (see *Enabling database partitions*).

Click **OK** to activate changes to the database rollover options.

Related tasks

Creating database partitions on page 218
Enabling database partitions on page 219

Configuring maintenance options

Use the Maintenance Configuration section of the page **Settings** > **Reporting** > **Log Database** to control certain aspects of database processing, such as the time for running the database maintenance job, some of the maintenance tasks performed, and deletion of database partitions and error logs.

Steps

1) For **Maintenance start time**, select the time of day for running the database maintenance job. Default value is 1:00.

   The time and system resources required by this job vary depending on the tasks you select in this area. To minimize any impact on other activities and systems, it is best to run this job during a slow email traffic period.

2) Mark the check box **Automatically delete a partition with an end date older than**, and then specify the number of days (from 1 to 365) after which partitions should be deleted (default is 365).

Warning

After a partition has been deleted, the data cannot be recovered. See *Enabling database partitions* for an alternative way to delete partitions.

3) Mark the check box **Enable automatic reindexing of partitions on**, and then select a day of the week to have this processing performed automatically (default is Saturday).

Reindexing the database is important to maintain database integrity and to optimize reporting speed.

Important

It is best to perform this processing during a quiet time for email traffic. Reindexing database partitions is resource intensive and time consuming. Reports should not be run during the reindexing process.

4) Mark the check box **Delete failed batches after** and then enter a number of days (from 1 to 365) after which to delete any failed batches. Default value is 20.

If this option is not checked, failed batches are retained indefinitely for future processing.

If there is insufficient disk space or inadequate database permissions to insert log records into the database, the records are marked as a failed batch. Typically, these batches are successfully reprocessed and inserted into the database during the nightly database maintenance job.

However, this reprocessing cannot be successful if the disk space or permission problem is not resolved. Additionally, if the **Process any unprocessed batches** option is not selected, failed batches are never reprocessed. They are deleted after the time specified here.

5) Mark the check box **Process any unprocessed batches** to have the nightly database maintenance job reprocess any failed batches.

If this option is not checked, failed batches are never reprocessed. They are deleted after the time specified in step 4, if any.

6) Mark the check box **Delete the log after**, and then enter a number of days (1 to 120) after which to delete database error records. Default value is 45.

If this option is not checked, error logs are retained indefinitely.

7) Click **OK** to activate changes to the maintenance configuration options.

Related tasks

Enabling database partitions on page 219

Creating database partitions

Database partitions store the individual log records of email traffic activity. Microsoft SQL Server users can configure the Log Database to start a new partition based on partition size or a date interval.

When partitions are based on size, all incoming log records are inserted into the most recent active partition that satisfies the size rule. When the partition reaches the designated maximum size, a new partition is created for inserting new log records.

When the partitions are based on date, new partitions are created according to the established cycle. For example, if the rollover option is monthly, a new partition is created as soon as any records are received for the new month. Incoming log records are inserted into the appropriate partition based on date.

Database partitions provide flexibility and performance advantages. For example, you can generate reports from a single partition to limit the scope of data that must be analyzed to locate the requested information.

Use the Database Partition Creation section of the page **Settings** > **Reporting** > **Log Database** to define characteristics for new database partitions, such as location and size options. This area also lets you create a new partition right away, rather than waiting for a planned rollover.

Steps

1) Under **Initial Size (MB)**, set the initial file size (from 100 to 2048 MB) for both the Data and Log files for new database partitions.

2) Enter the file path for creating both the data and log files for new database partitions.

Note

Best practice recommends calculating the average partition size over a period of time. Then, update the initial size to that value. This approach minimizes the number of times the partition must be expanded, and frees resources to process data into the partitions.

3) Under **Growth (MB)**, set the increment by which to increase the size (from 8 - 512 MB) of a partition's data and log files when additional space is required.

4) Click **OK** to implement the path, size, and growth changes entered. Database partitions created after these changes use the new settings.

5) Click **Create** to create a new partition immediately, regardless of the automatic rollover settings.

   To have the new partition use the changes made in this section, be sure to click **OK** before you click **Create**.

   Click the **Refresh** link in the content pane periodically. The Available Partitions area will show the new partition when the creation process is complete.

Next steps

If you later change the partition file path, you should be sure that the new database folder exists with write privileges.

Enabling database partitions

The Available Partitions section of the page **Settings** > **Reporting** > **Log Database** lists all the database partitions available for reporting. The list shows the dates covered by the partition, as well as the size and name of each partition.

Use this list to control what database partitions are included in reports, and to select individual partitions to be deleted.

Steps

1) Mark the check box in the **Enable** column next to each partition you want included in reports.

   Use the **Select all** and **Select none** options above the list, as appropriate.

   You must enable at least one partition for reporting. Use the **Select none** option to disable all partitions at one time so that you can enable just a few.

   Use these options to manage how much data must be analyzed when generating reports and speed report processing. For example, if you plan to generate a series of reports for June, select only partitions with dates in June.

   Important

   This selection affects scheduled reports as well as reports that are run interactively. To avoid generating reports with no data, make sure the relevant partitions are enabled when reports are scheduled to run.

2) Click the **Delete** option beside a partition name if that partition is no longer needed. The partition is actually deleted the next time the nightly database maintenance job runs.

   Warning

   Use this option with care. You cannot recover data from deleted partitions.

   Deleting obsolete partitions minimizes the number of partitions in the Log Database, which improves database and reporting performance. Use this Delete option to delete individual partitions as needed. See *Configuring maintenance options* if you prefer to delete older partitions according to a schedule.

3) Click **OK** to activate changes to the available partitions options.

Related tasks

Configuring maintenance options on page 217

Viewing log activity

Use the Log Activity section of the page **Settings** > **Reporting** > **Log Database** to review database maintenance status and event and error messages recorded during the jobs run on the Log Database. Use the **View** pull-down menu to select the maximum number of messages to display.

Changing the Log Database

The Log Database may need to be changed when one of the following situations occurs:

- The database IP address changes.
- The database username and password change.
- The user wants to change authentication settings.
- The user wants to use a named instance.

This type of change must be made in two locations: on the page **Settings** > **Reporting** > **Log Database** and in the Email Log Server Configuration wizard.

Use the following steps to change the Log Database configuration:

Steps

1) Enter the IP address for the new Log Database on the page **Settings** > **Reporting** > **Log Database**, in the **Log database** field.

2) Open the Email Log Server Configuration wizard for the Windows machine on which Log Server is installed (**Start** > **Forcepoint** > **Email Log Server Configuration**).

3) In the Database tab, click **Connection** to open the Select Data Source dialog box.

4) Select the Machine Data Source tab and click **New** to open the Create New Data Source dialog box.

5) Select **System Data Source (Applies to this machine only)**, and click **Next**.

6) Select **SQL Server** and click **Next**.

7) Click **Finish**.

8) In the Create a New Data Source to SQL Server dialog box, enter the server name, description, and IP address of the new SQL Server database in the **Name**, **Description**, and **Server** entry fields and click **Next**.

9) Select **With SQL Server authentication using a login ID and password entered by the user**.

10) Enter the username (**sa**) and a password and click **Next**.

11) In the p ull-down menu **Change the default database to**, select the **esglogdb76** database and click **Next**.

12) Click **Finish**.

13) In the ODBC Microsoft SQL Server Setup dialog box, click **Test Data Source** to test the server connection.

14) Click **OK**.

15) Enter the new username and password in the SQL Server Login dialog box.

16) In the Email Log Server Configuration wizard Database tab, notice that the ODBC Data Source Name (DSN) field contains the new server name, and click **Apply** to confirm the new configuration.

17) Click **OK** in the warning message. The Log Server must be stopped and restarted for the new settings to take effect.

18) In the Email Log Server Configuration wizard Connection tab, click **Stop** to stop the Log Server service.

19) In the same tab, click **Start** to restart the Log Server service. The new database settings are in effect.

Viewing Log Server settings

Use the page **Settings** > **Reporting** > **Log Database** to view the Log Server IP address or hostname and port number. Click **Check Status** to determine the availability of the server.

Configuring reporting preferences

Reporting preference settings determine how a scheduled report is distributed for review. You can also specify how long to retain a scheduled report and how much warning administrators receive before a report is deleted.

When reporting preferences settings are made on one appliance, they are applied to all the appliances in your network.

Use the page **Settings** > **Reporting** > **Preferences** to provide information used to distribute completed scheduled reports via email. Also define how long scheduled presentation reports are stored before they are deleted automatically, and how far in advance to warn administrators that reports are due to be deleted.

Steps

1) Enter the email address to appear in the From field when scheduled reports are distributed via email.

2) Enter the SMTP server IP address or name for the email server used to distribute scheduled reports via email.

3) Use the **Store reports for** pull-down menu to indicate how long scheduled reports are stored on the email management server (default is five days).

   As you increase the length of time that reports are stored, you affect the amount of disk space required on the email management server. This machine is not an appropriate location for a long-term reporting archive.

   Note

   If you reduce the report storage time after you have started to generate reports, stored reports that exceed this interval will be automatically deleted.

4) Use the **Give administrators this much warning before a scheduled report is deleted** pull-down menu to indicate how much warning (from 1–5 days) an administrator should have before a report is deleted (default is three days).

   The warning is intended to give administrators time to archive important reports in an appropriate location before they are deleted from the email management server.

5) Click **OK** to implement your changes.

Working with presentation reports

Presentation reports include a set of predefined charts and tabular report templates with which you can generate graphical reports of email message traffic activities. You can run a report, customize a report template, or mark a frequently used report as a

Favorite. You can run any presentation report immediately, or schedule it to run at a particular time or on a repeating cycle.

Not all report templates can be customized. Report templates that can be customized display a different icon from reports that cannot be customized. If the **Save As** button is enabled when you select a report name, then you can save and edit that report to suit your needs. The **Save As** button is not enabled if you select a report that cannot be customized.

Use the page **Main** > **Status** > **Presentation Reports** to generate charts and tabular reports based on templates in the Report Catalog.

The Report Catalog organizes a list of predefined report templates and custom reports into groups. Expand a group to see its corresponding templates and custom reports. Click on a template or report title to see a brief description of what it includes.

To run a presentation report, select the desired report template in the Report Catalog, click **Run**, and then follow the instructions given in *Running a presentation report*.

To use an existing report as a starting point for creating a report variation, select a custom report, and then click **Save As,** if this button is enabled. If the Save As button is not enabled when you select the report, you cannot edit the template. See *Copying a custom presentation report*.

To make changes to the report filter applied to any custom report you have created, select the report title in the Report Catalog, and then click **Edit**. You cannot modify or delete predefined report templates.

Reports that are used frequently can be marked as Favorites to help you find them more quickly. Just click the report title in the Report Catalog, and then click **Favorite** (see *Working with Favorites*). Mark **Show Only Favorites** to display only templates that you have marked as Favorites in the Report Catalog.

To delete a custom report you have created, click **Delete**. If a deleted report appears in any scheduled jobs, it will continue to be generated with that job. See *Viewing the scheduled jobs list* for information on editing and deleting scheduled jobs.

Note

Changes to report settings made on one appliance are applied to all network appliances.

Use the buttons at the top of the page to schedule reports to run later, view scheduled report jobs, and view and manage reports created by the scheduler.

- Click **Job Queue** to see and manage a list of existing scheduled jobs, along with the status of each job. See *Viewing the scheduled jobs list*.
- Click **Scheduler** to define a job containing one or more reports to be run at a specific time or on a repeating schedule. See *Scheduling a presentation report*.
- Click **Review Reports** to see and manage a list of reports that were successfully scheduled and run. See *Reviewing scheduled presentation reports*.

Related concepts

Scheduling a presentation report on page 231
Reviewing scheduled presentation reports on page 237

Related tasks

Running a presentation report on page 229
Copying a custom presentation report on page 224
Working with Favorites on page 229

Related reference

Viewing the scheduled jobs list on page 235

Copying a custom presentation report

Use the **Save As New Report** page to create an editable copy of a custom report template. Not all templates can be used to create a new custom report. Use the following steps to copy a custom presentation report:

Steps

1) Select the custom report in the Report Catalog and, if it is enabled, click **Save As**. If the **Save As** button is not enabled, you cannot copy and customize the selected report.

2) In the **Presentation Reports** > **Save As New Report** page, replace the report catalog name with a name that will make it easy to identify the new report. (The default name is the name of the original report template, with a number appended to indicate that it is a copy.) The name must be unique and can have up to 85 characters.

3) Click either **Save** or **Save and Edit**.
   - If you click **Save**, you are returned to the Presentation Reports page, where the new report appears in the Report Catalog. To customize the report at any time, select its name, and then click **Edit**.
   - If you click **Save and Edit**, you are taken directly to the Edit Report Filter page. The new report is also added to the Report Catalog.

4) Edit the report filter to modify the report. The report filter controls elements such as which email senders or recipients are included in your custom report.
   For instructions, see *Defining the report filter*.

Related concepts

Defining the report filter on page 224

Defining the report filter

Report filters let you control what information is included in a report. For example, you might choose to limit a report to selected email senders, email recipients, or message analysis results (for example, clean, virus, spam, commercial bulk, or data loss prevention). You can also give a new name and description for the entry in the Report Catalog, change the report title, specify a custom logo to appear, and designate the new report as a Favorite.

Note

Using a custom logo requires some preparation before you define the report filter. You must create the desired graphic in a supported graphic format and place the file in the appropriate location. See *Customizing the report logo*.

The filter for predefined report templates cannot be changed. You can edit the filter for a custom report when you create it by choosing **Save and Edit** on the Save As New Report page, or select the report in the Report Catalog at any time and click **Edit**.

On the Save tab, choose whether to run or schedule the report, and save the report filter. See *Saving the report filter definition*.

The Edit Report Filter page has separate tabs for managing different elements of the report. Select the items you want on each tab, then click **Next** to move to the next tab. For detailed instructions on completing each tab, see:

Related concepts

Selecting message analysis results for the report on page 228

Related tasks

Customizing the report logo on page 226
Setting general report options on page 225
Selecting email senders for the report on page 226
Selecting email recipients for the report on page 227
Saving the report filter definition on page 228

Setting general report options

Use the General tab of the page **Presentation Reports** > **Edit Report** to configure general report characteristics, as follows:

Steps

1) Modify the name that appears in the Report Catalog for this report by entering a new name in the **Report catalog name** entry field. The name can have up to 76 characters.

   This name does not appear on the report itself; it is used only for identifying the unique combination of report format and filter in the Report Catalog.

2) Modify the title that actually appears on the report in the **Report title** entry field. The title can have up to 85 characters.

3) Use the **Description** field to modify the brief report description that appears in the Report Catalog. The description can have up to 336 characters.

   The description should help you identify this unique combination of report format and filter in the Report Catalog.

4) Use the **Logo** pull-down menu to specify a logo for your report. The default entry is **Forcepoint Logo**. Select **No Logo** if you do not want a logo displayed on this report.

   The list also contains filenames for custom logo image files if you have created and stored supported image files in the appropriate directory. See *Customizing the report logo*, page 220.

5) Mark the **Save as Favorite** check box to have the report selected as a Favorite.

   The Report Catalog shows a star symbol beside Favorite reports. You can select Show only Favorites on the Report Catalog page to reduce the number of reports listed, which enables you to move more quickly to a particular report.

6) After all entries and selections are complete, click **Next** to open the Senders tab.

Related tasks

Customizing the report logo on page 226

Customizing the report logo

By default, presentation reports display the Forcepoint logo in the upper left corner. When you create a custom report and edit its report filter, you can choose a different logo, which you have already prepared and copied to the appropriate directory, as follows:

Steps

1) Create an image file in one of the following formats:

   .bmp, .gif, .jfif, .jpe, .jpeg, .jpg, .png, .ttf

   Use a maximum of 25 characters for the image file name, including the file extension.

2) Copy the image file to the following default installation directory (or to your own installation directory):

   `C:\Program Files (x86)\Websense\Email Security\ESG Manager\tomcat\PRTemplate\jasperreports\images`

   All supported image files in this directory automatically appear in the **Logo** pull-down menu on the General tab of the Edit Report Filter page. The image is automatically scaled to fit within the space allocated for the logo. (See *Setting general report options*.)

Related tasks

Setting general report options on page 225

Selecting email senders for the report

The Senders tab of the page **Presentation Reports** > **Edit Report** lets you control which senders are included in the report data. You can select only one type of sender for each report.

No selections are required on this tab to report on all senders.

Steps

1) Select a sender type from the pull-down menu.

2) Set the maximum number of search results from the **Search limit** pull-down menu (from 10–1000). Default value is 10.

   Depending on the email traffic in your organization, there may be large numbers of users, groups, or domains in the Log Database. This option manages the length of the results list, and the time required to display the search results.

3) Enter one or more characters for searching, and then click **Search**.

   Use an asterisk (*) as a wildcard to signify missing characters. For example, J*n might return Jackson, Jan, Jason, Jon, Joan, and so forth.

   Define your search string carefully, to ensure that all desired results are included within the number selected for limiting the search.

4) Highlight one or more entries in the results list, and click the right arrow button (>) to move them to the Selected Senders List.

5) Repeat steps 2–4 as needed to conduct additional searches and add more senders to the Selected Senders List.

6) To delete an entry from the Selected Senders List, select the entry and click **Remove**.

7) After you are finished making selections or deletions, click **Next** to open the Recipients tab.

Selecting email recipients for the report

The Recipients tab of the page **Presentation Reports** > **Edit Report** lets you control which recipients are included in the report data. You can select only one type of recipient for each report.

No selections are required on this tab to report on all recipients.

Steps

1) Select a recipient type from the pull-down menu.

2) Set the maximum number of search results from the **Search limits** pull-down menu (from 10–1000). Default value is 10.

   Depending on the email traffic in your organization, there may be large numbers of users, groups, or domains in the Log Database. This option manages the length of the results list, and the time required to display the search results.

3) Enter one or more characters for searching, and then click **Search**.

   Use an asterisk (*) as a wildcard to signify missing characters. For example, J*n might return Jackson, Jan, Jason, Jon, Joan, and so forth.

   Define your search string carefully, to ensure that all desired results are included within the number selected for limiting the search.

4) Highlight one or more entries in the results list, and click the right arrow button (>) to move them to the Selected Recipients List.

5) Repeat steps 2–4 as needed to conduct additional searches and add more recipients to the Selected Recipients List.

6) To delete an entry from the Selected Recipients List, select the entry and click **Remove**.

7) After you are finished making selections or deletions, click **Next** to open the Message Analysis Results tab.

Selecting message analysis results for the report

The Message Analysis Result tab of the page **Presentation Reports** > **Edit Report** lets you determine which results of email analysis are included in the report. Selections are **Clean**, **Virus**, **Spam**, **Data Loss Prevention, Commercial Bulk**, **Custom Content, Block List, Phishing, Advanced Malware Detection - Cloud**, **URL Analysis**, **Spoofed Email**, and **Advanced Malware Detection - On-Premises**. The Block List type applies to a message that is blocked by a Personal Email Manager Always Block List. By default, all available analysis result types are selected. You must select at least one type.

Click **Next** to open the Save tab.

Saving the report filter definition

The Save tab of the page **Presentation Reports** > **Edit Report** displays the name and description that will appear in the Report Catalog, and lets you choose how to proceed.

Steps

1) Review the Name and Description text.

   If any changes are needed, click **Back** to return to the General tab, where you can make those changes. You cannot edit the name or description text in the Save tab. (See *Setting general report options*.)

2) Indicate how you want to proceed:

   - Select **Save** to save the report filter and return to the Report Catalog.
   - Select **Save and run** to save the report filter and open the Run Report page. See *Running a presentation report*.
   - Select **Save and schedule** to save the report filter and open the Scheduler page. See *Scheduling a presentation report*.

3) Click **Finish** to save the report name and description and implement the selection made in step 2.

Related concepts

Scheduling a presentation report on page 231

Related tasks

Setting general report options on page 225
Running a presentation report on page 229

Working with Favorites

You can mark any presentation report, either template or custom, as a Favorite. Use this option to identify the reports you generate most frequently and want to be able to locate quickly in the Report Catalog.

To mark a report as a Favorite:

Steps

1) On the Presentation Reports page, select a report in the Report Catalog that you generate frequently, or want to be able to locate quickly.

2) Click **Favorite**.
   A star symbol appears beside any Favorite report name in the list, letting you quickly identify it when the Report Catalog is displayed.

3) Mark the **Show Only Favorites** check box above the Report Catalog to limit the list to those marked as Favorites. Clear this check box to restore the full list of reports.

Next steps

If your needs change and a favorite report is no longer being used as frequently, you can remove the Favorite designation as follows:

1) Select a report that shows the Favorite star symbol.

2) Click **Favorite**.
   The star symbol is removed from that report name in the Report Catalog. The report is now omitted from the list if you choose **Show Only Favorites**.

Running a presentation report

Use the page **Presentation Reports** > **Edit Report** to generate a single report immediately. You can also create jobs with one or more reports and schedule them to run once or on a repeating cycle (see *Scheduling a presentation report*).

Note

Before generating a report in PDF format, make sure that Adobe Reader v7.0 or later is installed on the machine from which you are accessing the email management server.

Before generating a report in XLS format, make sure that Microsoft Excel 2003 or later is installed on the machine from which you are accessing the email management server.

If the appropriate software is not installed, you have the option to save the file.

To run a report:

Steps

1) Select the report you want to run in the Report Catalog and click **Run** to open the Run Report page.

2) Select the **Report date range** to define the time period covered in the report.
If you select **Custom**, specify the **Report start date** and **Report end date** for the report.

3) Select a **Report output format** for the report.

XLS	Excel spreadsheet. XLS files are formatted for reuse, and can be opened in Microsoft Excel.
PDF	Portable Document Format. PDF files are formatted for viewing, and can be opened in Adobe Reader.
HTML	HyperText Markup Language. HTML files are formatted for viewing, and can be opened in a Web browser.

4) If you selected a Top N report type, choose the number of items to be reported.

5) Specify how you want the report to be generated:

- Select **Run the report in the background** (default) to have the report run immediately as a scheduled job. Optionally, you can provide an email address to receive a notification message when the report is complete or cannot be generated. (You can also monitor the job queue for report status.)
  If you run the report in the background, a copy of the completed report is automatically saved, and a link to the report appears on the Review Reports page.
- Deselect **Run the report in the background** to have the report run in the foreground. In this case, the report is not scheduled, and does not appear on the Review Reports page.
  If you run the report in the foreground, the report is not automatically saved when you close the application used to view the report (Microsoft Excel, Adobe Reader, or a Web browser, for example). You must save the report manually.

Note

If you plan to run multiple reports in the foreground, make sure that you use the embedded **Close** button to close the pop-up window used to display the “generating report” and “report complete” messages. If you use the browser’s close (X) button, subsequent attempts to run reports in the foreground may fail until you navigate away from the Presentation Reports page, come back, and run the report again.

6) Click **Run**.

- If you scheduled the report to run immediately, the completed report is added to the Review Reports list. To view, save, or delete the report, click **Review Reports** at the top of the Presentation Reports page.
- If you ran the report in the foreground, a new browser window appears, displaying report progress. HTML reports appear in the browser window when complete; with PDF or XLS formats, you have a choice of whether to open the report or save it.

7) To print a report, use the print option offered by the application used to display the report.
For best results, generate PDF output for printing. Then, use the print options in Adobe Reader.

Related concepts
Scheduling a presentation report on page 231

Scheduling a presentation report

You can run presentation reports as they are needed, or you can use the page **Presentation Reports** > **Scheduler** to create jobs that define a schedule for running one or more reports. In an appliance cluster, only the primary machine can schedule a report.

Reports generated by scheduled jobs are distributed to one or more recipients via email. As you create scheduled jobs, consider whether your email server will be able to handle the size and quantity of the attached report files.

The completed reports are also added to the page **Presentation Reports** > **Review Reports** (see *Reviewing scheduled presentation reports*).

You can access the Scheduler in one of the following ways:

- Click **Scheduler** at the top of the Presentation Reports page (above the Report Catalog).
- When editing a report filter, choose **Save and schedule** in the Save tab, and then click **Finish** (see *Defining the report filter*).
- Click the job name link on the Job Queue page to edit a job.
- Click **Add Job** on the Job Queue page to create a new job.

The Scheduler page contains several tabs for selecting the reports to run and the schedule for running them. For detailed instructions on completing each tab, see:

- *Setting the schedule*
- *Selecting reports to schedule*
- *Setting the date range*
- *Selecting output options*

After creating jobs, use the Job Queue to review job status and find other helpful information (see *Viewing the scheduled jobs list*).

When a scheduled presentation report has run, the report file is sent to recipients as an email attachment. The name of the attachment is the report name. For example, for a report with an output format of PDF, an attachment file may be named Email Hybrid Service Messages.pdf.

Scheduled reports are also automatically saved to a report output directory on the email management server (`C:\Program Files (x86)\Websense\Email Security\ESG Manager\tomcat\temp\report\output`, by default). The name of the attachment sent via email does not match the name of the file stored in the output directory. The best way to find a specific report is to use the Review Reports page, which can be searched by date or job name, as well as report name.

Reports are automatically deleted from the Review Reports page and the report output directory after the period specified on the page **Settings** > **Reporting** > **Preferences** (5 days, by default). to retain the reports for a longer time, include them in your backup routine or save them in a location that permits long-term storage.

An alert is displayed on the Review Reports page for a period of time before the report is deleted (3 days, by default). Use the page **Settings** > **Reporting** > **Preferences** to change this warning period.

Depending on the number of reports you generate daily, report files can occupy considerable amounts of disk space. Be sure adequate disk space is available on the email management server. If the report output directory grows too large before the files are automatically deleted, you can delete the files manually.

Forcepoint software generates the report in the format you choose: XLS (Microsoft Excel), PDF (Adobe Reader), or HTML. If you choose HTML format, the report may display in the Email module content pane. Reports displayed in the content pane cannot be printed or saved to a file. To print or save a report to file, choose the PDF or XLS output format.

Important

To display presentation reports in PDF format, Adobe Reader v7.0 or later must be installed on the machine from which you are accessing the email management server.

To display presentation reports in XLS format, Microsoft Excel 2003 or later must be installed on the machine from which you are accessing the email management server.

Related concepts

Reviewing scheduled presentation reports on page 237
Defining the report filter on page 224
Setting the date range on page 234

Related tasks

Setting the schedule on page 232
Selecting reports to schedule on page 233
Selecting output options on page 234

Related reference

Viewing the scheduled jobs list on page 235

Setting the schedule

Schedule a reporting job to occur once or on a repeating cycle on the Schedule Report tab of the page **Presentation Reports** > **Scheduler**.

Note

It is advisable to schedule report jobs on different days or at different times, to avoid overloading the Log Database and slowing performance for logging and interactive reporting.

Steps

1) Enter a name that uniquely identifies this scheduled job in the **Job name** field.

2) Select Recurrence Options for the job based on the Recurrence Pattern you want, as follows:

Recurrence Pattern	Recurrence Options
Once	Enter the exact date on which to run the job, or click the icon to select from a calendar.
Daily	No additional recurrence options are available.
Weekly	Mark the check box for each day of the week the job is to run.
Monthly	Enter the dates during the month for running the job. Dates must be a number between 1 and 31, and must be separated by commas (1,10,20). To run the job on consecutive dates each month, enter a start and end date separated by a hyphen (3-5).

3) In the Schedule Time box, set the start time for running the job.
The job begins according to the time on the email appliance.

Note

To start generating the scheduled reports today, select a time late enough that you can complete the job definition before the start time.

4) In the Schedule Period box, select a date for starting the job. Options for ending the job are as follows:

No end date	The job continues to run indefinitely, according to the established schedule. To discontinue the job at some time in the future, either edit or delete the job. See *Viewing the scheduled jobs list*.
End after	Select the number of times to run the job. After that number of occurrences, the job does not run again, but it stays in the Job Queue until you delete it. See *Viewing the scheduled jobs list*.
End by	Set the date when the job stops running. It does not run on or after this date.

5) Click **Next** to open the Select Report tab.

Related reference
Viewing the scheduled jobs list on page 235

Selecting reports to schedule

Use the Select Report tab of the page **Presentation Reports** > **Scheduler** to choose reports for the job.

Steps

1) Highlight a report for this job in the Report Catalog tree.

2) Click the right arrow (**>**) button to move that report to the Selected Reports list.

3) Repeat steps 1 and 2 until all reports for this job appear in the Selected Reports list.

4) Click **Next** to open the Date Range tab.

Setting the date range

Use the Date Range tab of the page **Presentation Reports** > **Scheduler** to set the date range for the job. If you selected **Once** in the Schedule Report tab, the **Specific dates** field displays the report date specified on that tab.

If you selected a recurring report schedule, you can specify the number of periods to report in the **Relative dates** field (Current, Last, Last 2, and so forth), along with the type of period (Days, Weeks, or Months). For example, the job might cover the Last 2 Weeks or Current Month.

Week represents a calendar week, Sunday through Saturday. Month represents a calendar month. For example, Current Week produces a report from Sunday through today; This Month produces a report from the first of the month through today; Last Week produces a report for the preceding Sunday through Saturday; and so forth.

After setting the date range for the job, click **Next** to display the Output tab.

Selecting output options

After you select the reports for a job, use the Output tab to select the output format and distribution options.

Steps

1) Select the file format for the finished report.

XLS	Excel Spreadsheet. Recipients must have Microsoft Excel 2003 or later to view the XLS reports.
PDF	Portable Document Format. Recipients must have Adobe Reader v7.0 or later to view the PDF reports.
HTML	HyperText Markup Language. Recipients must have a Web browser.

2) Select the number of items you want to appear in a Top format report from the **Top N** pull-down menu. The value range is from 1 to 200; default value is 10.

3) Enter recipient email addresses for report distribution. Each address should be separated by a semicolon.

4) Optionally, you can also enter email addresses to notify recipients that report generation failed.

5) Mark the **Customize subject and message body of notification email** check box, if desired. Then, enter the custom subject and body text for this job's distribution email.

6) Click **Save Job** to save and implement the job definition, and display the Job Queue page.

7) Review this job and any other scheduled jobs. See *Viewing the scheduled jobs list*.

Related reference
Viewing the scheduled jobs list on page 235

Viewing the scheduled jobs list

The page **Presentation Reports** > **Job Queue** lists the scheduled jobs created for presentation reports. The list gives the status for each job, as well as basic information about the job, such as how frequently it runs. From this page, you can add and delete scheduled jobs, temporarily suspend a job, and more.

You can search for a particular job by entering a search term in the **Job name** entry field at the top of the page. Click **Go** to begin the search.

Click **Clear** to remove the current search term, and then either perform a different search or click **Refresh** at the bottom of the page to display the complete list of reports.

The list provides the following information for each job:

Data Item	Description
Job Name	The name assigned when the job was created.
Status	Indicates whether the job is ■ running ■ scheduled (waiting for the next scheduled run time) ■ completed successfully ■ failed ■ misfired (did not run at the last scheduled time due to a problem such as low memory or server shutdown)
State	One of the following: ■ **Enabled** indicates a job that runs according to the established recurrence pattern. ■ **Disabled** indicates a job that is inactive, and does not run.
Recurrence	The recurrence pattern (Once, Daily, Weekly, or Monthly) set for this job.
History	Click the Details link to open the Job History page for the selected job. See *Viewing job history*.
Next Scheduled	Date and time for the next run.
Owner	The user name of the administrator who scheduled the job.

Use the options on the Job Queue page to manage the jobs. Some of the buttons require that you first mark the check box beside the name of each job to be included.

Action	Description
Job name link	Opens the Scheduler page, where you can edit the job definition. See *Scheduling a presentation report*.
Run Now	Starts running any job that has been selected in the list immediately. This is in addition to regularly scheduled job runs.
Add Job	Opens the Scheduler page where you can define a new job. See *Scheduling a presentation report*.
Delete	Deletes from the Job Queue any job that has been selected in the list. After a job has been deleted, it cannot be restored. To temporarily stop running a particular job, use the **Disable** button.
Enable	Reactivates a disabled job that has been selected in the list. The job begins running according to the established schedule.
Disable	Discontinues running an enabled job that is selected in the list. Use this option to temporarily suspend a job that you may want to restore in the future.
Refresh	Updates the page with the latest data

Related concepts
Scheduling a presentation report on page 231

Related reference
Viewing job history on page 236

Viewing job history

Click the **Details** link in the History column and use the page **Presentation Reports** > **Job Queue** > **Job History** to view information about recent attempts to run the selected job. The page lists each report separately, providing the following information:

Data Item	Description
Report Name	Title printed on the report
Start Date	Date and time the report started running
End Date	Date and time the report was completed
Status	Indicator of whether the report completed or failed

Data Item	Description
Message	Relevant information about the job, such as whether the report was successfully distributed

Reviewing scheduled presentation reports

Use the page **Presentation Reports** > **Review Reports** to find, access, and delete scheduled reports. By default, reports are listed from newest to oldest.

To view any report in the list, click the report name.

- If the report is a single PDF or XLS file, you may be given the option to save or open the report. This depends on your browser security settings and the plug-ins installed on your machine.
- If the report is very large, it may have been saved as multiple PDF or XLS files and stored in a ZIP file. The file is compressed using ZIP format. Save the ZIP file, then extract the PDF or XLS files it contains to view the report content.
- Hover the mouse pointer over the report icon next to the report name to see if the report is one or multiple files.

To limit the list to reports that will be deleted soon, mark the **Show only reports due to be purged** check box. When this option is selected, the report search functions are not available. The length of time that reports are stored is configured on the **Settings** > **Reporting** > **Preferences** page (see *Configuring reporting preferences*).

To search the report list, first select an entry from the **Filter by** pull-down menu, and then enter all or part of a job name or date. The search is case-sensitive. You can search by:

- The report or job name
- The date the report was created (Creation Date)
- The name of the administrator that scheduled the report (Requester)
- The date the report is due to be deleted (Purge Date)

Click **Go** to begin the search.

Click **Clear** to remove the current search term, and then either perform a different search or click **Refresh** to display the complete list of reports.

If a recently completed report does not appear on the Review Reports page, you can also click **Refresh** to update the page with the latest data.

To delete a report, mark the check box beside the report name and click **Delete**.

To see the status of a scheduled report job, click **Job Queue** at the top of the page. See *Viewing the scheduled jobs list* for more information about using the job queue.

To schedule a new report job, click **Scheduler** (see *Scheduling a presentation report*).

Related concepts

Scheduling a presentation report on page 231

Related tasks

Configuring reporting preferences on page 222

Related reference

Viewing the scheduled jobs list on page 235

Chapter 7

Configuring Personal Email Manager End User Options

Contents

Managing a Secure Sockets Layer (SSL) certificate

Use the page **Settings** > **Personal Email** > **SSL Certificate** to manage the Personal Email Manager SSL certificate, which enables secure email transmission for Personal Email Manager appliances. You can use the default certificate provided with Personal Email Manager, or you can import a new enterprise certificate from a certificate authority (CA).

After email product installation, default certificate information appears on the page **Settings** > **Personal Email** > **SSL Certificate**, in the Certificate Details section. Details include the certificate version, serial number, issuer, and expiration date.

Importing a certificate

Importing an SSL certificate to Personal Email Manager from a CA replaces the current certificate. Personal Email Manager certificate information is automatically copied to a new appliance when it is added to the Forcepoint Security Manager Email Security module.

Use the following procedure to import a certificate:

Steps

1) Click **Import** on the page **Settings** > **Personal Email** > **SSL Certificate**, below the Certificate Details area.

2) Click **Yes** in the confirmation dialog box.
   An Import Certificate area appears below the Import button.

3) Enter the certificate filename in the **Import Certificate** field or navigate to it using **Browse**.
File format must be .jks, .p12, or .pfx.

4) An SSL certificate file should be password protected. Enter a password in the **Certificate password** field.
Maximum length is 100 characters; do not use special characters.

5) Mark the **Private key alias** check box and enter an optional alias (or identifier) for the private key in the entry field.

6) Mark the **Private key password** field and enter an optional password for the private key in the entry field.
Maximum length is 100 characters.

7) Click **OK**.

8) Restart the Personal Email Manager service in the appliance manager to activate the new certificate.

Restoring the default certificate

You can restore the Personal Email Manager default certificate at any time by clicking **Restore Default Certificate** on the page **Settings** > **Personal Email** > **SSL Certificate**. This action replaces the current certificate.

Restart the Personal Email Manager service to activate the new certificate.

Creating the quarantine mail notification message

The Personal Email Manager notification message alerts users that email addressed to them has been blocked. The notification message list includes mail sent to all a user's email addresses, including alias addresses. The notification is sent to a user's primary email address.

The page **Settings** > **Personal Email** > **Notification Message** is composed of four sections:

- Notification Message Links, in which you specify the IP address and port for Personal Email Manager facility end-user access (see *Specifying Personal Email Manager access*).
- Notification Message Schedule, where you set the frequency with which a message is sent informing a user of blocked messages (see *Scheduling the notification message*).
- Notification Message Template, in which you format the content and appearance of the notification message. Users see this message in their inbox when they have blocked email (see *Using the notification message template*).
- Recipients List, in which you designate the user directories whose members will receive notification messages (see *Creating the notification message recipient list*).

After you complete all four sections, click **OK** to enable the delivery of notification messages.

Related concepts

Specifying Personal Email Manager access on page 241
Scheduling the notification message on page 242
Creating the notification message recipient list on page 243

Related tasks

Using the notification message template on page 242

Specifying Personal Email Manager access

Use the Notification Message Links section to designate the appliance that the end user accesses to manage blocked email in the Personal Email Manager tool. This setting is also used to create the hyperlinks to blocked mail listed in the user notification message. You can customize the URL for Personal Email Manager access to suit your needs.

Personal Email Manager users must have Personal Email Authentication permissions in order to use the facility. See *Managing user validation/authentication options* for information about granting Personal Email Manager permissions to end users.

Enter the IP address or hostname of the Personal Email Manager appliance.

Enter the port number (default is 9449). The port number should not be an email management server or appliance reserved port.

Note

If you use the C appliance interface for Personal Email Manager access, you must use the default port of 9449.

Use the Custom URL field to enter a URL path for Personal Email Manager user access that is different from the one automatically generated using the IP address and port entered above. This URL is also used for the notification message hyperlinks.

The path can have a maximum length of 250 alphanumeric characters, hyphens, and underscores; a hyphen cannot be the first character. The custom URL supports only one subdirectory (for example, www.mycompany.com/pemserver) and should use the port designated in the Port field.

Deploy a group of email appliances to handle Personal Email Manager end-user activities. Configuring an appliance cluster for Personal Email Manager access can enhance performance by activating an appliance load-balancing feature. If the appliance you access is configured in a cluster, the appliance forwards Personal Email Manager access requests to other cluster machines using a round robin mechanism.

Add and remove appliances from a cluster using the page **Settings** > **General** > **Cluster Mode** (see *Configuring an appliance cluster*).

Related concepts

Managing user validation/authentication options on page 103
Configuring an appliance cluster on page 90

Scheduling the notification message

You have several options for scheduling the frequency of the notification messages that tell users that they have blocked messages. Configure the schedule settings on the page **Settings** > **Personal Email** > **Notification Message**.

Select the frequency of notification messages in the pull-down menu **Send notifications**. By default, **None** is selected, and no other option in this section is enabled.

- If you select **Every day** in the **Send notifications** pull-down menu, the **Time** options are enabled for selection. You can choose as many time intervals as you like, in 1-hour increments.
- If you select **Every workday** in the **Send notifications** pull-down menu, the **Time** options are enabled for selection. You can choose as many time intervals as you like, in one-hour increments.
- If you select **Every week** in the **Send notifications** pull-down menu, the **Day of week** and **Time** fields are activated. Designate a day of the week for notification messages to be sent. You can choose as many time intervals as you like, in 1-hour increments.

Note

Notification messages will be sent only to protected domains. Unprotected domains will not receive notification messages.

Using the notification message template

The notification message template helps you determine the content and appearance of the email that informs users of blocked messages.

Any customizations you make to the notification message template are lost when upgrading to a new version of Forcepoint Email Security. After upgrade, you will need to reconfigure your customized templates.

Configure the notification message as follows:

Steps

1) Set the maximum number of messages that are included in each notification message. The default value is 50, maximum value is 100. A user with more than the maximum number of blocked messages waiting must handle the excess directly in the Personal Email Manager facility, via the Web Access link in the notification message.

2) Select the email actions you want the notification to include from among the following options:
   - **Deliver** (default selection), to allow the user to release a blocked message. The email may be delivered directly to the user's inbox, or it may be submitted for continued processing by subsequent filters if appropriate. The behavior is determined on the page **Settings** > **Personal Email** > **End-user Portal**, in the section Quarantined Message Delivery Options.
   - **Not Spam**, to allow the user to report a blocked message that should not be classified as spam
   - **Delete** (default selection), to remove a blocked message from the user's blocked message list
   - **Add to Always Block list**, to allow an authorized user to add an address to a personal Always Block List
   - **Add to Always Permit list**, to allow an authorized user to add an address to a personal Always Permit List

3) Enter your company name and other relevant information in the **Company** entry field.

4) Enter a brief description of the email filtering product in the **Description** entry field (default is “Forcepoint Email Protection Solutions”).

5) Enter the sender username in the **Sender username** field.

6) Enter the sender email address for the notification message in the **Sender email address** field.

7) Configure the subject line that you want the notification message to display in the **Subject** field. This subject will appear in the user’s inbox when the notification message is received.

8) Designate some appropriate header text for the notification message in the **Header** field.

9) Enter some appropriate footer text for the notification message in the **Footer** field.

Creating the notification message recipient list

Determine which Personal Email Manager users receive notification messages by entering their details into the Recipients List section. Only the users listed in the Recipients list receive notification messages alerting them about blocked email.

The Recipients list is based on user directories. All existing user directories are listed in the left-hand user directories box. Select a user directory and click the right arrow to add the directory to the **Recipients** list.

Click **Add user directory** to create a new directory on the Add User Directory page (see *Adding and configuring a user directory*). After you create a new user directory, it will appear in the user directories list on the Notification Message page.

To delete a user directory from the Recipients list, select the directory in the Recipients list and click **Delete**.

Related tasks

Adding and configuring a user directory on page 92

Setting user account options

Configure some Personal Email Manager user account options on the page **Settings** > **Personal Email** > **User Accounts**. Allow users to manage personal

Always Block and Always Permit lists, delegate blocked message management to another individual, and manage multiple user accounts in a single Personal Email Manager session.

User account management configuration settings made on one appliance are applied to all the appliances in your network.

Authorizing use of block and permit lists

Authorized users can manage their own Always Block and Always Permit lists after they log in to Personal Email Manager. Use the page **Settings** > **Personal Email** > **User Accounts** to specify users who can manage entries in personal block and permit lists.

Adding authorized users

Allow users to manage personal Always Block and Always Permit lists by specifying user directories that contain users with Personal Email Manager authentication privileges. Create user directories (in the User Directories page), and then specify authentication options for these user directories in the Add User Authentication page. (See *Adding and configuring a user directory* for user directory details and *Managing user validation/ authentication options* for information about user authentication settings.)

On the page **Settings** > **Personal Email** > **User Accounts**, user directories for which you have specified Personal Email Manager privileges appear as available user directories. To grant permission for a user directory group to manage personal block/permit lists, select a user directory in the available directories list by marking the check box next to the directory name, and click the arrow button to move it to the Recipients box.

Related concepts

Managing user validation/authentication options on page 103

Related tasks

Adding and configuring a user directory on page 92

Removing authorized users

Remove previously authorized users by selecting a user directory in the Recipients box and clicking **Delete**. The user directory still appears in the available directories box, but its members no longer have Always Block/Always Permit list management permissions.

Enabling user account management

Enable user account management functions for a Personal Email Manager end user by marking the check box **Enable user account management** on the page **Settings** > **Personal Email** > **User Accounts**. You can let end users delegate the management of blocked messages to one or more other individuals.

End users can configure these options in the User Account Access page, in the Personal Email Manager end-user interface. See *Personal Email Manager User Help* for details.

Personal Email Manager General Settings

Use the options on the Personal Email Manager General Settings page to configure both the end-user portal and Personal Email Manager notification messages.

Enabling end-user action auditing

Specify whether to maintain a record of end-user email management activities performed from either the Personal Email Manager notification message or from the Quarantined Messages List.

Enable the Personal Email Manager Audit Log

Steps

1) From the section End-user Audit Option, mark the check box **Audit end-user actions**.
   View the log at **Main** > **Status** > **Logs** > **Personal Email Manager**. See *Personal Email Manager Audit Log*.

2) Configure additional Personal Email Manager settings and click **OK**. The settings are saved.

Related concepts
Personal Email Manager Audit Log on page 50

Applying sender options

Select the content from incoming messages to be displayed in the Sender column of the end-user portal and in Personal Email Manager notification messages; Envelope Sender address or From: address. The selected option additionally applies when adding the sender to the Always Block and Always Permit lists.

Note

Both Envelope Sender and From: address are used to enforce Always Block and Always Permit policies.

Enable sender options

Steps

1) From the section Sender Options, select **Envelope Sender address** or **From: address**.
   The selected address displays in the end-user portal, Personal Email Manager notification messages, and Always Block and Always Permit lists.

2) Configure additional Personal Email Manager settings and click **OK**. The settings are saved.

Selecting quarantine message queue display

Select the queues for which messages are displayed to Personal Email Manager end users.

Steps

1) From the section Message Queue Display Settings, mark the check box next to the desired queue name.
   Multiple queues can be selected. *Example*: Select **spam**, **exception**, and **data-security**.

   Messages from the Spam, Exception, and Data Security message queues display in Personal Email Manager notification messages and in the Quarantined Messages List.

2) Configure additional Personal Email Manager settings and click **OK**.
   The settings are saved.

Enabling quarantine message delivery

Specify the Personal Email Manager behavior when an end user clicks Deliver for a selected message in the Quarantined Messages List.

Steps

1) From the section Quarantined Message Delivery Options, select the desired setting:
   - **Deliver quarantined message**
     Allows end users to release blocked email for direct delivery to their inbox.
   - **Resume quarantined message processing**
     Forces the analysis of blocked email to resume through all subsequent filters.

     A message triggering a subsequent filter may not be delivered to an end user if this option is selected.

2) Configure additional Personal Email Manager settings and click **OK**.
   The settings are saved.

Customizing the Personal Email Manager end-user portal

Use the page **Settings** > **Personal Email** > **End-user Portal** to customize the end-user facility's appearance and to designate the quarantined message queues whose messages are displayed in Personal Email Manager end-user notification email.

Choosing a logo display

By default, the Forcepoint company name and logo appear on the Personal Email Manager end-user page. You may choose to have no company name or logo appear on the portal. For this option, leave the Company name field blank and select **None** in the Logo field pull-down menu.

You can also customize the end-user portal by having your company name and logo appear there. Use the following procedures to customize your Personal Email Manager end-user portal in the End-user Portal Options section:

Steps

1) Enter your company name in the field **Company name**.

2) In the Logo field pull-down menu, select **Custom**.

3) The **Upload logo** field appears. Browse to your logo file and select it for upload. The logo file must be:
   - A .gif, .png, .jpeg, or .jpg file format
   - Up to 1 MB and 120 x 34 pixels in size

   You can change the logo file you use by clicking **Browse** next to your logo filename and browsing to a new logo file.

Enabling blocked message delivery

Specify the queue to which you want a message blocked by the Personal Email Manager Always Block list delivered.

Mark the check box **Save the original message to a queue**, and select a queue from the pull-down menu or add a new queue for this purpose.

Activating quarantined message list caching

Activate a list caching function for the Personal Email Manager end-user Quarantined Messages list that can enhance list display performance by reducing the number of database refresh operations. The following end-user actions do not automatically trigger a page refresh:

- Delete
- Deliver
- Reprocess
- Not spam

These operations reduce the size of the Quarantined Messages List until the page is less than half its original size, when an automatic refresh occurs.

Personal Email Manager end users may initiate a manual page refresh at any time by clicking **Refresh**.

Enabling quarantine message delivery

Specify Personal Email Manager behavior when an end user clicks **Deliver** for a selected message in the Quarantined Messages list. Select one of the following options:

- **Deliver quarantined message**, to allow end users to release blocked email for direct delivery to their inboxes
- **Resume quarantined message processing**, to force the analysis of blocked email to resume through all subsequent filters. If this option is used, a message may not be delivered to an end user if it triggers a subsequent filter.

Enabling images in quarantined messages

Use the Display Images Option section to determine whether to allow images to display in quarantined messages viewed in the Personal Email Manager end-user portal. For security, this option is disabled by default.

To enable this option, mark the check box **Display images within quarantined messages viewed in the Personal Email Manager**.

Warning

Enabling this feature is not recommended because a malicious script hosted remotely may be disguised in the email as an image, allowing the attacker to compromise your system.