FORCEPOINT
POWERED BY Raytheon

Administrator Help

Forcepoint™ TRITON® AP-EMAIL

v8.3.x

10900-A Stonelake Blvd, Quarry Oaks 1, Ste 350, Austin, TX 78759, USA

Published December 2016
Printed in the United States of America and Ireland.

Trademarks

Contents

1 Overview

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

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

TRITON AP-EMAIL may be deployed on a V- or X-Series appliance or as a virtual appliance. See TRITON appliance documentation for details on getting started with an appliance.

A TRITON Manager (or console) installed on a separate Windows machine is required for administration functions. An Email module administrator uses the manager to control email system configuration settings.

A subscription to the Email Hybrid Module adds support for an email hybrid service pre-filtering capability in the cloud, which analyzes incoming email against a database of known malware. This feature can save network bandwidth and maintenance costs by dropping malicious email before it ever reaches an organization's network.

Enhance your security by adding the Email Sandbox Module, which includes a set of cloud-based functions, to your product subscription:

- URL sandbox
- Advanced file analysis

The URL sandbox provides real-time analysis of uncategorized URLs that are embedded in inbound email. The advanced file analysis function inspects email attachment file types that commonly contain security threats. See *URL Sandbox*, page 98, and *Advanced file analysis*, page 129, for details about these features.

Integration with the Email DLP Module provides valuable protection for an organization's most sensitive data and facilitates message encryption. Configure a data loss prevention policy in the TRITON console Data module to enable message encryption options that are configured in the **Settings > Inbound/Outbound > Encryption** page.

If your network includes Forcepoint web protection, you can also use its URL analysis function. Your email protection software queries the Forcepoint URL category master database and determines the risk level of a URL found in an email message. See *URL analysis with Forcepoint Web protection solutions*, page 47, for information.

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

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

Administrator help overview

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

Administrator Help includes the following topics:

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

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

Embedded help

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

Access embedded Administrator Help from the **Help** button at the top right area of the screen, in the TRITON console module tray.

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

Important

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

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

Click **Help > Help Contents** to display the complete embedded Administrator Help. To find a Help topic in the Help viewer, select one of the following tabs:

- **Contents**

  Double-click a book icon to expand that book's topics.

  Click a table of contents entry to display the corresponding topic.

- **Search**

  Enter a word or phrase and click **Go**.

  Click an entry of the results list to display the corresponding topic.

Find Answers portal

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

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

- A Top Picks section containing external links to information related to the screen content
- A Search field that you can use to find topics of interest in the Forcepoint eSupport site

Technical Support

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

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

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

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

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

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

For telephone requests, please have ready:

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

2 Getting Started

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

Topics:

Using the First-time Configuration Wizard

Administrator Help | TRITON AP-EMAIL | Version 8.3.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 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 8).

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 6
- *Domain-based route*, page 7
- *Trusted IP addresses for inbound mail*, page 7
- *Email Log Server information*, page 7
- *System notification email address*, page 8

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)

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

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

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

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 *Protected Domain group*, page 65, 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

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

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 *Managing domain and IP address groups*, page 65, 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 | TRITON AP-EMAIL | Version 8.3.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 **Log Server** page. Click **Check Status** to receive Log Server availability information.

System notification email address

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

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

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

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

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

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 left navigation pane, just under the module tray, gives you access to 2 groups of menu items: Main and Settings. Use the Main menu to access email software status, reporting, and policy management features and functions. Use the Settings menu to perform system administration tasks. Hover over a menu item to view and select individual configuration screens. 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. 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.

The right navigation pane 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.

The dashboard

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

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 *Managing administrator accounts*, page 51).

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 14, 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 13, 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 13.
- **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

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

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 16).
- 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

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

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

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

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

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

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

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

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

Chart Name
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 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)

Chart Name
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

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

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

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

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 43, 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

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

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 18
- *Connection Log*, page 22
- *Audit Log*, page 25
- *Personal Email Manager Audit Log*, page 27
- *System Log*, page 29
- *Console Log*, page 30
- *Email Hybrid Service Log*, page 31

Message Log

Administrator Help | TRITON AP-EMAIL | Version 8.3.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 **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, URL Analysis, Data Loss Prevention, Exception, Commercial Bulk, Block List, Phishing, File Sandbox, Threat Protection, Spoofed Email, or Custom Content). The Block List type applies to a message that is blocked by a Personal Email Manager Always Block List. When a data loss prevention (DLP) policy is indicated, a **View Incident** link in this column opens the incident details in the 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. This item is blank for a message with a scanning result of Clean.

Detail Item	Description
Analysis Result	Message analysis results or filter type (Clean, Virus, Spam, URL Analysis, Data Loss Prevention, Exception, Commercial Bulk, Block List, Phishing, File Sandbox, Threat Protection, 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.

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
- Message Log ID
- Sender Address
- Recipient Address
- Sender IP
- Analysis Result
- Message Status

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. Separate email address entries by a semicolon (;).
By Analysis Result	Search by message analysis results or filter type (Clean, Virus, Spam, URL Analysis, Commercial Bulk, Data Loss Prevention, Custom Content, Exception, Block List, Phishing, File Sandbox, Threat Protection, or Spoofed Email) 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

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

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). Status details are displayed in a hover-over pop-up box. Possible **Blocked** status details are as follows: ● HELO/EHLO received before SMTP server greeting ● Connection from <*server address*> failed SPF check. ● Reverse DNS lookup failed. ● Simultaneous connections from <*server address*> exceeded limit. ● Message volume exceeded limits. ● Message size exceeded limit. Message was forwarded to <*queue id*> queue. ● File size exceeded limit. Message was forwarded to <*queue id*> queue. ● Data size per connection exceeded limit. Message was forwarded to <*queue id*> queue. ● HELO command syntax error ● EHLO command syntax error ● Percentage of invalid recipients exceeded limit. ● Connection attempt by <*server name*> failed global Always Block list check. ● Connection attempt by <*server name*> failed recipient validation check. ● Connection attempt by <*server name*> failed user authentication. ● Open relay from <*sender name*> blocked. Possible **Accepted** status details are as follows: ● Email Hybrid Service IP Group entry match ● Trusted IP group entry match ● Access list entry match ● Global Always Permit List entry match ● BATV bypass entry match ● True source IP address matched a Trusted IP group entry ● True source IP address matched an access list entry ● True source IP address matched an Email Hybrid Service IP Group entry ● True source IP address matched a global Always Permit List entry ● True source IP address matched a BATV bypass 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. See *Message Log data*, page 19, for details.

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

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

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. 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 | 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

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

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

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

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. 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

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

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. 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

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

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 35, 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 41, 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

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

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

Administrator Help | TRITON AP-EMAIL | Version 8.3.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.

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 send a confirmation message to the configured SIEM server. To ensure that the SIEM server is properly configured, you should check the SIEM server log entries to confirm that the test message is delivered.

Email hybrid service configuration

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

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 35, 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 31, for information about the contents of this log. See *Configuring the Email Hybrid Service Log*, page 41, for details about enabling and scheduling Email Hybrid Service Log updates.

Registering the Email Hybrid Module

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

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 36
2. *Define delivery routes*, page 37
3. *Configure your DNS*, page 38
4. *Set up your firewall*, page 39
5. *Configure your MX records*, page 40
6. *Modifying email hybrid service configuration*, page 40

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

Administrator Help | TRITON AP-EMAIL | Version 8.3.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.

Define delivery routes

Administrator Help | TRITON AP-EMAIL | Version 8.3.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.

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 *Managing domain and IP address groups*, page 65, 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 *Advanced email encryption*, page 115, 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

Administrator Help | TRITON AP-EMAIL | Version 8.3.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 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

Administrator Help | TRITON AP-EMAIL | Version 8.3.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.

Configure your MX records

Administrator Help | TRITON AP-EMAIL | Version 8.3.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**.

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

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

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

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

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

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

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 *Enabling data loss prevention policies*, page 141, 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 *Creating and configuring a filter action*, page 135, 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

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

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

Administrator Help | TRITON AP-EMAIL | Version 8.3.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 **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

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

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

Administrator Help | TRITON AP-EMAIL | Version 8.3.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, 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 44, 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.

Use the following steps to configure the URL analysis server in the **Settings > General > URL Analysis** page:

1. Specify the URL analysis service installed with your Web protection deployment:
   - **Filtering Service** (default)

     The Filtering Service is used for master database access and update.
   - **Linking Service**

     The Linking Service is used for database access and for enhanced database functionality, including dynamic custom URL category and category mapping updates from the web protection solution master database. Because Linking Service is an optional web protection component, you must ensure that it is installed before you configure URL analysis to use it.
2. Specify the location of the master database, based on the service selected in step 1:
   - Enter the IP address or hostname for the Filtering Service.
   - For the Linking Service, enter the IP address or hostname and port for the service.
3. Click **Test Connection** to verify the connection to the selected URL analysis service.
4. Click the refresh icon for an immediate update to your URL categories list (available only for the Linking Service).

Activate URL analysis in the **Main > Policy Management > Filters > Add URL Analysis Filter** page by configuring and enabling a URL Analysis filter. See *URL analysis*, page 125, 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 *Advanced file analysis*, page 129, 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 (prod1 [P] interface) in the **Controller IP address** field.
3. Click the **Check Status** button to verify the connection to the Threat Protection Controller appliance.
4. Click **OK** to save your platform settings.

Using a proxy server

Administrator Help | TRITON AP-EMAIL | Version 8.3.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

Note that you can use the same proxy server for all 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. Mark the **Enable advanced file analysis proxy server** check box if the proxy is used for advanced file analysis purposes.

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.

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.

3 Configuring System Settings

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

Topics:

Managing administrator accounts

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

Email module administrator accounts are created in the TRITON Manager. Only a Super Administrator can add, edit, or delete an administrator account in the TRITON Settings page. Click **TRITON Settings** in the module tray to access the **TRITON Settings > Administrators** page.

A Super Administrator can create 2 types of accounts: local and network. A local account is stored in the local TRITON Manager database and contains a single user. A network account can contain a single user or a group of users and is stored on a network server. Details about managing TRITON console administrators on this page can be found in *TRITON Manager Help*.

Administrator account settings and role assignments that are configured on 1 appliance are applied to all the appliances in your network.

Administrator accounts

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

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

A new administrator is created with the role of Auditor. An Email module Super Administrator can assign a default role to a new administrator account or create a new role for that administrator. Click the administrator name to open the Edit Administrator page.

Assign this administrator to a default role by selecting it in the **Role** drop-down list. You can also click **New Role** if you want to create a new role with different permissions for this administrator. See *Administrator roles*, page 52, for information about adding a new role and defining permissions.

The following default roles are available for selection:

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

Click **View Permission** on the Edit Administrator page to see a read-only screen showing that administrator's current role and permissions.

Administrator roles

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

A Super Administrator can create several delegated administrators with a variety of roles and permissions. When you create roles for delegated administrators, you specify the users or groups managed by the role along with the permissions associated with the role. Then assign an administrator to that role. An administrator may be assigned to only 1 role at a time.

Note

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

- Policies
- Reports
- Queues and quarantined messages

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

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

Note

Only 1 Super Administrator may access an email appliance at a time. Subsequent Super Administrators are assigned an Auditor (or read-only) role when they access the appliance.

Add role

Click **Add** and use the following steps to create a new administrator role:

1. Enter a name for the new role, along with a brief, clear description of the role.
2. Define the users or user groups to be managed by this role:
   a. Click **Add** under the Managed Users and Groups table to open the Add Managed Users and Groups dialog box.
   b. Enter the email addresses of managed users or groups in 1 of the following ways:
      - Browse to an email address file, a text file that contains 1 email address per line and is no larger than 10 MB.
      - Enter the desired email addresses in the User email address box, separating addresses by a semicolon.

3. Define the permissions you want for this role in the Permissions table. The following options are available:

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

4. Click **Assign Role** to open the Assign Role dialog box.
5. Select the administrator to which you want to assign this role. This role replaces the administrator's current role.
6. Click **OK**.

Setting system preferences

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

You can accomplish the following email system preferences on the **Settings > General > System Settings** page:

- *Entering the fully qualified domain name*
- *Setting the SMTP greeting message*
- *Setting system notification email addresses*
- *Configuring administrator console preferences*

Entering the fully qualified domain name

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

The SMTP protocol requires the use of fully qualified domain names (FQDN) for message transfer. If you completed the First-Time Configuration Wizard, the FQDN you entered there appears on this page as the default entry.

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

Important

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

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

Setting the SMTP greeting message

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

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

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

Change the default message by entering text in the **SMTP greeting** field.

Setting system notification email addresses

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

The email system can automatically send notifications of system events like a stopped service to a predefined address, often an administrator address. Enter the desired recipient address in the **Administrator email address** field.

If you want notification messages sent to or from an administrator email address for other than system events, you must enter an address in this field as well. For example, configuring a notification to be sent to or from an administrator address when a message triggers a filter (in **Main > Policy Management > Actions**) requires that this field on the System Settings page contain an administrator address.

User notification messages may be sent from a predefined address. Enter the desired sender address in the **Default sender email address** field.

Configuring administrator console preferences

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

The Administrator Console Preferences section lets you configure your desired character set encoding and console language.

Select a character set for encoding messages from the **Preferred character encoding** drop-down list. The preferred character encoding setting is used to decode email attachments, including those for which no character encoding information is available.

Set the language you want the appliance to use in the **Administrator console language** drop-down list.

Managing appliances

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

Before you add an appliance to the Email module, you should have already installed and configured a V-Series or X-Series appliance. Interface information includes IP address, subnet mask, default gateway, and up to 3 DNS server IP addresses. See the Forcepoint Appliance *Getting Started Guide* for more details about setting up and configuring an appliance.

TRITON AP-EMAIL may also be deployed as a virtual appliance. See the Forcepoint appliance *Getting Started Guide* for complete information about deploying and configuring a virtual appliance.

Note

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

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

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

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

Appliances overview

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

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

An appliance may operate in standalone mode, which is the default mode when an appliance is added to the Email module. You can also create appliance clusters by designating an appliance as a primary machine or as a secondary machine associated with a primary machine. See *Designating a primary appliance in a cluster*, page 59, for more information about appliance clusters.

The Email Appliances page lists all current system appliances in a table that shows the appliance hostname, platform, system communication IP address, system connection status, and mode. It also contains an Action column, with links that allow you to switch to a different appliance (**Launch**) that is in standalone mode or remove an unconnected primary appliance from a cluster (**Remove**). When a primary appliance is removed, all its secondary appliances change to standalone mode. The current appliance and all secondary appliances have an Action entry of **N/A**.

To add an appliance to the appliances list in the **Settings > General > Email Appliances** page:

1. Click **Add**.
2. In the Add Appliance dialog box, enter the IP address used for communication with the Email module in the **System Communication IP Address** field.
3. Click **OK**.

Important

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

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

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

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

You can remove an appliance from the appliances list by selecting the appliance and clicking **Delete**. Note that you cannot delete an appliance that is being accessed by another user. Once you remove an appliance from the list, you cannot manage it from the Email Appliances page.

Editing appliance settings from the appliances list

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

You can edit the appliance communication IP address by clicking the appliance name in the appliances list. Note that the system connection status and mode cannot be changed on this page.

Configuring an appliance cluster

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

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

Some platform limitations apply to appliances in a cluster. A V10000 appliance cannot be configured in a cluster with a V5000 appliance. A virtual appliance may be clustered with other virtual appliances, but not with a physical appliance. See Forcepoint Documentation for more information.

Platform versions must match in a cluster.

Appliances in a cluster should also have the same message queue configurations. Messages in a secondary appliance queue may be lost if that queue is not configured on the primary machine before the cluster is created.

Important

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

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

Designating a primary appliance in a cluster

A primary appliance maintains and displays the configuration settings for all the appliances in its cluster. Use the following steps to specify a primary appliance in a cluster:

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

   Note

   Use of the C appliance interface IP address is recommended. If you use this interface, you need to define a route in the appliance CLI.

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

2. Click **Add** to open the **Add Secondary Appliance** page, where you can designate the secondary appliances in this cluster.
3. Select the secondary appliances that you want to add to this cluster from the list of standalone appliances on the left (up to 7 appliances).

   If you want to add a new appliance that is not already on the list, click **Add New Appliance** to open the Add Appliance page.
4. Click the arrow button to add the appliances to the Secondary Appliances list.

5. Click **OK**. The appliance is added to the Secondary Appliances list along with its status.
6. Click **OK** in the main Cluster Mode page to complete the addition of the appliance to the cluster.

Click the appliance name in the Secondary Appliances list to open an Appliance Properties message box that contains all the details about the appliance.

You can remove a secondary appliance from a cluster by selecting the appliance in the Secondary Appliances list and clicking **Remove**.

Managing user directories

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

A user directory is an important component of email traffic analysis, when it is used to set sender/recipient conditions for a policy. It can also provide recipient validation capabilities and be the basis of user logon authentication settings. See *Managing user validation/authentication options*, page 69, for information regarding user authentication settings.

You can add a user directory from the **Settings > Users > User Directories** page.

Perform a keyword search of a user directory by clicking the **View** link in the Cache Size column on the **Settings > Users > User Directories** page for the appropriate directory. Enter a keyword in the search field (up to 100 characters) and click **Submit Query** to complete the search. Click **Clear** to empty the search field and display the complete user directory.

You can delete a user directory by selecting it in the user directories list and clicking **Delete**. You may delete a user directory only if that directory is not currently being used by an email function. For example, if the directory is being used as part of a policy or as part of user authentication settings, it cannot be removed.

Adding and configuring a user directory

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

Click **Add** on the **Settings > Users > User Directories** page to open the Add User Directory page. After you name your user directory, select a user directory type from the drop-down list. Note that a new user directory has a status of **Not referenced**, because it is not yet being used by an email function. User directory creation entries are different depending on the type of user directory you want.

Create a user directory by following the steps for the desired directory type:

- *Microsoft Active Directory*
- *IBM LDAP Server Directory*
- *Generic LDAP Server Directory*

- *Recipient List*
- *ESMTP Server Directory*

Microsoft Active Directory

Microsoft Active Directory provides user information management in a Windows environment. Use the following procedures to configure a Microsoft Active Directory in the User Directory Properties section:

1. Enter the IP address or hostname of your LDAP server in the **Server IP address or hostname** field.
2. Enter the port number in the **Port** field (default is 389).
3. Select the **Enable secure LDAP** check box if you want to enable secure LDAP, a nonstandard protocol also known as LDAP over SSL.

   Note that marking this check box changes the default port number to 636.
4. Enter the username and password for this appliance in the **Username** and **Password** fields. The Username field can contain the user's username, email address, or distinguished name.
5. Enter the LDAP server's search domain name in the **Search domain** field. This value is used when the search filter is applied.
6. The **Search filter** field should contain a standard LDAP query that can use validation variables, for example:

   ```
   (|(mail=%email%)(userPrincipalName=%email%)
   (proxyAddresses=smtp:%email%))
   ```
7. Select either **Mirror** or **Cache address** as your cache setting.
   - The **Mirror** setting means that valid addresses are cached all at once by synchronizing the cache with all the addresses stored on the LDAP server. You can manually synchronize the cache with the LDAP server any time after that by clicking the **Synchronize** action for this directory on the User Directories page.
   - The **Cache address** setting means the cache is updated dynamically. A new, valid address is cached after it is verified with the LDAP server. Remove all addresses from the cache by clicking **Clear cache**.
8. Enter a value in the cache timeout field. The timeout is the amount of time that a valid address remains in the memory cache. If an email message is sent from a previously validated address during this timeout period, the email is delivered without contacting the validation server. However, if another message is sent from this address after the timeout has expired, the server will be contacted to validate the address. Default value is 60 minutes.

IBM LDAP Server Directory

An IBM LDAP Server Directory provides user information management on an IBM server. Use the following procedures to configure an IBM LDAP Server Directory in the User Directory Properties section:

1. Enter the IP address or hostname of your LDAP server in the **Server IP address or hostname** field.
2. Enter the port number in the **Port** field (default is 389).
3. Select the **Enable secure LDAP** check box if you want to enable secure LDAP, a nonstandard protocol also known as LDAP over SSL.

   Note that marking this check box changes the default port number to 636.
4. Enter the username and password for this appliance in the **Username** and **Password** fields. The Username field can contain the user's username or distinguished name.
5. Select either **Mirror** or **Cache address** as your cache setting.
   - The **Mirror** setting means that valid addresses are cached all at once by synchronizing the cache with all the addresses stored on the LDAP server. You can manually synchronize the cache with the LDAP server any time after that by clicking the **Synchronize** action for this directory on the User Directories page.
   - The **Cache address** setting means the cache is updated dynamically. A new, valid address is cached after it is verified with the LDAP server. Remove all addresses from the cache by clicking **Clear cache**.
6. Enter a value in the cache timeout field. The timeout is the amount of time that a valid address remains in the memory cache. If an email message is sent from a previously validated address during this timeout period, the email is delivered without contacting the validation server. However, if another message is sent from this address after the timeout has expired, the server will be contacted to validate the address. Default value is 60 minutes.

Generic LDAP Server Directory

A generic LDAP directory provides user information management that is supported on any LDAP server. Use the following procedures to configure a generic LDAP Server Directory in the User Directory Properties section:

1. Enter the IP address or hostname of your LDAP server in the **Server IP address or hostname** field.
2. Enter the port number in the **Port** field (default is 389).
3. Select the **Enable secure LDAP** check box if you want to enable secure LDAP, a nonstandard protocol also known as LDAP over SSL.

   Note that marking this check box changes the default port number to 636.
4. Enter the username and password for this appliance in the **Username** and **Password** fields. The Username field can contain the user's username or distinguished name.
5. Enter the LDAP server's search domain name in the **Search domain** field. This value is used when the search filter is applied.
6. The **Search filter** field should contain a standard LDAP query that can use validation variables, for example:

   ```
   (mail=%email%)
   ```

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

7. Enter any optional email addresses to import in the **Mail field** text box.
8. Select either **Mirror** or **Cache address** as your cache setting.
   - The **Mirror** setting means that valid addresses are cached all at once by synchronizing the cache with all the addresses stored on the LDAP server. You can manually synchronize the cache with the LDAP server any time after that by clicking the **Synchronize** action for this directory on the User Directories page.
   - The **Cache address** setting means the cache is updated dynamically. A new, valid address is cached after it is verified with the LDAP server. Remove all addresses from the cache by clicking **Clear cache**.
9. Enter a value in the cache timeout field. The timeout is the amount of time that a valid address remains in the memory cache. If an email message is sent from a previously validated address during this timeout period, the email is delivered without contacting the validation server. However, if another message is sent from this address after the timeout has expired, the server will be contacted to validate the address. Default value is 60 minutes.

Recipient List

A recipient list is a text file that contains a list of email addresses and their associated passwords, 1 set per line. This file can be used for user recipient validation.

You can perform a keyword search on a recipient list by using the keyword entry field and Search button at the top of the Recipient List table. When your search results appear, a **View All** option allows you to view the entire recipient list.

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

Use the following procedures to configure a recipient list in the User Directory Properties section:

1. Enable a strong password policy by marking the **Enforce strong password policy** check box. With this policy in force, a password must meet the following requirements:
   - Between 8 and 15 characters
   - At least 1 uppercase letter
   - At least 1 lowercase letter
   - At least 1 number
   - At least 1 special character; supported characters include:
     ! “ # $ & ‘ ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~

2. Add a predefined recipient list file by clicking **Browse** next to the **Recipient information file** entry field and navigating to the desired text file. The file format should be 1 email address and password per line, up to a maximum of 1000 entries.

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

3. You can also create a recipient list by entering an individual email address and associated password in the **Enter Recipient Information** box and clicking the arrow button to add the information to the **Recipient List** box on the right.
4. Click **Search** if you want to perform a keyword search on your recipient list.
5. Click **OK**.

   You cannot save a recipient list that contains weak passwords if you have chosen to use the strong password policy.

After you finish your recipient list entries, you can export the list to your local drive as a text file by clicking **Export**.

Remove an individual entry by selecting it in the **Recipient List** box and clicking **Delete**.

ESMTP Server Directory

An ESMTP Server Directory provides user authentication and recipient validation using the features in extended SMTP. Use the following procedures to configure an ESMTP Server Directory in the User Directory Properties section:

1. Determine your desired email verification method. Select **Use the return status of the VRFY command** to verify the email user name. Select **Use the return status of the RCPT command** to verify the email recipient.
2. Enter an email address for the user directory in the **Sender email address** field.
3. Enter a value in the cache timeout field. The cache timeout is the amount of time that a valid address remains in the memory cache. If an email message is sent from a previously validated address during this timeout period, the email is delivered without contacting the validation server. However, if another message is sent from this address after the timeout has expired, the server will be contacted to validate the address. Default value is 60 minutes.

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

Managing domain and IP address groups

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

A collection of domain names or IP addresses can be defined in a single group for use in email functions. For example, you can define a domain name group to establish domain-based delivery options, or you can define an IP address group for which Reputation Service, Real-time Blacklist (RBL), or directory attack prevention analysis is not performed. IP address groups can also be used for the email encryption functions.

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

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

You may delete a domain or IP address group from its respective list by selecting the check box to the right of the name and clicking **Delete**.

You should note the following two special default groups of domain or IP addresses:

- Protected Domain group
- Trusted IP Address group

See *Third-party encryption application*, page 116, for information about using the Encryption Gateway default IP address group. Default groups cannot be deleted.

Protected Domain group

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

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

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

Unless you entered a protected domain name in the Domain-based Route page of the First-time Configuration Wizard, the default Protected Domain group is empty after

product installation. Domains may be added to or deleted from the Protected Domain group, but you cannot delete the Protected Domain group itself.

Important

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

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

The email hybrid service uses the Protected Domain group during Email Hybrid Module registration to verify that the domains specified in its delivery routes are all from this group. The Protected Domain group should not be used to configure email delivery routes (in the **Settings > Inbound/Outbound > Mail Routing** page) if you need to define domain-based delivery routes via multiple SMTP servers. See *User directory-based routes*, page 94, for information.

Trusted IP Address group

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

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

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

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

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

Note

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

Adding a domain group

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

Click **Add** on the **Settings > Users > Domain Groups** page to open the Add Domain Group page. Use the following procedures to add a domain group:

1. Enter a name for the new domain group in the **Domain Group Name** field.
2. Enter a brief description of your domain group.

In the Domain Group Details section, add a predefined domain group by clicking **Browse** next to the **Domain address file** field and navigating to the desired text file. The file format should be 1 domain address per line, and its maximum size is 10 MB. If a file contains any invalid entries, only valid entries are accepted. Invalid entries are rejected.

1. You can also create a domain group by entering an individual domain address in the **Domain Address** field and clicking the arrow button to add the information to the **Added Domains** box on the right. Use wildcards to include subdomain entries (e.g., *.domain.com).
2. Click **OK**.

After you finish adding your domain address entries, you can export the list to your local drive as a text file by clicking the Added Domains **Export** button.

Remove an individual entry by selecting it in the **Added Domains** box and clicking **Delete**.

Editing a domain group

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

You can edit a domain group by clicking the domain group name in the **Settings > Users > Domain Groups** page Domain Groups List to open the Edit Domain Group page. Add or remove individual domains on this page. You can also edit the domain group description.

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

Adding an IP address group

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

Click **Add** on the **Settings > Inbound/Outbound > IP Groups** page to open the Add IP Address Group page. Use the following procedures to add an IP address group:

1. Enter a name for the new IP address group in the **IP Address Group Name** field.
2. Enter a brief description of your IP address group.
3. Add a predefined IP address group by clicking **Browse** next to the **IP address file** field and navigating to the desired text file. The file format should be 1 IP address per line, and its maximum size is 10 MB.

   Note

   The default Encryption Gateway IP address group supports only the entry of individual IP addresses. Subnet address entries are considered invalid and are not accepted for this IP address group.

   Subnet addresses may be entered for other default and custom IP address groups.

4. You can also create an IP address group by entering an individual IP address in the **IP Address** box and clicking the arrow button to add the information to the **Added IP Addresses** box on the right.
5. Click **OK**.

After you finish adding your IP address entries, you can export the list to your local drive as a text file by clicking the Added IP Addresses **Export** button.

Remove an individual entry by selecting it in the **Added IP Addresses** box and clicking **Remove**.

Editing an IP address group

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

You can edit an IP address group by clicking the IP address group name in the IP Address Groups List to open the Edit IP Address Group page. Add or remove individual IP addresses on this page. You can also edit the IP address group description.

Note that if an IP address is in use, you will be asked to confirm any changes that involve that address.

Managing user validation/authentication options

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

After you define your domain groups, you can determine recipient validation and user authentication settings for users in the user directories you create. See *Managing domain and IP address groups*, page 65, for information about creating domain groups.

The following types of user validation/authentication are available:

- **Recipient validation**, in which a message recipient is validated before a message is received
- **SMTP authentication**, in which a message sender is authenticated before a message is received
- **Personal Email authentication**, in which a user is authenticated before accessing the Personal Email Manager facility for managing blocked email. See *Configuring Personal Email Manager End User Options*, page 171, for details about the Personal Email Manager end-user tool.
- **Distribution list validation**, in which individual members of an email distribution list are validated. If an individual recipient in the group is invalid, the message is rejected for that individual. Other, valid recipients in the distribution list receive the message.

  Ensure you include group email addresses in your user directories if you want to use the distribution list validation option. A message to an invalid group alias is rejected for the entire group of recipients.

Users in a domain group are verified against the corresponding user directory, and specified authentication settings are applied.

Important

You may create multiple Personal Email Manager user authentication groups. However, any protected domain group (as defined in **Settings > Users > Domain Groups**) may be included in only 1 Personal Email Manager user authentication group.

Including a protected domain group in more than 1 Personal Email Manager user authentication group may result in that domain group's users being denied access to the Personal Email Manager facility.

Be sure that you add all the user directories that contain the users in this protected domain group to the associated Personal Email Manager authentication group.

Click **Add** to create new recipient validation/authentication settings.

Click the name of existing authentication settings to modify the settings.

Remove a set of authentication settings by selecting it on the User Authentication page. Mark the check box next to the name of the settings. Click **Delete**.

Adding user authentication settings

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

Use the **Settings > Users > User Authentication** page to add new user validation/authentication settings for domain/user directory groups.

1. Click **Add** to open the Add User Authentication page.
2. Give this set of authentication settings a name.
3. Select the types of user validation/authentication settings that you want to apply: recipient validation, SMTP authentication, Personal Email authentication, or distribution list validation.
   - If you specify recipient validation, you can mark the associated check box to allow the system to continue a recipient search in the next user directory listed in the User Directories section Recipients box if the current user directory cannot be accessed (e.g., server is down or not connected).
   - If you specify SMTP authentication, you must ensure that the **Allow relays only for senders from trusted IP addresses** option is selected for both outbound and internal relays (**Settings > Inbound/Outbound > Relay Control**).
4. Select the domain group you want to target with your authentication settings.

   You can add or remove domain names from your domain group by clicking **Edit** in the Domains area of the User Authentication page to open the Edit Domain Group page. Changes you make here are also reflected in the **Settings > Users > Domain Groups** page.
5. Select the corresponding user directories to which you want these authentication settings to apply by marking the check box next to the directory name and clicking the arrow button to add it to the Recipients box.

   Click **Add user directory** if you want to create a new user directory for these authentication settings. The Add User Directory page opens for you to create a new directory. See *Adding and configuring a user directory*, page 60, for user directory creation instructions.

   You can move selected user directories up or down in the Recipients box via the **Move up** and **Move down** buttons.

   You can delete a user directory reference from the Recipients box by selecting it and clicking **Delete**. This action removes the user directory from the Recipients list, but does not delete it from the **Settings > Users > User Directories** page.

Editing user authentication settings

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

Edit existing authentication settings by clicking the name of the settings in the User Authentication page. Change any settings on the Edit User Authentication page. See *Adding user authentication settings*, page 70, for information about authentication settings.

Note that a user directory may be added or deleted from user validation/authentication settings. User directory entries are modified in the **Settings > Users > User Directories** page.

Managing Transport Layer Security (TLS) certificates

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

Transport Layer Security (TLS) is a protocol that provides an extra layer of security for email communications. Use of this protocol helps prevent devices such as non-trusted routers from allowing a third party to monitor or alter the communications between a server and client. The email security system can receive messages transferred over TLS and can also send messages via this protocol to particular domains.

A default TLS certificate is supplied with TRITON AP-EMAIL for incoming connections. The email system presents this certificate during TLS communications.

After email product installation, default TLS certificate information appears in the **Settings > Inbound/Outbound > TLS Certificate** page, in the TLS Certificate for Incoming Connection section. Details include the certificate version, serial number, issuer, and expiration date.

You can generate a new certificate when that default one expires. On the **Settings > Inbound/Outbound > TLS Certificate** page, click **Generate** to create the new certificate. You should note that generating a new certificate overwrites any certificate that currently exists.

Import and export capabilities for TLS certificates are available.

You can also manage trusted Certificate Authority (CA) certificates for outgoing connections. TRITON AP-EMAIL uses CA-issued root and intermediate certificates (along with the default CA certificate bundle) to verify a server certificate presented by a third-party mail server during TLS communications.

A table on the TLS Certificate page displays information about the certificate, including common name, issuer, and expiration date. An import function lets you browse to the location of a trusted certificate and add it to the Trusted CA Certificate for Outgoing Connection table. A search function allows you to perform a keyword search of all your trusted CA certificates.

See the following sections for details on importing and exporting TLS and CA certificates:

- *Importing a TLS certificate*, page 72
- *Exporting a TLS certificate*, page 72
- *Importing a trusted CA certificate*, page 72

Importing a TLS certificate

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

You may want to import a certificate rather than generate a new one. You should note that importing a certificate overwrites any certificate that currently exists.

Import a certificate that is already located on your network as follows:

1. On the **Settings > Inbound/Outbound > TLS Certificate** page, click **Import**.
2. Click **Yes** in the confirmation dialog box. An Import Certificate area appears below the Import button.
3. Use **Browse** to navigate to the certificate file. When you select a file, its filename appears in the **Certificate file** field. File format must be .p12 or .pfx.
4. Enter a password in the **Password** field (maximum length is 100 characters).
5. Click **OK**.

Exporting a TLS certificate

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

If you want to export a TLS certificate and password to a location on your network, click **Export**. In the Save box, browse to the location where you want the certificate and password to be stored.

Importing a trusted CA certificate

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

Import a trusted CA certificate as follows:

1. In the Trusted CA Certificate for Outgoing Connection section, click **Import**.
2. In the Import Trusted CA Certificate dialog box, enter the desired certificate file name or browse to its location in your network.
3. Click **OK**.

The certificate is added to the trusted CA certificate table. Select a CA certificate and click **Delete** to remove a CA certificate from the table.

Backing up and restoring manager settings

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

The email management server maintains several important configuration setting files, including

- Database configuration
- Appliances list
- Administrator settings
- Presentation report templates and data

You may want to retain a backup copy of these settings to use if a system recovery operation is necessary. A backup and restore utility is included with the Email module.

The Backup/Restore function includes a Backup and Restore Log, which displays time-stamped backup and restore activities for the manager.

Note
Because the Backup/Restore utility stops the Email module service, backup and restore activities are recorded only in the Backup and Restore log.

Backup and restore functions for an appliance cluster work properly only when cluster settings have not changed between the backup and restore operations. You may have unexpected results if any of the following settings have been changed between the backup and restore.

- Appliance mode (cluster or standalone)
- IP address or hostname

You may need to rebuild a cluster if a restore operation encounters problems.

Note
If you specify your backup file location for a remote server, ensure that your restore operation is configured to restore configuration files from that remote server location.

Backing up settings

Backup and restore functions are available on the **Settings > General > Backup/Restore** page. Backup and restore settings made on 1 appliance are applied to all the appliances in your network.

To back up your Email module configuration settings, click **Backup** to activate the utility and specify a local folder for the backup file. That folder location appears in the File Location field in the Restore Settings section of the page.

If you want to save your backup settings on the Log Database server, mark the check box next to that option in the Backup Settings section. When you make this selection, the Remote Log Database Server Access box is enabled for you to enter the following server information:

- **Domain/Hostname.** Enter the domain if a domain account is used; otherwise, enter the hostname of the SQL Server machine.
- **User name.** Enter a user with SQL Server log-in permission.
- **Password.** The password may not contain more than 1 double quotation mark.
- **Backup/Restore file path.** Enter the shared folder path on the remote SQL Server machine (for example, \\10.1.1.2\shared\).

Note

- The version of the backed up settings must match the version of the currently installed product.
- Backup and restore settings must both use either local or remote file storage. You cannot restore a local file using remote settings.
- The backup settings file size may not exceed 10 MB.
- The following special characters are not supported in backup server entries: |, <, >, and &.

Click **Check Status** to ensure that the remote log database server is accessible.

Restoring the settings

Click **Restore** to use the backup/restore utility to return your settings to their original, backed up state on the Log Database server. The restore function retrieves the location of the backed up settings and applies them to the Email module configuration files. The Email module service restarts automatically after configuration settings are restored.

4 Managing Messages

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

Topics

Configuring message properties

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

Email message control properties allow you to set message size and volume limits, and determine how invalid recipients are handled. Select **Settings > Inbound/Outbound > Message Control** to configure the following settings:

- *Setting size properties*, page 76
- *Setting volume properties*, page 76
- *Configuring invalid recipient settings*, page 77
- *Enabling archive message options*, page 77
- *Enabling message sender verification*, page 77
- *Enabling bounce address tag validation (BATV)*, page 77

Click **OK** when you finish setting message properties.

Setting size properties

Use the Message Size Options to configure message size properties:

1. Select **Limit message size** (default setting) if you want to set a maximum message size.
2. Enter a maximum message size in the corresponding **Maximum message size (KB)** field, from 1 - 102400 (default is 10240). This setting can prevent very large messages from using valuable bandwidth.
3. Select **Limit data size per connection** if you want to set a maximum message size per connection.
4. Enter a maximum data size in the corresponding **Maximum data size (KB)** field, from 1 - 204800 (default is 20480). This setting can help limit the receipt of messages with very large attachments, which can take up valuable bandwidth.

Setting volume properties

Use the Message Volume Options to configure message volume properties:

1. Select **Limit number of messages per connection** to enable that option.
2. Enter a maximum number of messages per connection in the associated **Maximum number of messages** field, from 1 - 65535 (default is 30).
3. Select **Limit number of recipients per message** to enable that option.
4. Enter a maximum number of recipients in the corresponding **Maximum number of recipients** field, from 1 - 4096 (default is 20). This can save bandwidth by preventing one message from being sent to hundreds of users.

Configuring invalid recipient settings

Use the Invalid Recipient Options to configure invalid recipient settings:

1. Mark the **Allow invalid recipients** check box if you want to permit mail containing invalid recipients into your system. This option is available only when the recipient validation is used (see **Settings > Users > User Authentication)**.
2. Enter a value for the percentage of invalid recipients that determines if a message is blocked (default is 100).
3. Mark the appropriate check box to enable the system to send a non-delivery report (NDR) notification only if a message is not blocked.

Enabling archive message options

Mark the **Enable archive queue storage** check box if you want all incoming messages saved to an archive message queue before they are scanned. You should note that enabling this feature can impact storage capacity and system performance. This option is disabled by default.

View the archive queue by clicking **archive** in the queue list on the **Main > Message Management > Message Queues** page.

Enabling message sender verification

Ensure that an internal email sender is an authenticated user by enabling the internal sender verification function. This operation performs a check to confirm that an email sender from an internal domain is also an authenticated user. For email to pass this check function, a mail sender's address must match the sender's log in authentication entry.

Mark the **Enable internal sender verification** check box in the Internal Sender Verification section to activate this function. By default, this function is disabled.

Enabling bounce address tag validation (BATV)

Bounce address tag validation (BATV) is a method for determining whether a bounce message to an address in your protected domain is valid. This method helps to prevent backscatter spam, in which a bounce message to your organization contains a forged recipient address.

With BATV enabled, the sender address of outbound email is marked with a unique tag. A bounce message addressed to that sender is examined for the presence of that unique tag. If the tag is detected, the bounce message is cleared for delivery. A bounce message without the tag is blocked.

Enable BATV in the **Settings > Inbound/Outbound > Message Control** page. Mark the **Enable Bounce Address Tag Validation** check box in the Bounce Address Tag Validation section.

You may want mail from some user and IP address groups to bypass the BATV function. These groups can be defined in the Bounce Address Tag Validation section. Select a group from among the following drop-down lists:

- Inbound IP address group
- Inbound domain group
- Outbound domain group

Note that a domain group selected for outbound bypass must also be selected for inbound bypass.

The default setting for each group is **None**. Only user-defined domain and IP address groups are available in the drop-down lists. See *Managing domain and IP address groups*, page 65, for information about creating domain and IP address groups.

Managing connection options

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

You can improve system performance by limiting the number of simultaneous connections. In the **Settings > Inbound/Outbound > Connection Control** page, Connection Options section, enter the maximum number of allowed simultaneous connections per IP address, from 1 - 500 (default is 10). Specify the maximum number of seconds of inactivity allowed before a connection is dropped, from 1 - 43200 (default is 300).

You can also configure the following settings in the Connection Control page:

- *Using a real-time blacklist (RBL)*, page 79
- *Using reverse DNS verification*, page 79
- *Using the reputation service*, page 80
- *Delaying the SMTP greeting*, page 80
- *Enabling the SMTP VRFY command*, page 80
- *Enabling SMTP authentication for email hybrid service*, page 81
- *Changing the SMTP port*, page 81
- *Using access lists*, page 81

If you want to collect and view detailed information about some connections, you can allow connection control functions to save these details in the mail processing log, accessed via an appliance. When the function is activated, the log collects detailed data regardless of whether the connection control itself is enabled. This function is available for the following connection control options:

- Real-time blacklist (RBL)
- Reverse DNS lookup
- Reputation service
- SMTP greeting delay

Click **OK** when you finish configuring connection control settings.

Using a real-time blacklist (RBL)

A Real-Time Blacklist (RBL) is a third-party published list of IP addresses that are known sources of spam. When RBL checking is enabled, messages from a sender listed on an RBL are prevented from entering your system. The Email module supports the use of the Spamhaus Datafeed server or the entry of up to 3 third-party RBLs for RBL lookups.

In the Real-time Blacklist (RBL) Options section, mark the **Perform RBL check** box to enable RBL checking. Select 1 of the following RBL lookup methods:

- **Spamhaus service.** Use the Spamhaus server for RBL lookups
- **Domain address.** Enter up to 3 domain addresses of the RBL services you want to use. Separate multiple addresses with a semicolon (;).

This feature is not enabled by default.

Mark the **Save connection details in the mail processing log** check box to save detailed connection information in the appliance mail processing log. If you enable this option without designating a third-party RBL, the email protection system still collects log information that email content filters can use for subsequent message analysis.

Using reverse DNS verification

Reverse DNS lookup uses a pointer (PTR) record to determine the domain name that is associated with an individual sender IP address. The reverse DNS lookup function can determine whether email sent to your system is from a legitimate domain. Use of this option can enhance the detection of commercial bulk email. See *Commercial bulk email*, page 128, for information about this type of email.

Note, however, that if you enable Reverse DNS, server performance may be affected, or legitimate users may be rejected. This function is not enabled by default.

Mark the **Enable reverse DNS lookup** check box in the Reverse DNS Lookup Options section to activate the reverse DNS function. You can then determine the response to a reverse DNS lookup by selecting 1 or more of the following options:

- **Disconnect if the PTR record does not exist.**
- **Disconnect if the PTR record does not match the A record.**
- **Disconnect if a soft failure occurs during a reverse DNS lookup.**

  If you select this option, a connection is terminated when the following events occur:

  - Named DNS lookup cache service is down.
  - Your DNS server is down.
  - A timeout occurs during a DNS lookup.

- **Disconnect if the PTR record does not match the SMTP EHLO/HELO greeting.**

Mark the **Save connection details in the mail processing log** check box to save detailed connection information in the appliance mail processing log.

Using the reputation service

The email protection system can check an email sender's IP address against the reputation service, which classifies email senders based on past behavior. With this function, the email system can block mail from known spam senders.

To use the reputation service, mark the **Enable Reputation Service** check box (the default setting) in the Reputation Service Options section. Then select 1 of the following analysis levels to specify the threshold for blocking mail:

- **Conservative**, which blocks mail from addresses that send spam 100% of the time
- **Medium**, which blocks mail from addresses that send spam 99% of the time
- **Aggressive**, which blocks mail from addresses that send spam 97% of the time
- **Custom**, which you can use to enter a custom spam percentage. The email system blocks mail from addresses that send spam the specified percentage of time.

Mark the **Save connection details in the mail processing log** check box to save detailed connection information in the appliance mail processing log.

Delaying the SMTP greeting

You can specify that an SMTP greeting message be delayed for a specified time interval, so that a connection from a client will be dropped if the client tries to send data during this time interval. This option can help prevent mail from spam-sending applications that send a high volume of messages very quickly. The connection is dropped as soon as a message is sent to the SMTP server before it is ready.

Enable the SMTP greeting delay by marking the **Enable SMTP greeting delay** check box in the SMTP Greeting Delay Options section. Specify the delay time, in seconds, from 1 - 60 (default is 3).

This feature is not enabled by default.

Mark the **Save connection details in the mail processing log** check box to save detailed connection information in the appliance mail processing log.

Enabling the SMTP VRFY command

The SMTP VRFY command can be used to verify an email username. When asked to validate a username, a receiving mail server responds with the user's login name. Enable this command by marking the **Enable SMTP VRFY command** check box

(the default setting) on the **Settings > Inbound/Outbound > Connection Control** page in the SMTP VRFY Command Option section.

Important

Use this command with care. Although helpful in validating a user, this command can also create a network security issue if the user information is retrieved by someone with malicious intent.

Enabling SMTP authentication for email hybrid service

By default, SMTP authentication is enabled for inbound messages that enter the system via the email hybrid service. This type of authentication provides additional authentication protection for email that is relayed to the email protection system from the hybrid service.

This option is available only when your subscription includes the Email Hybrid Module and the hybrid service is registered and enabled.

To disable this option on the **Settings > Inbound/Outbound > Connection Control**, deselect the **Enable email hybrid service SMTP authentication** check box.

Changing the SMTP port

The default SMTP port number is 25. Proper communication with the email hybrid service requires the use of port 25 for SMTP.

However, if you need to customize this port number for any reason, you can change it on the **Settings > Inbound/Outbound > Connection Control** page in the SMTP Port Option section. Valid values are from 25 to 5000.

Note

Changing this port setting causes Email module services to restart.

Using access lists

An access list enables you to specify an IP address group for which certain email analysis is not performed. The Allow Access List Options in the **Settings > Inbound/Outbound > Connection Control** page let you identify these IP addresses. Mail from these addresses bypasses the following email analysis:

- Connections per IP address
- RBL checks
- Reverse DNS lookup
- Reputation service
- SMTP greeting delay

- Directory harvest attack prevention
- Inbound relay control
- True Source IP detection

Because mail from the Trusted IP Addresses group bypasses additional email analysis, that group should not be entered in the Allow Access List. See *Managing domain and IP address groups*, page 65, for details.

You define IP address groups in **Settings > Inbound/Outbound > IP Groups**. The groups you have defined on that page appear in the Connection Control Allow Access List Options section, in the **IP group** drop-down list.

To create and modify an access list:

1. Select an IP group name in the **IP group** drop-down to display the addresses in the **IP addresses** list and enable the **Edit** button.
2. Click **Edit** to modify the access list in the Edit IP Groups page.
3. Add a predefined IP address group by clicking **Browse** next to the **IP address file** field and navigating to the desired text file. The file format should be 1 IP address per line.
4. You can also enter an individual IP address in the **IP Address** box and click the arrow button to add the information to the **Added IP Addresses** box on the right.

Note

Any changes made here to an IP address group are reflected in the **Settings > Inbound/Outbound > IP Groups** page.

5. Click **OK**.

When you have finished your access list, you can export the list to a location in your network. Click **Export** to save the access list file to another location.

You can delete an IP address from the Added IP Addresses list by selecting it and clicking **Remove**.

DomainKeys Identified Mail (DKIM) integration

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

The DomainKeys Identified Mail (DKIM) functionality provides an email authentication method to help ensure that a message is not modified while it is in transit from an organization's protected domains. The implementation depends on a set of keys (private and public), which a recipient domain can use to verify the sender domain.

A DKIM integration has the following components:

- Email signing

- Email verification

For the signing element, a private key resides in the mail transfer agent, providing a digital signature that is added to the header of each message sent from a protected domain. A public key is generated and published in the DNS as a text record that is used by a recipient mail system in the verification process.

A signing rule associates specified sender domains with a private and public key set.

Configuring a DKIM signing key

A signing key provides a digital signature for email sent from your protected domains. You may create a signing (private) key, import a key from a local directory, or export a key to a local directory.

You may also delete an existing key, unless it is currently in use by a signing rule. Select the desired key by marking its associated check box and click **Delete**.

The DKIM Signing Keys section contains a table of key information. You can configure the number of signing key entries per page, between 25 and 100, in the **Per page** drop-down list at the top of the table.

You can perform a keyword search by entering a term in the entry field at the top right of the table and clicking **Search**. Click **Show all keys** to clear the Search field and refresh the signing keys list.

The signing keys table includes the following information about each key:

Signing Key Item	Description
Key Name	Name of the signing key; link that opens the Edit Signing Key page
Key Size (bits)	Number of bits in the signing key. Currently, the only key size supported is 1024 bits.
Rule Name	Name of the rule with which the signing key is associated
Public Key	Link that opens a View Public Key box, which displays the public key text record

Adding a key

Use the following steps to create a DKIM signing key in the **Settings > Inbound/Outbound > DKIM Settings** page:

1. Click **Add** in the DKIM Signing Keys section to open the Add Signing Key page.
2. Enter a name for your key in the **Key name** entry field.
3. Select one of the following options for creating your key:
   - **Generate key** (default) to create the private key. Only 1024-bit keys are supported.

- **Private key** to enter a key you have already created. Paste the key in the entry box.

4. Click **OK**.

Importing or exporting a key

To import a DKIM signing key in the **Settings > Inbound/Outbound > DKIM Settings** page, click **Import** to open a browser window. Navigate to the desired key file and click **Open**. You cannot import a duplicate key file.

To export a key, select the desired key in the signing keys table by marking its associated check box and click **Export** to open a browser window. Navigate to the desired directory location and click **Save**.

Creating a DKIM signing rule

A DKIM signing rule associates a private/public key pair with a set of domains and email addresses. Signing rule options let you determine which message headers to sign, how much of the message body to sign, and whether to attach additional signature tags for such items as signature date/time or expiration time.

You may create a signing rule, import an existing rule from a local directory, or export a rule to a local directory on the **Settings > Inbound/Outbound > DKIM Settings** page.

You may also delete a signing rule. Select the desired rule by marking its associated check box and click **Delete**.

The DKIM Signing Rules section contains a table of rule information. You can configure the number of signing rule entries per page, between 25 and 100, in the **Per page** drop-down list at the top of the table.

You can perform a keyword search by entering a term in the entry field at the top right of the table and clicking **Search**. Click **Show all rules** to clear the Search field and refresh the signing rules list.

The signing rules table includes the following information about each rule:

Signing Rule Item	Description
Rule Name	Name of the signing rule; link that opens the Edit Signing Rule page
Domain	Domain name to which the signing rule applies
Selector	Name component in addition to the domain name used in the DNS query. A given domain may have multiple selectors (e.g., for location or organization division).
Signing Key Name	Name of the signing key associated with this rule
DNS Text Record	Link that opens a Generate DNS Text Record dialog box. See *Generating a DNS text record (public key)*, page 87, for information about creating a text record.

Signing Rule Item	Description
Test Rule	Link to test whether the signing rule is valid. A successful test must be performed before a rule can be enabled.
Status	Indicator of signing rule status (i.e., enabled or disabled). A rule must be enabled in order to take effect.

Adding a signing rule

Use the following steps to create a DKIM signing rule in the **Settings > Inbound/Outbound > DKIM Settings** page:

1. Click **Add** in the DKIM Signing Rules section to open the Add Signing Rule page.
2. Enter a name for your rule in the **Rule name** entry field.
3. Enter the name of the domain to which this signing rule applies.
4. If desired, mark the **Include user identifier** check box to include the identity of the user or agent for whom the message is signed.
5. Enter the user identifier in the **User identifier** entry field (optional). This field is not enabled if the **Include user identifier** check box is not marked.
6. Enter the domain name selector in the **Selector** entry field. A selector is a name component provided in addition to the domain name used in the DNS public key query. A given domain may have multiple selectors.
7. Select the signing key you want to associate with this rule from the **Signing key** drop-down list of existing keys.
8. Click **Advanced Options** to open a box with additional optional rule settings:
   - Select an encryption algorithm from the **Algorithm** drop-down list. Options include RSA-SHA-1 (default) or RSA-SHA-256.
   - Specify a canonicalization method for message header and body in the **Canonicalization** section. The canonicalization process prepares a message header and body before email is signed. Canonicalization is required because email processing may introduce minor changes to a message.

The following header and body changes are made, based on the selection of **Simple** or **Relaxed**:

	Simple (default)	Relaxed
Message Header	No header changes made	• Header names changed to lowercase • Header line breaks removed • Linear white spaces (including tabs and carriage returns) reduced to a single space • Leading and trailing spaces stripped
Message Body	Empty lines at end of body stripped	• Empty lines at end of message body stripped • Linear white spaces (including tabs and carriage returns) reduced to a single space • Trailing spaces stripped

- Indicate the message headers you want to sign from the list of standard headers. You can include other headers as a comma-separated list in the **Additional headers** field.
- Specify whether you want the entire message body signed or only a portion of it signed. For the latter selection, enter the maximum number of Kbytes you want signed (default is 1024).
- Select any optional signature tags for the signing rule:
  - **t** lets you add a signature creation timestamp
  - **x** lets you specify a signature expiration time in seconds (default is 3600)
  - **z** adds the list of signed header fields to the signature

9. From the Signing rule options drop-down list, select either **Sign email messages** or **Do not sign email messages**. Then create a list of email addresses to which this option applies.

   For example, if you select **Sign email messages**, then email from the addresses in the list are signed. Email from other addresses is not signed.

   If you select **Do not sign email messages**, then email from the addresses in the list are not signed, and email from all other users is signed.

   You may search the email address list by entering a keyword in the search entry field and clicking **Search**.

   You may remove an email address from the list by selecting it and clicking **Remove**.

10. Click **OK**.

Importing or exporting a rule

To import a DKIM signing rule in the **Settings > Inbound/Outbound > DKIM Settings** page, click **Import** to open a browser window. Navigate to the desired rule file and click **Open**. You cannot import a duplicate key rule.

To export a rule, select the desired rule in the signing rules table by marking its associated check box and click **Export** to open a browser window. Navigate to the desired directory location and click **Save**.

Generating a DNS text record (public key)

Generate a public key for a rule from the DKIM Signing Rules table by clicking the link for the desired rule in the DNS Text Record column. A Generate DNS Text Record box that contains the new public key appears.

You can view a public key by clicking **View** for a particular private key in the DKIM Signing Keys table Public Key column.

Testing a rule

Ensure that you have created a valid rule by clicking the **Test** link in the **Test Rule** column of the DKIM Signing Rules table for the desired signing rule. The test performs a DNS lookup query. You receive confirmation of success or failure when the test is complete.

You must have performed a successful rule test before a rule can be enabled.

Enabling DKIM verification

The DKIM validation method uses the message header digital signature to associate a domain name with the email. The DKIM signature verification function retrieves signer information, including the public key, from the DNS. This signer information is analyzed and verified to determine message legitimacy.

You can enable DKIM verification in the **Settings > Inbound/Outbound > DKIM Settings** page, in the DomainKeys Identified Mail (DKIM) Verification section. Mark any of the following check boxes to activate DKIM verification:

- **Enable DomainKeys Identified Mail (DKIM) verification for inbound messages**
- **Enable DomainKeys Identified Mail (DKIM) verification for outbound messages**
- **Enable DomainKeys Identified Mail (DKIM) verification for internal messages**

By default, these check boxes are not marked.

You can configure a custom content policy filter to scan for a DKIM signature in the message header, along with a filter action to take when a message header triggers the filter. See *Custom content*, page 123, for information about creating this filter.

Domain-based Message Authentication, Reporting and Conformance (DMARC) validation integration

Domain-based Message Authentication, Reporting and Conformance (DMARC) uses the results of its Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) validation processes, along with the sender domain's DMARC policy to determine message disposition. Published in the sender's DNS record, a DMARC policy includes the sender's affirmation that its email is protected by SPF and DKIM validation, and provides instructions for handling mail that does not pass either of those checks on the recipient's end. A mechanism for reporting DMARC results is also provided.

SPF and DKIM analyses enabled and configured in the Email module are independent of DMARC verification. SPF checks are configured in **Settings > Inbound/Outbound > Relay Control**, whereas DKIM validation is configured on the **Settings > Inbound/Outbound > DKIM Settings** page. If either SPF or DKIM analysis is enabled in the TRITON Manager, DMARC can use the results in its own verification analysis.

Assuming a message is not dropped for failing either the SPF or DKIM check, DMARC validation comprises the following steps:

1. Extract the sender domain in the email header "From" field.
2. Query the DNS to determine if a DMARC policy exists for this domain.
   - Retrieve the policy if one is found and continue with step 3.
   - End the DMARC process if a policy is not found.
3. Perform DKIM validation checks.
4. Perform SPF validation checks.
5. Perform DMARC identifier checks to determine if the sender information in the message aligns with what the recipient knows about that sender as a result of the SPF and DKIM analyses.
6. After completing the DMARC analysis, apply the DMARC policy to the message.

When you enable DMARC validation, a reporting mechanism is also included to provide the sender with information about the number of messages received from that sender domain and the results of the recipient's validation checks. Reports are sent to the email address specified in the sender domain's DNS text record via the RUA (reporting URL of aggregate reports) tag.

If SPF and DKIM are not enabled in the Email module, DMARC performs these checks. In this case, message disposition is determined only by the DMARC policy. A message is not rejected based on the individual SPF or DKIM analysis results.

For optimal protection, both SPF and DKIM validation settings should be configured and enabled on your email protection system, along with DMARC. See *Configuring relay control options*, page 92, and *DomainKeys Identified Mail (DKIM) integration*, page 82, for information about these settings.

Configure DMARC verification on the **Settings > Inbound/Outbound > DMARC Settings** page. Mark the check box for any of the following options:

- **Enable DMARC verification for inbound messages**
- **Enable DMARC verification for outbound messages**
- **Enable DMARC verification for internal messages**

True source IP detection

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

True Source IP detection uses message header information and the number of network hops to an email appliance to determine the IP address of the first sender outside the network perimeter. This feature allows Connection Control techniques (such as reverse DNS lookup and reputation checks) to be applied effectively to sender information, even when the appliance is downstream from a firewall or an internal mail relay.

You define direct relays and network edge locations to determine whether True Source IP detection is performed. A direct relay is the network device that connects directly to the email appliance. All mail from a direct relay device is subject to True Source IP Detection. A network edge is the network device that connects directly to the Internet (e.g., a firewall).

If your subscription includes the Email Hybrid Module, you can use True Source IP detection with email hybrid service analysis. An Email Hybrid Service IP Group is created based on information entered during a successful Email Hybrid Module registration. The IP group appears in the direct relay IP address list on the **Settings > Inbound/Outbound > True Source IP** page. Although this IP group cannot be edited directly, its content is modified whenever you change an email hybrid service IP address (**Settings > Hybrid Service > Hybrid Configuration**).

Note

If Email Hybrid Module registration is not successful, the Email Hybrid Service IP Group is empty.

Mark the **Use True Source IP Detection with email hybrid service analysis** check box to enable True Source IP detection with hybrid service and display the Email Hybrid Service IP Group in the direct relay IP address list. The Email Hybrid Service IP Group does not appear if the check box is not marked.

Configure your direct relay and all network edge devices in the **Settings > Inbound/Outbound > True Source IP** page as follows:

1. Click **Add** to open the Add Direct Relay IP Address/IP Group page.
2. Enter the IP address for the direct relay device to the email appliance, or specify the IP group you would like to use for your direct relay.

By default, the direct relay hop number is 1, because it is the closest network device to the email appliance.

Important

The IP address or group that you enter here must not already be defined in the Trusted IP Addresses group (**Settings > Inbound/Outbound > IP Groups**) or appear in the connection control Allow Access List (**Settings > Inbound/Outbound > Connection Control**).

3. Enter header text you want to match for true source IP detection in the **Check header** entry field.

   If this field is empty, the message Received field is analyzed for the true source IP.
4. Click **Add Network Edge** to add the network edge device IP address and hop number to the email appliance.

Enforced TLS connections

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

You can specify that connections to or from a specific IP or domain group use mandatory Transport Layer Security (TLS) and determine the security level used by that connection. Use the **Settings > Inbound/Outbound > Enforced TLS Connections** page to specify the IP addresses or domain groups for which TLS connections are forced.

You define connection directions relative to the email SMTP server. Incoming connections are those from a protected or external domain or IP address group to the email protection system. Outgoing connections are those from the email system to a protected or external domain or IP address group.

After you define a group, you can change its order in the incoming or outgoing direction list. Select the group by marking its associated check box and use the **Move Up** or **Move Down** button to modify list order.

Delete a group by marking the check box and clicking **Delete**.

You may configure up to 32 incoming or outgoing connections.

Use the following steps to add an incoming or outgoing connection for which you want to use TLS:

1. Click **Add**.
2. Enter a name for your enforced TLS connection.
3. Select a priority order for the connection in the **Priority order** drop-down list.
4. Specify the security level for that connection. Security level options include the following:
   - **Encrypt**, the minimum enforcement level, used in all security levels

This security level is the only option available for incoming connections.

- **Encrypt and check CN**, validation of a certificate's common name
- **Verify**, validation that the certificate is from a trusted CA
- **Verify and check CN**, validation of the certificate's common name and that the certificate is from a trusted CA

Important

To use the 2 "verify" options, you must have imported a trusted CA certificate. See *Managing Transport Layer Security (TLS) certificates*, page 71, for information about trusted certificates.

5. Select 1 of the following connection encryption strength options:
   - Medium, which involves the use of cipher suites that use 128-bit encryption
   - High, which includes most cipher suites with key lengths larger than 128 bits
6. Define the IP address or domain group subject to forced TLS connection. Select 1 of the following options:
   - **Any (for all connections).** This option applies to any connection, regardless of IP or domain address.
   - **IP address group.** Select an existing IP address group in the drop-down list or create a new group using **Add New IP Group**.
   - **Domain address group.** Select an existing domain address group in the drop-down list or create a new group using **Add New Domain Group**.

Controlling directory harvest attacks

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

A directory harvest attack is used by questionable sources to gain access to an organization's internal email accounts. A directory attack not only consumes large amounts of system resource but also, through the acquisition of email accounts, creates spam problems for email end users. With directory attack prevention settings, you can limit the maximum number of messages and connections coming from an IP address over a given time period.

To configure directory attack control:

1. Select **Settings > Inbound/Outbound > Directory Attacks**.
2. Select the **Limit the number of messages/connections per IP every** check box to enable the directory harvest attack prevention function.
3. Set the time period, from 1 second to 60 minutes, in the drop-down list (default is 60 seconds).
4. Set the maximum number of messages allowed from an individual IP address during the specified time period (default is 30).

5. Set the maximum number of connections allowed from an individual IP address during the specified time period (default is 30).
6. If you have enabled the directory attack prevention option, you can also enable settings to block an IP address when a specific set of recipient conditions occurs. Mark the **Block the IP address for** check box, and enter the time interval during which you want an IP address blocked (default is 3 hours).
7. Enter the conditions for blocking the IP address:
   - Maximum number of message recipients (default is 5)
   - Maximum percentage of invalid addresses among the recipients (default is 50%)

   When these recipient limitations are exceeded, the connection is dropped automatically.

   This option is available only when the recipient validation option is used (see *Adding user authentication settings*, page 70).

Configuring relay control options

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

You can prevent the unauthorized use of your mail system as an open relay by limiting the domains and IP address groups for which your server is allowed to relay mail. Protected domains are defined in the **Settings > Users > Domain Groups** page. Trusted IP address groups are defined in the **Settings > Inbound/Outbound > IP Groups** page.

Configure relay control settings in the **Settings > Inbound/Outbound > Relay Control** page as follows:

1. In the Inbound Relay Options section, set any desired option that is based on the Sender Policy Framework (SPF) of the sender domain:
   - **Reject mail if no SPF record exists.**
   - **Reject mail if the SPF record does not match the sender's domain or a soft fail occurs.**

     A "soft fail" result means the result of the check is inconclusive regarding the sender domain.
   - **Reject mail if an SPF error occurs.**

   By default, these options are not enabled.
2. In the Bypass SPF Option box, you can specify a sender domain group for which SPF settings are bypassed.
   a. Mark the **Bypass SPF validation for senders in the following domain group** check box.
   b. Select a sender domain from the **Domain group** drop-down list.

3. In the Outbound Relay Options section, select the relay setting for senders in protected domains when SMTP authentication is not required. Default setting is **Allow relays only for senders from trusted IP addresses**.

   You must use the default setting if you use SMTP authentication.

   Note that allowing all outbound relays may create a security vulnerability in your system.

4. In the Internal Relay Options section, select the relay setting for mail between protected domains when SMTP authentication is not required. Default setting is **Allow relays only for senders from trusted IP addresses**.

   You must use the default setting if you use SMTP authentication.

   Note that allowing all outbound relays may create a security vulnerability in your system.

Configuring delivery routes

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

Configure delivery routes in the **Settings > Inbound/Outbound > Mail Routing** page. You can create the following types of message routes:

- *User directory-based routes*, page 94
- *Domain-based routes*, page 95

Change the order of a user directory- or domain-based route by marking its associated check box and using the **Move Up** or **Move Down** buttons.

Copying a route

Use the following steps to copy a route in the **Settings > Inbound/Outbound > Mail Routing** page:

1. Select a route in the route list by marking the check box next to its name.
2. Click **Copy**. A new route appears in the route list, using the original route name followed by a number in parentheses. The number added indicates the order that copies of the original route are created (1, 2, 3, etc.).
3. Click the new route name to edit route properties as desired.

Removing a route

If you want to remove a route, select the route by marking the check box next to its name and click **Delete**.

Note that the default domain-based route cannot be deleted.

User directory-based routes

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

Delivery routes based on user directory entries are examined first for a match with an email message recipient. Domain group entries are validated against the selected user directory to determine whether email will be delivered via a specified route.

Adding a user directory-based route

Use the following steps to add a user directory-based delivery route on the **Settings > Inbound/Outbound > Mail Routing** page:

1. Click **Add** to open the Add User Directory-based Route page.
2. Enter a name for your new route in the **Name** field (length between 4 - 50 characters).
3. Select an order number from the **Route order** drop-down list to determine the route's scanning order.
4. Select a destination domain from the pre-defined domains in the **Domain group** drop-down list. Default is Protected Domain. Information about the domain group appears in the Domain details box.

   If you want to edit your selected domain group, click Edit to open the Edit Domain Group page. See *Editing a domain group*, page 67, for details.
5. Select the user directories you want to use to define your route in the User Directories section. Select from the list of currently defined user directories and click the arrow button to move them to the Selected User Directories box.

   Note

   ESMTP user directories are not included in the directory list. ESMTP user directories cannot be used for user directory-based routes.

   If you want to add a new user directory, click **Add user directory** to open the Add User Directory page. See *Adding and configuring a user directory*, page 60, for information.

   If you want to remove a user directory from the Recipients list, select it and click **Delete**.
6. Select the delivery method:
   - Based on the recipient's domain (using the Domain Name System [DNS])
   - Based on SMTP server IP address designation (using smart host). If you select this option, an SMTP Server List opens.
     a. Click **Add** to open the Add SMTP Server dialog box.
     b. Enter the SMTP server IP address or hostname and port.

c. Mark the **Enable MX lookup** check box to enable the MX lookup function.

Important

If you entered an IP address in the previous step, the MX lookup option is not available.

If you entered a hostname in the previous step, this option is available.

- Mark the **Enable MX lookup** check box for message delivery based on the hostname MX record.
- If you do not mark this check box, message delivery is based on the hostname A record.

d. Enter a preference number for this server (from 1 - 65535; default value is 5).

If a single route has multiple defined server addresses, mail is delivered in order of server preference. When multiple routes have the same preference, round robin delivery is used.

You may enter no more than 16 addresses in the SMTP Server List.

7. Select any desired security delivery options.
   a. Select **Use opportunistic Transport Layer Security (TLS)** if you want email traffic to use opportunistic TLS protocol.
   b. Select **Require authentication** when you want users to supply credentials. Enter the appropriate user name and password in the Authentication Information box. You must use the SMTP server IP address delivery method when you want users to authenticate.

Domain-based routes

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

Delivery routes based on domain groups are examined after defined user directory-based routes for a match with an email message recipient. If a match is made with a user directory-based route, domain-based routes are not examined for matches.

Important

The Protected Domain group defined in the **Settings > Users > Domain Groups** page should not be used to configure delivery routes if you need to define domain-based delivery routes via multiple SMTP servers.

Create domain groups that contain subsets of the Protected Domain group for mail routing purposes.

Adding a domain-based route

Use the following steps to add a domain-based delivery route on the **Settings > Inbound/Outbound > Mail Routing** page:

1. Click **Add** to open the Add Domain-based Route page.
2. Enter a name for your new route in the **Name** field.
3. Select an order number from the **Route order** drop-down list to determine the route's scanning order.
4. Select a destination domain from the pre-defined domains in the **Domain group** drop-down list. Default is Protected Domain. Information about the domain group appears in the Domain details box.

   If you want to edit your selected domain group, click Edit to open the Edit Domain Group page. See *Editing a domain group*, page 67, for details.
5. Select the delivery method:
   - Based on the recipient's domain (using the Domain Name System [DNS])
   - Based on SMTP server IP address designation (using smart host). If you select this option, an SMTP Server List opens.
     a. Click **Add** to open the Add SMTP Server dialog box.
     b. Enter the SMTP server IP address or hostname and port.
     c. Mark the **Enable MX lookup** check box to enable the MX lookup function.

     Important

     If you entered an IP address in the previous step, the MX lookup option is not available.

     If you entered a hostname in the previous step, this option is available.

     - Mark the **Enable MX lookup** check box for message delivery based on the hostname MX record.
     - If you do not mark this check box, message delivery is based on the hostname A record.

     d. Enter a preference number for this server (from 1 - 65535; default value is 5).

     If a single route has multiple defined server addresses, mail is delivered in order of server preference. When multiple routes have the same preference, round robin delivery is used.

     You may enter no more than 16 addresses in the SMTP Server List.
6. Select any desired security delivery options.
   a. Select **Use opportunistic Transport Layer Security (TLS)** if you want email traffic to use opportunistic TLS protocol.

b. Select **Require authentication** when you want users to supply credentials. Enter the appropriate user name and password in the Authentication Information box. You must use the SMTP server IP address delivery method when you want users to authenticate.

Rewriting email and domain addresses

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

An email envelope recipient address can be rewritten to redirect message delivery to a different address. Envelope sender and message header addresses can also be rewritten to mask address details from message recipients. You can configure address rewriting for inbound, outbound, and internal email on the **Settings > Inbound/Outbound > Address Rewriting** page.

You can export all the email or domain addresses in an address rewrite list to a text file by clicking **Export** when that list is displayed.

Remove an email or domain address from one of your address rewrite lists by selecting it and clicking **Delete**.

Adding recipient address rewrite entries

Use the Inbound Messages tab to specify recipient address rewrite entries for inbound messages and the Outbound and Internal Messages tab for outbound or internal message redirection. The email envelope recipient address is rewritten based on the entries in the Envelope Recipient Address Rewrite List.

Use the following steps to add recipient rewrite entries:

1. Click **Add** in the Envelope Recipient Address Rewrite List to open the Add Recipient Email or Domain Address page.
2. Enter your addresses in 1 of 2 ways:
   - Mark the **Individual email address or domain rewrite entry** check box and enter the original recipient address and the rewrite address in the appropriate entry fields.

     An email address entry may have multiple rewrite entries, with each entry separated by a space. A domain address may have only 1 rewrite entry.
   - If you have an existing email or domain address rewrite entry file, mark the **Email address or domain rewrite entry file** check box and browse to the file. File size may not exceed 10 MB.
3. Click **OK**. Your entries appear in the Envelope Recipient Address Rewrite List.

Adding message header address rewrite entries

Use the Inbound Messages tab to add message header address rewrite entries for inbound messages and the Outbound and Internal Messages tab for outbound or

internal message address masking. The email envelope sender address and message header addresses are rewritten based on the entries in the Envelope Sender and Message Header Rewrite List.

Use the following steps to add address rewrite entries:

1. Click **Add** in the Envelope Sender and Message Header Rewrite List to open the Add Sender Email or Domain Address page.
2. Enter your addresses in 1 of 2 ways:
   - Mark the **Individual email address or domain rewrite entry** check box and enter the original sender address and the rewrite address in the appropriate entry fields.

     Each email or domain address entry may have only 1 rewrite entry.
   - If you have an existing email or domain address rewrite entry file, mark the **Email address or domain rewrite entry file** check box and browse to the file. File size may not exceed 10 MB.
3. Click **OK**. Your entries appear in the Envelope Sender and Message Header Rewrite List.

URL Sandbox

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

The URL sandbox function provides real-time analysis of uncategorized URLs that are embedded in inbound email. When a user clicks an uncategorized URL, a landing page prompts the user to initiate URL analysis. If the analysis determines that the link is malicious, the site is blocked. If the link is not malicious, the user receives notification that they may proceed to the site.

Your subscription must include the Email Sandbox Module and Email Hybrid Module. URL sandbox capability is available only after the email hybrid service is successfully registered and enabled.

The URL sandbox configuration settings include 3 components:

- Default settings that apply to any recipient not covered by specific settings
- Recipient-specific settings that apply to an individual domain or email address
- List of domains to which sandbox settings do not apply

Use the **Settings > Inbound/Outbound > URL Sandbox** page to configure the URL sandbox feature:

1. In the Default Settings section, specify the settings that apply to any recipient not covered by recipient-specific settings.
   a. Mark the **Analyze suspicious URLs** check box to activate the URL sandbox function. By default, the check box is not marked.

b. If the URL sandbox is enabled, mark the **Allow the recipient to follow links to unclassified URLs** check box to allow users to click unclassified URL links. By default, the check box is not marked.

c. Mark the **Allow the recipient to follow links with an unsupported protocol** check box to allow users to click a link that may redirect to a site with an unsupported protocol (e.g., HTTPS).

d. If you want the original URL replaced by other text, enter the string in the entry field below the check box. Leave this field blank if you want the original URL to appear.

2. Use the Recipient-specific Settings area to add custom sandbox settings for individual domain or email addresses.

   a. Click **Add** to create sandbox settings for a particular group of addresses.

   b. In the Recipient Email/Domain Address List, enter comma-separated email or domain addresses to which you want the settings to apply. No wildcards are permitted.

   c. Mark the **Analyze suspicious URLs** check box to activate the URL sandbox function for these addresses. By default, the check box is not marked.

   d. If the URL sandbox is enabled, mark the **Allow the recipient to follow links to unclassified URLs** check box to allow the specified users to click unclassified URL links. By default, the check box is not marked.

   e. Mark the **Allow the recipient to follow links with an unsupported protocol** check box to allow users to click a link that may redirect to a site with an unsupported protocol (e.g., HTTPS).

   f. If you want the original URL replaced by other text, enter the string in the entry field below the check box. Leave this field blank if you want the original URL to appear.

3. At the bottom of the URL Sandbox section, mark the **Analyze suspicious URLs that appear in digitally signed email** check box if you want the sandbox to examine URLs even if they appear in a message that contains the digital signature of a trusted sender. By default, the check box is not marked.

4. In the entry field above the check box, enter the URL domains that you want to bypass the URL sandbox. Do not use wildcards, and separate multiple entries with a comma.

If you want to delete a set of recipient-specific settings, mark the check box next to the address list and click **Delete**.

Phishing detection and education

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

Phishing involves an attempt to obtain personal information like passwords or credit card numbers via email while pretending to be a trusted entity. For example, an email message that purports to be from a known financial institution or popular web site may actually be an attempt to steal personal information.

The phishing detection and education function provides cloud-based analysis of an inbound message for phishing email characteristics. In order to use the phishing detection and education feature, your subscription must include the Email Hybrid Module. You must have successfully registered with the email hybrid service before you configure phishing detection and education capabilities.

You define the rules that determine which sender domains are analyzed and how a suspected phishing email is handled. Suspect email may be treated the same as spam (blocked and saved to a spam queue) or be replaced by a message that educates the recipient about phishing attack email.

Dashboard charts and presentation reports can be configured to display suspected phishing attack data.

The **Settings > Inbound/Outbound > Phishing Detection** page includes the following tabs for configuring phishing detection:

- **Phishing Rules**, which contains a list of all your phishing rules. A default rule applies to domains that are not included in any other defined rule. See *Adding a phishing detection rule*, page 100, for information.

  The default rule cannot be deleted. You can delete any other phishing rule from the list by marking its associated check box and clicking **Delete** and then clicking **Save to Cloud Service**.
- **Phishing Education Pages**, which contains a list of all the education pages you have defined. A default page applies when a custom page is not specified for a phishing rule. See *Creating a phishing education page*, page 101, for information.

  You can delete any phishing education page (except the default page) from the list by marking its associated check box and clicking **Delete**. You may not delete a page that is being used by a phishing rule.

  Click **Save to Cloud Service** only if you receive an error message regarding a synchronization issue with the cloud service.

Adding a phishing detection rule

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

Use the following steps to configure a phishing detection rule:

1. Click **Add Rule** on the Phishing Rules tab to open the Add Rule page.
2. Enter a name for the rule in the **Phishing rule name** entry field.
3. Specify the domains to which this phishing rule applies in the **Domain names** entry field. Separate multiple domains with a semicolon.
4. Select a phishing action option for this phishing rule:
   - **Treat as spam.** Quarantine the suspected phishing message.
   - **Educate**: **Replace the URL with a link to the selected phishing education page and deliver the message.**

5. Configure individual user exceptions to the phishing rule. For example, you may want to select a different action for a particular user or group or present a different phishing education page for that user or group.
   a. Click **Add User Exception** to open the Add User Exception dialog box.
   b. Enter a brief description of this exception in the **Description** entry field.
   c. Specify the email addresses for the users or groups to whom this exception applies in the **Email addresses** entry field.
   d. Select a phishing action option for this user exception:
      - **Treat as spam**. Quarantine the suspected phishing message.
      - **Educate: Replace the URL with a link to the selected phishing education page and deliver the message.**
   e. Click **Add**.
6. Click **OK** to save your phishing rule.
7. Click **Save to Cloud Service** in the Phishing Rules tab to send your phishing detection settings to the email hybrid service.

Creating a phishing education page

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

You can create a new phishing education page by copying an existing page and renaming it. You can also customize the default message template to suit your needs. A default page is used when a custom page is not specified for a phishing rule.

Use the following steps to copy an existing phishing education page:

1. Click **Copy Page** in the Phishing Education Pages tab.
2. Enter a name for the phishing education page copy in the **Page name** entry field.
3. Click **OK**.

Use the following steps to create a custom phishing education page:

1. Click **Add Page** in the Phishing Education Pages tab to open the Add Phishing Education Page screen.
2. Enter a name and description for the phishing education page.
3. Specify a title for the page in the **Page title** field. This title appears as the browser window name.
4. Specify the desired text and images in the **Phishing Education Page Editor**.
5. Click **OK**.

Note

If you receive an error message regarding a synchronization issue with the cloud service, you should click **Save to Cloud Service** in the Phishing Education Pages tab to send your phishing education page settings to the email hybrid service.

Managing message queues

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

You can view, create, and configure message queues on the **Main > Message Management > Message Queues** page. You can also modify the following default queues:

- virus
- spam
- exception
- encryption-fail
- decryption-fail
- archive
- secure-encryption
- data-security
- url-analysis

All blocked messages across all queues are accessed in the **Main > Message Management > Blocked Messages** page (see *Managing the blocked message queue* for details). Temporarily delayed messages can be viewed in the **Main > Message Management > Delayed Messages** page (see *Managing the delayed message queue* for information).

Message queues list

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

The Queue List on the Message Queues page contains the following information about each queue:

- Queue name. Click a queue name in the Queue List to view and manage the messages in the queue. See *Viewing a message queue*, page 104, for details.
- Queue status, indicating whether the queue is in use or not. Click the **Referenced** link in this column to see a list of the email functions that use the queue. During a queue move operation, an icon in this column indicates whether the move is in progress or has failed.

- Message volume, indicating the total number of messages in that queue. The number of messages a delegated administrator sees may be less than the total displayed in this column, depending on the permissions granted to that administrator.
- Size/Total, indicating the queue's current size as a portion of its maximum configured size
- Storage location, showing the location of queue storage (Local, via Network File System [NFS], or via Samba). Icons in this column indicate storage status, such as low disk space or a lost connection.
- The Properties column contains a link to a page displaying the queue's current settings. Click this **Edit** link to change any queue settings.

You can remove a user-created queue by marking the check box next to the queue name in the Queue List and clicking **Delete**. You cannot delete a default queue.

Creating a message queue

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

Use the following steps to create a new message queue on the **Main > Message Management > Message Queues** page:

1. Click **Add** below the Queue List to open the Add Queue page.
2. Enter a name for the new queue in the **Queue name** field.
3. Select the location for this queue's storage.
   - Use **Local** to store the queue locally.
   - Select **Via Network File System (NFS)** to use the NFS protocol for file storage. Enter the IP address or hostname of the storage location, along with its shared path.

     Note
     NFS version 3 or later is supported.

   - Select **Via Samba** to use Samba to facilitate file storage. Enter the following information for Samba:
     - IP address or hostname of the storage location
     - Its shared path
     - Username
     - Password
4. Configure the maximum number of days a message is retained in the queue, from 1 to 180 days, in the **Maximum message retention** field. Default is 180 for default queues, 30 for administrator-created queues.
5. Configure the maximum queue size, from 1 to 51200 MB (default is 1024).
6. For an appliance in a cluster, specify the maximum storage size (in MB) assigned to each cluster machine.

Changing message queue properties

To change a message queue's properties, click **Edit** in the Queue List Properties column for that queue to open the Edit Queue page.

Viewing a message queue

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

Click a queue name in the Message Queues page Queue List to open that queue. Use the **View from/to** fields to specify the desired date/time range for the 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. Click the arrow to the right of the **View** date/time range to display the desired queue items.

You can also perform a keyword search of the message queue, or refine the search by specifying that only message IDs, senders, recipients, subjects, or policies applied are searched. You can also search on the name of the appliance that processed the messages (Processed By category). Enter a keyword and click **Search**.

Configure how many messages you want to view on each page of the queue in the **per page** drop-down list (25 [the default], 50, or 100).

Information displayed in the list of messages includes the following items:

- Sender email address
- Recipient email address
- Message subject. You can view message information and message contents by clicking the link in the Subject column to open the View Message page. See *Viewing a message in a queue*, page 110.
- Message size
- Date/time of message receipt
- The policy and rule applied to the message. If a data loss prevention (DLP) policy is applied to a message, a **View Incident** link opens the DLP incident information in the Data module, where the processing of this message occurs.

  This column does not appear in the archive queue.
- Message type (for example, spam, virus, exception, commercial bulk, file sandbox, Threat Protection, spoofed email, URL analysis, encryption error, or decryption error)

- The name of the appliance that processed the message is included in the **Processed By** column.
- The **Reason for Quarantine** column contains an entry indicating why a message has been sent to a quarantine queue:
  - Antivirus filter
  - Email hybrid service
  - URL analysis filter
  - Bounce address tag validation
  - Digital fingerprinting antispam tool
  - LexiRules antispam tool
  - Heuristics antispam tool
  - Commercial bulk email filter
  - Custom content filter
  - Block List (Personal Email Manager Always Block List entry)
  - Archive feature (a **Settings > Inbound/Outbound > Message Control** setting)
  - Data loss prevention
  - Exception (message exception)
  - For a message attachment analyzed by Threat Protection, a **View report(s)** link opens a pop-up box with links to a Threat Protection report on each file examined

You can select a message in the queue and perform the following actions:

Action	Description
Deliver	Deliver the message to its recipient(s).
Delete	Delete the message from the queue.
Reprocess	Delete the message from the queue and restart the email processing function as if the email system were receiving it for the first time. For the archive queue, this action is called **Process**.
Not Spam	Report that the message should not be classified as spam and release the message for delivery. This option is available only when spam messages are selected.
Refresh	Refresh the queue contents list to view up-to-date queue contents.

The More Actions drop-down list includes the following operations:

Action	Description
Resume Processing	A message that has both spam and virus characteristics may be isolated by 1 type of filter before it has been processed by the other type. If the original quarantine is a false positive, use this action to make sure the message is processed by all relevant filters rather than delivered after only the first analysis.
Add to Always Block List	Add the message sender to the Always Block List.
Add to Always Permit List	Add the message sender to the Always Permit List.
Forward	Forward the message to 1 or more recipients. The forwarded message is added as an attachment to the forwarding message.
Download	Download the message in .eml format. Downloaded email is saved in a zip file.
Clear message queue	Delete all the messages in the queue.
Reprocess all messages	Reprocess messages in your search result. Only the first 5000 entries in your search result are reprocessed.
Delete all messages	Delete messages in your search result. Only the first 5000 entries in your search result are deleted.

Managing the blocked message queue

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

The **Main > Message Management > Blocked Messages** page lists all blocked messages from most queues across all appliances together in a single table, with a column entry that indicates the name of the queue in which a message is stored. Messages in the archive and Delayed Messages queues are not included on this page.

Use the **View from/to** fields to specify the desired date/time range for the 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. Click the arrow to the right of the **View** date/time range to display the desired queue items.

You can also perform a keyword search of all blocked messages, or refine the search by specifying that only message IDs, senders, recipients, subjects, or policies applied are searched. You can also search on an individual queue or on the name of the

appliance that processed the messages (Processed By category). Enter a keyword and click **Search**.

Configure how many messages you want to view on each page of the queue in the **per page** drop-down list (25 [the default], 50, or 100).

Information displayed in the list of messages includes the following items:

- Sender email address
- Recipient email address
- Message subject. You can view message information and message contents by clicking the link in the Subject column to open the View Message page. See *Viewing a message in a queue*, page 110.
- Message size
- Date/time of message receipt
- The policy and rule applied to the message. If a DLP policy is applied to a message, a **View Incident** link opens DLP incident information in the Data module, where processing of this message occurs.
- Queue name (for example, spam, virus, exception, encryption-fail, or decryption-fail)
- Message type (for example, spam, virus, exception, commercial bulk, spoofed email, URL analysis, encryption error, or decryption error)
- The name of the appliance that processed the message is included in the **Processed By** column.
- The **Reason for Quarantine** column contains an entry indicating why a message has been sent to a quarantine queue:
  - Antivirus filter
  - Email hybrid service
  - URL analysis filter
  - Bounce address tag validation
  - Digital fingerprinting antispam tool
  - LexiRules antispam tool
  - Heuristics antispam tool
  - Commercial bulk email filter
  - Custom content filter
  - Block List (Personal Email Manager Always Block List entry)
  - Archive feature (a **Settings > Inbound/Outbound > Message Control** setting)
  - Data loss prevention
  - Exception (message exception)
  - For a message attachment analyzed by Threat Protection, a **View report(s)** link opens a pop-up box with links to a Threat Protection report on each file examined

You can select a message in the blocked messages queue and perform the following actions:

Action	Description
Deliver	Deliver the message to its recipient(s).
Delete	Delete the message from the queue.
Reprocess	Delete the message from the queue and restart the email processing function as if the email system were receiving it for the first time.
Not Spam	Report that the message should not be classified as spam and release the message for delivery. This option is available only when spam messages are selected.
Refresh	Refresh the queue contents list to view up-to-date queue contents.

The More Actions drop-down list includes the following operations:

Action	Description
Resume Processing	A message that has both spam and virus characteristics may be isolated by 1 type of filter before it has been processed by the other type. If the original quarantine is a false positive, use this action to make sure the message is processed by all relevant filters rather than delivered after only the first analysis.
Add to Always Block List	Add the message sender to the Always Block List.
Add to Always Permit List	Add the message sender to the Always Permit List.
Forward	Forward the message to 1 or more recipients. The forwarded message is added as an attachment to the forwarding message.
Download	Download the message in .eml format. Downloaded email is saved in a zip file.
Reprocess all messages	Reprocess the messages in your search result. Only the first 5000 entries in your search result are reprocessed.
Delete all messages	Delete the messages in your search result. Only the first 5000 entries in your search result are deleted.

Managing the delayed message queue

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

Email that is temporarily undeliverable as a result of various connection issues is sent to the delayed messages queue. Delayed messages may be automatically resent by the system. See *Handling undelivered messages*, page 112, for information about setting the delayed messages delivery retry interval and configuring a notification message to be sent for undelivered email.

Delayed message delivery may also be scheduled for a future date using a custom content filter action. See *Custom content*, page 123, for information about custom content filters and *Creating and configuring a filter action*, page 135, for details about scheduling a delayed message delivery.

You may view the messages in this queue and perform any necessary processing activities manually on the **Main > Message Management > Delayed Messages** page. When the Delayed Messages page appears, the most recent messages are shown. Use the **View from/to** fields to specify the desired date/time range for the messages 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. Click the arrow to the right of the **View** date/time range to display the desired queue items.

You can also perform a keyword search of the message queue, or refine the search by specifying that only message IDs, senders, recipients, subjects, or reasons for delay are searched. If appliances are configured in a cluster, you can also search on the name of the appliance that processed the messages. Enter a keyword and click **Search**.

You can configure the number of messages per page, between 25 and 100, in the **Per page** drop-down list in the queue list banner (25 [the default], 50, or 100).

Information displayed in the list of messages includes the following items:

- Sender email address
- Recipient email address
- Message subject. You can view message information and message contents by clicking the link in the Subject column to open the View Message page. See *Viewing a message in a queue*, page 110.
- Message size
- Date/time of message receipt
- The policy and rule applied to the message. If a DLP policy is applied to a message, a **View Incident** link opens DLP incident information in the Data module, where processing of this message occurs.
- Date of the next scheduled message delivery attempt
- The reason a message is delayed. Entries in this column may be 1 of the following:
  - Temporary connection issue delay *n*. A temporary delay due to connection issues; *n* is the number of retry attempts remaining for the message.

- Scheduled delay. An intentional delay that is scheduled via a custom content filter action (see *Creating and configuring a filter action*, page 135, for information).
- File sandbox or Threat Protection analysis delay. A temporary delay due to in-progress advanced file analysis.

- The name of the appliance that processed the message is included in the **Processed By** column.

You can select a message in the queue and perform the following actions:

Action	Description
Release	Attempt the message delivery immediately.
Delete	Delete the message from the queue.
Refresh	Refresh the queue contents list to view up-to-date queue contents.

The More Actions drop-down list includes the following operations:

Action	Description
Forward	Forward the message to 1 or more recipients. The forwarded message is added as an attachment to the forwarding message.
Download	Download the message in .eml format. Downloaded email is saved in a zip file.
Release all messages	Attempt to deliver all the messages in the queue.
Delete all messages	Delete the messages in your search result. Only the first 5000 entries in your search result are deleted.

Viewing a message in a queue

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

Click the link for a message in the Subject column of a queue to open the View Message page, which contains details about the message as well as the message contents. The **Back** link at the top of the page returns you to the View Queue page. The **Previous** and **Next** links let you navigate to the previous or next message in the queue messages list.

The following information about a selected message is displayed on the View Message page:

Field Name	Description
Sender	Sender's email address
Recipient	Recipient's email address
From	Name of the sender

Field Name	Description
To	Name of the recipient
Date	Date the message was received
Policy	Name of the policy applied to the message
Message type	Message type, indicating message analysis result or filter type (Clean, Virus, Spam, Data Loss Prevention, Exception, Commercial Bulk, Phishing, File Sandbox, Threat Protection, Spoofed Email, URL Analysis, or Custom Content)
Processed by	Name of the appliance that processed the message
Header	Click the link to view the message header
Attachment	If the message contains an attachment, a link allows you to open it.
Subject	Message subject

The message actions available to you on any View Queue page are also available on the View Message page, except Clear All Messages or Release All Messages. See *Viewing a message queue*, page 104, for descriptions of these actions. You can also choose to view message contents in either text or HTML format or to **Clear message queue**, options in the More Actions drop-down list.

Configuring message exception settings

The **Settings > Inbound/Outbound > Exceptions** page specifies how messages that cannot be processed for some reason are handled. Configure message exception settings as follows:

1. Specify the action to perform on a message that cannot be processed:
   - Deliver the message when an exception is caused by an antivirus filter.
   - Deliver the message when an exception is caused by an antispam filter (default setting).
   - Deliver the message when an exception is caused by the advanced file analysis filter.
   - Deliver the message when an exception is caused by the commercial bulk email filter.
   - Deliver the message when an exception is caused by a data loss prevention policy (default setting).
   - Deliver messages when an exception is caused by any other system operation.
   - Save exception messages to a queue (default setting).

Select the desired folder from the drop-down list (default is **exception**). The list includes all the default queue names and any administrator-created queues. If you want to add a new queue, select **Add Folder** from the drop-down list to open the Add Queue screen.

Warning

You must have the save option selected in order to save undelivered messages to a queue. If this option is not selected, messages may be dropped

2. If you want a notification sent regarding the unprocessed message, mark the **Send notification** check box to enable the Notification Properties section.
3. Specify the notification message sender from the following choices:
   - Original email sender (the default)
   - Administrator. If you use this option, you must configure a valid administrator email address in the **Settings > General > System Settings** page (see *Setting system notification email addresses*, page 56).
   - Custom. Specify a single email address in this field.
4. Specify 1 or more notification message recipients from among the following choices:
   - Original email sender
   - Original email recipient
   - Administrator (the default). If you use this option, you must configure a valid administrator email address in the **Settings > General > System Settings** page (see *Setting system notification email addresses*, page 56).
   - User specified. Enter 1 or more email addresses, separated by semicolons, in this field.
5. Specify the subject line of your notification message in the **Subject** field.
6. Enter the body of your notification message in the **Content** field.
7. If you want the original message to be attached to the notification message, mark the **Attach original message** check box.

Handling undelivered messages

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

Message delivery options help you control how undeliverable mail is handled. Options for these operations appear on the **Settings > Inbound/Outbound > Message Non-Delivery Options** page.

Use the following steps to determine how to handle messages that are temporarily undeliverable due to error situations:

1. In the Undelivered Message Options section, enter the time (in minutes) for the message retry interval in the **Retry interval** field.

   Important

   Message delivery retry intervals are calculated exponentially. For example, using the default entry of 15, retry attempts are made in 15, 30, 60, 120, 240, etc., minutes.

2. Enter the time (in minutes) for the maximum period for retrying message delivery in the **Maximum retry period** field (default is 1440).
3. In the **Notification email address** field, enter an email address to which you want to send notifications that a non-delivery report (NDR) cannot be delivered to the original sender at the end of the retry period.

   Mark the **Use Administrator email address** check box to send these messages to the administrator. You must configure the administrator address in the **Settings > General > System Settings** page (see *Setting system notification email addresses*, page 56).

Traffic shaping options

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

The **Settings > Inbound/Outbound > Traffic Shaping** screen lets you determine the rate of traffic delivery for a specified source or destination group based on domain group or user directory settings. For example, these settings allow you to send large volumes of email at a rate that prevents possible blacklisting of the domain.

Change the order of a traffic shaping group by marking its associated check box and using the **Move Up** and **Move Down** buttons. Copy an existing traffic shaping group by marking its associated check box and clicking **Copy**. You can delete a traffic shaping group by marking its associated check box and clicking **Delete**.

In addition to specifying source and destination user groups, the following message delivery settings may be modified as part of traffic shaping:

- Maximum number of concurrent connections
- Maximum number of messages per connection within a designated time period
- Maximum number of recipients per message
- Use of the SMTP session cache, for which the maximum number of messages per session and the session duration are specified

The default traffic shaping group contains no traffic source or destination user groups.

Click **Add** and use the following steps to establish message traffic shaping controls in your system:

1. Name your traffic shaping group.

2. Specify the location in which you want this group to appear in the traffic shaping group list by selecting it in the **Order** drop-down list.
3. Select the status of your traffic shaping group: **Active** or **Disabled**.
4. Configure an email source traffic shaping group, if desired. Designate 1 of the following source types:
   - All sources
   - Domain group (default selection). Select the domain group from the drop-down list. Modify the selected domain group by clicking **Edit**.
   - User directory. Select a user directory from the list, or create a new user directory by clicking **Add user directory**.
5. Configure an email destination traffic shaping group, if desired. Designate 1 of the following destination types:
   - All destinations
   - Domain group (default selection). Select the domain group from the drop-down list. Modify the selected domain group by clicking **Edit**.
   - User directory. Select a user directory from the list, or create a new user directory by clicking **Add user directory**.
6. Enter the maximum number of simultaneous message deliveries to an individual routing address in the **Maximum number of concurrent connections** field. Range of values is 5 - 50; default value is 20.
7. Enter the maximum number of messages per connection within a defined time period in the **Maximum number of messages per connection** field. Number of messages range is 1 - 10000; default value is 10000. Time range is 60 seconds to 30 minutes; default value is 60 seconds.
8. Enter the maximum number of message recipients per message delivery in the **Maximum number of recipients** field. Range of values is 5 - 100; default value is 50.
9. If you want to use an SMTP session cache, mark the **Enable SMTP session cache** check box (default setting).
   a. Specify the maximum number of messages allowed per SMTP session. Range of values is 5 - 100; default is 10. You can enter zero (0) to specify an unlimited number of messages per session.
   b. Specify the duration of the SMTP session, in seconds. Range of values is 60 - 600 seconds; default value is 300 seconds.

Handling encrypted messages

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

An email content policy configured in the Data module may specify that a message should be encrypted for delivery. If you want to encrypt specific outbound messages, you must create an email DLP policy that includes an encryption action plan in the Data module (**Main > Policy Management > DLP Policies**).

The following types of message encryption are supported:

- *Mandatory Transport Layer Security (TLS) encryption*
- *Advanced email encryption*
- *Third-party encryption application*
- *Secure Message Delivery*

Use the **Settings > Inbound/Outbound > Encryption** page to specify the type of encryption you want to use.

Mandatory Transport Layer Security (TLS) encryption

TLS is an Internet protocol that provides security for all email transmissions—inbound, outbound, and internal. The client and server negotiate a secure "handshake" connection for the transmission to occur, provided both the client and the server support the same version of TLS.

In the Email module, if you select only TLS for message encryption and the client and server cannot negotiate a secure TLS connection, the message is sent to a delayed message queue for a later delivery attempt. Select **Transport Layer Security (TLS)** in the **Encryption method** drop-down list and the **Use TLS only (no backup encryption method; message is queued for later delivery attempt)** option to use only TLS for message encryption.

If you select TLS for message encryption, you can designate another encryption options as a backup method, in case the TLS connection fails. Specifying a backup option allows you a second opportunity for message encryption in the event of an unsuccessful TLS connection. If both the TLS and backup connections fail, the message is sent to a delayed message queue for a later connection attempt.

Select the **Transport Layer Security (TLS)** option in the **Encryption method** drop-down list to enable TLS encryption. Then mark 1 of the following options to enable a backup encryption method:

- **Use Advanced Email Encryption as backup encryption method.** This option is available only if your subscription includes the Email Hybrid Module.
- **Use third-party application as backup encryption method**
- **Use secure message delivery as backup encryption method**

Advanced email encryption

If you want the email hybrid service to perform message encryption on outbound messages, select the **Advanced Email Encryption** option in the **Encryption method** drop-down list. Advanced email encryption is available only if your subscription includes the Email Hybrid Module and the Email Encryption Module, and the email hybrid service is registered and enabled.

You can also specify advanced email encryption as a backup encryption method if mandatory TLS encryption is selected. See *Mandatory Transport Layer Security (TLS) encryption*, page 115, for details.

When an email DLP policy identifies an outbound message for encryption, the message is sent to the email hybrid service via a TLS connection. If the secure connection is not made, the message is placed in a delayed message queue for a later delivery attempt.

The SMTP server addresses used to route email to the email hybrid service for encryption are configured in the Email Hybrid Module registration process. Use the Delivery Route page under **Settings > Hybrid Service > Hybrid Configuration** to add outbound SMTP server addresses (see *Define delivery routes*, page 37).

If the email hybrid service detects spam or a virus in an encrypted outbound message, the mail is returned to the message sender.

The email hybrid service attempts to decrypt inbound encrypted mail, and adds an x-header to the message to indicate whether the decryption operation succeeded. Message analysis is performed regardless of whether message decryption is successful.

The hybrid service does not encrypt inbound or internal mail. A DLP policy must be modified to designate only outbound messages for encryption when the email hybrid service is used.

Find more information about advanced email encryption in Forcepoint Email Encryption in Forcepoint Documentation.

Third-party encryption application

The email protection system supports the use of third-party software for email encryption. The third-party application used must support the use of x-headers for communication with the email system.

You can also specify third-party application encryption as a backup encryption method if mandatory TLS encryption is selected. See *Mandatory Transport Layer Security (TLS) encryption*, page 115, for details.

The email protection system can be configured to add an x-header to a message that triggers a DLP encryption policy. Other x-headers indicate encryption success or failure. These x-headers facilitate communication between the email system and the encryption software. You must ensure that the x-header settings made in the Encryption page match the corresponding settings in the third-party software configuration.

X-header settings are entered on the **Settings > Inbound/Outbound > Encryption** page. Select **Third-party application** in the **Encryption method** drop-down list to configure the use of external encryption software. Use the following steps to configure third-party application encryption:

1. Add encryption servers (up to 32) to the Encryption Server List:
   a. Enter each server's IP address or hostname and port number.
   b. If you want to use the MX lookup feature, mark the **Enable MX lookup** check box.

If you entered an IP address in the previous step, the MX lookup option is not available.

c. Click the arrow to the right of the Add Encryption Server box to add the server to the Encryption Server List.

If you want to delete a server from the list, select it and click **Remove**.

2. In the **Encrypted IP address group** drop-down list, specify an IP address group if decryption is enabled or if encrypted email is configured to route back to the email software. Default is Encryption Gateway.
3. If you want users to present credentials to view encrypted mail, mark the **Require authentication** check box and supply the desired user name and password in the appropriate fields. Authentication must be supported and configured on your encryption server to use this function.
4. In the **Encryption X-Header** field, specify an x-header to be added to a message that should be encrypted. This x-header value must also be set and enabled on your encryption server.
5. In the **Encryption Success X-Header** field, specify an x-header to be added to a message that has been successfully encrypted. This x-header value must also be set and enabled on your encryption server.
6. In the **Encryption Failure X-Header** field, specify an x-header to be added to a message for which encryption has failed. This x-header value must also be set and enabled on your encryption server.
7. Select any desired encryption failure options:
   - Mark the **Send messages to queue** check box if you want to enable that option. Select a queue for these messages from the drop-down list (default is the virus queue).
   - Mark the **Send notification to original sender** check box if you want to enable that option.

     In the Notification Details section, enter the notification message subject and content in the appropriate fields. Mark the **Attach original message** check box if you want the original message included as an attachment to the notification message.
   - Select **Deliver message** (default) if you want the message that failed the encryption operation delivered.
   - Select **Drop message** if you do not want the message that failed the encryption operation delivered.
8. Mark the **Enable decryption** check box if you want to decrypt encrypted messages.
9. Select any desired decryption options:
   - In the **Content type** field, enter the message content types to decrypt, separated by semicolons. Maximum length is 49 characters. Default entries include multipart/signed, multipart/encrypted, and application/pkcs7-mime.
   - In the **X-Header** field, specify a message x-header that identifies a message to decrypt. This x-header value must also be set and enabled on your encryption server.

- In the **Decryption X-Header** field, specify an x-header to be added to a message that should be decrypted. This x-header value must also be set and enabled on your encryption server.
- In the **Decryption Success X-Header** field, specify an x-header to be added to a message that has been successfully decrypted. This x-header value must also be set and enabled on your encryption server.
- In the **Decryption Failure X-Header** field, specify an x-header to be added to a message for which decryption has failed. This x-header value must also be set and enabled on your encryption server.
- If you want to forward a message that has failed decryption to a specific queue, mark the **On decryption failure** check box, and select a queue for these messages from the drop-down list (default is the virus queue).

Secure Message Delivery

Secure Message Delivery is an on-premises encryption method that lets you configure delivery options for a secure portal in which recipients of your organization's email may view, send, and manage encrypted email. For example, you may wish to include sensitive personal financial information in a message to a client. The portal provides a secure location for the transmission of this data.

Users within your organization who send and receive secure messages handle these messages via their local email clients, not the secure portal.

Secure messages are stored in a default secure-encryption queue (**Main > Message Management > Message Queues**). You can search for and delete messages in the secure-encryption queue view. Message details may not be viewed. The maximum queue size and number of days a message is retained are configured on the Edit Queue page.

Select **Secure Message Delivery** from the **Encryption method** drop-down list to display secure messaging options, including a template for the notification that users receive to alert them to encrypted mail.

You can also specify Secure Message Delivery as a backup encryption method for outbound email if mandatory TLS encryption is selected. See *Mandatory Transport Layer Security (TLS) encryption*, page 115, for details.

Use the following steps to configure Secure Message Delivery encryption:

1. Enter the IP address or hostname for the appliance that hosts the secure message delivery portal (maximum length for hostname is 64 characters).

Entering a hostname rather than an IP address is recommended in order to avoid potential Microsoft Outlook warning messages generated in an end user's inbox by the notification message.

Important

The entry in this field should be mapped to the E1 interface (for a V10000 appliance) or the P1 interface (for a V5000 appliance). Ensure that the interface you use is visible from outside your internal network.

If you have an appliance cluster, enter the IP address or hostname for 1 cluster appliance (primary or secondary). The cluster load balancing function directs traffic appropriately.

Note

Secure messaging uses the same port configured for the Personal Email Manager portal (**Settings > Personal Email > Notification Message**).

2. Specify the actions that your customers are allowed to perform in the secure portal, along with the types of recipients to whom these users can send secure messages:
   - **Enforce strong password policy.** With this policy in force, an end-user password must meet the following requirements:
     - Between 8 and 15 characters
     - At least 1 uppercase letter
     - At least 1 lowercase letter
     - At least 1 number
     - At least 1 special character; supported characters include:
       ! " # $ & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~

     End users are prompted to create strong passwords in the Secure Messaging portal.
   - **Maximum message size.** Customer message size includes any attachments. Default value is 50 MB; maximum value is 100 MB.
   - **Reply all to secure messages received in the portal**. Customer may reply to all message recipients. However, if the **Internal domain email addresses only** option is selected for Allowed Recipients, user may reply only to recipients inside your organization.

     The recipient list cannot be modified for this type of message.
   - **Forward secure messages received in the portal**. Customer may forward to allowed recipients any secure message received.
   - **Compose new secure messages within the portal**. Customer may compose and send a new secure message to allowed recipients.
   - **Attach files to secure messages sent from the portal.** Customer may send an attachment in a secure message

These options are all selected by default.

The Allowed Recipients box offers options for the types of recipients to whom your customer may reply, forward, or send new secure messages. For security purposes, the recipient list must include at least 1 email address within your organization.

- **Internal domain email addresses only**. Only email addresses within your organization's protected domains may be specified as recipients.
- **Internal and external domain email addresses (at least one internal email address required)**. Email addresses outside your organization's protected domains may be specified as recipients, but at least 1 address within your domains must be entered (default selection).

  See *Protected Domain group*, page 65, for more information about determining your protected domains.

The Secure Email End-User Notification area contains a message template for the email that users receive when secure messages sent to them have been delivered to the portal for viewing. Use the default template, or customize it to suit your needs. You must include the URL field in your notification, because that creates the link your customer clicks to access the secure email portal.

Enter 1 sender address for the notification in the **Sender** field, and specify an email subject in the **Subject** field. The sender address must belong to your internal protected domain. Because you do not want responses to the notification, ensure that the sender address is configured to drop any direct replies to the notification.

After you have configured your notification message, click **Preview Message** to view it.

The portal can be displayed in 1 of 9 languages, which the user selects during the registration process. The Forcepoint Secure Messaging User Help is available in Forcepoint Documentation, also in 9 languages. It describes the user registration process and how to use the secure message portal.

5 Working with Filters and Policies

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

Topics:

Managing filters

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

The following predefined default filter types can be used in email analysis: virus, URL analysis, spam, commercial bulk email, advanced file analysis, spoofed email, and disclaimer.

- The virus filter analyzes an email message and its attachments for the presence of viruses and other threats.
- URL analysis examines email content for embedded URLs and classifies them according to a database of known spam URLs.
- The spam filter analyzes email content and compares it against a database of known spam characteristics. You can select from a variety of antispam tools, including digital fingerprinting, LexiRules, and heuristics analysis tools.
- The commercial bulk email filter analyzes a message to determine whether it was sent from a business for advertising purposes.
- The advanced file analysis filter inspects email attachment file types that commonly contain security threats.
- A spoofed email filter can help reduce instances of email sender impersonation.
- If you want to add text at the beginning or end of a message, use the disclaimer filter.

You can also create a custom content filter to scan a message based on message component conditions you configure. The Email module does not provide a default custom content filter.

Filters are created and managed via the **Main > Policy Management > Filters** page. Click **Add** to open the Add Filter page and set the properties of your new filter (see *Creating and configuring a filter*, page 122).

You can also copy a filter whether or not it is in use by a policy. A filter can be deleted, as long as it is not in use by any policy. However, you cannot copy or delete any default filter.

Copying a filter

Copy an existing filter by marking the check box to the left of the filter name to select it and clicking **Copy**. Enter a new filter name in the Copy Filter dialog box, and click **OK**. Click the new filter name in the Filters list to open the Edit Filter page and modify filter attributes.

Deleting a filter

Delete a filter from the Filters list by marking the check box to the left of the filter name and clicking **Delete**. You can delete a filter only if it is not being used by a policy.

Creating and configuring a filter

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

To create a new filter, click **Add** on the **Main > Policy Management > Filters** page. Enter a filter name and description, then select the filter type you want to use. The filter type you choose determines the filter settings you can configure. Select from the following types:

- *Custom content*, page 123
- *URL analysis*, page 125
- *Antivirus*, page 126
- *Antispam*, page 127
- *Commercial bulk email*, page 128
- *Advanced file analysis*, page 129
- *Spoofed email*, page 131
- *Disclaimer*, page 134

Custom content

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

Use a custom content filter to allow message analysis based on conditions you configure. Add or modify a custom content filter on the **Main > Policy Management > Filters > Add** (or **Edit**) **Filter** page. The Email module does not provide a default custom content filter.

You can choose to trigger your filter on the match of a single condition or the match of all defined conditions by selecting 1 of the following options in the Filter Properties section:

- **Match all conditions**
- **Match any condition**

Specify the conditions of your custom filter from a selection of criteria, including message attributes and operators, by clicking **Add** in the Filter Conditions box. In the Add Condition dialog box, select from among the following message attributes and operators to configure your custom filter (all message attributes except DKIM verification include a user-configurable **Filtering criteria** entry field):

Message Attribute	Operator Options	Additional Options
Sender IP address	Is, Is not	None
Envelope sender	Contains, Does not contain, Matches regular expression, Does not match regular expression	None
Envelope recipient	Contains, Does not contain, Matches regular expression, Does not match regular expression	None
Number of envelope recipients	Equals, Does not equal, Is less than, Is greater than	None
From field address	Contains, Does not contain, Matches regular expression, Does not match regular expression	None
To field address	Contains, Does not contain, Matches regular expression, Does not match regular expression	None
Cc field address	Contains, Does not contain, Matches regular expression, Does not match regular expression	None
Message subject	Contains, Does not contain, Matches regular expression, Does not match regular expression	Match case

Message Attribute	Operator Options	Additional Options
Message header: partial	Contains, Does not contain, Matches regular expression, Does not match regular expression	Message attribute text (user configured), Match case
Message header: complete	Contains, Does not contain, Matches regular expression, Does not match regular expression	Match case
Message body text	Contains, Does not contain, Matches regular expression, Does not match regular expression	Match case
Message size	Equals, Does not equal, Is less than, Is greater than	Filtering criteria is in KB
DKIM verification result	DKIM verification is successful, DKIM verification failed	None
True Source IP	Is, Is not	None
Digital Fingerprinting analysis result	Is spam, Is clean	None
LexiRules analysis result	Is spam, Is clean	None
Heuristics analysis result	Equals, Is less than, Is greater than	Enter a floating-point value from 0 - 25. For example, the value 6 corresponds to a heuristics analysis level of Medium.
Email hybrid service analysis result (available only when your subscription includes the Email Hybrid Module)	Equals, Is less than, Is greater than	Enter a floating-point value from 0 - 25. For example, the email hybrid service uses a threshold value of 6 to designate a message as spam.

You can change the order of your filter conditions by marking the check box next to the filter in the Filter Conditions list and clicking **Move Up** or **Move Down**.

Delete a set of filter conditions from the list by marking the check box next to the filter and clicking **Remove**.

Note

You can use the Add (or Edit) Rule page to add a rule for a custom content filter. You must have already defined a custom content filter before you attempt to add a custom content rule. See *Adding a rule*, page 143, for information.

URL analysis

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

URL analysis examines email content for embedded URLs and classifies them according to a Forcepoint database of known spam URLs. Select the URL analysis filter type in the **Main > Policy Management > Filters > Add** (or **Edit**) **Filter** page, and then select the URL categories that you want the filter to detect in the Filter Properties area categories list. When the filter detects a URL in a message from a selected category, it applies any configured filter response.

This filter is available only when your system includes a Forcepoint Web protection solution and a download server is configured. See *URL analysis with Forcepoint Web protection solutions*, page 47, for more information about integrating with Forcepoint Web solutions.

Select the URL categories you want the filter to detect in the **URL Categories** list by marking the appropriate check boxes. Use the **select all** or **unselect all** link shown when a major category is expanded to select or deselect all the "child" categories for that major category. Mark the **All** check box to select all URL categories in the list.

When the URL analysis filter triggers, the default action calls for dropping a message and saving it to the spam queue, where it may be released and delivered by a Personal Email Manager user. As a result, a message that contains a malicious link may be delivered to an inbox in your network.

You may not want a malicious URL to be available to a Personal Email Manager user. For this situation, you can create and configure multiple URL analysis policy rules to detect and handle messages that may contain malicious URLs so that they cannot be released by a Personal Email Manager end user. When you configure a URL Analysis filter for this case, ensure that all **Security** URL categories are selected in the URL Categories list. Open the **Security** category in the tree and click **select all**. See *Managing filter actions*, page 134, to create a URL analysis filter action for handling email that may contain a malicious URL.

Note

A filter action option of "Resume message analysis" is also available so that message analysis can continue after a URL match is detected. See *Creating and configuring a filter action*, page 135, for information.

Configure any of the following filter responses:

- **Replace matching URLs with.** Mark this check box to enable the filter to replace a URL in a message from a target category with a text string. Enter the

replacement text in the entry field to the right of the check box (maximum length is 128 characters).

> **Note**
> When a matching URL is detected during message analysis, the rest of the message is not examined by the URL filter and a subsequent URL may not be replaced. For example, if a URL is detected in a message header, the message body is not analyzed, and a URL in the message body will not be detected and replaced.

- **Bypass URL analysis if message size exceeds.** If you want message size to determine whether URL analysis is bypassed, mark this check box and enter a message size in KB (default is 128).

Dashboard charts summarize the instances of embedded URLs that are detected. See *Available dashboard charts*, page 14, for the names of these charts. A URL Analysis message type appears in the message type or message analysis result fields in presentation reports and dashboard charts.

Antivirus

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

Antivirus analysis checks email and any attachments for the presence of email-borne viruses and threats.

If your subscription includes the Email Hybrid Module, you can mark the **Use hybrid service analysis results** check box to use the email hybrid service analysis score in addition to the on-premises email protection system antivirus analysis.

Configure how you want the filter to examine messages for viruses from among the **Filter analysis** options:

- **Treat errors as infected**. If antivirus analysis encounters errors, the email is handled as if it is infected. The default setting is on.
- **Treat encrypted files as infected**. A message that is encrypted in a way that the antivirus engine does not understand is treated as infected. The default setting is on.
- **Analyze message body for viruses**. Message content is analyzed for embedded malicious scripts or attachments that cannot be examined properly. If message format problems cause attachments to be seen as part of the message body, the attachments are analyzed and viruses are detected. Default setting is off.

The **Main > Policy Management > Filters > Add** (or **Edit**) **Filter** page includes the following types of analysis:

- **Standard analysis.** Performs standard email content and attachment analysis for virus threats
- **Advanced analysis.** Performs email attachment analysis for Microsoft Office documents.

You may select either one or both types of analysis to perform, along with the sensitivity level of each analysis type. If you select both types of analysis, standard analysis is performed first, then advanced analysis. The higher the sensitivity level, the larger the volume of email that is designated as virus. Note that enabling the advanced antivirus engine may affect system performance.

Configure 1 of the following filter responses:

- **Remove infected attachments.** Deletes the attachment that triggers the antivirus filter.
- **Take no action.** This is the default action. The attachment and virus are stored in a predefined location (see *Creating and configuring a filter action*, page 135, for information). If required, a message may be sent to the administrator stating that a virus has been found.

You may also add a notification to a suspected virus email, to alert a recipient that the message may be infected. Use the **Advanced** settings to configure the notification function:

1. Mark the **Notify recipient** check box to enable the notification function.
2. Enter the desired notification text in the entry field below the check box (maximum length of 8192 characters total, up to 990 characters per line; a line break is 2 characters).
3. Specify whether the notification should appear at the top of the message or at the bottom. Default location is at the top of the message.

Antispam

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

The antispam analysis function checks email for various characteristics of spam. If the email hybrid service is enabled and configured, it performs antispam analysis as well. (Email Hybrid Module is required.) If email hybrid service is not configured or available, a combination of other on-premises tools is used for effective antispam analysis.

The email hybrid service analyzes incoming email and blocks any message that it recognizes as spam. Mail that the hybrid service allows into the system for processing includes a header that contains an analysis result score. The email system uses this score to determine how to handle the message. If that score exceeds a specified spam threshold, the email system treats the message as spam and handles it according to applicable policy. In this case, the on-premises email protection software does not perform its own, separate antispam analysis.

Email hybrid service must be configured and running for this option to be displayed. In the **Email Hybrid Service Analysis** box, mark the **Use email hybrid service analysis with a threshold score for spam of** check box to enable email hybrid service spam scoring. Select a spam score from the drop-down list (floating point number between 0 and 20; default is 6).

If this check box is not marked (the default) or email hybrid service is not enabled, the on-premises software performs a complete antispam examination using any or all of the following tools in the Filter Properties Tools list.

- **Digital Fingerprinting analysis.** When enabled, digital fingerprint analysis checks content for any digital fingerprint of known spam.
- **LexiRules analysis.** When enabled, the LexiRules tool analyzes email content for word patterns commonly found in spam.
- **Heuristics analysis.** When enabled, heuristics analysis checks the message header or content for spam characteristics.

  Set the heuristics analysis sensitivity level, from lowest to highest (default is Medium).

If you want message size to determine whether antispam analysis is bypassed, mark the **Bypass antispam analysis if message size exceeds** check box and enter a message size in KB (default is 1024).

Commercial bulk email

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

Unlike spam email, commercial bulk email is often solicited by its recipients, sometimes inadvertently. For example, a user might neglect to clear a check box to "Share my personal information with selected partners" on a typical "opt out" privacy rights form. The commercial bulk email filter can analyze a message to determine whether it was sent from a third-party bulk email management company or directly from a business.

If your subscription includes the Email Hybrid Module, you can activate commercial bulk email analysis as part of the email hybrid service pre-filtering process. The results of pre-filtering are added in the message header passed to on-premises email protection software, which uses the hybrid service score to determine how the message is processed. Mark the **Use the results of the email hybrid service analysis for on-premises commercial bulk email analysis** option to enable this function.

After you select the commercial bulk email filter type, choose the sensitivity level for the filter:

- **Normal: Analyze email source.** Use this option if you want the filter to detect email only from indirect (third-party) sources of bulk email (default).
- **High: Analyze email source and content.** Use this option if you want the filter to detect both direct and indirect sources of bulk email.

If you want message size to determine whether commercial bulk email analysis is bypassed, mark the **Bypass commercial bulk email detection if message size exceeds** check box and enter a message size in KB (default is 1024).

A commercial bulk default filter action can be used along with this filter. See *Managing filter actions*, page 134, for information.

Advanced file analysis

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

Advanced file analysis is a cloud-hosted or on-premises sandbox for deep content inspection of types of files that are common threat vectors (for example, document, executable, data, or archive files). Use the advanced file analysis filter to configure file type analysis for your network.

The cloud sandbox capability is available only if your subscription includes the Email Sandbox Module. For on-premises analysis, you need to deploy a separate Threat Protection appliance environment.

Configure your advanced file analysis platform on the **Settings > General > Advanced File Analysis** page. You may select only one platform for advanced file analysis. See *Selecting advanced file analysis platform*, page 47, for information.

When you configure an advanced file analysis filter, the platform selected on the Advanced File Analysis page is reflected in the Add/Edit Filter page **File analysis platform** entry field. Available filter settings depend on the platform used, as noted in the following sections.

The filter can be used in either monitor or enforce mode, with an option for sending a notification message when the enforce mode is active, the filter is triggered, and the attachment is sent to advanced file analysis. You can define conditions that, when met, allow a message to bypass the advanced file analysis filter.

After you select the advanced file analysis filter type and enter a name and description, specify 1 of the following operational modes for the filter:

- **Monitor** (default). Message is delivered to its recipient, and a copy is sent to advanced file analysis. If analysis determines that the attachment is clean, no report is returned. If analysis determines the attachment is malicious, the message is copied to a specified queue. A notification email regarding the analysis result can be sent.

  The corresponding filter action should be configured to ensure that the email message that triggered the filter is delivered to its recipient along with the attachment (**Main > Policy Management > Actions)**.
- **Enforce.** Message is held in a queue until advanced file analysis is performed. If analysis determines that the attachment is clean, message processing is resumed. If analysis determines the attachment is malicious, the email is quarantined. A notification email regarding the analysis result can be sent.

  The corresponding filter action should be configured to ensure that the email message that triggered the filter is dropped and saved to a specified queue (**Main > Policy Management > Actions)**. Default queue is the virus queue.
- **Enforce and notify.** Message is held in a queue until advanced file analysis is performed, and an email notifying the recipient that analysis is underway can be sent. Mark the **Send enforcement notification** check box to configure this message, which contains the original message as an attachment. The message attachment is handled as follows:

- Some file types are converted to plain text (for example, .pdf, .doc/.docx, .xls/.xlsx, and .ppt/.pptx).
- Files of other types are removed and only the filename appears in the message (for example, .exe and archive files).

The corresponding filter action should be configured to ensure that the email message that triggered the filter is dropped and saved to a specified queue (**Main > Policy Management > Actions)**. Default queue is the virus queue.

The email notification contains the following components:

- **Sender.** Identify the notification message sender, from among the following options:
  - Original email sender
  - Administrator (default). If you use this option, you must configure a valid administrator email address in the **Settings > General > System Settings** page (see *Setting system notification email addresses*, page 56).
  - Custom. If you choose this option, you can designate only 1 sender address.
- **Recipient.** Identify the notification message recipient, from among the following options:
  - Original email recipient
  - Administrator. If you use this option, you must configure a valid administrator email address in the **Settings > General > System Settings** page (see *Setting system notification email addresses*, page 56).
  - Custom. If you choose this option, you can designate 1 or more recipient addresses, separated by semicolons.
- **Subject.** Enter the subject that you want to be displayed when the notification is received.
- **Content.** Enter the text that you want to be displayed in the notification message body.
- **Attachment.** Specify whether you want to include the original message as an attachment to the notification message. Select from among the following:
  - Do not attach message (default)
  - Attach filtered message

See *Creating and configuring a filter action*, page 135, for information about configuring an action for the advanced file analysis filter.

Select the file types you want the cloud-hosted file sandbox to find and analyze by marking the appropriate check boxes. This option is not available for the Threat Protection platform.

You can configure bypass options for messages that you want to skip advanced file analysis. Click **Add** in the bypass conditions section and specify the following information:

- **Condition name.** Specify a name for each set of bypass conditions.

- **Sender email address/domain.** Enter an individual email address or domain. Use an asterisk (*) for wildcard entries, and separate multiple entries with a semicolon (;).
- **Attachment filename keyword.** Enter a character string that is included in the attachment filename.

Edit an existing bypass condition set by clicking the condition name in the bypass conditions table.

If you want message size to determine whether advanced file analysis is bypassed, mark the **Bypass advanced file analysis if message size exceeds** check box and enter the target file size. Enter a value from 1 to 32 for the cloud-hosted file sandbox (default is 32 MB). For Threat Protection, enter a value that equals the maximum file size accepted by the Threat Protection appliance.

Spoofed email

The spoofed email filter can help determine the validity of message senders and reduce instances of sender impersonation via a set of header sender comparisons and SPF, DKIM, and Sender ID analysis results.

Spoofed email filter message header comparisons involve the From:, envelope Sender:, and Reply-To: fields. The From: field indicates the entity (e.g., person or mailbox) that is responsible for authoring the message. The envelope Sender: field contains information about the entity responsible for the actual transmission of the message (e.g., someone who sends a message on behalf of another person). If present, the Reply-To: field specifies the address to which a message reply should be sent. If Reply-To: is not present, a reply is sent to the From: address.

Note

The spoofed email filter provides SPF analysis in addition to the inbound relay SPF email rejection options in **Settings > Inbound/Outbound > Mail Routing** page. You should consider the following issues regarding the use of these two SPF-based analyses:

- A message that triggers a mail routing SPF connection rejection option and is dropped will not be processed by the spoofed email filter and email content is not analyzed.
- When a message triggers a mail routing SPF connection rejection option but is not dropped, the SPF score from this analysis is stored for use by the spoofed email filter.

After you select the spoofed email filter type and enter a name and description on the **Main > Policy Management > Filters > Add** (or **Edit**) **Filter** page, you can configure the following header comparisons:

- **Sender address comparison** (default setting). Mark the check box to enable the selection of any of the following options:
  - **Verify that the From: address matches the envelope sender address** (default setting)
  - **Verify that the From: address matches the Reply-To: address**
  - **Verify that the envelope sender address matches the Reply-To: address** (default setting)

  The filter is triggered if any selected address comparison fails, and the message sender is presumed to be forged.

Note

When an envelope sender has been changed as a result of an address rewriting rule (**Settings > Inbound/Outbound > Address Rewriting**), the spoofed email filter uses the original envelope sender address rather than the rewritten address for SPF analysis.

For other checks like header comparison and bypass conditions, the rewritten envelope sender is used.

Advanced options for sender authentication analysis allow the configuration of filter conditions using combinations of SPF, DKIM, and SIDF analysis results. Click **Advanced** to open these options, and enable the use of these conditions by marking the **Sender authentication analysis** check box. Default condition sets include the following (operator between SPF and DKIM results is **AND**):

Condition Name	SPF Result	DKIM Result	Sender ID Validation
Default Condition 1	Fail **or** SoftFail	Fail **or** Invalid **or** TempError	Enabled
Default Condition 2	PermError **or** TempError **or** None **or** Neutral	Fail	Enabled

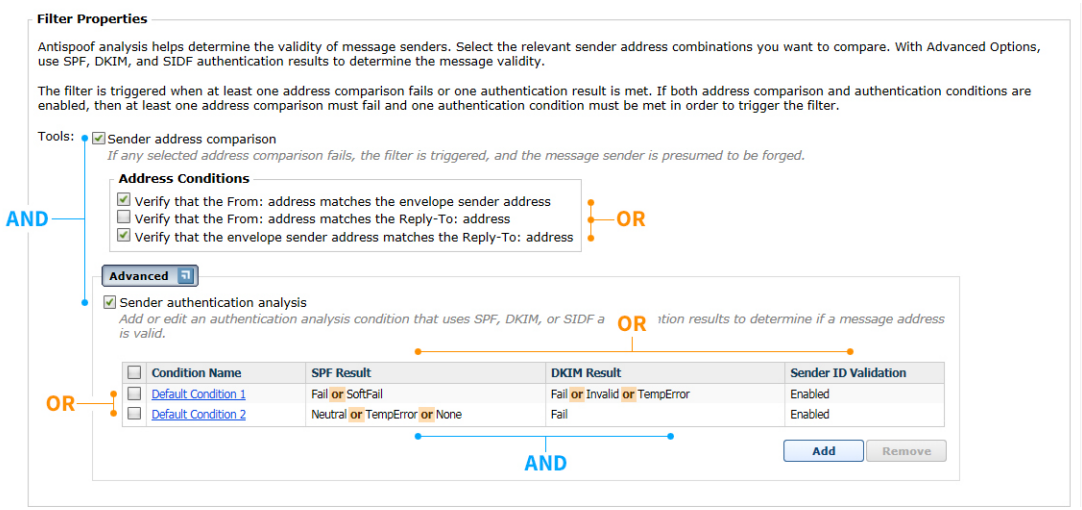
For Default Condition 1, the filter is triggered if:

- The SPF result is either Fail **or** SoftFail **AND** the DKIM result is Fail, Invalid, **or** TempError. The operator between SPF results and sender ID validation is **OR**.

For Default Condition 2, the filter is triggered if:

- The SPF result is PermError, TempError, None, **or** Neutral **AND** the DKIM result is Fail. The operator between SPF results and sender ID validation is **OR**.

The following graphic summarizes the relationships among the spoofed email filter options:



If both sender address comparison and sender authentication condition tools are enabled, then at least one address comparison must fail **and** one authentication condition must be met in order to trigger the filter.

Click a condition name to edit an existing condition, or click **Add** to create a new set of conditions in the Add Condition dialog box. Use the following steps to add or edit a spoofed email condition:

1. If you are adding a new condition, enter a name in the **Condition Name** entry field. For an edit operation, this field is prefilled with the existing condition name.
2. Select the SPF results, if any, that you want the filter to detect. The operator between multiple SPF result selections is "**or**."
3. Select the DKIM results, if any, that you want the filter to detect. The operator between multiple DKIM result selections is "**or**."

> **Important**
> The operator that joins selected SPF and DKIM results in a condition rule is "**and**."

4. Mark the **Validate Sender ID** check box to enable additional sender authentication. Selected SPF results are also used if the Sender ID option is selected.

   You must have selected at least 1 SPF result in order to use the sender ID validation function. The operator between these 2 options is "**or**."

   For example, when both SPF and sender ID options are selected, if a message passes the SPF check but fails sender ID validation, the condition is considered failed. If only SPF options are selected, that same message passes the SPF check, and the condition is considered passed.

5. Click **OK**.

Disclaimer

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

The disclaimer filter automatically adds defined text to the beginning or end of a message. Specify the desired text in the Filter Properties section of the Add Filter or Edit Filter page for the Disclaimer filter.

A primary disclaimer may be written in any language, as long as the email message supports the same character set.

The secondary disclaimer must be written in English, to be used when the email does not support the primary disclaimer character set.

Disclaimer text may be between 4 and 8192 characters in length. A line break uses 2 characters.

Specify where the disclaimer should appear in the email:

- **Beginning of message**
- **End of message**

Mark the **Enable Report Spam feature** check box to allow message recipients to report a message as spam. The link in the disclaimer text sends the recipient to the Personal Email Manager, where the message can be reported from the quarantined message list to Forcepoint as spam.

Managing filter actions

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

A filter action determines a message's final disposition. The email protection software analyzes messages and their attachments, and then performs an action based on applicable policy settings. Actions are created in the **Main > Policy Management > Actions** page. You can add a defined action to a policy rule when you configure your email policies.

In addition to defining an action used in an email policy, you can create an action for use in an email DLP action plan in the Data module. See *Data Security Manager Help* for information about DLP action plans.

For most network configurations (i.e., single standalone appliance or single appliance cluster), the property settings available for creating an action for an email DLP policy are the same as those for a policy action configured for the email protection software. However, if your network includes multiple standalone appliances or multiple clusters, the DLP policy action settings available when an action is initially created are limited. Unless otherwise noted, the following procedures apply to both email and DLP policy actions.

Create a new filter action by clicking **Add** and selecting action properties (see *Creating and configuring a filter action*, page 135).

You can remove a filter action by marking the check box to the left of the filter name to select it and clicking **Delete**. You can delete a filter action only if its current status is **Not referenced**, which means that the action is not currently used in a policy rule or action plan. A filter action that is currently referenced by a filter or action plan does not have a check box for selection. You cannot remove a default email filter action.

The following default actions are available:

- **Virus.** Drop the filtered message and save the original message to the virus queue. Allow a Personal Email Manager end user to view and manage the message.
- **URL Analysis.** Drop the analyzed message and save the original message to the spam queue. Allow a Personal Email Manager end user to view and manage the message.

  You can configure multiple URL analysis rules if you are concerned that a Personal Email Manager end user may inadvertently release email that contains a malicious URL. In that case, you can set the following characteristics for your action:

  1. Set the action taken to **Drop Message**.
  2. In the Drop Message Options section, set the **Save the original, unanalyzed message to a queue** drop-down list to the **url-analysis** default queue.
  3. Select **Do not display** for the Personal Email Manager end-user portal option, to prevent an end user from controlling message delivery.
  4. Click **OK** to save the new action.
- **Spoof.** Deliver the analyzed message and add “POSSIBLY SPOOFED:” to the message subject. Allow a Personal Email Manager end user to view and manage the message.
- **Spam.** Drop the analyzed message and save the original message to the spam queue. Allow a Personal Email Manager end user to view and manage the message.
- **Commercial Bulk.** Deliver the analyzed message and add “COMMERCIAL:” to the message subject. Allow a Personal Email Manager end user to view and manage the message.
- **Advanced File Analysis.** Drop the analyzed message and save the original message to the virus queue. Send a notification message without attaching the original email to the original email sender.

Creating and configuring a filter action

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

You can add a filter action and configure its properties on the **Main > Policy Management > Actions** page. Click **Add** to open the Add Action page and enter an action name.

In the **Used by** drop-down list, select the policy type for which this action can be used: **Email** or **Data**. Your selection here determines which action properties are available when you create the action.

Email policy action options include:

- Deliver message (default)
- Resume processing
- Drop message

DLP policy action options include:

- Deliver message (default)
- Drop message

The deliver message option includes the same action properties for both email and DLP actions. However, in some cases, their behavior for an email policy action and a DLP policy action in a single appliance/single cluster network is different from that for a DLP policy action that is created in a multiple appliance/multiple cluster environment.

Deliver message

Select **Deliver message** when you want an email message delivered to its intended recipient. This option is the default selection for both an email policy action and a DLP action.

If you choose this option, you can also define the following message delivery options:

- **Enable header modification.** Mark this check box to open a set of header modification condition entry fields. Options include the following:

Condition	Parameters
Add or rewrite header value	Header name, To value
Remove header	Header name
Remove header if condition matches	Header name, If header contains the value
Find and replace header value	Header name, Find, Replace with
Add or append to header value	Header name, Add/append value
Add or prepend to header value	Header name, Add/prepend value

  Click the icons at the end of each condition line to delete the current header modification condition or to add a new condition below the current condition.
- **Bcc the original unanalyzed message to.** Enter at least 1 email address to which you want a blind copy of the unanalyzed message sent, for example, the email system administrator. Separate multiple email addresses with a semicolon.
- **Delay message delivery until.** Specify a day and time for a delayed message delivery. You may select this option if you want to delay the delivery of a message for some reason, for example, to send a large volume of marketing email at a time

of low corporate email activity. This action option is recommended for use with a Custom Content filter in a policy rule. See *Custom content*, page 123, for information about a custom content filter.

- **Use IP address**. Specify an appliance IP address from the drop-down list for message delivery. Only standalone appliances are included in the IP address list.

  Note

  This option is available for a DLP action being created in a multiple standalone appliance environment. The default setting is the appliance E1 or P1 interface.

  This setting may be customized for each standalone appliance.

  The IP addresses in the list are configured in the Forcepoint appliance. (See the *Forcepoint Appliances Getting Started Guide* or *Using the X-Series Command Line Interface (CLI)* for information.)

  This feature is useful if you want to route a large volume of outbound email. This action option is recommended for use with a Custom Content filter in a policy rule. See *Custom content*, page 123, for information about a custom content filter.

- **Deliver email messages based on domain-based route.** Specify message delivery via a defined domain-based route. Select the desired route from the drop-down list. You can also modify the selected route by clicking **Edit Route**.

  Note

  This option is available for a DLP action being created in a multiple appliance/multiple cluster environment. The default setting is the domain-based route (**Settings > Inbound/Outbound > Mail Routing**). Change the default setting by selecting **Add Domain Based Route** in the drop-down list.

  This setting may be customized for each appliance.

- **Save the original message to a queue.** Send the message to a specified message queue for further processing. Select the **Add Queue** option to add a new queue for this filter action.

  Note

  This option is available for a DLP action being created in a multiple appliance/multiple cluster environment. The default setting is **data-security**. Change the default setting by selecting **Add Queue**.

  This setting may be customized for each appliance.

- **Personal Email Manager portal options.** This option is enabled only when the **Save the original message to a queue** option is marked. Specify how the queued

message is handled in the Personal Email Manager end-user facility by selecting 1 of the following:

- **View and manage messages.** Allow the end user to view the message and perform any action available in the Personal Email Manager end-user tool.
- **Do not display.** Ensure the message does not appear in the Personal Email Manager end-user portal.
- **Message log only.** Pertinent information about the message appears in the Personal Email Manager end-user portal, but the end user has only limited access. The user cannot view message content; deliver, download, or forward the message; or add the address to the personal Always Block or Always Permit lists.

Resume processing

Select **Resume processing** when you want to continue message analysis using the next filter in sequence if the current filter is triggered (for example, after a URL match is detected in a message). If this option is the final triggered filter's action, the message is delivered.

Additional message action options are the same as for message delivery.

Drop message

Select **Drop message** when you want to delete a message without delivering it to its intended recipient. This option is available for both email and DLP policy actions.

You can forward a dropped message by marking the **Forward to** option and entering at least 1 email address.

You can also configure the **Save the original message to a queue** option to send the message to a specified message queue for further processing. Marking this check box enables the **Personal Email Manager portal options** described for the message delivery filter action.

Note

This option is available for a DLP action being created in a multiple appliance/multiple cluster environment. The default setting is **data-security**. Change the default setting by selecting **Add Queue**.

This setting may be customized for each appliance.

Drop attachment

Select **Drop attachment** if you want to remove an attachment from an email message as part of the policy action. This option is available only for DLP policy actions.

Send notification

The **Send notification** option is available for configuring a predefined notification about an email sent to specified recipients. The notification contains the following components:

- **Sender.** Identify the notification message sender, from among the following options:
  - Original email sender
  - Administrator (default). If you use this option, you must configure a valid administrator email address in the **Settings > General > System Settings** page (see *Setting system notification email addresses*, page 56).
  - Custom. If you choose this option, you can designate only 1 sender address.
- **Recipient.** Identify the notification message recipient, from among the following options:
  - Original email sender
  - Original email recipient
  - Administrator. If you use this option, you must configure a valid administrator email address in the **Settings > General > System Settings** page (see *Setting system notification email addresses*, page 56).
  - Custom. If you choose this option, you can designate 1 or more recipient addresses, separated by semicolons.
- **Subject.** Enter the subject that you want to be displayed when the notification is received.
- **Content.** Enter the text that you want to be displayed in the notification message body.
- **Attachment.** Specify whether you want to include the original message as an attachment to the notification message. Select from among the following:
  - Do not attach message (default)
  - Attach original unanalyzed message
  - Attach analyzed message

Editing an existing filter action

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

You can edit an existing filter action by clicking the action name on the **Main > Policy Management > Actions** page. The Edit Action page opens, displaying the current action properties. Modify any of the options listed in *Creating and configuring a filter action*, page 135.

You can also use this operation to change any default property configured when you created a data action. See *Resume processing*, page 138, for default setting details.

Managing policies

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

An email policy is applied based on defined sender/recipient conditions and the direction of the email. You can apply a different policy to different groups of senders and recipients. For example, you might apply a policy to a marketing department group in your organization and a different policy to a human resources group. After you define a set of senders and recipients in a policy, you can add the policy rules to apply when the sender/recipient conditions of the email match the policy.

Policy rules comprise the filters and filter actions that determine how a message that matches a policy's sender/recipient conditions is handled. Filters provide the basis for email analysis, and filter actions determine the final disposition of a message when it triggers a particular filter. After you have created and configured filters and filter actions, they are available for inclusion in your policies. See *Managing filters*, page 121, and *Managing filter actions*, page 134, for information about configuring filters and filter actions.

Three types of policies are available, depending on the direction of the email—inbound, outbound, or internal. Message direction is determined on the basis of an organization's protected domain addresses:

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

One predefined default policy is available for each email direction, along with a default data loss prevention (DLP) policy for each direction.

Data loss prevention policies may be applied to email in any direction. These policies are configured in the Data module of the TRITON Manager and are enabled or disabled in the Email module. You need to register the Email module with the Data module and click **Deploy** in the Data module for the policies to be active. See *Enabling data loss prevention policies*, page 141 for details.

Changing policy order

After you add a policy, you can select it and use the **Move Up** and **Move Down** buttons to move it up or down in the policy list in order to specify when the policy is applied. When message conditions match a policy, subsequent policies in the list are not applied.

You cannot change the order of default policies. They are applied last when a message matches no other policy.

Deleting a policy

You can remove a policy by marking the check box next to the policy name on the Policies page and clicking **Delete**. Note that a default policy cannot be deleted.

Enabling data loss prevention policies

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

In addition to creating and enabling policies that protect your email system from email threats, you can enable DLP policies that can detect the presence of sensitive data in your organization's email and execute appropriate actions to prevent data loss. You can use DLP policies for inbound, outbound, and internal email.

Email DLP policies must be 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 detailed information.

You should create a DLP policy in the Data module if you want to use message encryption. Ensure the policy has an action plan of "encrypt." See *Handling encrypted messages*, page 114, for information about email encryption options.

You can also create filter actions for use in a DLP action plan. See *Creating and configuring a filter action*, page 135, for information about configuring a DLP filter action.

Data loss prevention policies are enabled by default in the Email module. However, the Email module must be registered with the Data module before the policies are applied to email. See *Registering the Email DLP Module*, page 41, for instructions on how to register with the Data module.

If you need to enable DLP policies for some reason, click the DLP policy name on the **Main > Policy Management > Policies** page for inbound, outbound, or internal email, and set the following options in the Edit Policy page:

- **Status:** Enabled or Disabled. Enable or disable the DLP policy. Data loss prevention policies are enabled by default.
- **Mode:** Monitor or Enforce. Select **Monitor** if you want the data loss prevention function to simply monitor your email, and select **Enforce** if you want to apply DLP policies to your email.
- **Notification.** Add a notification to a message when an email attachment to that message has been dropped as a result of a DLP policy.
  1. Mark the **Send notification when a message attachment is dropped** check box to enable the sending of notifications.
  2. Enter the notification message text.
  3. Determine whether the notification text appears above or below the message body of the mail whose attachment was dropped.

Note

A message that triggers a DLP policy whose action is Quarantine is isolated in the Data module quarantine queue, not in an Email module queue. The message can be released for delivery by the Data module.

Adding or editing a policy

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

Use the **Main > Policy Management > Policies** page to create a new inbound, outbound, or internal policy.

1. Click **Add** to open the Add Policy page and enter a unique **Policy name**. The policy name must be between 4 and 50 characters long. Use of the following special characters in the policy name is not recommended:

   * < > { } ~ ! $ % & @ # . " | \ & + = ? / ; : ,

   Policy names can include spaces, dashes, and apostrophes.
2. Enter a clear and concise **Description** of the policy.

   The special character recommendations that apply to policy names also apply to descriptions.
3. Select a status of **Enabled** or **Disabled** for your policy.
4. Define the order in which this policy is applied in the **Order** field.

   By default the new policy is placed at the top of the list. You cannot have multiple policies with the same order number. If you select a number that is already in use, the policy that currently has that number and all those below it move down 1 place in the list.
5. Define your **Sender/Recipient Conditions**.

   By default, each new policy contains a sender/recipient condition that applies the policy to all email senders and recipients. To add more conditions click **Add**, and then see *Adding Sender/Recipient Conditions*, page 142.

   Note

   You must define at least 1 sender/recipient condition. A policy that does not contain a sender/recipient condition will not be applied.
6. Edit the available **Rules** to tailor the filters and actions to this policy. Click a rule name, and then see *Editing rules*, page 144.
7. Click **OK** to save your policy.

Adding Sender/Recipient Conditions

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

Use the **Add Policy > Add Sender/Recipient Condition** page to specify the senders and recipients to which this policy applies. You can make the policy as wide-ranging as required, for example applying it to all users, or all users receiving mail in a particular domain, or specific email addresses only.

For each sender/recipient condition, you must select a **Sender Source** and **Recipient Source**:

- If you select **Local Address**, enter the sender or recipient email addresses to use with the policy. You can use the asterisk wildcard to specify combinations, for example:
  - *.mycompany.com applies the policy to all users with a mycompany.com email address
  - *sales@mycompany.com applies the policy to a subset of all email addresses in mycompany.com, such as us_sales@mycompany.com and uk_sales@mycompany.com
  - john.doe@mycompany.com applies the policy to a specific user.

  To apply the policy to all email addresses, enter an asterisk (*).
- If you select **User directory**, select the directory source from the drop-down list. You must set up a user directory to connect to before selecting this option. Select **Add User Directory** to create a new directory source.
- If you select **Domain group**, select the domain source from the drop-down list of existing domain groups or add a new domain group by selecting **Add Domain Group**.

Once you have made your selections, click **OK** to return to the Add or Edit Policy page.

Deleting Sender/Recipient Conditions

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

To delete a sender/recipient condition, on the Add or Edit Policy page check the box next to the condition ID and then click **Delete**.

A policy should contain at least 1 sender/recipient condition.

Adding a rule

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

A policy rule comprises the filter applied to a message that matches a policy's sender/recipient conditions and the action taken when that message triggers the filter. The following default rules are available:

- **Antivirus.** Rule is enabled and uses the default virus filter and filter action.
- **URL Analysis.** Rule is enabled and uses the default URL analysis filter and filter action.

  You can configure multiple URL Analysis rules if you want to use settings other than the defaults. See *URL analysis*, page 125, and *Managing filter actions*, page 134, for more information.
- **Antispoof.** Rule is enabled and uses the default spoofed email filter and filter action.
- **Antispam.** Rule is enabled and uses the default spam filter and filter action.
- **Commercial Bulk.** Rule is enabled and uses the default commercial bulk filter and filter action.

- **Advanced File Analysis.** Rule is enabled and uses the default advanced file analysis filter and filter action.
- **Disclaimer.** Rule is disabled, but when enabled, uses the default disclaimer filter.

You may create a new rule in combination with a custom content filter or a URL analysis filter.

Use the following steps to add a policy rule with a custom content filter:

1. Click **Add** in the Rules section to open the Add Rule page.
2. Enter a name for your rule in the **Rule Name** entry field.
3. Select the desired policy status, **Enabled** (the default) or **Disabled**.
4. Select the order in which you want your rule applied. By default, a new custom content rule is created in the first position. Use the **Move Up** and **Move Down** buttons to adjust custom content rule order. The Disclaimer rule is always applied last.
5. Select a custom content or URL analysis filter from the **Filter name** drop-down list. If you have not created either filter type, this list contains only the entry **Add filter**. Choose this entry to open the Add Filter page to define a new custom content or URL analysis filter. See *Creating and configuring a filter*, page 122, for information.
6. Configure a filter action in 1 of the following ways:
   - Select a default filter action from the **Action name** drop-down list. If you want to change the default action settings, click **Edit**.
   - You can also create a new action for your rule by selecting **Add Action** from the drop-down list.

   See *Creating and configuring a filter action*, page 135, for information.

Editing rules

Click a rule name, and use the **Add Policy > Edit Rule** page to define what happens to an email message that matches the sender/recipient conditions and triggers the policy. This page contains the filter and filter action that currently define the rule that you clicked. You can also define message sender/recipient conditions that, when met, allow a message to bypass the filter.

Editing the filter

To edit the filter, click **Edit** in the Filter section to open the Edit Filter page. Modify filter characteristics as described in *Creating and configuring a filter*, page 122.

Editing the filter action

To edit the filter action, click **Edit** in the Action section to open the Edit Action page. Modify action options as described in *Creating and configuring a filter action*, page 135.

> **Note**
> Any change you make to existing rule components will be reflected in the filter and action definitions you configured in the **Main > Policy Management > Filters** and **Main > Policy Management > Actions** pages. The changes are not unique to the individual policy.

Adding filter bypass conditions

To add filter bypass conditions, click **Add** in the Filter Bypass Condition section to open the Add Filter Bypass Conditions page. You can create filter bypass entries in the Sender Email Addresses, Recipient Email Addresses, and IP Address Groups sections in 1 of the following ways:

- Add a predefined email address list by clicking **Browse** next to the Email Address File field and navigating to the desired text file. The file format should be 1 email address per line, up to a maximum of 8 addresses.
- Enter an individual email address in the **Email address** field. Click the right arrow button to add the individual entry to the **Email Address List** on the right.
- Select the IP address groups you want to bypass analysis, and click the arrow button to add them to the Added IP Address Groups box. You can also define a new IP address group on this page if desired.

An asterisk (*) may be used in an address as a wildcard.

Click **OK** to save your bypass entries.

You can delete an entry in an Email Address List by selecting it and clicking **Remove**. Export and save an address list as a text file by clicking **Export All**.

You cannot use these settings to bypass a custom content filter.

Editing an existing policy

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

You can edit an existing policy by clicking its name on the Policies page to open the Edit Policy page. Edit the Description, Status, Sender/Recipient Conditions, and Rules as described in *Adding or editing a policy*, page 142. You will not be able to edit the policy name.

You can edit policy order only for a policy you have created. You cannot edit policy order for a default policy.

Managing global Always Block and Always Permit lists

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

Maintaining lists of IP and email addresses that are either always blocked or always permitted can contribute to the efficiency of your email protection system. Bandwidth and time can be saved when trusted mail can bypass some analysis features (including antispam, commercial bulk, and URL analysis).

Note

Mail from addresses in the global Always Permit list is subject to other email analysis, including antivirus analysis, message control, connection control, directory harvest attack, and relay control.

Managing the Always Block List

You can add an IP or email address directly into the Always Block List from the **Main > Policy Management > Always Block/Permit** page. You can also add a predefined IP or email address list, remove individual entries from a list, export a list to your desktop as a text file, and search a list.

Messages from an email address that appears in both the Always Block and Always Permit lists will be permitted. Messages from an IP address that appears in both lists will be blocked.

After you finish adding your address entries, you can export the list as a text file by clicking the **Export All** button and opening your text file or saving it to a desired location.

Remove an individual entry by selecting it in the IP or Email Address List and clicking **Remove**. You can also search your list for entries by entering keywords in the search field and clicking **Search**.

Adding an IP address to the Always Block List

Use the following procedures to add IP addresses to the Always Block list:

1. Click the **Always Block** tab.
2. In the IP Address Block List section of the page, add a predefined IP address list by clicking **Browse** and navigating to the desired text file. The file format should be 1 IP address per line, and its maximum size is 10 MB.
3. You can also enter an individual IP/subnet address in the **IP/Subnet address** field. Click the right arrow button to add the individual entry to the **IP Address List** on the right.
4. Click **OK**.

Adding an email address to the Always Block List

Use the following procedures to add email addresses to the Always Block list:

1. Click the **Always Block** tab.
2. In the Email Address Block List section, add a predefined email address list by clicking **Browse** and navigating to the desired text file. The file format should be 1 email address per line, and its maximum size is 10 MB.
3. You can also enter an individual email address in the **Email address** field. Click the right arrow button to add the individual entry to the **Email Address List** on the right.
4. Click **OK**.

Managing the Always Permit List

You can add an IP or email address directly into the Always Permit List from the **Main > Policy Management > Always Block/Permit** page. You can also add a predefined IP or email address list, remove individual entries from a list, export a list to your desktop as a text file, and search a list.

Email from an address that appears in both the Always Block and Always Permit lists will be permitted. Messages from an IP address that appears in both lists will be blocked.

After you finish adding your address entries, you can export the list as a text file by clicking the **Export All** button and opening your text file or saving it to a desired location.

Remove an individual entry by selecting it in the IP or Email Address List and clicking **Remove**. You can also search your list for entries by entering keywords in the search field and clicking **Search**.

Adding an IP address to the Always Permit List

Use the following procedures to add IP addresses to the Always Permit List:

1. Click the **Always Permit** tab.
2. In the IP Address Permit List section of the page, add a predefined IP address list by clicking **Browse** and navigating to the desired text file. The file format should be 1 IP address per line, and its maximum size is 10 MB.
3. You can also enter an individual IP/subnet address in the **IP/Subnet address** field. Click the right arrow button to add the individual entry to the **IP Address List** on the right.
4. Click **OK**.

Adding an email address to the Always Permit List

Use the following procedures to add email addresses to the Always Permit list:

1. Click the **Always Permit** tab.

2. In the Email Address Permit List section, add a predefined email address list by clicking **Browse** and navigating to the desired text file. The file format should be 1 email address per line, and its maximum size is 10 MB.
3. You can also enter an individual email address in the **Email address** field. Click the right arrow button to add the individual entry to the **Email Address List** on the right.
4. Click **OK**.

Enabling the Dynamic Always Permit List

Enabling the Dynamic Always Permit List function allows some mail exchanged between a sender/recipient address pair to bypass antispam filtering. When mail between a sender to a recipient does not trigger an antispam filter a specified number of times, that sender/recipient address pair is added to the Dynamic Always Permit List. Antispam analysis is not performed on mail between this sender/recipient address pair. When a specified timeout period has elapsed, the address pair is removed from the list.

The **Enable Dynamic Always Permit list** check box is enabled by default in the Dynamic Always Permit List section. The following settings can be modified:

1. In the **Occurrence** field, specify the number of spam-free email exchanges (from 1 to 5) required before a sender/recipient pair is added to the list. Default is 1.
2. In the **Timeout** field, enter a value for the timeout interval in hours (from 1 to 720). Default is 720.

Clear the list manually by clicking the **Clear Dynamic Always Permit List** button. Note that if you disable this function, the list is automatically cleared.

6 Working with Reports

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

Topics:

Configuring Log Database options

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

The Log Database stores the records of email traffic activity and the associated email analysis on that traffic. These data records are used to generate presentation reports of email activity, including size and volume of email messages and identification of senders and recipients. They are also used to generate the status charts on the dashboard.

Administering the Log Database involves controlling many aspects of database operations, including the timing of maintenance tasks, the conditions for creating new database partitions, and which partitions are available for reporting. Use the **Settings > Reporting > Log Database** page to manage Log Database operations.

Click the **OK** button within each section of the Log Database page to save and implement the changes in that section.

Making changes to Log Database settings on 1 appliance applies those changes to all the appliances in your network.

A Log Database Location section at the top of the page lets you enter the IP address\instance or hostname\instance of your Log Database server. By default, the Log Database created at installation is entered. If you chose to encrypt the database connection at product installation, the **Encrypt connection** check box is marked. If

you did not select the encryption option during installation, you can encrypt the database connection by marking the check box here.

Important

You must have imported a trusted SSL certificate to the Log Server machine in order to use SSL for the encryption option. See your database documentation for information about importing a trusted certificate.

Other settings created at installation and displayed here include the designated authentication method (Windows or SQL Server), user name, and password.

Click **Check Status** to determine the availability of the server.

The top of the Log Database Options section displays the name of the active Log Database and a Refresh link. Click **Refresh** to update the information shown on the Log Database page. Be sure you save your settings before you click **Refresh**, because any unsaved changes on the page will be cleared.

Use the Database Rollover Options section of the **Settings > Reporting > Log Database** page to specify when you want the Log Database to create a new database partition, a process called a rollover.

Use the **Roll over every** option to indicate whether database partitions should roll over based on size (MB) or date (weeks or months).

- For size-based rollovers, select MB and specify the number of megabytes the database must reach for the rollover to begin, from 100 - 10240 MB (default is 5120).
- For date-based rollovers, select either weeks or months as the unit of measure, and specify how many full calendar weeks (from 1 - 52) or months (from 1 - 12) to keep in a database partition before a new one is created.

Note

If the rollover begins during a busy part of the day, performance may slow during the rollover process.

To avoid this possibility, some environments choose to set the automatic rollover to a long time period or large maximum size. Then, they perform regular manual rollovers to prevent the automatic rollover from occurring.

See *Creating database partitions*, page 152, for information on manual rollovers.

Keep in mind that extremely large individual partitions are not recommended. Reporting performance can slow if data is not divided into multiple, smaller partitions.

When a new database partition is created, reporting is automatically enabled for the partition (see *Enabling database partitions*, page 153).

Click **OK** to activate changes to the database rollover options.

Configuring maintenance options

Use the Maintenance Configuration section of the **Settings > Reporting > Log Database** page to control certain aspects of database processing, such as the time for running the database maintenance job, some of the maintenance tasks performed, and deletion of database partitions and error logs.

1. For **Maintenance start time**, select the time of day for running the database maintenance job. Default value is 1:00.

   The time and system resources required by this job vary depending on the tasks you select in this area. To minimize any impact on other activities and systems, it is best to run this job during a slow email traffic period.

2. Mark the **Automatically delete a partition with an end date older than** check box, and then specify the number of days (from 1 to 365) after which partitions should be deleted (default is 365).

   Warning

   After a partition has been deleted, the data cannot be recovered. See *Enabling database partitions*, page 153, for an alternative way to delete partitions.

3. Mark the **Enable automatic reindexing of partitions on** check box, and then select a day of the week to have this processing performed automatically (default is Saturday).

   Reindexing the database is important to maintain database integrity and to optimize reporting speed.

   Important

   It is best to perform this processing during a quiet time for email traffic. Reindexing database partitions is resource intensive and time consuming. Reports should not be run during the reindexing process.

4. Mark the **Delete failed batches after** check box and then enter a number of days (from 1 to 365) after which to delete any failed batches. Default value is 20.

   If this option is not checked, failed batches are retained indefinitely for future processing.

   If there is insufficient disk space or inadequate database permissions to insert log records into the database, the records are marked as a failed batch. Typically, these batches are successfully reprocessed and inserted into the database during the nightly database maintenance job.

   However, this reprocessing cannot be successful if the disk space or permission problem is not resolved. Additionally, if the **Process any unprocessed batches** option is not selected, failed batches are never reprocessed. They are deleted after the time specified here.

5. Mark the **Process any unprocessed batches** check box to have the nightly database maintenance job reprocess any failed batches.

   If this option is not checked, failed batches are never reprocessed. They are deleted after the time specified in step 4, if any.

6. Mark the **Delete the log after** check box, and then enter a number of days (1 to 120) after which to delete database error records. Default value is 45.

   If this option is not checked, error logs are retained indefinitely.

7. Click **OK** to activate changes to the maintenance configuration options.

Creating database partitions

Database partitions store the individual log records of email traffic activity. Microsoft SQL Server users can configure the Log Database to start a new partition based on partition size or a date interval.

When partitions are based on size, all incoming log records are inserted into the most recent active partition that satisfies the size rule. When the partition reaches the designated maximum size, a new partition is created for inserting new log records.

When the partitions are based on date, new partitions are created according to the established cycle. For example, if the rollover option is monthly, a new partition is created as soon as any records are received for the new month. Incoming log records are inserted into the appropriate partition based on date.

Database partitions provide flexibility and performance advantages. For example, you can generate reports from a single partition to limit the scope of data that must be analyzed to locate the requested information.

Use the Database Partition Creation section of the **Settings > Reporting > Log Database** page to define characteristics for new database partitions, such as location and size options. This area also lets you create a new partition right away, rather than waiting for a planned rollover.

1. Enter the file path for creating both the data and log files for new database partitions.
2. Under **Initial Size (MB)**, set the initial file size (from 100 to 2048 MB) for both the Data and Log files for new database partitions.

   Note

   Best practice recommends calculating the average partition size over a period of time. Then, update the initial size to that value. This approach minimizes the number of times the partition must be expanded, and frees resources to process data into the partitions.

3. Under **Growth (MB)**, set the increment by which to increase the size (from 8 - 512 MB) of a partition's data and log files when additional space is required.
4. Click **OK** to implement the path, size, and growth changes entered.

Database partitions created after these changes use the new settings.

5. Click **Create** to create a new partition immediately, regardless of the automatic rollover settings.

   To have the new partition use the changes made in this section, be sure to click **OK** before you click **Create**.

   Click the **Refresh** link in the content pane periodically. The Available Partitions area will show the new partition when the creation process is complete.

If you later change the partition file path, you should be sure that the new database folder exists with write privileges.

Enabling database partitions

The Available Partitions section of the **Settings > Reporting > Log Database** page lists all the database partitions available for reporting. The list shows the dates covered by the partition, as well as the size and name of each partition.

Use this list to control what database partitions are included in reports, and to select individual partitions to be deleted.

1. Mark the check box in the **Enable** column next to each partition you want included in reports.

   Use the **Select all** and **Select none** options above the list, as appropriate.

   You must enable at least 1 partition for reporting. Use the **Select none** option to disable all partitions at 1 time so that you can enable just a few.

   Use these options to manage how much data must be analyzed when generating reports and speed report processing. For example, if you plan to generate a series of reports for June, select only partitions with dates in June.

   Important

   This selection affects scheduled reports as well as reports that are run interactively. To avoid generating reports with no data, make sure the relevant partitions are enabled when reports are scheduled to run.

2. Click the **Delete** option beside a partition name if that partition is no longer needed. The partition is actually deleted the next time the nightly database maintenance job runs.

   Warning

   Use this option with care. You cannot recover data from deleted partitions.

   Deleting obsolete partitions minimizes the number of partitions in the Log Database, which improves database and reporting performance. Use this Delete option to delete individual partitions as needed. See *Configuring maintenance options*, page 151, if you prefer to delete older partitions according to a schedule.

3. Click **OK** to activate changes to the available partitions options.

Viewing log activity

Use the Log Activity section of the **Settings > Reporting > Log Database** page to review database maintenance status and event and error messages recorded during the jobs run on the Log Database. Use the **View** drop-down list to select the maximum number of messages to display.

Changing the Log Database

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

The Log Database may need to be changed when 1 of the following situations occurs:

- The database IP address changes.
- The database username and password change.
- The user wants to change authentication settings.
- The user wants to use a named instance.

This type of change must be made in 2 locations: in the **Settings > Reporting > Log Database** page and in the Email Log Server Configuration wizard.

Use the following steps to change the Log Database configuration:

1. Enter the IP address for the new Log Database in the **Settings > Reporting > Log Database** page, in the **Log database** field.
2. Open the Email Log Server Configuration wizard for the Windows machine on which Log Server is installed (**Start > All Programs > Websense > Email Log Server Configuration**).
3. In the Database tab, click **Connection** to open the Select Data Source dialog box.
4. Select the Machine Data Source tab and click **New** to open the Create New Data Source dialog box.
5. Select **System Data Source (Applies to this machine only)**, and click **Next**.
6. Select **SQL Server** and click **Next**.
7. Click **Finish**.
8. In the Create a New Data Source to SQL Server dialog box, enter the server name, description, and IP address of the new SQL Server database in the **Name**, **Description**, and **Server** entry fields and click **Next**.
9. Select **With SQL Server authentication using a login ID and password entered by the user**.
10. Enter the username (**sa**) and a password and click **Next**.
11. In the **Change the default database to** drop-down list, select the **esglogdb76** database and click **Next**.
12. Click **Finish**.

13. In the ODBC Microsoft SQL Server Setup dialog box, click **Test Data Source** to test the server connection.
14. Click **OK**.
15. Enter the new username and password in the SQL Server Login dialog box.
16. In the Email Log Server Configuration wizard Database tab, notice that the ODBC Data Source Name (DSN) field contains the new server name, and click **Apply** to confirm the new configuration.
17. Click **OK** in the warning message. The Log Server must be stopped and restarted for the new settings to take effect.
18. In the Email Log Server Configuration wizard Connection tab, click **Stop** to stop the Log Server service.
19. In the same tab, click **Start** to restart the Log Server service. The new database settings are in effect.

Viewing Log Server settings

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

Use the **Settings > Reporting > Log Server** page to view the Log Server IP address or hostname and port number. Click **Check Status** to determine the availability of the server.

Configuring reporting preferences

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

Reporting preference settings determine how a scheduled report is distributed for review. You can also specify how long to retain a scheduled report and how much warning administrators receive before a report is deleted.

When reporting preferences settings are made on 1 appliance, they are applied to all the appliances in your network.

Use the **Settings > Reporting > Preferences** page to provide information used to distribute completed scheduled reports via email. Also define how long scheduled presentation reports are stored before they are deleted automatically, and how far in advance to warn administrators that reports are due to be deleted.

1. Enter the email address to appear in the From field when scheduled reports are distributed via email.
2. Enter the SMTP server IP address or name for the email server used to distribute scheduled reports via email.
3. Use the **Store reports for** drop-down list to indicate how long scheduled reports are stored on the email management server (default is 5 days).

Note that as you increase the length of time that reports are stored, you affect the amount of disk space required on the email management server. This machine is not an appropriate location for a long-term reporting archive.

Note

If you reduce the report storage time after you have started to generate reports, stored reports that exceed this interval will be automatically deleted.

4. Use the **Give administrators this much warning before a scheduled report is deleted** drop-down list to indicate how much warning (from 1 - 5 days) an administrator should have before a report is deleted (default is 3 days).

   The warning is intended to give administrators time to archive important reports in an appropriate location before they are deleted from the email management server.

5. Click **OK** to implement your changes.

Working with presentation reports

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

Presentation reports include a set of predefined charts and tabular report templates with which you can generate graphical reports of email message traffic activities. You can run a report, customize a report template, or mark a frequently used report as a Favorite. You can run any presentation report immediately, or schedule it to run at a particular time or on a repeating cycle.

Not all report templates can be customized. Report templates that can be customized display a different icon from reports that cannot be customized. If the **Save As** button is enabled when you select a report name, then you can save and edit that report to suit your needs. The **Save As** button is not enabled if you select a report that cannot be customized.

Use the **Main > Status > Presentation Reports** page to generate charts and tabular reports based on templates in the Report Catalog.

The Report Catalog organizes a list of predefined report templates and custom reports into groups. Expand a group to see its corresponding templates and custom reports. Click on a template or report title to see a brief description of what it includes.

To run a presentation report, select the desired report template in the Report Catalog, click **Run**, and then follow the instructions given in *Running a presentation report*, page 162.

To use an existing report as a starting point for creating a report variation, select a custom report, and then click **Save As,** if this button is enabled. If the Save As button is not enabled when you select the report, you cannot edit the template. See *Copying a custom presentation report*, page 157, for detailed instructions.

To make changes to the report filter applied to any custom report you have created, select the report title in the Report Catalog, and then click **Edit**. You cannot modify or delete predefined report templates.

Reports that are used frequently can be marked as Favorites to help you find them more quickly. Just click the report title in the Report Catalog, and then click **Favorite** (see *Working with Favorites*, page 161). Mark **Show Only Favorites** to display only templates that you have marked as Favorites in the Report Catalog.

To delete a custom report you have created, click **Delete**. If a deleted report appears in any scheduled jobs, it will continue to be generated with that job. See *Viewing the scheduled jobs list*, page 168, for information on editing and deleting scheduled jobs.

Note

Changes to report settings made on 1 appliance are applied to all network appliances.

Use the buttons at the top of the page to schedule reports to run later, view scheduled report jobs, and view and manage reports created by the scheduler.

- Click **Job Queue** to see and manage a list of existing scheduled jobs, along with the status of each job. See *Viewing the scheduled jobs list*, page 168.
- Click **Scheduler** to define a job containing 1 or more reports to be run at a specific time or on a repeating schedule. See *Scheduling a presentation report*, page 164.
- Click **Review Reports** to see and manage a list of reports that were successfully scheduled and run. See *Reviewing scheduled presentation reports*, page 169.

Copying a custom presentation report

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

Use the **Save As New Report** page to create an editable copy of a custom report template. Not all templates can be used to create a new custom report. Use the following steps to copy a custom presentation report:

1. Select the custom report in the Report Catalog and, if it is enabled, click **Save As**. If the **Save As** button is not enabled, you cannot copy and customize the selected report.
2. In the **Presentation Reports > Save As New Report** page, replace the report catalog name with a name that will make it easy to identify the new report. (The default name is the name of the original report template, with a number appended to indicate that it is a copy.) The name must be unique and can have up to 85 characters.
3. Click either **Save** or **Save and Edit**.
   - If you click **Save**, you are returned to the Presentation Reports page, where the new report appears in the Report Catalog. To customize the report at any time, select its name, and then click **Edit**.
   - If you click **Save and Edit**, you are taken directly to the Edit Report Filter page. The new report is also added to the Report Catalog.

4. Edit the report filter to modify the report. The report filter controls elements such as which email senders or recipients are included in your custom report.

   For instructions, see *Defining the report filter*, page 158.

Defining the report filter

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

Report filters let you control what information is included in a report. For example, you might choose to limit a report to selected email senders, email recipients, or message analysis results (for example, clean, virus, spam, commercial bulk, or data loss prevention). You can also give a new name and description for the entry in the Report Catalog, change the report title, specify a custom logo to appear, and designate the new report as a Favorite.

> **Note**
> Using a custom logo requires some preparation before you define the report filter. You must create the desired graphic in a supported graphic format and place the file in the appropriate location. See *Customizing the report logo*, page 159.

The filter for predefined report templates cannot be changed. You can edit the filter for a custom report when you create it by choosing **Save and Edit** on the Save As New Report page, or select the report in the Report Catalog at any time and click **Edit**.

The Edit Report Filter page has separate tabs for managing different elements of the report. Select the items you want on each tab, then click **Next** to move to the next tab. For detailed instructions on completing each tab, see:

- *Setting general report options*, page 158
- *Selecting email senders for the report*, page 159
- *Selecting email recipients for the report*, page 160
- *Selecting message analysis results for the report*, page 161

On the Save tab, choose whether to run or schedule the report, and save the report filter. See *Saving the report filter definition*, page 161.

Setting general report options

Use the General tab of the **Presentation Reports > Edit Report** page to configure general report characteristics, as follows:

1. Modify the name that appears in the Report Catalog for this report by entering a new name in the **Report catalog name** entry field. The name can have up to 76 characters.

   This name does not appear on the report itself; it is used only for identifying the unique combination of report format and filter in the Report Catalog.

2. Modify the title that actually appears on the report in the **Report title** entry field. The title can have up to 85 characters.
3. Use the **Description** field to modify the brief report description that appears in the Report Catalog. The description can have up to 336 characters.

   The description should help you identify this unique combination of report format and filter in the Report Catalog.
4. Use the **Logo** drop-down list to specify a logo for your report. The default entry is **Forcepoint Logo**. Select **No Logo** if you do not want a logo displayed on this report.

   The list also contains filenames for custom logo image files if you have created and stored supported image files in the appropriate directory. See *Customizing the report logo*, page 159.
5. Mark the **Save as Favorite** check box to have the report selected as a Favorite.

   The Report Catalog shows a star symbol beside Favorite reports. You can select Show only Favorites on the Report Catalog page to reduce the number of reports listed, which enables you to move more quickly to a particular report.
6. After all entries and selections are complete, click **Next** to open the Senders tab.

Customizing the report logo

By default, presentation reports display the Forcepoint logo in the upper left corner. When you create a custom report and edit its report filter, you can choose a different logo, which you have already prepared and copied to the appropriate directory, as follows:

1. Create an image file in one of the following formats:

   .bmp, .gif, .jfif, .jpe, .jpeg, .jpg, .png, .ttf

   Use a maximum of 25 characters for the image file name, including the file extension.
2. Copy the image file to the following default installation directory (or to your own installation directory):

   C:\Program Files (x86)\Websense\Email Security\ESG Manager\tomcat\PRTemplate\jasperreports\images

   All supported image files in this directory automatically appear in the **Logo** drop-down list on the General tab of the Edit Report Filter page. The image is automatically scaled to fit within the space allocated for the logo. (See *Setting general report options*, page 158.)

Selecting email senders for the report

The Senders tab of the **Presentation Reports > Edit Report** page lets you control which senders are included in the report data. You can select only 1 type of sender for each report.

No selections are required on this tab if you want to report on all senders.

1. Select a sender type from the drop-down list.

2. Set the maximum number of search results from the **Search limits** drop-down list (from 10 - 1000). Default value is 10.

   Depending on the email traffic in your organization, there may be large numbers of users, groups, or domains in the Log Database. This option manages the length of the results list, and the time required to display the search results.

3. Enter 1 or more characters for searching, and then click **Search**.

   Use an asterisk (*) as a wildcard to signify missing characters. For example, J*n might return Jackson, Jan, Jason, Jon, Joan, and so forth.

   Define your search string carefully, to ensure that all desired results are included within the number selected for limiting the search.

4. Highlight 1 or more entries in the results list, and click the right arrow button (>) to move them to the Selected Senders List.
5. Repeat steps 2 - 4 as needed to conduct additional searches and add more senders to the Selected Senders List.
6. To delete an entry from the Selected Senders List, select the entry and click **Remove**.
7. After you are finished making selections or deletions, click **Next** to open the Recipients tab.

Selecting email recipients for the report

The Recipients tab of the **Presentation Reports > Edit Report** page lets you control which recipients are included in the report data. You can select only 1 type of recipient for each report.

No selections are required on this tab if you want to report on all recipients.

1. Select a recipient type from the drop-down list.
2. Set the maximum number of search results from the **Search limits** drop-down list (from 10 - 1000). Default value is 10.

   Depending on the email traffic in your organization, there may be large numbers of users, groups, or domains in the Log Database. This option manages the length of the results list, and the time required to display the search results.

3. Enter 1 or more characters for searching, and then click **Search**.

   Use an asterisk (*) as a wildcard to signify missing characters. For example, J*n might return Jackson, Jan, Jason, Jon, Joan, and so forth.

   Define your search string carefully, to ensure that all desired results are included within the number selected for limiting the search.

4. Highlight 1 or more entries in the results list, and click the right arrow button (>) to move them to the Selected Recipients List.
5. Repeat steps 2 - 4 as needed to conduct additional searches and add more recipients to the Selected Recipients List.
6. To delete an entry from the Selected Recipients List, select the entry and click **Remove**.

7. After you are finished making selections or deletions, click **Next** to open the Message Analysis Results tab.

Selecting message analysis results for the report

The Message Analysis Result tab of the **Presentation Reports > Edit Report** page lets you determine which results of email analysis are included in the report. Selections are **Clean**, **Virus**, **Spam**, **Data Loss Prevention, Commercial Bulk**, **Custom Content, Block List, Phishing, File Sandbox**, **URL Analysis**, **Spoofed Email**, and **Threat Protection**. The Block List type applies to a message that is blocked by a Personal Email Manager Always Block List. By default, all available analysis result types are selected. You must select at least 1 type.

Click **Next** to open the Save tab.

Saving the report filter definition

The Save tab of the **Presentation Reports > Edit Report** page displays the name and description that will appear in the Report Catalog, and lets you choose how to proceed.

1. Review the Name and Description text.

   If any changes are needed, click **Back** to return to the General tab, where you can make those changes. You cannot edit the name or description text in the Save tab. (See *Setting general report options*, page 158.)
2. Indicate how you want to proceed:
   - Select **Save** to save the report filter and return to the Report Catalog.
   - Select **Save and run** to save the report filter and open the Run Report page. See *Running a presentation report*, page 162.
   - Select **Save and schedule** to save the report filter and open the Scheduler page. See *Scheduling a presentation report*, page 164.
3. Click **Finish** to save the report name and description and implement the selection made in step 2.

Working with Favorites

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

You can mark any presentation report, either template or custom, as a Favorite. Use this option to identify the reports you generate most frequently and want to be able to locate quickly in the Report Catalog.

To mark a report as a Favorite:

1. On the Presentation Reports page, select a report in the Report Catalog that you generate frequently, or want to be able to locate quickly.
2. Click **Favorite**.

   A star symbol appears beside any Favorite report name in the list, letting you quickly identify it when the Report Catalog is displayed.

3. Mark the **Show Only Favorites** check box above the Report Catalog to limit the list to those marked as Favorites. Clear this check box to restore the full list of reports.

If your needs change and a favorite report is no longer being used as frequently, you can remove the Favorite designation as follows:

1. Select a report that shows the Favorite star symbol.
2. Click **Favorite**.

   The star symbol is removed from that report name in the Report Catalog. The report is now omitted from the list if you choose **Show Only Favorites**.

Running a presentation report

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

Use the **Presentation Reports > Run Report** page to generate a single report immediately. You can also create jobs with 1 or more reports and schedule them to run once or on a repeating cycle (see *Scheduling a presentation report*, page 164).

Note

Before generating a report in PDF format, make sure that Adobe Reader v7.0 or later is installed on the machine from which you are accessing the email management server.

Before generating a report in XLS format, make sure that Microsoft Excel 2003 or later is installed on the machine from which you are accessing the email management server.

If the appropriate software is not installed, you have the option to save the file.

To run a report:

1. Select the report you want to run in the Report Catalog and click **Run** to open the Run Report page.
2. Select the **Report date range** to define the time period covered in the report.

   If you select **Custom**, specify the **Report start date** and **Report end date** for the report.
3. Select a **Report output format** for the report.

XLS	Excel spreadsheet. XLS files are formatted for reuse, and can be opened in Microsoft Excel.
PDF	Portable Document Format. PDF files are formatted for viewing, and can be opened in Adobe Reader.
HTML	HyperText Markup Language. HTML files are formatted for viewing, and can be opened in a Web browser.

4. If you selected a Top N report type, choose the number of items to be reported.
5. Specify how you want the report to be generated:
   - Select **Run the report in the background** (default) to have the report run immediately as a scheduled job. Optionally, you can provide an email address to receive a notification message when the report is complete or cannot be generated. (You can also monitor the job queue for report status.)

     If you run the report in the background, a copy of the completed report is automatically saved, and a link to the report appears on the Review Reports page.
   - Deselect **Run the report in the background** to have the report run in the foreground. In this case, the report is not scheduled, and does not appear on the Review Reports page.

     If you run the report in the foreground, the report is not automatically saved when you close the application used to view the report (Microsoft Excel, Adobe Reader, or a Web browser, for example). You must save the report manually.

     Note

     If you plan to run multiple reports in the foreground, make sure that you use the embedded **Close** button to close the pop-up window used to display the "generating report" and "report complete" messages. If you use the browser's close (X) button, subsequent attempts to run reports in the foreground may fail until you navigate away from the Presentation Reports page, come back, and run the report again.

6. Click **Run**.
   - If you scheduled the report to run immediately, the completed report is added to the Review Reports list. To view, save, or delete the report, click **Review Reports** at the top of the Presentation Reports page.
   - If you ran the report in the foreground, a new browser window appears, displaying report progress. HTML reports appear in the browser window when complete; with PDF or XLS formats, you have a choice of whether to open the report or save it.
7. To print a report, use the print option offered by the application used to display the report.

   For best results, generate PDF output for printing. Then, use the print options in Adobe Reader.

Scheduling a presentation report

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

You can run presentation reports as they are needed, or you can use the **Presentation Reports > Scheduler** page to create jobs that define a schedule for running 1 or more reports. In an appliance cluster, only the primary machine can schedule a report.

Reports generated by scheduled jobs are distributed to 1 or more recipients via email. As you create scheduled jobs, consider whether your email server will be able to handle the size and quantity of the attached report files.

The completed reports are also added to the **Presentation Reports > Review Reports** page (see *Reviewing scheduled presentation reports*, page 169).

You can access the Scheduler in one of the following ways:

- Click **Scheduler** at the top of the Presentation Reports page (above the Report Catalog).
- When editing a report filter, choose **Save and schedule** in the Save tab, and then click **Finish** (see *Defining the report filter*, page 158).
- Click the job name link on the Job Queue page to edit a job.
- Click **Add Job** on the Job Queue page to create a new job.

The Scheduler page contains several tabs for selecting the reports to run and the schedule for running them. For detailed instructions on completing each tab, see:

- *Setting the schedule*, page 165
- *Selecting reports to schedule*, page 166
- *Setting the date range*, page 167
- *Selecting output options*, page 167

After creating jobs, use the Job Queue to review job status and find other helpful information (see *Viewing the scheduled jobs list*, page 168).

When a scheduled presentation report has run, the report file is sent to recipients as an email attachment. The name of the attachment is the report name. For example, for a report with an output format of PDF, an attachment file may be named Hybrid Service Messages.pdf.

Scheduled reports are also automatically saved to a report output directory on the email management server (**C:\Program Files (x86)\Websense\Email Security\ESG Manager\tomcat\temp\report\output**, by default). Note that the name of the attachment sent via email does not match the name of the file stored in the output directory. The best way to find a specific report is to use the Review Reports page, which can be searched by date or job name, as well as report name.

Reports are automatically deleted from the Review Reports page and the report output directory after the period specified on the **Settings > Reporting > Preferences** page (5 days, by default). If you want to retain the reports for a longer time, include them in your backup routine or save them in a location that permits long-term storage.

An alert is displayed on the Review Reports page for a period of time before the report is deleted (3 days, by default). Use the **Settings > Reporting > Preferences** page to change this warning period.

Depending on the number of reports you generate daily, report files can occupy considerable amounts of disk space. Be sure adequate disk space is available on the email management server. If the report output directory grows too large before the files are automatically deleted, you can delete the files manually.

Forcepoint software generates the report in the format you choose: XLS (Microsoft Excel), PDF (Adobe Reader), or HTML. If you choose HTML format, the report may display in the Email module content pane. Reports displayed in the content pane cannot be printed or saved to a file. To print or save a report to file, choose the PDF or XLS output format.

Important

To display presentation reports in PDF format, Adobe Reader v7.0 or later must be installed on the machine from which you are accessing the email management server.

To display presentation reports in XLS format, Microsoft Excel 2003 or later must be installed on the machine from which you are accessing the email management server.

Setting the schedule

Schedule a reporting job to occur once or on a repeating cycle on the Schedule Report tab of the **Presentation Reports > Scheduler** page.

Note

It is advisable to schedule report jobs on different days or at different times, to avoid overloading the Log Database and slowing performance for logging and interactive reporting.

1. Enter a name that uniquely identifies this scheduled job in the **Job name** field.
2. Select Recurrence Options for the job based on the Recurrence Pattern you want, as follows:

Recurrence Pattern	Recurrence Options
Once	Enter the exact date on which to run the job, or click the icon to select from a calendar.
Daily	No additional recurrence options are available.

Recurrence Pattern	Recurrence Options
Weekly	Mark the check box for each day of the week the job is to run.
Monthly	Enter the dates during the month for running the job. Dates must be a number between 1 and 31, and must be separated by commas (1,10,20). To run the job on consecutive dates each month, enter a start and end date separated by a hyphen (3-5).

3. In the Schedule Time box, set the start time for running the job.

   The job begins according to the time on the email appliance.

   Note

   To start generating the scheduled reports today, select a time late enough that you can complete the job definition before the start time.

4. In the Schedule Period box, select a date for starting the job. Options for ending the job are as follows:

No end date	The job continues to run indefinitely, according to the established schedule. To discontinue the job at some time in the future, either edit or delete the job. See *Viewing the scheduled jobs list*, page 168.
End after	Select the number of times to run the job. After that number of occurrences, the job does not run again, but it stays in the Job Queue until you delete it. See *Viewing the scheduled jobs list*, page 168.
End by	Set the date when the job stops running. It does not run on or after this date.

5. Click **Next** to open the Select Report tab.

Selecting reports to schedule

Use the Select Report tab of the **Presentation Reports > Scheduler** page to choose reports for the job.

1. Highlight a report for this job in the Report Catalog tree.
2. Click the right arrow (>) button to move that report to the Selected Reports list.
3. Repeat steps 1 and 2 until all reports for this job appear in the Selected Reports list.
4. Click **Next** to open the Date Range tab.

Setting the date range

Use the Date Range tab of the **Presentation Reports > Scheduler** page to set the date range for the job. If you selected **Once** in the Schedule Report tab, the **Specific dates** field displays the report date specified on that tab.

If you selected a recurring report schedule, you can specify the number of periods to report in the **Relative dates** field (Current, Last, Last 2, and so forth), along with the type of period (Days, Weeks, or Months). For example, the job might cover the Last 2 Weeks or Current Month.

Week represents a calendar week, Sunday through Saturday. Month represents a calendar month. For example, Current Week produces a report from Sunday through today; This Month produces a report from the first of the month through today; Last Week produces a report for the preceding Sunday through Saturday; and so forth.

After setting the date range for the job, click **Next** to display the Output tab.

Selecting output options

After you select the reports for a job, use the Output tab to select the output format and distribution options.

1. Select the file format for the finished report.

XLS	Excel Spreadsheet. Recipients must have Microsoft Excel 2003 or later to view the XLS reports.
PDF	Portable Document Format. Recipients must have Adobe Reader v7.0 or later to view the PDF reports.
HTML	HyperText Markup Language. Recipients must have a Web browser.

2. Select the number of items you want to appear in a Top format report from the **Top N** drop-down list. The value range is from 1 to 200; default value is 10.
3. Enter recipient email addresses for report distribution.

   Each address should be separated by a semicolon.
4. Optionally, you can also enter email addresses to notify recipients that report generation failed.
5. Mark the **Customize subject and message body of notification email** check box, if desired. Then, enter the custom subject and body text for this job's distribution email.
6. Click **Save Job** to save and implement the job definition, and display the Job Queue page.
7. Review this job and any other scheduled jobs. See *Viewing the scheduled jobs list*, page 168.

Viewing the scheduled jobs list

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

The **Presentation Reports > Job Queue** page lists the scheduled jobs created for presentation reports. The list gives the status for each job, as well as basic information about the job, such as how frequently it runs. From this page, you can add and delete scheduled jobs, temporarily suspend a job, and more.

You can search for a particular job by entering a search term in the **Job name** entry field at the top of the page. Click **Go** to begin the search.

Click **Clear** to remove the current search term, and then either perform a different search or click **Refresh** at the bottom of the page to display the complete list of reports.

The list provides the following information for each job:

Data Item	Description
Job Name	The name assigned when the job was created.
Status	Indicates whether the job is ● running ● scheduled (waiting for the next scheduled run time) ● completed successfully ● failed ● misfired (did not run at the last scheduled time due to a problem such as low memory or server shutdown)
State	One of the following: ● **Enabled** indicates a job that runs according to the established recurrence pattern. ● **Disabled** indicates a job that is inactive, and does not run.
Recurrence	The recurrence pattern (Once, Daily, Weekly, or Monthly) set for this job.
History	Click the Details link to open the Job History page for the selected job. See *Viewing job history*, page 169.
Next Scheduled	Date and time for the next run.
Owner	The user name of the administrator who scheduled the job.

Use the options on the Job Queue page to manage the jobs. Some of the buttons require that you first mark the check box beside the name of each job to be included.

Action	Description
Job name link	Opens the Scheduler page, where you can edit the job definition. See *Scheduling a presentation report*, page 164.
Run Now	Starts running any job that has been selected in the list immediately. This is in addition to regularly scheduled job runs.

Action	Description
Add Job	Opens the Scheduler page where you can define a new job. See *Scheduling a presentation report*, page 164.
Delete	Deletes from the Job Queue any job that has been selected in the list. After a job has been deleted, it cannot be restored. To temporarily stop running a particular job, use the **Disable** button.
Enable	Reactivates a disabled job that has been selected in the list. The job begins running according to the established schedule.
Disable	Discontinues running an enabled job that is selected in the list. Use this option to temporarily suspend a job that you may want to restore in the future.
Refresh	Updates the page with the latest data

Viewing job history

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

Click the **Details** link in the History column and use the **Presentation Reports > Job Queue > Job History** page to view information about recent attempts to run the selected job. The page lists each report separately, providing the following information:

Data Item	Description
Report Name	Title printed on the report
Start Date	Date and time the report started running
End Date	Date and time the report was completed
Status	Indicator of whether the report completed or failed
Message	Relevant information about the job, such as whether the report was successfully distributed

Reviewing scheduled presentation reports

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

Use the **Presentation Reports > Review Reports** page to find, access, and delete scheduled reports. By default, reports are listed from newest to oldest.

To view any report in the list, click the report name.

- If the report is a single PDF or XLS file, you may be given the option to save or open the report. This depends on your browser security settings and the plug-ins installed on your machine.
- If the report is very large, it may have been saved as multiple PDF or XLS files and stored in a ZIP file. The file is compressed using ZIP format. Save the ZIP file, then extract the PDF or XLS files it contains to view the report content.

- Hover the mouse pointer over the report icon next to the report name to see if the report is 1 or multiple files.

To limit the list to reports that will be deleted soon, mark the **Show only reports due to be purged** check box. When this option is selected, the report search functions are not available. The length of time that reports are stored is configured on the **Settings > Reporting > Preferences** page (see *Configuring reporting preferences*, page 155).

To search the report list, first select an entry from the **Filter by** drop-down list, and then enter all or part of a job name or date. Note that the search is case-sensitive. You can search by:

- The report or job name
- The date the report was created (Creation Date)
- The name of the administrator that scheduled the report (Requester)
- The date the report is due to be deleted (Purge Date)

Click **Go** to begin the search.

Click **Clear** to remove the current search term, and then either perform a different search or click **Refresh** to display the complete list of reports.

If a recently completed report does not appear on the Review Reports page, you can also click **Refresh** to update the page with the latest data.

To delete a report, mark the check box beside the report name and click **Delete**.

To see the status of a scheduled report job, click **Job Queue** at the top of the page. See *Viewing the scheduled jobs list*, page 168, for more information about using the job queue.

To schedule a new report job, click **Scheduler** (see *Scheduling a presentation report*, page 164).

7 Configuring Personal Email Manager End User Options

Topics:

Managing a Secure Sockets Layer (SSL) certificate

Use the **Settings > Personal Email > SSL Certificate** page to manage the Personal Email Manager SSL certificate, which enables secure email transmission for Personal Email Manager appliances. You can use the default certificate provided with Personal Email Manager, or you can import a new enterprise certificate from a certificate authority (CA).

After email product installation, default certificate information appears in the **Settings > Personal Email > SSL Certificate** page, in the Certificate Details section. Details include the certificate version, serial number, issuer, and expiration date.

Importing a certificate

Importing an SSL certificate to Personal Email Manager from a CA replaces the current certificate. Personal Email Manager certificate information is automatically copied to a new appliance when it is added to the TRITON Manager Email module.

Use the following procedure to import a certificate:

1. Click **Import** in the **Settings > Personal Email > SSL Certificate** page, below the Certificate Details area.
2. Click **Yes** in the confirmation dialog box. An Import Certificate area appears below the Import button.
3. Enter the certificate filename in the **Import Certificate** field or navigate to it using **Browse**. File format must be .jks, .p12, or .pfx.
4. An SSL certificate file should be password protected. Enter a password in the **Certificate password** field (maximum length is 100 characters; do not use special characters).
5. Mark the **Private key alias** check box and enter an optional alias (or identifier) for the private key in the entry field.
6. Mark the **Private key password** field and enter an optional password for the private key in the entry field (maximum length is 100 characters).
7. Click **OK**.
8. Restart the Personal Email Manager service in the appliance manager to activate the new certificate.

Restoring the default certificate

You can restore the Personal Email Manager default certificate at any time by clicking **Restore Default Certificate** in the **Settings > Personal Email > SSL Certificate** page. This action replaces the current certificate.

You should restart the Personal Email Manager service to activate the new certificate.

Creating the quarantine mail notification message

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

The Personal Email Manager notification message alerts users that email addressed to them has been blocked. The notification message list includes mail sent to all a user's email addresses, including alias addresses. The notification is sent to a user's primary email address.

The **Settings > Personal Email > Notification Message** page is composed of 4 sections:

- Notification Message Links, in which you specify the IP address and port for Personal Email Manager facility end-user access (see *Specifying Personal Email Manager access*, page 173)
- Notification Message Schedule, where you set the frequency with which a message is sent informing a user of blocked messages (see *Scheduling the notification message*, page 173)
- Notification Message Template, in which you format the content and appearance of the notification message. Users see this message in their inbox when they have blocked email. (See *Using the notification message template*, page 174.)

- Recipients List, in which you designate the user directories whose members will receive notification messages. (See *Creating the notification message recipient list*, page 175.)

After you complete all 4 sections, click **OK** to enable the delivery of notification messages.

Specifying Personal Email Manager access

Use the Notification Message Links section to designate the appliance that the end user accesses to manage blocked email in the Personal Email Manager tool. This setting is also used to create the hyperlinks to blocked mail listed in the user notification message. You can customize the URL for Personal Email Manager access to suit your needs.

Personal Email Manager users must have Personal Email Authentication permissions in order to use the facility. See *Managing user validation/authentication options*, page 69, for information about granting Personal Email Manager permissions to end users.

Enter the IP address or hostname of the Personal Email Manager appliance.

Enter the port number (default is 9449). The port number should not be an email management server or appliance reserved port.

Note

If you use the C appliance interface for Personal Email Manager access, you must use the default port of 9449.

Use the Custom URL field to enter a URL path for Personal Email Manager user access that is different from the one automatically generated using the IP address and port entered above. This URL is also used for the notification message hyperlinks. The path can have a maximum length of 250 alphanumeric characters, hyphens, and underscores; a hyphen cannot be the first character. The custom URL supports only 1 subdirectory (for example, www.mycompany.com/pemserver) and should use the port designated in the Port field.

Deploy a group of email appliances to handle Personal Email Manager end-user activities. Configuring an appliance cluster for Personal Email Manager access can enhance performance by activating an appliance load-balancing feature. If the appliance you access is configured in a cluster, the appliance forwards Personal Email Manager access requests to other cluster machines using a round robin mechanism.

Add and remove appliances from a cluster using the **Settings > General > Cluster Mode** page (see *Configuring an appliance cluster*, page 58, for information).

Scheduling the notification message

You have several options for scheduling the frequency of the notification messages that tell users that they have blocked messages. Configure the schedule settings in **Settings > Personal Email > Notification Message**.

Select the frequency of notification messages in the **Send notifications** drop-down list. By default, **None** is selected, and no other option in this section is enabled.

- If you select **Every day** in the **Send notifications** drop-down list, the **Time** options are enabled for selection. You can choose as many time intervals as you like, in 1-hour increments.
- If you select **Every workday** in the **Send notifications** drop-down list, the **Time** options are enabled for selection. You can choose as many time intervals as you like, in 1-hour increments.
- If you select **Every week** in the **Send notifications** drop-down list, the **Day of week** and **Time** fields are activated. Designate a day of the week for notification messages to be sent. You can choose as many time intervals as you like, in 1-hour increments.

Note

Notification messages will be sent only to protected domains. Unprotected domains will not receive notification messages.

Using the notification message template

The notification message template helps you determine the content and appearance of the email that informs users of blocked messages. Configure the notification message as follows:

1. Set the maximum number of messages that are included in each notification message. The default value is 50, maximum value is 100. A user with more than the maximum number of blocked messages waiting must handle the excess directly in the Personal Email Manager facility, via the Web Access link in the notification message.
2. Select the email actions you want the notification to include from among the following options:
   - **Deliver** (default selection), to allow the user to release a blocked message. The email may be delivered directly to the user's inbox, or it may be submitted for continued processing by subsequent filters if appropriate. The behavior is determined in the **Settings > Personal Email > End-user Portal** page, in the Quarantined Message Delivery Options section.
   - **Not Spam**, to allow the user to report a blocked message that should not be classified as spam
   - **Delete** (default selection), to remove a blocked message from the user's blocked message list
   - **Add to Always Block list**, to allow an authorized user to add an address to a personal Always Block List
   - **Add to Always Permit list**, to allow an authorized user to add an address to a personal Always Permit List
3. Enter your company name and other relevant information in the **Company** entry field.

4. Enter a brief description of the email filtering product in the **Description** entry field (default is “Forcepoint Email Protection Solutions”).
5. Enter the sender username in the **Sender username** field.
6. Enter the sender email address for the notification message in the **Sender email address** field.
7. Configure the subject line that you want the notification message to display in the **Subject** field. This subject will appear in the user’s inbox when the notification message is received.
8. Designate some appropriate header text for the notification message in the **Header** field.
9. Enter some appropriate footer text for the notification message in the **Footer** field.

Creating the notification message recipient list

You can determine which Personal Email Manager users receive notification messages by entering their details into the Recipients List section. Only the users listed in the Recipients list receive notification messages alerting them about blocked email.

The Recipients list is based on user directories. All existing user directories are listed in the left-hand user directories box. Select a user directory and click the right arrow to add the directory to the **Recipients** list.

Click **Add user directory** to create a new directory on the Add User Directory page (see *Adding and configuring a user directory*, page 60, for details). After you create a new user directory, it will appear in the user directories list on the Notification Message page.

If you want to delete a user directory from the Recipients list, select the directory in the Recipients list and click **Delete**.

Setting user account options

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

You can configure some Personal Email Manager user account options in the **Settings > Personal Email > User Accounts** page. Allow users to manage personal Always Block and Always Permit lists, delegate blocked message management to another individual, and manage multiple user accounts in a single Personal Email Manager session.

User account management configuration settings made on 1 appliance are applied to all the appliances in your network.

Authorizing use of block and permit lists

Authorized users can manage their own Always Block and Always Permit lists after they log in to Personal Email Manager. Use the **Settings** > **Personal Email > User Accounts** page to specify users who can manage entries in personal block and permit lists.

Adding authorized users

You can allow users to manage personal Always Block and Always Permit lists by specifying user directories that contain users with Personal Email Manager authentication privileges. Create user directories (in the User Directories page), and then specify authentication options for these user directories in the Add User Authentication page. (See *Adding and configuring a user directory*, page 60, for user directory details and *Managing user validation/authentication options*, page 69, for information about user authentication settings.)

In the **Settings > Personal Email > User Accounts** page, user directories for which you have specified Personal Email Manager privileges appear as available user directories. To grant permission for a user directory group to manage personal block/permit lists, select a user directory in the available directories list by marking the check box next to the directory name, and click the arrow button to move it to the Recipients box.

Removing authorized users

Remove previously authorized users by selecting a user directory in the Recipients box and clicking **Delete**. The user directory still appears in the available directories box, but its members no longer have Always Block/Always Permit list management permissions.

Enabling user account management

You can enable user account management functions for a Personal Email Manager end user by marking the **Enable user account management** check box in the **Settings > Personal Email > User Accounts** page. You can let end users delegate the management of blocked messages to 1 or more other individuals.

End users can configure these options in the User Account Access page, in the Personal Email Manager end-user interface. See *Personal Email Manager User Help* for details.

Customizing the Personal Email Manager end-user portal

Administrator Help | TRITON AP-EMAIL | Version 8.3.x

You can use the **Settings > Personal Email > End-user Portal** page to customize the end-user facility's appearance and to designate the quarantined message queues whose messages are displayed in Personal Email Manager end-user notification email.

Choosing a logo display

By default, the Forcepoint company name and logo appear on the Personal Email Manager end-user page. You may choose to have no company name or logo appear on the portal. For this option, leave the Company name field blank and select **None** in the Logo field drop-down list.

You can also customize the end-user portal by having your company name and logo appear there. Use the following procedures to customize your Personal Email Manager end-user portal in the End-user Portal Options section:

1. Enter your company name in the **Company name** field.
2. In the Logo field drop-down list, select **Custom**.
3. The **Upload logo** field appears. Browse to your logo file and select it for upload. The logo file must be:
   - A .gif, .png, .jpeg, or .jpg file format
   - Up to 1 MB and 120 x 34 pixels in size

You can change the logo file you use by clicking **Browse** next to your logo filename and browsing to a new logo file.

Enabling blocked message delivery

Specify the queue to which you want a message blocked by the Personal Email Manager Always Block list delivered.

Mark the **Save the original message to a queue** check box, and select a queue from the drop-down list or add a new queue for this purpose.

Enabling end-user action auditing

Specify whether you want to maintain a record of end-user email management activities performed from either the Personal Email Manager notification message or the Quarantined Messages List.

Mark the **Audit end-user actions** check box in the End-user Audit Option section to enable the Personal Email Manager Audit Log. View this log at **Main > Status > Logs > Personal Email Manager**. See *Personal Email Manager Audit Log*, page 27, for information about this log.

Activating quarantined message list caching

You can activate a list caching function for the Personal Email Manager end-user Quarantined Messages list that can enhance list display performance by reducing the number of database refresh operations. The following end-user actions do not automatically trigger a page refresh:

- Delete
- Deliver
- Reprocess
- Not spam

These operations reduce the size of the Quarantined Messages List until the page is less than half its original size, when an automatic refresh occurs.

Personal Email Manager end users may initiate a manual page refresh at any time by clicking **Refresh**.

Choosing quarantine message queue display

Select the queues whose messages are displayed to Personal Email Manager end users by marking the check box next to the desired queue name in the Message Queue Display Settings section.

Enabling quarantine message delivery

You can specify Personal Email Manager behavior when an end user clicks **Deliver** for a selected message in the Quarantined Messages list. Select 1 of the following options:

- **Deliver quarantined message**, to allow end users to release blocked email for direct delivery to their inboxes
- **Resume quarantined message processing**, to force the analysis of blocked email to resume through all subsequent filters. If this option is used, a message may not be delivered to an end user if it triggers a subsequent filter.