

Configuration Information

Administrator Help | Forcepoint Email Security Configuration Information | Version 8.5.x

Topics:

- [Using the First-time Configuration Wizard, page 1](#)
- [Entering and viewing subscription information, page 5](#)
- [Navigating the Forcepoint Security Manager, page 7](#)
- [The dashboard, page 12](#)
- [Viewing and searching logs, page 24](#)
- [Real-time monitor, page 46](#)
- [Security Information and Event Management \(SIEM\) integration, page 47](#)
- [Email hybrid service configuration, page 48](#)
- [Registering the DLP Module, page 55](#)
- [Email filtering database updates, page 57](#)
- [Configuring system alerts, page 58](#)
- [URL analysis, page 62](#)
- [Selecting advanced file analysis platform, page 64](#)
- [Using a proxy server, page 65](#)
- [Using the Common Tasks pane, page 66](#)

Using the First-time Configuration Wizard

Administrator Help | Forcepoint Email Security | Version 8.5.x

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, page 5](#)).

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 \(FQDN\), page 2](#)
- [Domain-based route, page 3](#)
- [Trusted IP addresses for inbound mail, page 3](#)
- [Email Log Server information, page 3](#)
- [System notification email address, page 4](#)

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.

Fully qualified domain name (FQDN)

Administrator Help | Forcepoint Email Security | Version 8.5.x

The FQDN page of the Configuration Wizard is used to specify the appliance fully qualified domain name (FQDN). This setting is important 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 appliancehostname.parentdomain.com.

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

Domain-based route

Administrator Help | Forcepoint Email Security | Version 8.5.x

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, page 17](#).

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

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.

Trusted IP addresses for inbound mail

Administrator Help | Forcepoint Email Security | Version 8.5.x

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, page 16](#), 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**.

Email Log Server information

Administrator Help | Forcepoint Email Security | Version 8.5.x

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

Administrator Help | Forcepoint Email Security | Version 8.5.x

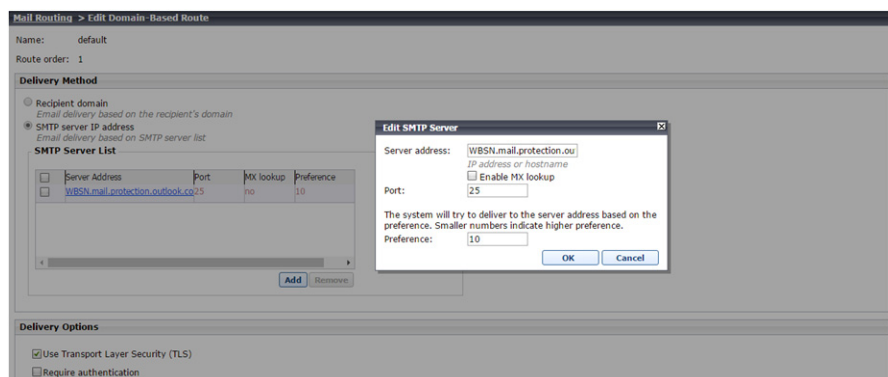
Identify an email address to which you want system notification messages sent on the wizard page **Notifications**. Typically, this is an administrator address. Enter the desired address in the field **Notification email address**.

Configure the appliance in the Forcepoint Security Manager

Forcepoint DLP Email Gateway steps

Some initial configuration settings are important for Forcepoint DLP Email Gateway operation. Perform the following activities after you install Forcepoint DLP Email Gateway management components.

1. Log on to the Forcepoint Security Manager and select the tab **Email**.
The Email module displays.
2. At the prompt, enter your subscription key and click **OK**.
If you skip this step, you can enter your subscription key later on the page **Settings > General > Subscription**.
3. Register the Forcepoint Email Security DLP Module.
The DLP Module can be registered at any point, but it is recommended to do this before any other configuration is completed.
4. Configure the system to send email through Office 365 to Forcepoint DLP Email Gateway.
 - a. Navigate to **Settings > Inbound/Outbound > Mail Routing**.
 - b. Select the default route.
 - c. From Delivery Method, select **SMTP server IP address**.
 - d. Under SMTP Server List, click **Add**.



- e. For Server Address, add the FQDN of your organization's Microsoft Office 365 account. This is the same as the MX record of the Office 365-hosted domain. To find it:
 - In the Office 365 Admin Center, select **Settings > Domains**.

- Select the domain name you configured for your organization.
 - Under Exchange Online, you will see a row for MX. The MX record is listed in that row.
- f. For Port, enter **25**.
 - g. Enter a Preference.
 - h. Click **OK**.
 - i. Under Delivery Options, select **Use Transport Layer Security (TLS)**.
 - j. Click **OK**.
 - k. Repeat this step for each Forcepoint DLP Email Gateway VM you have.
5. Specify an email address to which system notification messages should be sent. This is typically an administrator address. See [Setting system notification email addresses, page 14](#).
 6. In the Email module, data loss prevention policies are enabled by default. To manage DLP policies, navigate to **Main > Policy Management > DLP Policies > Manage Policies**.
 7. In the Data module, you can view all of the VMs in the System Modules list. Select the Data tab and click **Deploy**.
Click **Help** on any Forcepoint Security Manager page for help about the page. See [Forcepoint DLP Administrator Help](#) for complete information about the DLP Module.

Forcepoint Security Manager steps

These steps are necessary if you have existing DLP policies.

1. From the Forcepoint Security Manager, select the tab **Data**.
2. Add the network email destination to any existing policies that should be used for this appliance.
3. Click **Deploy**. No other configuration steps are required.

The Forcepoint DLP Email Gateway module is shown on the System Modules page, as well as System Health and System Logs.

Use the System Modules page to edit the display name or description for the appliance. If desired, you can balance the load on the gateway by selecting **System Modules > Load Balancing** and then editing the Forcepoint DLP Email Gateway module.

Refer to [Forcepoint DLP Administrator Help](#) for more information.

Entering and viewing subscription information

Administrator Help | Forcepoint Email Security | Version 8.5.x

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.

Add subscription key

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](#), page 28.

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, page 49](#).

Navigating the Forcepoint Security Manager

Administrator Help | Forcepoint Email Security | Version 8.5.x

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

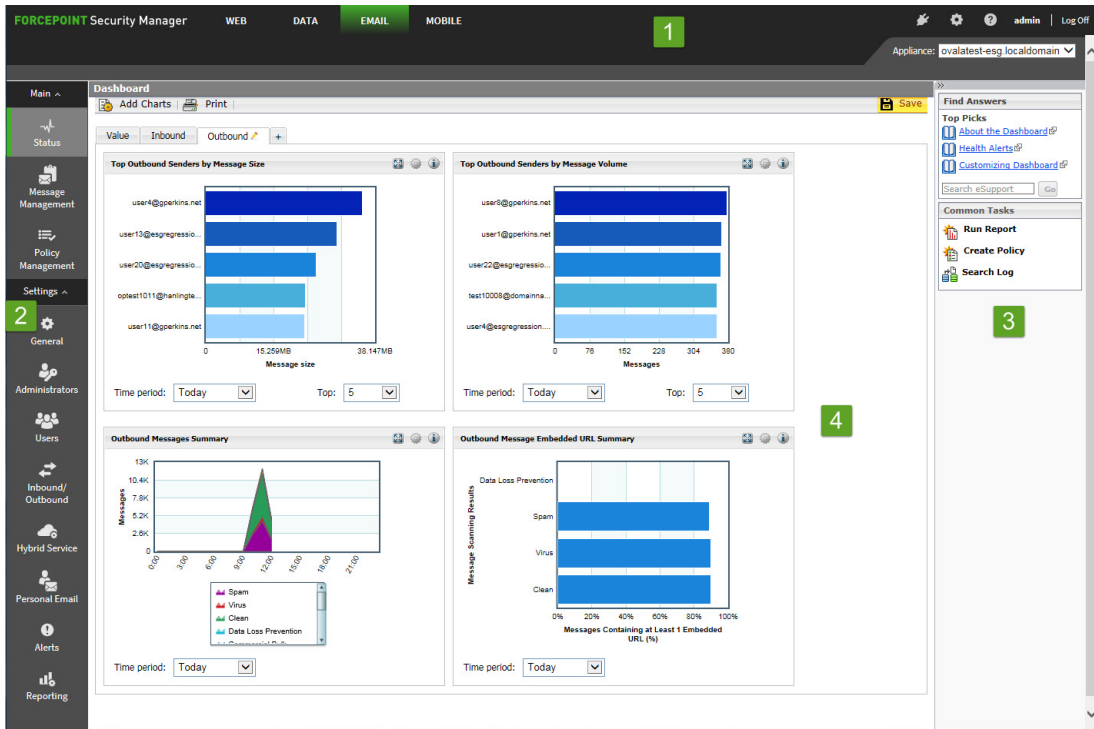
- The Security Manager toolbar
- The left navigation pane
- The right shortcut pane
- The context pane

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.

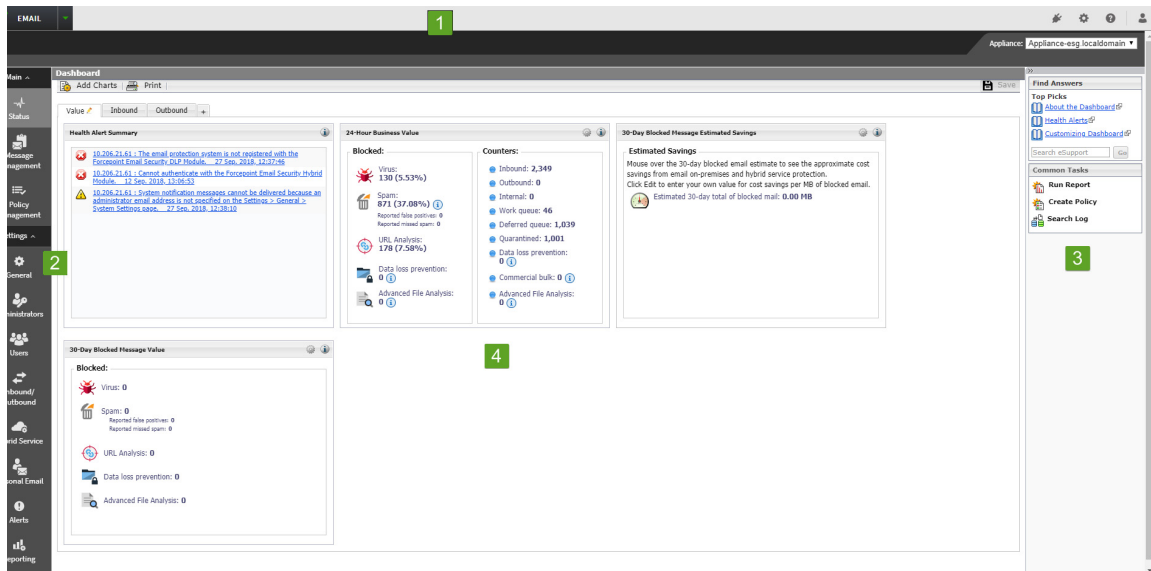
This section describes the options available to users with Super Administrator privileges.

Certain menu options were changed in versions 8.5.3 and 8.5.4. The following image

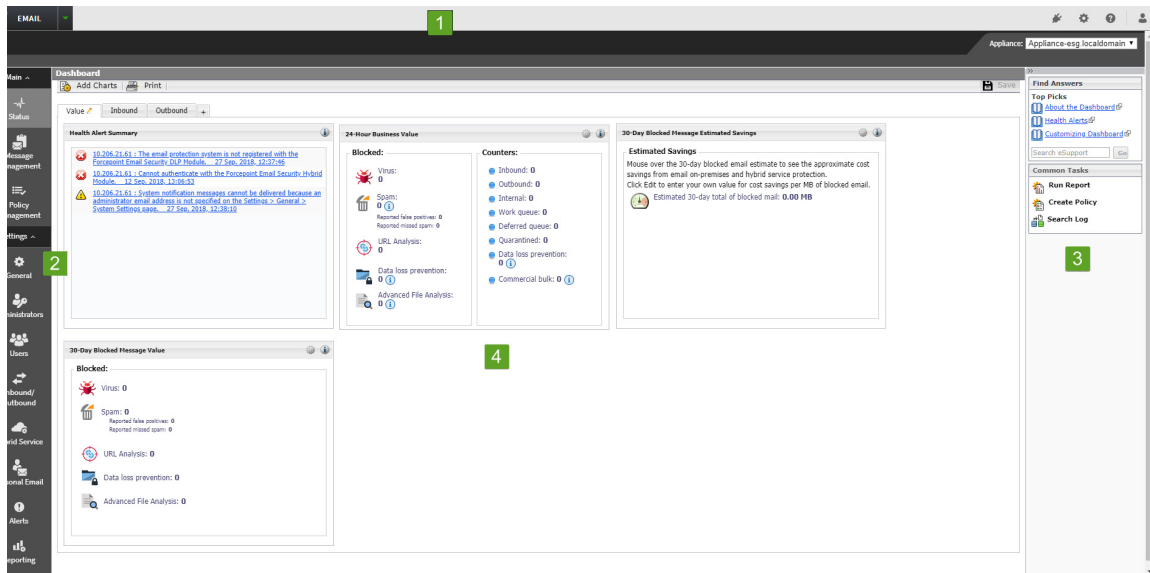
displays the user interface for Security Manager version 8.5:



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

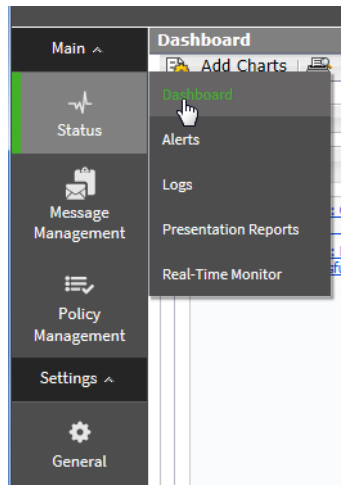
1. From the Security Manager banner, click the icon **Help**.
The Help options display.
2. Click **Explain This page**.
A new tab displays, showing the Help topic for the current page of the Forcepoint Security Manager.
3. *(Optional)* From the Help topic, click **Open topic with navigation**.
The complete 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

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

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.

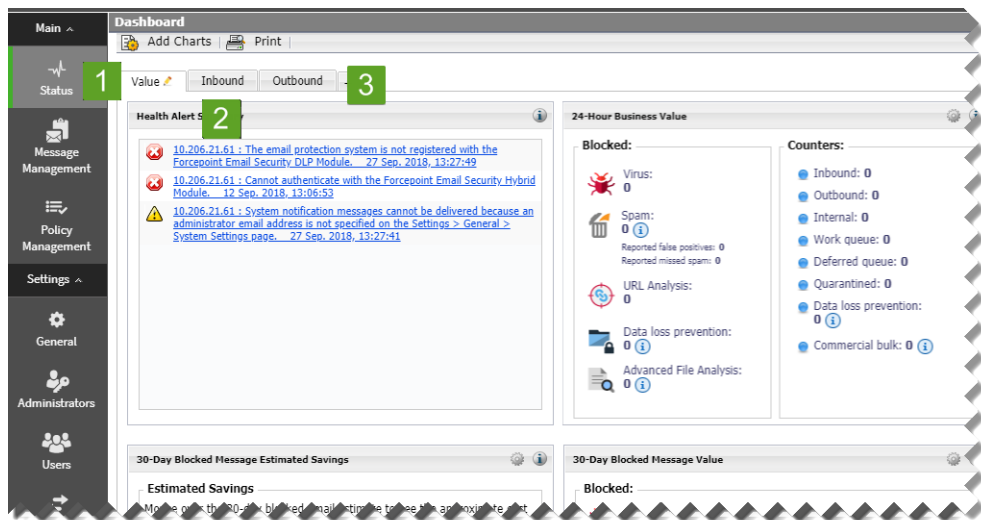
The dashboard

Administrator Help | Forcepoint Email Security | Version 8.5.x

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.

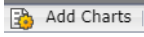


The following image displays the dashboard in version 8.5.4:



- 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	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 , page 19.
	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	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.

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](#), page 20, 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.

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](#), page 19.

Move a chart on a dashboard tab

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

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

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

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.

- From the dashboard, click **Save**.

The dashboard configuration is saved.

View a larger version of a chart

- 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.

- From the section Chart Options, configure options for the selected chart.

Example: chart type, time period, top numerical designation.

- (Optional) Print the chart; select **Print Chart**.
- When finished, click **Close**.

Value dashboard tab

Administrator Help | Forcepoint Security Manager | Version 8.5.x

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 8.5.4:

- 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](#), page 22).

- 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.

Change the name of the Value dashboard tab

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](#), page 19.

Remove a chart from the Value dashboard tab

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

Administrator Help | Forcepoint Email Security | Version 8.5.x

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

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](#), page 19.

Remove a chart from the Inbound dashboard tab

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

Administrator Help | Forcepoint Email Security | Version 8.5.x

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

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](#), page 19.

Remove a chart from the Outbound dashboard tab

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

Administrator Help | Forcepoint Email Security | Version 8.5.x

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, page 20 , 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.

Add charts to a dashboard tab

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 its 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

Administrator Help | Forcepoint Email Security | Version 8.5.x

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, page 19](#). 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
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

Chart Name
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
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

Chart Name
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)

Viewing system alerts

Administrator Help | Forcepoint Email Security | Version 8.5.x

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**.

System health alerts

Administrator Help | Forcepoint Email Security | Version 8.5.x

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
- 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, page 58](#), 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, page 22](#).

Viewing and searching logs

Administrator Help | Forcepoint Email Security | Version 8.5.x

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:

- [Message Log, page 25](#)
- [Connection Log, page 32](#)
- [Audit Log, page 35](#)
- [Personal Email Manager Audit Log, page 37](#)
- [System Log, page 40](#)
- [Console Log, page 42](#)
- [Email Hybrid Service Log, page 43](#)

Message Log

Administrator Help | Forcepoint Email Security | Version 8.5.x

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	<p>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).</p> <p>The Block List type applies to a message that is blocked by a Personal Email Manager Always Block List.</p> <p>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.</p>
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	<p>Pull-down menu functionality to select a message element on which to search:</p> <ul style="list-style-type: none"> ● Subject ● Sender Address ● Sender IP ● Recipient Address ● Analysis Result ● Message Status ● To: Header ● From: Header ● Spam Score ● Message Size (KB) ● Appliance
Condition	<p>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:</p> <ul style="list-style-type: none"> ● 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 <p>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.</p> <p>Note: 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.</p>
Value	User-defined text field to enter a value for the filter and condition.

Option	Description
Add/Remove	Selection adds or removes a row of filtering options to further narrow the search.
Advanced Options	<p>Selection displays additional sort conditions to refine the search:</p> <ul style="list-style-type: none"> ● By Direction <ul style="list-style-type: none"> ■ Inbound ■ Outbound ■ Internal ■ Open Relay ● By Analysis Result <ul style="list-style-type: none"> ■ 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 <ul style="list-style-type: none"> ■ Delivered ■ Delayed ■ Dropped ■ Exception ■ Failed ■ Expired ■ Rejected

Search the Message Log

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

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

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.
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

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](#), page 31.

3. Return to the Message Log, click **Back**.

The Message Log page displays.

View quarantined message details

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

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

Administrator Help | Forcepoint Email Security | Version 8.5.x

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.

Connection Data Item	Description
Security Level	Encrypted or Not Encrypted.
Connection Status	<p>Current connection status (Accepted or Blocked). Status details are displayed in a hover-over pop-up box. Possible Blocked status details are as follows:</p> <ul style="list-style-type: none"> ● 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. <p>Possible Accepted status details are as follows:</p> <ul style="list-style-type: none"> ● 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

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

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

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](#), page 30.

Audit Log

Administrator Help | Forcepoint Email Security | Version 8.5.x

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.

Column	Description
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 Email Security 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

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

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

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

Administrator Help | Forcepoint Email Security | Version 8.5.x

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, Forward, or Clear All Messages; does not include the actions Add to Always Block list, Add to Always Permit list, 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

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

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

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

Administrator Help | Forcepoint Email Security | Version 8.5.x

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

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

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

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

Administrator Help | Forcepoint Email Security | Version 8.5.x

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

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

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

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

Administrator Help | Forcepoint Email Security | Version 8.5.x

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, page 49](#)).

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, page 55](#). Access the Email Hybrid Service Log from the Email Hybrid Service tab of the page **Main > Status > Logs**.

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

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

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

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

Administrator Help | Forcepoint Email Security | Version 8.5.x

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	<p>Check box functionality to select any or all of the available types of log information for display:</p> <ul style="list-style-type: none"> • 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.
Real-Time logs	Displays the selected log entries or search results.

Display log entries

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

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

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

Administrator Help | Forcepoint Email Security | Version 8.5.x

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

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

Administrator Help | Forcepoint Email Security | Version 8.5.x

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, page 49](#).

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, page 43](#), for information about the contents of this log. See [Configuring the Email Hybrid Service Log, page 55](#), 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](#).

Registering the Email Security Hybrid Module

Administrator Help | Forcepoint Email Security | Version 8.5.x

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, page 50](#)
2. [Define delivery routes, page 51](#)
3. [Configure your DNS, page 52](#)
4. [Set up your firewall, page 53](#)

5. [Configure your MX records, page 53](#)
6. [Modifying email hybrid service configuration, page 54](#)



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:

1. Add all your appliances to the Security ManagerEmail Securitymodule (**Settings > General > Email Appliances**)
2. Create an appliance cluster, if desired (**Settings > General > Cluster Mode**)
3. Enter your subscription key (**Settings > General > Subscription**)
4. Register the Forcepoint Email Security Hybrid Module (**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 Email Security 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.

Enter customer information

Administrator Help | Forcepoint Email Security | Version 8.5.x

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](#).

Define delivery routes

Administrator Help | Forcepoint Email Security | Version 8.5.x

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 (e.g., `postmaster@mydomain.com`), you should add it manually before completing this step.

Add a delivery route

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](#), page 16.

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 [Third-party encryption application, page 25](#), 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](#).

Configure your DNS

Administrator Help | Forcepoint Email Security | Version 8.5.x

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:

```
abcdefghijklm.mydomain.com CNAME automain.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
- automain.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 **automain.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](#).

Set up your firewall

Administrator Help | Forcepoint Email Security | Version 8.5.x

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](#).

Configure your MX records

Administrator Help | Forcepoint Email Security | Version 8.5.x

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

Administrator Help | Forcepoint Email Security | Version 8.5.x

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

Administrator Help | Forcepoint Email Security | Version 8.5.x

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](#), page 49.

Configure Email Hybrid Service Log options

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.

Registering the DLP Module

Administrator Help | Forcepoint Email Security | Version 8.5.x

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](#), page 28, 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 [Managing policies, page 28](#), 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:

Manually register the DLP module

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**.

- 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

Administrator Help | Forcepoint Email Security | Version 8.5.x

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

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

Administrator Help | Forcepoint Email Security | Version 8.5.x

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*.

Enabling system alerts

Administrator Help | Forcepoint Email Security | Version 8.5.x

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

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**

Email 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

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.

Alert events

Administrator Help | Forcepoint Email Security | Version 8.5.x

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](#), page 58.

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

Select alerts for event types

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.

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:

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:

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

Administrator Help | Forcepoint Email Security | Version 8.5.x

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](#).

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

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

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 URL database.
4. Verify the connection to the URL analysis service; click **Test Connection**.
5. Click **OK**.
The settings are saved.

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

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 URL 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

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.

Using a proxy server

Administrator Help | Forcepoint Email Security | Version 8.5.x

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

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

Administrator Help | Forcepoint Email Security | Version 8.5.x

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

Use the Common Tasks pane

- Click an item in the list.
The page displays on which the task is performed.

© 2022 Forcepoint. Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint. Raytheon is a registered trademark of Raytheon Company. All other trademarks used in this document are the property of their respective owners.