# Configuration Information

TRITON AP-EMAIL Configuration Information | Version 8.2.x

Topics:



## Using the First-time Configuration Wizard

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

Click the Email module in the TRITON console 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 in the **Settings > General > Subscription** page (see *Entering and viewing information*, page 4).

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 2
- *Trusted IP addresses for inbound mail*, page 3
- *Email Log Server information*, page 3
- *System notification email address*, page 3

In order to save your settings, you must review them in the wizard's Confirmation page and click **Complete**.

Note that 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 to view the appropriate wizard page. 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)

The FQDN page of the Configuration Wizard lets you 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 **Fully Qualified Domain Name** field (FQDN format is appliancehostname.parentdomain.com).

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

## Domain-based route

The **Domain-based Route** page of the Configuration Wizard lets you identify a domain that you want protected and designate the SMTP server to which mail to this

domain should be sent. You can add more protected domains in the **Settings > Inbound/Outbound > Mail Routing** page. See the topic titled *Protected Domain group* in TRITON AP-EMAIL Administrator Help for information about protected domains.

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

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

## Trusted IP addresses for inbound mail

In the Trusted Inbound Mail page, 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 the topic titled *Managing domain and IP address groups* in TRITON AP-EMAIL Administrator Help 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

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 **Log Server** page. Click **Check Status** to receive Log Server availability information.

## System notification email address

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

## Entering and viewing information

You should receive a subscription key after you purchase TRITON AP-EMAIL. If you did not enter the subscription key the first time you opened the Email module, enter it in the **Settings > General > Subscription** page. This subscription key can be entered in 1 appliance and is applied to all the appliances controlled by the Email module.

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.

Use the **Subscription key** field to enter a new key any time you receive one. If your subscription includes the Email 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.

## Navigating the TRITON Manager Email module

The Email module user interface can be divided into 6 main areas:

- Banner
- Module tray
- Email module toolbar
- Left navigation pane
- Right shortcut pane
- Content pane

The TRITON Manager banner shows:

- Your current logon account
- A Log Off button, for when you want to end your administrative session

The content displayed in the Email 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.

The module tray lets you launch other modules of the TRITON Manager. For Forcepoint web or data protection customers, click **Web** or **Data** to open the Web or Data modules.

An Appliances button in the module tray opens a Manage Appliances window, which lets you add and remove an appliance in your system.

A TRITON Settings button lets you:

- Manage your administrator account.

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

See the TRITON Manager Help for more details.

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

The Email module toolbar, just under the module tray, lets you switch between the Main and Settings tabs of the left navigation pane. Use the Main tab to access email software status, reporting, and policy management features and functions. Use the Settings tab to perform system administration tasks. The toolbar also includes a drop-down list of system appliances.

The right shortcut pane contains a Find Answers portal that may include links to topics related to the active screen and step-by-step tutorials for specific tasks. A search function lets you find relevant information in the Forcepoint eSupport web site. The right pane also includes links to common administrative tasks. Click an item in the list to jump to the page where the task is performed.

Both the left and right navigation panes can be minimized by clicking the double arrow (<< or >>) icon at the top of the pane. Click the reverse icon (>> or <<) to view the pane. Click a shortcut icon on the minimized left navigation pane to access various groups of email security functions without maximizing the pane.

## The dashboard

The **Value** tab of the **Status > Dashboard** page appears first when you log on to the TRITON console and select the Email module. It shows information about the value of TRITON AP-EMAIL in your network, along with a summary of system health alerts.

The type of information and level of detail shown depends on your subscription level. The Email Hybrid Module is required, for example, to display information about the email hybrid service and how it safeguards your system. You must have purchased the Email Sandbox Module to view metrics on URL or advanced file analysis file sandbox functions. You must purchase a Threat Protection appliance to view advanced file analysis Threat Protection metrics.

Dashboard elements are visible to Super Administrators and those delegated administrators with permission to view reports on the email dashboard (see the topic titled *Managing administrator accounts* in TRITON AP-EMAIL Administrator Help).

The **Save** button in the upper right area of the dashboard activates when an administrator makes dashboard changes, for example when charts are added,

removed, edited, or moved to another location on the dashboard. Renaming a tab also activates the **Save** button. Ensure that you save any changes before you navigate away from the dashboard.

The dashboard includes 2 other default tabs, in addition to the *Value dashboard tab*:

- *Inbound dashboard tab* 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.
- *Outbound dashboard tab* 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.

Add a new custom tab by clicking the tab that displays the "plus" sign icon (+). Enter a name in the Add Tab dialog box (maximum of 10 alphanumeric characters, including underscores). Click **Add Charts** to add elements to your new tab. You may add up to 4 custom tabs.

Click the edit icon for an active tab to open the Edit Tab dialog box, where you can change the tab name. You can also remove the tab by clicking **Delete Tab**. You can rename the default tabs if desired, but these tabs cannot be removed.

The default Value, Inbound, and Outbound dashboard tabs can each display up to 12 charts at a time. Most dashboard charts can be customized 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 9, for a list of charts for dashboard display.

- Most dashboard elements are updated every 2 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 Email Hybrid Module.
- To add an element to the tab, click **Add Charts**, then see *Adding elements to a dashboard tab*, page 9, for instructions.
- Use a drag-and-drop function to move an element from one location on a tab to a different location on the same tab. Click the chart title area and drag the chart to its new location.
- To remove an element from the tab, click the Options icon in the element title bar, then select **Remove**.
- To access all editing options for an element, click the Options icon in the element title bar, then select **Edit**. Drill-down capabilities are available as well. You can perform the following edit operations:
  - Change:

    - 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)
- To print a chart, click the Options icon and select **Print**. You can also right-click a chart and select the print option.
- To view a larger version of a chart, click the Enlarge icon in the element title bar. You can access some editing options in this view (for example, chart type, time period, top numerical designation), as well as drill-down capabilities. Click **Print Chart** to print the current chart. When you click **Close**, any changes you have made to the chart in this view are not retained in the dashboard.
- 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 1-hour increments. These capabilities are available in the Edit, Enlarge, and Preview chart views.

Two buttons appear in the dashboard toolbar:

- **Add Charts** allows administrators to customize their view of the selected dashboard tab by adding elements to the page. See *Adding elements to a dashboard tab*, page 9.
- **Print** opens a secondary window with a printer-friendly version of the charts displayed on the page. Use browser options to print the page.

## Value dashboard tab

The Value dashboard tab displays alert messages and graphical charts that show the current state of your email protection system, focusing on email traffic activity in your network. Default tab elements include the following:

- The **Health Alert Summary** shows the status of your Forcepoint software. Click an error or warning alert message to open the Alerts page, where more detailed alert information is available (see *Viewing system alerts*, page 11).
- In the **24-Hour Business Value** chart, view 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 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 Email 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. Click the Options icon in the element's title bar and select **Edit** to set the cost savings per MB of blocked mail.

- In **30-Day Blocked Message Value**, view 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.

You can rename a default tab, but you cannot remove it. You can remove any chart that appears on the tab, and click **Add Charts** to add a different chart to the tab.

## Inbound dashboard tab

The Inbound dashboard tab provides summary data on inbound message traffic. Default charts 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.
- A **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.

You can rename a default tab, but you cannot remove it. You can remove any chart that appears on the tab, and click **Add Charts** to add a different chart to the tab.

## Outbound dashboard tab

The Outbound dashboard tab provides summary data on outbound message traffic. Default charts 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.
- A **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).
- An **Outbound Message Embedded URL Summary** chart shows the percentage of analyzed outbound messages that contain at least 1 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).

You can rename a default tab, but you cannot remove it. You can remove any chart that appears on the tab, and click **Add Charts** to add a different chart to the tab.

## Adding elements to a dashboard tab

Use the **Status > Dashboard > Add Charts** page to add elements to the Value, Inbound, Outbound, or any custom dashboard tab.

To start, use the **Add elements to tab** drop-down list to select a tab, then select the element that you want to add from the **Dashboard Elements** list. A **Restore Tab Defaults** button is available in the Available Tabs section only for the default tabs, not for custom tabs.

- 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).

When you select an element in the list, a sample is displayed in the **Preview** pane. You can use the preview pane to make changes to the chart **Name** and, if applicable, **Chart type**, **Time period**, and **Top** value (for example, top 1-5 categories, or top 16-20 users). 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. Which types are available depends 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 5 values, 6-10 values, 11-15 values, or 16-20 values.

When you are finished making changes, click **Add**. The dashboard tab is updated immediately.

If you have been editing a chart and would like to start over, click **Restore Defaults** to reset the chart to is default time period, type, and top value (if any).

## Available dashboard charts

The dashboard charts in the following table are available in the Add Charts page Dashboard Elements list.

Some charts show potentially sensitive information, such as usernames or IP addresses. Be sure 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 |
| 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 |

| Chart Name |
| --- |
| 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 File Sandbox Analysis Volume (requires Email Sandbox Module) |
| Top File Sandbox-Detected Attachments Received (requires Email Sandbox Module) |
| File Sandbox-Detected Attachments by File Type (requires Email Sandbox Module) |
| Top File Sandbox-Protected Recipients (requires Email Sandbox Module) |
| Inbound Threat Protection Analysis Volume (requires Threat Protection appliance deployment) |
| Top Malicious Attachments Detected by Threat Protection (requires Threat Protection appliance deployment) |
| Top Recipients Protected by Threat Protection (requires Threat Protection appliance deployment) |
| Attachment File Types Detected by Threat Protection (requires Threat Protection appliance deployment) |
| Email Hybrid Service Message Size Summary (requires Email Hybrid Module) |
| Email Hybrid Service Message Volume Summary (requires Email Hybrid Module) |

## Viewing system alerts

The **Health Alert Summary** on the dashboard shows the status of your email protection software. Click an error or warning message to open the **Status > Alerts** page, where more detailed alert information is available.

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

The Active Alerts list shows the status of monitored Forcepoint software components. For detailed information about which components are monitored, click **What is monitored?** above the list of alert messages.

To troubleshoot a problem, click **Solutions** next to an error or warning message. Click **Learn More** to find more details about an informational alert.

## System health alerts

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

- Subscription expiration issues or subscription key problems
- Email services unavailable or not running
- Email software configuration problems
- Master 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 Email 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:

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

See *Configuring system alerts*, page 38, 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.

Click an alert message in the Health Alerts Summary to go to the Alerts page, which provides additional information about current alert conditions. Click **Learn More** (for informational alerts) or **Solutions** (for errors or warnings) for details and troubleshooting tips.

## Viewing and searching logs

Several logs are available to help you monitor system and email message status. These logs are searchable by predefined time periods, or you can customize the time period you want searched. The Message Log also allows you to refine your search for messages, using search conditions like email address, message analysis result, or message status.

You can export any log's search results to a comma-separated value (CSV) or HTML file. Note that the maximum number of log entries exported cannot be greater than 100,000.

The following logs are accessed from the **Main > Status > Logs** page:

- *Message Log*, page 13
- *Connection Log*, page 18
- *Audit Log*, page 20
- *Personal Email Manager Audit Log*, page 22
- *System Log*, page 24
- *Console Log*, page 25
- *Email Hybrid Service Log*, page 26

### Message Log

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

You can configure the number of entries per log page, between 25 and 200, in the **Per page** drop-down list in the log table banner. At the top and bottom of the page, scroll through Message Log pages by clicking the back and next arrows, or enter a specific page number in the **Page** field and click **Go**.

The length of time message records are saved in the database depends on your message volume and database partition capacity. To preserve message records, use the Export option to export the log on a regular basis. Exporting does not remove records from the Message Log. It copies log data to a CSV or HTML file.

When the Message Log page appears, the most recent records are shown. Use the **View from/to** fields to specify the date/time range for the log entries you want to see. The calendar includes the following options:

- Change the month and year by using the back and next arrows around the month and year at the top of the calendar.
- Set the calendar to the current date by clicking the date in the lower left corner of the calendar.
- Click **Clean** to clear the current date/time calendar selection.
- Click **Today** to set the calendar date to today's date.

Set the time range in hours and minutes in the entry fields to the right of the calendar.

## Message Log data

The following message data is collected and displayed in table format:

| Message Data Item | Description |
|---|---|
| Message Log ID | A database-generated message identifier |
| Received Date/Time | The date and time a message was received |
| Subject | The message subject |
| Sender Address | Message sender email address |
| Sender IP | Message sender IP address |
| Recipient Address | Message recipient email address. If the message has multiple recipients, the first recipient address is displayed. |
| Analysis Result | Message analysis results or filter type (Clean, Virus, Spam, Data Loss Prevention, Exception, Commercial Bulk, Block List, Phishing, File Sandbox, Threat Protection, or Custom Content).<br>The Block List type applies to a message that is blocked by a Personal Email Manager Always Block List.<br>When a data loss prevention (DLP) policy is indicated, a **View Incident** link in this column opens the incident details in the TRITON console Data module. |
| 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. |

## Message recipient details

When you click an individual message log identifier, details about that message are displayed. The following message detail items appear in table format:

| 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.<br>This item is blank for a message with a scanning result of Clean. |
| Analysis Result | Message analysis results or filter type (Clean, Virus, Spam, Data Loss Prevention, Exception, Commercial Bulk, Block List, Phishing, File Sandbox, Threat Protection, or Custom Content)<br>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. |

## Message Log details

After you click a message in the Message Log ID column to view recipient details, a new **View Log Details** button is available at the bottom of the page. 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

### Message Log search options

The Message Log includes several search options, including date range or keyword searches. Determine the date/time range for a search by selecting dates in the **View from/to** field calendar controls. Default value for the **from** or **to** field is the date and time that you open the log.

You can perform a keyword search by selecting the log elements on which you want the search done from the **Keyword search** drop-down list and then entering a term in the field to the right of the list.

You can search for a keyword in 1 of the following Message Log components:

| Keyword Search Option | Supported Keyword |
|---|---|
| Message Log ID | Enter the complete Message Log ID number. Wildcards (*) and non-numeric characters are not supported. |
| Subject | Enter any part of a message subject. Wildcards (*) are supported only at the beginning or end of a Subject keyword (e.g., *subject, subject*, *subject*). |
| Sender Address | Enter a complete email address (e.g., sender@domain.com). Wildcards (*) are supported only at the beginning or end of an address (e.g., *@domain.com, sender@*, *sender@domain*). |
| Sender IP | Enter a complete sender IP address. Wildcards (*) are supported only at the end of a partial IP address and only after a period (e.g., 10.*, 10.20.*, 10.20.30.*). Non-numeric characters are not supported. |
| Recipient Address | Enter a complete email address (e.g., sender@domain.com). Wildcards (*) are supported only at the beginning or end of an address (e.g., *@domain.com, recipient@*, *recipient@domain*). |
| Analysis Result | Enter any part of the message analysis result. Wildcards (*) are supported only at the beginning or end of an analysis result keyword (e.g., *result, result*, *result*). |
| Message Status | Enter any part of the message status. Wildcards (*) are supported only at the beginning or end of a message status keyword (e.g., *status, status*, *status*). |

Use the **All** keyword search option to search using a combination of the following Message Log elements:

- Subject
- Sender Address
- Recipient Address

- Sender IP

Alphanumeric characters are supported in the keyword search entry field.

Click **Set to Default** to return the keyword search options to the default settings (all Message Log components and keyword field blank).

View advanced search options for narrowing your message search by clicking **Advanced Options** to the right of the Keyword search box. Refine your search by selecting options in 1 or more of the following categories:

| Category | Description |
|---|---|
| By Email Address | Click **Specify Email Addresses** to open the Specify Email Addresses dialog box. Specify your matching conditions, including email addresses and whether the address can be a sender, a recipient, or both. The search results include matches for any address you enter in the Condition Details box. Wildcard entries are not supported.<br>Separate email address entries by a semicolon (;). |
| By Analysis Result | Search by message analysis results or filter type (Clean, Virus, Spam, Commercial Bulk, Data Loss Prevention, Custom Content, Exception, Block List, Phishing, File Sandbox, or Threat Protection)<br>The Block List type applies to a message that is blocked by a Personal Email Manager Always Block List. |
| By Message Status | Search by current message status (Delivered, Delayed, Dropped, Exception, Expired, or Failed) |

Click **Search** to generate search results.

Click **Set to Default** to return all your search option settings to their default state.

### Message Log export options

To export Message Log search results:

1. Click **Export** to open the Export Log dialog box.
2. Select the desired output file type (CSV or HTML).
   - If you select **CSV**, a dialog box opens to let you open or save a text file in comma-separated value format.
   - If you select **HTML**, a dialog box opens to let you open or save an HTML file containing the log data.
3. Indicate the pages you want to export (All, Current Page, or a page range).
4. Click **OK**.

## Connection Log

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

You can configure the number of entries per log page, between 25 and 200, in the **Per page** drop-down list in the log table banner. At the top and bottom of the page, scroll through Connection Log pages by clicking the back and next arrows in the banner, or enter a specific page number in the **Page** field and click **Go**.

The length of time connection records are saved in the database depends on your connection volume and database partition capacity. To preserve connection records, use the Export option to export log data on a regular basis. Exporting does not remove records from the Connection Log. It copies log data to a CSV or HTML file.

When the Connection Log page appears, the most recent records are shown. Use the **View from/to** fields to specify the date/time range for the log entries you want to see. The calendar includes the following options:

- Change the month and year by using the back and next arrows around the month and year at the top of the calendar.
- Set the calendar to the current date by clicking the date in the lower left corner of the calendar.
- Click **Clean** to clear the current date/time calendar selection.
- Click **Today** to set the calendar date to today's date.

Set the time range in hours and minutes in the entry fields to the right of the calendar.

### Connection Log data

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

When you click an individual sender IP address link in the Connection Log, the Message Log opens and displays details about the message or messages associated with the selected connection.

### Connection Log search options

The Connection Log includes several search options, including date range or keyword searches. Determine the date/time range for a search by selecting dates in the **View from/to** field calendar controls. Default value for the **from** or **to** field is the date and time that you open the log.

You can perform a keyword search by selecting the log elements on which you want the search done from the **Keyword search** drop-down list and then entering a term in the field to the right of the list. Search for a keyword in all Connection Log elements, or in 1 of the following components:

- Sender IP address (wildcards and special characters are not supported in the keyword)
- Security Level
- Connection Status

Click **Search** to generate search results.

Click **Set to Default** to return the keyword search options to the default settings (**All** Connection Log components with the keyword field blank).

### Connection Log export options

To export Connection Log search results:

1. Click **Export** to open the Export Log dialog box.
2. Select the desired output file type (CSV or HTML).
   - If you select **CSV**, a dialog box opens to let you open or save a text file in comma-separated value format.
   - If you select **HTML**, a dialog box opens to let you open or save an HTML file containing the log data.
3. Indicate the pages you want to export (All, Current Page, or a page range).
4. Click **OK**.

## Audit Log

The email protection system provides an audit trail showing which administrators have accessed the TRITON console Email module, as well as any changes made to policies and settings. This information is available only to Super Administrators. Monitoring administrator changes through the Audit Log enables you to ensure that system control is handled responsibly and in accordance with your organization's acceptable use policies.

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

Audit records are saved for 30 days. To preserve audit records longer than 30 days, use the Export option to export 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.

When the Audit Log page opens, the most recent records are shown. Use the **View** drop-down list options located above the log to select the range of log entries you want to see: All, One Day, One Week, One Month, or Custom. When you select **Custom**, use the **View from/to** fields to specify the desired date/time range for the log entries you want to see. The calendar includes the following options:

- Change the month and year by using the back and next arrows around the month and year at the top of the calendar.
- Set the calendar to the current date by clicking the date in the lower left corner of the calendar.
- Click **Clean** to clear the current date/time calendar selection.
- Click **Today** to set the calendar date to today's date.

Set the time range in hours and minutes in the entry fields to the right of the calendar.

Below the View options, choose the number of log entries you want to view per log page from the **Per page** drop-down list (from 25 to 200). Default is 25. At the top and bottom of the page, scroll through the log using the back and next arrow buttons, or identify the page you want to see in the **Page** field and click **Go**.

### Audit Log data

The log displays the following system audit information in table format:

| Column | Description |
|---|---|
| Date | Date and time of the change, adjusted for time zones.<br>To ensure consistent data in the Audit Log, be sure all machines running Forcepoint components have their date and time settings synchronized. |
| User | Username of the administrator who made the change |
| Server | IP address of the appliance affected by the change |
| Client | IP address of the administrator machine that made the change |
| Role | Administrator role (Super Administrator, Auditor, Quarantine Administrator, Reporting Administrator, Security Administrator, Policy Administrator, or Group Reporting Administrator) |
| Type | The location of the change in the Email module interface (for example, if you enter a new subscription key, this column displays **General Settings \| 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, or reset) |
| Action Detail | A link that opens a Details message box with information about the change made |

### Audit Log export options

To export Audit Log records:

1. Select a time period from the **Export range** drop-down list (Current page, Last 24 hours, Last 7 days, or Last 30 days).

   Choose **Last 30 days** to export the entire Audit Log file.
2. Click **Go**.
3. Select the desired output file type in the **Export Log** dialog box.
   - If you select **CSV**, a dialog box opens to let you open or save a text file in comma-separated value format.
   - If you select **HTML**, a dialog box opens to let you open or save an HTML file containing the log data.
4. Click **OK**.

## Personal Email Manager Audit Log

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

You can configure the number of entries per log page, between 25 and 200, in the **Per page** drop-down list in the log table banner. At the top and bottom of the page, scroll through Personal Email Manager Audit Log pages by clicking the back and next arrows, or enter a specific page number in the **Page** field and click **Go**.

The length of time message records are saved in the database depends on your message volume and database partition capacity. To preserve message records, use the Export option to export the log on a regular basis. Exporting does not remove records from the Personal Email Manager Audit Log. It transfers log data to a CSV or HTML file.

When the Personal Email Manager Audit Log page appears, the most recent records are shown. Use the **View** drop-down list options located above the log to select the range of log entries you want to see: All, One Day, One Week, One Month, or Custom. When you select **Custom**, use the **View from/to** fields to specify the date/time range for the log entries you want to see. The calendar includes the following options:

- Change the month and year by using the back and next arrows around the month and year at the top of the calendar.
- Set the calendar to the current date by clicking the date in the lower left corner of the calendar.
- Click **Clean** to clear the current date/time calendar selection.
- Click **Today** to set the calendar date to today's date.

Set the time range in hours and minutes in the entry fields to the right of the calendar.

### Personal Email Manager Audit Log data

The following data is collected and displayed 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, and Reprocess; does not include the Add to Always Block list, Add to Always Permit list, or Download actions) |
| 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

You can perform a keyword search by selecting the log elements on which you want the search done from the **Keyword search** drop-down list and then entering a term in the field to the right of the list. Search for a keyword in 1 of the following Personal Email Manager Audit Log components:

- Message ID
- User Name

Specify the appliance on which you want to perform your search in the **Appliance** drop-down list. The default entry is the active appliance.

Click **Set to Default** to return the keyword search options to the default settings (keyword field blank).

### Personal Email Manager Audit Log export options

To export Personal Email Manager Audit Log records:

1. Select a time period from the **Export range** drop-down list (Current page, Last 24 hours, or Last 3 days).
2. Click **Go**.
3. Select the desired output file type in the **Export Log** dialog box.
   - If you select **CSV**, a dialog box opens to let you open or save a text file in comma-separated value format.
   - If you select **HTML**, a dialog box opens to let you open or save an HTML file containing the log data.
4. Click **OK**.

## System Log

System Log records reflect the current state of the email system, along with any errors or warnings produced. Click the System Log tab on the **Main > Status > Logs** page to view the System Log, and to export selected portions of it to a CSV or HTML file, if desired.

System Log records are saved for 30 days. To preserve System Log records longer than 30 days, use the Export option to export 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.

When the System Log page opens, the most recent records are shown. Use the **View** drop-down list options located above the log to select the range of log entries you want to see: All, One Day, One Week, One Month, or Custom. When you select **Custom**, use the **View from/to** fields to specify the desired date/time range for the log entries you want to see. The calendar includes the following options:

- Change the month and year by using the back and next arrows around the month and year at the top of the calendar.
- Set the calendar to the current date by clicking the date in the lower left corner of the calendar.
- Click **Clean** to clear the current date/time calendar selection.
- Click **Today** to set the calendar date to today's date.

Set the time range in hours and minutes in the entry fields to the right of the calendar.

You can also view log entries by type of system event by selecting an event type in the View by type drop-down list.

Below the View options, choose the number of log entries you want to view per log page from the **Per page** drop-down list (from 25 to 200). Default is 25. At the top and bottom of the page, scroll through the log using the back and next arrow buttons, or identify the page you want to see in the **Page** field and click **Go**.

### System Log data

The log displays the following information:

| Column | Description |
|---|---|
| Date | Date and time of the system event, adjusted for time zones.<br>To ensure consistent data in the System Log, be sure 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 export options

To export System Log records:

1. Select a time period from the **Export range** drop-down list (Current page, Last 24 hours, Last 7 days, or Last 30 days).

   Choose **Last 30 days** to export the entire System Log file.
2. Click **Go**.
3. Select the desired output file type in the **Export Log** dialog box.
   - If you select **CSV**, a dialog box opens to let you open or save a text file in comma-separated value format.
   - If you select **HTML**, a dialog box opens to let you open or save an HTML file containing the log data.
4. Click **OK**.

## Console Log

The Console Log is a record of any administrator activities or changes made to the Email module of the TRITON Manager. Click the Console Log tab on the **Main > Status > Logs** page to view the Console Log, and to export selected portions of it to a CSV or HTML file, if desired.

The length of time Console Log records are saved in the database depends on your database partition capacity. To preserve Console Log records, use the Export option to export the log on a regular basis. Exporting does not remove records from the Console Log. It transfers log data to a CSV or HTML file.

When the Console Log page opens, the most recent records are shown. Use the **View** drop-down list options located above the log to select the range of log entries you want to see: All, One Day, One Week, One Month, or Custom. When you select **Custom**, use the **View from/to** fields to specify the desired date/time range for the log entries you want to see. The calendar includes the following options:

- Change the month and year by using the back and next arrows around the month and year at the top of the calendar.
- Set the calendar to the current date by clicking the date in the lower left corner of the calendar.
- Click **Clean** to clear the current date/time calendar selection.
- Click **Today** to set the calendar date to today's date.

Set the time range in hours and minutes in the entry fields to the right of the calendar.

Below the View options, choose the number of log entries you want to view per log page from the **Per page** drop-down list (from 25 to 200). Default is 25. At the top and bottom of the page, scroll through the log using the back and next arrow buttons, or identify the page you want to see in the **Page** field and click **Go**.

### Console Log data

The log displays the following information:

| Column | Description |
|---|---|
| Date | Date and time of the change, adjusted for time zones.<br>To ensure consistent data in the Console Log, be sure 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 export options

To export Console Log records:

1. Select a time period from the **Export range** drop-down list (Current page, Last 24 hours, Last 7 days, or Last 30 days).

   Choose **Last 30 days** to export the entire Console Log file.
2. Click **Go**.
3. Select the desired output file type in the **Export Log** dialog box.
   - If you select **CSV**, a dialog box opens to let you open or save a text file in comma-separated value format.
   - If you select **HTML**, a dialog box opens to let you open or save an HTML file containing the log data.
4. Click **OK**.

## Email Hybrid Service Log

The Email Hybrid Service Log contains records of email messages that are blocked by the email hybrid service before they reach the network. You must have entered a valid subscription key for the Email Hybrid Module and successfully registered with the module for the Email Hybrid Service Log to be available (see *Registering the Email Hybrid Module*, page 30, for information).

After you register with the email hybrid service, you can enable the Email Hybrid Service Log and set data delivery options on the **Settings > Hybrid Service > Hybrid Service Log Options** page. See *Configuring the Email Hybrid Service Log*, page 35, for information.

Access the Email Hybrid Service Log on the **Main > Status > Logs** page by clicking the Email Hybrid Service tab.

You can configure the number of entries per log page, between 25 and 200 (default is 25), in the **Per page** drop-down list in the log table banner. At the top and bottom of the page, scroll through Email Hybrid Service Log pages by clicking the back and next arrows, or enter a specific page number in the **Page** field and click **Go**.

The length of time message records are saved in the database depends on your message volume and database partition capacity. To preserve message records, use the Export option to export log contents on a regular basis. Exporting does not remove records from the Email Hybrid Service Log. It copies log data to a CSV or HTML file.

When the Email Hybrid Service Log page appears, the most recent records are shown. Use the **View from/to** fields to specify the date/time range for the log entries you want to see. The calendar includes the following options:

- Change the month and year by using the back and next arrows around the month and year at the top of the calendar.
- Set the calendar to the current date by clicking the date in the lower left corner of the calendar.
- Click **Clean** to clear the current date/time calendar selection.
- Click **Today** to set the calendar date to today's date.

Set the time range in hours and minutes in the entry fields to the right of the calendar.

### Email Hybrid Service Log data

The following message data is collected and displayed 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 has several search options, including date range or keyword searches. Determine the date/time range for a search by selecting dates in the **View from/to** field calendar controls. Default value for the **from** or **to** field is the date and time that you open the log.

You can perform a keyword search by selecting the log elements on which you want the search done from the **Keyword search** drop-down list and then entering a term in the field to the right of the list. Click **Search** to initiate the search function.

Search for a keyword in all Email Hybrid Service Log elements, or in 1 of the following Email Hybrid Service Log components:

- Email Hybrid Service Log ID
- Subject
- Sender Address
- Recipient Address
- Sender IP
- Message Status

Click **Set to Default** to return the keyword search options to the default settings (all Email Hybrid Service Log components and keyword field blank).

### Email Hybrid Service Log export options

To export Email Hybrid Service Log search results:

1. Click **Export** to open the Export Log dialog box.
2. Select the desired output file type (CSV or HTML).
   - If you select **CSV**, a dialog box opens to let you open or save a text file in comma-separated value format.
   - If you select **HTML**, a dialog box opens to let you open or save an HTML file containing the log data.
3. Indicate the pages you want to export (All, Current Page, or a page range).
4. Click **OK**.

## Real-time monitor

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

Specify any or all of the following types of log information for display by marking the associated check box:

- Message status (default selection)
- Connection status
- Message delivery status
- Message analysis result

By default, the current appliance is monitored. To monitor multiple appliances in cluster mode, click **Select** and mark the appropriate check boxes in the **Select Appliance** list. Ensure that the primary cluster appliance is selected.

The monitor starts automatically when a user opens the Real-Time Monitor screen. Use the following buttons to control the monitor runtime:

**Pause** to temporarily halt the real-time log stream

**Start** to open a running log of email traffic data for specified appliances

Perform a keyword search of individual log entries by entering a term in the **Search filter** field.

Click **Advanced Search** to open other search filter options. You can search log entries and display records by message subject, IP address (source, destination, or both), or email address (sender, recipient, or both).

## Security Information and Event Management (SIEM) integration

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

Access SIEM integration settings on the **Settings > General > SIEM Integration** page. Mark the **Enable SIEM integration** check box to activate SIEM integration functions.

After you enable SIEM integration, use the following steps to configure the SIEM server and transport protocol:

1. Enter the IP address or hostname for the SIEM integration server in the **IP address or hostname** entry field.
2. Enter the port number for the SIEM integration server in the **Port** field. Default is 514.
3. Select the protocol used for data transport, either **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 it can be unreliable. Like UDP, TCP is a transport layer protocol, but it provides reliable, ordered data delivery at the expense of transport speed.
4. Click **Send Test Message** to confirm that the SIEM product is properly configured and can receive messages from your email software.

# Email hybrid service configuration

TRITON AP-EMAIL combined with the Email Hybrid Module offers a flexible, comprehensive email security solution that lets you 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 Email Encryption Module for this feature).

You can create policies for on-premises and hybrid analysis in the same user interface—the Email 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 Email Hybrid Module and configure a number of settings in the Email 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 Hybrid Module*, page 30, for details.

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 26, for information about the contents of this log. See *Configuring the Email Hybrid Service Log*, page 35, for details about enabling and scheduling Email Hybrid Service Log updates.

## Registering the Email Hybrid Module

Select **Settings > Hybrid Service > Hybrid Configuration** to activate your Email Hybrid Module account. When you click **Register**, a registration wizard opens. Work through the pages in the wizard as follows:

1. *Enter customer information*, page 31
2. *Define delivery routes*, page 32
3. *Configure your DNS*, page 33
4. *Set up your firewall*, page 34
5. *Configure your MX records*, page 34
6. *Modifying email hybrid service configuration*, page 35

**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 1 appliance with the email hybrid service from the same email management server, you should:

1. Add all your appliances to the TRITON Manager Email module (**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 Email 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 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

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.

## Define delivery routes

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

**Important**

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

To add a delivery route:

1. On the Delivery Route page, click **Add**.
2. Enter a **Delivery route name**.
3. To add domains to your delivery route, click **Add** under Protected Domains.
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 **Settings > Users > Domain Groups** page. See the topic titled *Managing domain and IP address groups* in TRITON AP-EMAIL Administrator Help for information.

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

   To add more servers, click **Add** again. 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.

To change the preference order, check the box next to a server name, then click **Move up** or **Move down**.

9. To add outbound SMTP servers to your delivery route, click **Add** under SMTP Outbound Server Addresses. The email system uses these IP addresses to send email to the hybrid service for encryption. See the topic titled *Advanced email encryption* in TRITON AP-EMAIL Administrator Help for information about this encryption function.
10. 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.

    To add more servers, click **Add** again. 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.
11. Click **OK**.

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

Click **Next** to continue with hybrid configuration.

## Configure your DNS

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

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

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

A CNAME record has the following format:

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

Where:

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

Make sure the trailing period is included in the associated domain name.

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

After you have created your CNAME records, click **Check Status** to verify that your entries are correctly set in your DNS. Resolve any error situations if necessary. If the

**Check Status** button does not appear on the page, simply click **Next** to continue. If the registration process stalls or fails at this point, see this Forcepoint Knowledge Base article.

**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.

## Set up your firewall

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

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

Click **Next** to continue with hybrid configuration.

## Configure your MX records

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

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

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

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

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

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

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

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

### Modifying email hybrid service configuration

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

**Note**

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

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

## Configuring the Email Hybrid Service Log

Email Hybrid Service Log options are set on the **Settings > Hybrid Service > Hybrid Service Log Options** page. You can enable the Email Hybrid Service Log and determine the log's data transfer schedule on this page.

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

Configure Email Hybrid Service Log options as follows:

1. Enable the Email Hybrid Service Log by marking the **Enable the Email Hybrid Service Log** check box.
2. Specify the time interval for retrieving the most recent Email Hybrid Service Log information in the **Retrieve Email Hybrid Service Log data every** drop-down box, from 15 minutes to 24 hours. Default is 15 minutes.
3. Specify the time interval for sending Email Hybrid Service Log information to the log database in the **Send the Email Hybrid Service Log data to the database every** drop-down box, from 15 minutes to 24 hours. Default is 15 minutes.
4. Click **OK**.

# Registering the Email DLP Module

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

See the topic titled *Enabling data loss prevention policies* in TRITON AP-EMAIL Administrator Help for more information about activating DLP policies.

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

If you plan to use email encryption functions, you must configure an email DLP policy with an action plan that includes message encryption. See *Data Security Manager Help* for details.

You can also create filter actions for use in a DLP policy action plan. See the topic titled *Creating and configuring a filter action* in TRITON AP-EMAIL Administrator Help for information.

You must register email appliances with the Email 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 TRITON Manager from the Email module interface.

If the Status field in the Email module **Settings > General > Data Loss Prevention** page displays **Unregistered**, you must register with the Email DLP Module manually.

Use the following steps in the Email module **Settings > General > Data Loss Prevention** page to register a standalone appliance manually with the Email DLP Module:

1. Enter a valid subscription key in the **Settings > General > Subscription** page.
2. Specify the IP address used for communication with the email protection system in the **Communication IP address** drop-down list.

   

   **Note**

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

3. Select the **Manual** registration method to enable the Properties entry fields.
4. Specify the following data management server properties:
   - IP address

- User name
- Password

5. Click **Register**.
6. You must deploy DLP policies in the Data module to complete the process. Click the Data module and then click **Deploy**.

**Important**

You should wait until DLP policies are completely deployed before you register another standalone appliance.

The following issues apply if you are deploying TRITON AP-EMAIL in an appliance cluster:

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

# Email filtering database updates

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

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. A default update schedule of once every hour is included for each filter with your first database download.

To edit the update schedule for an individual filter, click **Edit** next to the database you want to change. In the Reschedule Update dialog box, configure the following settings, as desired:

| | |
|---|---|
| Frequency | How often you want the update to occur, from every 5 minutes to once every week |
| Day of week | This field is enabled only when the frequency selected is **Every week**. Choose the day of the week for the update. |
| Time | This field is enabled only when the frequency selected is **Every day** or **Every week**. Choose the time of day for the update. |

Use **Update Now** to perform an immediate update of all Forcepoint databases.

# Configuring system alerts

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

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

## Enabling system alerts

You can determine how alerts are distributed using 1 or more of the following delivery methods:

- To a specified individual via an email message
- To specified computers as a pop-up message on the **Main > Status > Alerts** page
- To a specified community via an SNMP Trap system

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

When you are finished enabling alert methods, click **OK**.

### Email alerts

Mark the **Enable email alerts** check box to have alerts and notifications delivered to administrators by email. Then, configure the following email settings:

| Field | Description |
|---|---|
| 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 completed report notification recipients. Each address must be separated by a semicolon. |

### Pop-up alerts

Mark the **Enable pop-up alerts** check box to have alerts delivered via pop-up messages on the **Main > Status > Alerts** page for specific computers. Then, enter the IP address or machine name for the desired computers, each entry separated by a semicolon.

### SNMP alerts

Mark the **Enable SNMP alerts** check box to deliver alert messages through an SNMP Trap system installed in your network. Provide the following information about your SNMP Trap system:

| Field | Description |
|---|---|
| Community name | Name of the trap community on your SNMP Trap server |
| Server IP or name | IP address or name of the SNMP Trap server |
| Port | Port number SNMP messages use |

Click **Check Status** to send a test message to your SNMP server and verify that the specified SNMP port is open.

## Alert events

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

Use the **Settings > Alerts > Enable Alerts** page to select the method used to send these alerts to Forcepoint administrators. See *Enabling system alerts*, page 38, for information.

Use the **Settings > Alerts > Alert Events** page to select categories of alerts to be delivered. Indicate how you want the alerts delivered (email, pop-up, or SNMP).

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

For each event type in the Alerts list, mark the check boxes for the desired delivery methods. Marking the check box in the column heading for each alert delivery method selects all the event types in that column. You must have enabled a delivery method in the Enable Alerts page in order to select that method for an event type.

In some cases, you can configure threshold values to trigger the delivery of an alert. The following alert events allow you to set such values:

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

Alerts are sent at 30-minute intervals when the configured threshold is exceeded.

**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.

Use the following steps to set thresholds for sending inbound undelivered email alerts:

1. Click the **Configure alert thresholds** link to open a configuration dialog box.
2. Enter the number of connection errors you want to trigger an alert notification (default is 1). The notification is sent at 30-minute intervals after the connections threshold is exceeded.
3. Click the **Configure backup destination address to send alerts when the mail server is down** check box.
4. Enter up to 3 email addresses different from your mail server address as backup alert email destinations.
5. Click **OK**.

**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. Click the **Configure alert thresholds** link to open a configuration dialog box.
2. Select the alert sensitivity level, based on how much warning you want regarding the queue growth rate and the probability of reaching the work queue size limit:
   - **High**. Work queue capacity reached in less than 4 days (default)
   - **Medium**. Work queue capacity reached in less than 2 days
   - **Low**. Work queue capacity reached in less than 1 day
3. Click **OK**.

**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. Click the **Configure alert thresholds** link to open a configuration dialog box.
2. Select the percentage of queue capacity at which you want to be warned about exception queue size (50% to 90%; default is 90%).
3. Click **OK**.

When you are finished enabling all alert types and notifications, click **OK**.

## URL analysis with Forcepoint Web protection solutions

TRITON AP-EMAIL can use Forcepoint Web protection solution URL analysis for accurate and efficient spam detection. The Web management server maintains an updated URL master database from the product download server. The email protection system queries the URL category master database and determines the risk level of a URL found in an email message. Note that the Web module version must be supported by Email module for this function to be available.

Specify the location of the master database in the **Settings > General > URL Analysis** page:

- Use the **Local** option if the Web and Email modules are installed on the same appliance.
- Use the **Remote** option to use a remote database. Enter the IP address or host name of the remote database.

Activate URL analysis in the **Main > Policy Management > Filters > Add URL Analysis Filter** page by marking the **URL analysis** check box in the Filter Properties section and selecting the URL categories to analysis. See the topic titled *URL analysis* in TRITON AP-EMAIL Administrator Help for details.

## 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 the Email Sandbox Module. The on-premises sandbox is available only if you have purchased a separate Threat Protection appliance system.

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

See the topic titled *Advanced file analysis* in TRITON AP-EMAIL Administrator Help for details about configuring an advanced file analysis filter.

Use the following steps to set the advanced file analysis platform:

1. In the **Settings > General > Advanced File Analysis** page, select a platform from the **File analysis platform** drop-down list (File Sandbox or Threat Protection).
2. If you selected Threat Protection, enter the Controller appliance IP address in the **Controller IP address** field.
3. Click the **Check Status** button to verify the connection to the Controller appliance.
4. Click **OK** to save your platform settings.

## Using a proxy server

You can configure a proxy server for email filtering database updates or for email traffic between the email hybrid service and the Internet. Note that you can use the same proxy server for both functions.

Mark the **Enable filtering database update proxy server** check box if the proxy is used for database updates. Mark the **Enable email hybrid service proxy server** check box if the proxy is used for email hybrid service communication.

**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.

If you have TRITON AP-EMAIL and TRITON AP-WEB running on the same appliance, the Web system can be set as the proxy server.

Use the **Settings > General > Proxy Server** page to enter proxy server information as follows:

1. Enter the IP address or hostname of the proxy server in the **Server IP address or hostname** field.
2. Enter the port number of the proxy server in the **Port** field.
3. Enter the username and password for the proxy server in the **User name** and **Password** fields.

## Using the Common Tasks pane

The right shortcut Common Tasks pane provides shortcuts to frequently performed administrative tasks like running a report, creating a policy, or searching a log. Click an item in the list to jump to the page where the task is performed.