McAfee®
An Intel Company

Administration Guide
Revision A

SaaS Email Protection

Contents

Preface

This guide provides the information you need to configure, use, and maintain your McAfee SaaS service.

Contents

About this guide

This information describes the guide's target audience, the typographical conventions and icons used in this guide, and how the guide is organized.

Audience

McAfee SaaS documentation is carefully researched and written for the target audience.

The information in this guide is intended primarily for:

- **Administrators** — People who configure and manage specific features of a service.

Conventions

This guide uses the following typographical conventions and icons.

Book title or *Emphasis*	Title of a book, chapter, or topic; introduction of a new term; emphasis.
Bold	Text that is strongly emphasized.
`User input` or `Path`	Commands and other text that the user types; the path of a folder or program.
`Code`	A code sample.
User interface	Words in the user interface including options, menus, buttons, and dialog boxes.
Hypertext blue	A live link to a topic or to a web site.
	**Note:** Additional information, like an alternate method of accessing an option.
	**Tip:** Suggestions and recommendations.
	**Important/Caution:** Valuable advice to protect your computer system, software installation, network, business, or data.

What's in this guide

This guide is organized to help you find the information you need.

It's divided into functional parts intended to support the goals you need to accomplish when using your McAfee SaaS service. Each part is further divided into chapters that group relevant information together by feature and associated tasks, so you can go directly to the topic you need to successfully accomplish your goals.

Find McAfee SaaS service documentation

McAfee provides the information you need during each phase of service implementation, from setup to daily use and troubleshooting. After a service update is released, information is added to the McAfee SaaS Email and Web Security Support site.

Task

1 Go to the McAfee SaaS Email and Web Security Support page at http://support.mcafeesaas.com/.

2 Under **Knowledge Base**, click **Reference Materials**.

3 Under **Reference Materials**, scroll down to access information that you need:

- **Service Enhancements and Release Notes**
- **Training Materials**
- **Service Reference Guides**

1 Email Protection

Email Protection provides security services that safeguard corporations from unsolicited spam email, junk mail, viruses, worms, and unwanted content at the network perimeter before they can enter your internal network. Multiple layers of Email Protection provide secure and complete email filtering to protect your users. You can enable or disable specific layers by changing the licensed packages of features or through configuring the specific email policies in the Control Console.

2 Overview

The **Overview** page provides high-level information about email traffic to your domain over the last 24 hours. By default, the page displays **Disaster Recovery Current Status** and **Disaster Recovery Activity**.

Contents

Overview page

Use the **Overview** page to view status information for Disaster Recovery, as well as the 24 hour snapshot.

Table 2-1 Overview page options

Option	Definition
Overview	Click the **Overview** tab to view the default information. • **Disaster Recovery Current Status** • **Disaster Recovery Activity**
Display Statistics	Click the **Display Statistics** button to view the snapshot information. Statistics for last 24 hours are based on your local time zone. • **Inbound 24 Hour Snap Shot** • **Outbound 24 Hour Snap Shot** • **Traffic (Last 24 hours - time zone)** • **Policy Enforcement (Last 24 Hours - time zone)** • **Disaster Recovery Current Status** • **Disaster Recovery Activity**

Display Statistics view

Click **Display Statistics** to view the 24-hour snapshot of inbound and outbound email traffic.

Table 2-2 Display Statistics view

Option	Definition
Inbound 24 Hour Snap Shot	Displays a 24-hour snapshot of inbound email traffic: • **Bandwidth** — Average bandwidth used by inbound messages. • **Avg Size** — Average size of inbound messages, including attachments. • **Denied** — Messages refused because they contain a virus, unwanted content, attachments, HTML, bounces or are probably spam. Delivery is denied. • **Content** — All inbound emails that violated the content keyword policies. • **Virus** — Number of inbound emails that contained viruses. • **Messages** — Number of inbound messages processed. • **Quarantined** — Total number of inbound emails that were quarantined for any reason including spam, virus, etc. • **Attachment** — All inbound emails that had attachments that violated the attachment policies. • **Spam** — Number of inbound emails that were potentially spam.
Outbound 24 Hour Snap Shot	Displays a 24-hour snapshot of outbound email traffic: • **Bandwidth** — Average bandwidth used by outbound messages. • **Avg Size** — Average size of outbound messages, including attachments. • **Denied** — Messages refused because they contain a virus, unwanted content, attachments, HTML, bounces or are probably spam. Delivery is denied. • **Attachment** — All outbound emails that had attachments that violated the attachment policies. • **Virus** — Number of outbound emails that contained viruses. • **Messages** — Number of outbound messages processed. • **Quarantined** — Total number of outbound emails that were quarantined for any reason, including spam, virus, etc. • **Encrypted** — All outbound emails that violated any encrypted policies. • **Content** — All outbound emails that violated the any content keyword policies.
Traffic (Last 24 Hours – EST)	Displays a graphical representation of traffic volume within the last 24 hours of the designated time zone that displays the total number of inbound and outbound emails.
Policy Enforcement (Last 24 Hours - EST)	Displays the percentage of messages that had the different email actions applied (for example, stripped, blocked, tagged, quarantined, cleaned, or normally delivered) over the past 24 hours of the designated time zone.
Disaster Recovery Current Status	Displays a list of domains that are currently in disaster recovery. Email Protection is currently spooling the specified domain's email.
Disaster Recovery Activity	Displays a snapshot of spooled and unspooled messages if your company is in disaster recovery mode. The number of messages is listed, along with the total KB size that is spooled or unspooled. Choose from one of the three mechanisms provided that allows you into the Web Protection system. The default for the time zone is mountain time.

3 Quarantine

The quarantine feature in Email Protection allows you to review suspicious email messages and determine whether or not they are spam.

Contents

Search quarantine messages

Use the search options to filter quarantined messages and take action as necessary.

To change customers, select the link in the upper right of the opened window. In the **Select Customer** pop-up, enter the name of the customer and select the name when the list of options updates.

Task

For option definitions, click **Help** in the interface.

1. In Email Protection, select **Quarantine**.
2. Select your **Search Criteria**.
3. Click **Search**.

Review the results and take actions on quarantined messages as necessary.

Quarantine page

The **Quarantine** tab allows you to search quarantined emails and review, release, allow, or delete them for users as necessary.

Table 3-1 Search Criteria option definitions

Option	Definition
Domain	Specifies the domains included in the search. Select to filter by domain.
To	Specifies the recipient's email address to use in the search. You can use wildcards to search for multiple email addresses that match part of the address.
From	Specifies the sender's email address to use in the search. You can use wildcards to search for multiple email addresses that match part of the address.
Threat	Specifies the threat type to use in the search.

Table 3-1 Search Criteria option definitions *(continued)*

Option	Definition
Day	Specifies the date to use in the search.
Direction	Specifies the direction of the email traffic to use in the search (inbound, outbound, or both).

Table 3-2 Search Results option definitions

Option	Definition
Release	Click to release the selected messages.
Always Allow for User	Click to add the selected senders to the user's **Allow** list and release the messages (applies to spam messages only).
Delete	Click to delete the selected messages.
Delete All	Click to delete all messages.
View	Click to view a message in the **Safe Message View** tab.
Search Results list	• **Date** — Displays the date of the message. • **From** — Displays the from email address of the message. • **To** — Displays the to email address of the message. • **Subject** — Displays the subject of the message. • **Threat** — Displays the threat type of the message. • **Score** — Displays the quarantine score of the message. • **Size** — Displays the size of the message.

Quarantined Messages page

The **Message Quarantine** window lists all of the quarantined spam messages for the account of the user currently logged on.

Table 3-3 Quarantined Messages option definitions

Option	Definition
"View all quarantined messages" drop-down	Specifies the date range for messages displayed in the **Message Quarantine** tab. Select to view messages for a specific day.
Sent To:	Specifies the email addresses displayed in the **Message Quarantine** tab.
Release	Click to release the selected messages.
Always Allow	Click to add the selected senders to the **Allow** list and release the messages (applies to spam messages only).
Always Deny	Click to block the selected senders.
Delete	Click to delete the selected messages.
View	Click to view a message in the **Safe Message View** tab.
Message Quarantine list	• **Date** — Displays the date of the message. • **From** — Displays the from email address of the message. • **Subject** — Displays the subject of the message. • **Score** — Displays the quarantine score of the message. • **Size** — Displays the size of the message.

Safe Message View

The **Safe Message View** window provides more information about the quarantined message you have selected. You can also view the message content when policy settings Safe Message View is enabled.

Table 3-4 Safe Message View

Option	Definition
Release	Click to release a selected message from the quarantine list and have it moved to your email inbox.
Delete	Click to delete a selected message from the quarantine list.
Always Allow for User	Click to release messages through to the email recipients. All senders' email addresses are added to the recipient's **Allow List**. All future messages from the senders will no longer be quarantined.
Always Deny	Click to block messages to the email recipients.

4 Email Continuity

Email Continuity is a comprehensive managed disaster recovery service that enables Web-based email access, management, and use during planned or unplanned outages. The service retains all inbound and outbound mail sent or received during the outage, and intelligently synchronizes an accurate record of all outage-period message activity with the business email server(s).

Contents

Email Continuity features and limitations

Email Continuity provides most of the features of your standard email client during an outage. However, some features may be unavailable or may work in a different way than you are accustomed to.

Table 4-1 Email Continuity features and limitations

Email Features...	Description
That you can use during an outage	• Standard email options, including Compose, Print, Reply, Reply All, Forward, Delete. • Can take Actions on email (select item from drop-down list, then click the **Apply** button). Actions include Mark as Read or Mark as Unread. • Attach files • Search messages by From, Subject, or Date columns.
That are unavailable during an outage	• Cannot change your **From**: email address. • No access to your Global Address List or Personal Contact List. These Distribution Lists are on the corporate server, and during an outage, the corporate server is not available. • No Spell Check. • No Drafts Folder. • No "Check names" functionality to verify email address prior to sending. • Cannot search for words in the body of a message.
That may be different from your standard email client	• You must separate multiple email addresses with commas, no spaces after the comma. • You must enter a fully qualified email address in the **To**: field when composing a new message. • If you have opened several messages, a tab for each message will appear. • Messages deleted in Email Continuity are not permanently deleted. Once your email outage is over, all email activity is synchronized with your organization's email server(s), which handles final message disposition. • Attaching files to messages should be done using the **Browse** button to browse to the desired file rather than by typing in the path and filename.

Email Continuity page

When active, the Email Continuity page allows you to access your email directly from the Control Console. You can send and receive emails, reply to messages, view attachments, and search available folders.

Table 4-2 Email Continuity page option definitions

Option	Definitions
Tools	To search a folder for email: • **Search** — Specifies one or more columns to search. • **In** — Specifies a folder to search. • **For** — Specifies text to search for. • **Date** — Click to view the calendar and select a date to search. • **OK** — Click to search. To send an email: • **Compose** — Click to open a new tab and compose an email.
Folders	To view a folder in a new tab, select an option: • **Inbox** • **Sent** • **Deleted**

Inbox	Displays your incoming email messages.
	• **Print** — Click to print the selected email.
	• **Reply** — Click to write a reply to the sender of the selected email.
	• **Reply All** — Click to write a reply to the sender and all of the other recipients of the selected email.
	• **Forward** — Click to forward the selected email.
	• **Delete** — Click to delete the selected email.
	• **Actions** — Select an action to mark the selected email as read or unread.
	  • **Mark as read**
	  • **Mark as unread**
	  • **Apply** — Click to apply the selected the action.
	• Paging — Select options to view additional pages.
	• Refresh — Click the refresh icon to update the inbox.
	• **Preview** — Displays a preview of the selected email.
	  • **Show Headers** — Select to view message headers in the email preview.

Table 4-2 Email Continuity page option definitions *(continued)*

Option	Definitions
Sent	Displays email messages you have sent. • **Print** — Click to print the selected email. • **Reply** — Click to write a reply to the sender of the selected email. • **Reply All** — Click to write a reply to the sender and all of the other recipients of the selected email. • **Forward** — Click to forward the selected email. • Paging — Select options to view additional pages. • Refresh — Click the refresh icon to update the inbox. • **Preview** — Displays a preview of the selected email.

Deleted	Displays email messages you have deleted.
	• **Print** — Click to print the selected email.
	• **Reply** — Click to write a reply to the sender of the selected email.
	• **Reply All** — Click to write a reply to the sender and all of the other recipients of the selected email.
	• **Forward** — Click to forward the selected email.
	• **Actions** — Select an action to mark the selected email as read or unread, or move it to the inbox folder.
	  • **Mark as read**
	  • **Mark as unread**
	  • **Move to Inbox**
	  • **Apply** — Click to apply the selected the action.
	• Paging — Select options to view additional pages.
	• Refresh — Click the refresh icon to update the inbox.
	• **Preview** — Displays a preview of the selected email.
	  • **Show Headers** — Select to view message headers in the email preview.

Table 4-2 Email Continuity page option definitions *(continued)*

Option	Definitions
Compose	Write and send a new email message. • **Send** — Click to send the email. • **Attach File** — Click to attach a file to the email. File upload is limited to 10 MB. • **Switch to HTML/Switch to Text** — Click to switch the format of the email. • **Show Bcc/Hide Bcc** — Click to show or hide the Bcc field.

Message	Double-click any email to view the message in a separate tab.
	• **Print** — Click to print the email.
	• **Reply** — Click to write a reply to the sender of the email.
	• **Reply All** — Click to write a reply to the sender and all of the other recipients of the email.
	• **Forward** — Click to forward the email.
	• **Delete** — Click to delete the email.
	• **Actions** — Select an action to mark the email as read or unread.
	  • **Mark as read**
	  • **Mark as unread**
	  • **Apply** — Click to apply the selected the action.
	• **Show Headers** — Select to view message headers.

5 Policies

Policies define the rules that Email Protection should follow and the actions it should take when filtering email. The service includes a default inbound and outbound policy which are automatically assigned to each of your domains. You can create custom policies for any domain or group.

Contents

Policies page

The **Policies** page allows you to configure inbound and outbound email filters.

Table 5-1 Policies tab options

Option	Definition
Inbound Policies	Click to configure inbound policies for a domain or group.
Outbound Policies	Click to configure outbound policies for a domain or group. • Outbound policies can ensure the safety and appropriateness of information being sent from your email system. • Outbound email is not filtered for spam. • You can not customize allow or deny lists for outbound email.

Table 5-2 Inbound/Outbound Policies options

Option	Definition
Apply	Click to save changes to a policy.
Reset	Click to restore previously saved changes.
New	Click to create a new policy.
Edit	Click to edit an existing policy.
Delete	Click to delete an existing policy.
Policies list	• **Name** — Specifies the name of the policy. • **Owner** — Specifies whether the policy belongs to a customer or a group. • **Priority** — Specifies the priority order that the policy is applied in relation to other policies. • **Description** — Specifies the description of the policy.

New Policy Set window

Create a new policy set to apply custom email filtering rules to a customer or group.

Table 5-3 New Policy Set window options

Option	Definition
Save	Click to save changes.
Cancel	Click to close the window without saving changes.
Name	Enter a name for the policy.
Priority	Displays the priority order of the policy.
Direction	Displays whether the policy is for Inbound or Outbound SMTP.
Description	Enter a brief description of the policy.
Owner	Select the owner to specify who can edit the policy: • **Customer** — Specifies that customer administrators and higher can edit the policy. • **Group** — Specifies that group administrators for the specified group as well as customer administrators and higher can edit the policy. Select the group from the drop-down.
Copy From	If necessary, select an existing policy to copy configuration settings into the new policy set. The following options apply for inbound options: • **Copy Sender Allow List** — Select to copy the current sender allow list. • **Copy Sender Deny List** — Select to copy the current sender deny list. • **Copy Recipient Shield List** — Select to copy the current recipient shield list. • **Copy ClickProtect Allow List** — Select to copy the current ClickProtect allow list.

Managing Policy Sets

Email Protection has default inbound and outbound mail filters to block and clean malicious email or, quarantine malicious email. The filters are configured by using policies, which are the parameters for the filters. Default policies are automatically assigned to each of your domains.

Details

The **Details** tab displays the basic set up information for an existing policy set.

Details tab

View and edit the name and description for the policy set.

Table 5-4 Details tab option definitions

Option	Definition
Save	Click to save changes.
Cancel	Click to reset without saving changes.
Name	Specifies the name of the policy.
Priority	Specifies the priority order of the policy (read only).
Direction	Specifies whether the policy is for Inbound or Outbound SMTP (read only).
Owner	Specifies who can edit the policy (read only).
Description	Specifies the brief description for the policy.

Virus

Email Protection provides highly effective, organization-wide virus and worm protection. By identifying viruses and worms on your network perimeter before they enter or leave your messaging infrastructure, Email Protection minimizes outbreak and infection risks to your system.

Email Protection virus protection:

- Provides maximum protection using multiple, industry-leading, anti-virus engines to allow Email Protection to customize the protection to meet the latest threats.
- Defines virus definition updates every 5 minutes, providing up-to-the-minute defense against the latest threats.
- Provides safe, external virus scanning and quarantine management for protection against viruses before they reach your network. Protects your users, networks, and data from harm.

Actions against a virus

The **Actions** subtab allows you to configure how the system reacts if an email is received that contains a known virus. It has two subtabs: **Actions** and **Notifications**.

Task

1 In the **If a Message Contains a Virus** field, select one of the following options.

Option	Description
Do Nothing	Send email to the recipient with no filtering or notification (not recommended).
Quarantine the message after attachment is stripped	Strip the infected attachment from the email and send it to the virus quarantine area without notification to the recipient. Text is inserted into the email notifying the recipient that an attachment has been stripped.
Strip the attachment	Strip the infected attachment from the email and send it to the recipient. Text is inserted into the email notifying the recipient that an attachment has been stripped.
Deny Delivery	The email is denied delivery.
Clean the message	The system attempts to remove the virus content and save the remainder of the message. If the clean is successful, the email is sent to the recipient with inserted text indicating that the email had been cleaned of a virus. If this action is selected, you must also select an action for the **If a Message Cannot be Cleaned** feature.

2 In the **If a Message Cannot be Cleaned** field, select one of the options provided. This option is only available if the **Clean the message** option has been selected.

Notifications for a virus policy

The Notifications subtab allows you to configure whether the sender or recipient is notified if an email violates a specific email filtering policy, other than spam policies, and a specific action is applied to it.

Virus Subtabs

The **Virus** subtab allows you to configure whether infected emails are quarantined, denied, or stripped of infection. The following table lists the type of configurations available.

Table 5-5 Virus Subtabs

Option	Definition
Actions	The **Actions** subtab allows you to configure how the system reacts if an email is received that contains a known virus.
Notifications	The **Notifications** subtab allows you to configure whether the sender or recipient is notified if an email violates a specific email filtering policy

Spam

Email Protection provides the most comprehensive and effective spam-blocking product available, blocking 98 percent of spam and providing an industry-leading low false positive rate. Email is assigned a high or medium likelihood of being spam as appropriate and a separate action can be assigned to each likelihood.

Contents

What is spam?

Spam can include unsolicited, and usually unwanted, commercial email sent to a large number of addresses.

In addition, spam has become a tool of hackers and electronic terrorists who deliberately attempt to gather proprietary information from computer systems or attempt to cause harm to a company's email system. Typically, these types of spammers deliberately use naming standards, hijacked from addresses, scrambled content, and so on to bypass spam filters such as blacklists and keyword lists.

Spam blocking and bounce flood protection

Spam Blocking Protection via Real-Time BlackHole Lists (RBLs) and Bounce Flood Protection are two spam protection methods used to block offending IP addresses or messages.

Spam protection method	Definition
Spam Blocking Protection via Real-Time BlackHole Lists (RBLs)	• Real-time Blackhole Lists (RBLs) are used to identify email distributed from known spammer IP addresses. • RBLs are enabled by default for all new policy sets to ensure the highest level of spam identification and, will automatically block messages from suspect IP addresses. • Customer-level and user-level allow lists supersede the RBLs on a per address basis. Sending addresses are compared to the customer-level and user-level allow list prior to RBL filtering and will deliver the message if the address appears on an allow list, while still blocking other undefined email addresses from offending sending IPs. • Customers may prefer to opt out of utilizing the RBL protection. However, for security purposes, opting out of RBL protection is not recommended.
Bounce Flood Protection	Block receipt of unrecognized bounce messages denies unrecognized bounce messages from being received in a user's incoming email but allows valid bounces that contain a secure header provided by the outbound service.

Filtering graymail

Email Protection includes a pre-built content policy for easily identifying and blocking graymail.

Unlike spam, graymail is legitimate bulk email messages that you once subscribed to, but no longer want to receive, and now prefer to block.

Defining content groups

Spam content filtering is controlled by comparing the content of an email against predefined lists of keywords or phrases (spam content groups). You can define a different action for each spam content group. The action in this window overrides all other spam actions (for example, if the email had a medium likelihood of being spam and contained content that was in a spam content group, the action defined for the spam content group would be applied).

This email policy is separate from the Content Keyword email filtering controlled by the **Content Groups** tab because emails that are quarantined, due to defined policy violations, are placed in the content quarantine area for the user account, which is accessible only by quarantine managers or higher-level users.

If the same content is defined in the **Spam Content** tab and in the **Content Groups** tab, the policies in the **Content Groups** window are used (that is, the content keyword policies will override the spam content policies in the case of a conflict).

The following two wildcards, an asterisk (*) and a question mark (?), are recognized characters that can be used in defining your action. For example, add* or shell?.

Configure the spam classification policy

Setting an action for each spam classification allows you to automatically manage and process spam emails as well as email designated as graymail.

Task

For option definitions, click **Help** in the interface.

1 Under Email Protection, select **Policies** and open a policy set.

2 In the policy set window, select **Spam** | **Classification**.

3 Select an option for each spam likelihood level to specify what should happen **When a message is**

- **probably spam (medium likelihood)**
- **almost certainly spam (high likelihood)**
- **graymail**

4 Select additional policy actions as necessary.

5 Click **Save**.

Classification subtab

Use the **Classification** subtab to designate the action to take when an email is assigned a spam likelihood level of medium or high, or is graymail. You can designate separate actions for each likelihood level.

Table 5-6 Classification subtab option definitions

Option	Definition
Save	Click to save changes.
Cancel	Click to clear changes.
When a message is	Specifies the settings for medium and high spam likelihood as well as the setting for graymail. For each, select the appropriate option: • **Tag the message subject with "[SPAM]"** — The phrase **[SPAM]** is added to the subject line of the email at the beginning of the subject text and the email is sent to the recipient email address. This action can be combined with rules, on your email client or server to sort spam locally. • **Tag subject with "[Graymail]"** — This option is available only for email classified as graymail. The word **[GRAYMAIL]** is added to the beginning of the subject line before the message is delivered to the recipient. This action can be combined with rules on the email client or server to sort graymail locally. • **Quarantine** — The email is not delivered but instead is accepted from the sender and stored in the recipient's quarantine. • **Deny delivery** — The email is not accepted from the sender and the sender is notified the message has been rejected. • **Do nothing** — The email is delivered to the recipient and no additional action is applied. **Do nothing** is reported on the **Threats: Spam** report as **Other** for **probably spam (medium likelihood)** and **almost certainly spam (high likelihood)** only.
More options	Specifies additional options you can enable, including: • **Enable real-time blackhole lists (RBLs)** — Denies email distributed from known spammer IP addresses. • **Block unrecognized bounce messages ("backscatter")** — Denies unrecognized bounce messages from being received.

Configure content groups policies

Designate what action to take if an email contains any content that is defined as spam content for groups.

Task

For option definitions, click **Help** in the interface.

1. Under Email Protection, select **Policies** and open a policy set.
2. In the policy set window, select **Spam** | **Content Groups**.
3. Click **New**.
4. Type a unique**Group Name** for the new content group.
5. Enter keywords and phrases associated with the content group in the **Content** field.
6. Select an **Action**.
7. Select **Enable**.
8. Click **Save**.

Content Groups subtab

Use the **Content Groups** subtab to define content groups and assign the actions to take if an email matches those keywords or phrases.

Table 5-7 Content Groups option definitions

Option	Definition
New	Click to create a new content group.
Edit	Click to edit an existing content group.
Delete	Click to delete a content group.
Content groups table	Displays a list of current content groups. • **Group Name** — Displays the name of the content group. • **Action** — Displays the action to take. • **Enabled** — Displays whether the content group is currently enabled.

Content groups options	Specifies the settings when creating a new content group or editing an existing group name.
	• **Group Name** — Specifies the content group name.
	• **Content** — Specifies the keywords or phrases associated with the content group.
	• **Action** — Specifies the action to take.
	  • **Quarantine**
	  • **Deny**
	  • **Allow**
	  • **Tag subject**
	• **Enable** — Select to enable the content group.
	• **Save** — Click to save changes.
	• **Cancel** — Click to close the content group options without saving.

Reporting tab

The **Reporting** tab allows you to configure the Spam Report.

Table 5-8 Reporting option definitions

Option	Definition
Save	Click to save changes.
Cancel	Click to clear changes.

Default Settings	• **Email a Spam Report to** — Specifies who receives the report.
	  • **All users assigned to this policy** — All user accounts associated with the policy set.
	  • **Selected users** — Only those user accounts configured for Spam Reports on the user management windows.
	  • **No users** — No users associated with this policy set.
	• **Format** — Specifies the format and type of content to include in the Spam Report.
	  • **HTML - with Actions** — This HTML report allows the recipient to perform actions directly from the Spam Report. You can **Release**, **Always Allow**, or (if allowed) **Always Deny** each message in the report. You can also **Delete All** messages in the spam quarantine.
	  • **HTML - without Actions** — The HTML Report does not contain any of the action links.
	  • **Plain text** — Report is plain text.
	• **Type** — Specifies what should be included in the Spam Report.
	  • **New Items Since Last Report** — Contains any new quarantined spam messages added since the last generated report. This does not apply to the on-demand Spam Reports.
	  • **All quarantined items** — Contains all quarantined spam messages.
	• **Spam Report Links to the Control Console** — Specifies the number of days links are active before they expire. Two additional values allow you to customize the link:
	  • **Require authentication** — The link does not expire but it does require the user to log on.
	  • **Never expire** — The link never expires.
	• **Custom Message** — Specifies custom text that you can add to the Spam Report. Text is limited to 4000 characters.

Schedule and Frequency	• **Frequency** — Specifies the days of the week that the report is sent. Select one or more days. • **Deliver reports by** — Specifies the time of day that the reports are scheduled to be delivered by. You can schedule Spam Reports to be sent once or twice a day. Reports are sent out no later than the time specified.  All times are based on your time zone setting. To set your time zone, select **Account Management** | **Customers** | **Details**. Select the **update** link next to **Time Zone Default** In the pop-up, select your time zone, click **Update**.

Table 5-8 Reporting option definitions *(continued)*

Option	Definition
Allow users to...	• **personalize spam filtering options** — When enabled, users can select the actions for spam from the **Preferences** tab. • **personalize Spam Report delivery time and frequency** — When enabled, users can select the frequency of reports from the **Preferences** tab. • **personalize report type** — When enabled, users can change the report type from the **Preferences** tab. • **disable spam filtering** — When enabled, users can turn off spam filtering from the **Preferences** tab. • **configure alternate email address for spam report delivery** — When enabled, users can specify their alternate email address from the **Preferences** tab. Redirecting the report allows the alternate recipient to have full access to a user's Control Console account. Encourage users to choose their alternate email address carefully. • **download Spam Control For Outlook** ® — When enabled, users can download the Spam Control For Outlook utility. You can specify the location for the download on the branding settings page. Access to Spam Control for Outlook can also be enabled or disabled at the system level.
Other Options	Specifies additional options enabled for reports. • **Allow non-admin users to login directly to the Control Console** — When enabled, allows users to log onto the Control Console using the logon page. Does not affect the ability of users to log on by selecting a link in the Spam Report. If Control Console access is not enabled and users do not receive the Spam Report, the quarantine manager or higher-level roles must perform any changes to user settings. • **Display messages in quarantine using Safe Message View** — When enabled, allows users to view the body content of an email in the safe message view window. Otherwise, the user must release the email to see what it contains in the body content. • **Display user email address in the Spam Report** — When enabled, displays user addresses and aliases in the Spam Report. • **Enable the "Deny" shortcut from the Spam Report** — When enabled, displays the **Always Deny** link in the Spam Report, the **Message Quarantine** page, and the **Safe Message View** page. Otherwise, users must go to the **Allow/Deny Sender Lists** window to change their **Allow** or **Deny** lists. • **Show the spam score on the Spam Report** — When enabled, displays the spam likelihood score for each quarantined message in the Spam Report.

ClickProtect

ClickProtect safeguards your organization from web-based threats that may arrive by email using McAfee GTI® URL Reputation. URLs are evaluated during processing ("scan-time") as well as when

users click on a link ("click-time"). Click-time scanning ensures that users are protected from changes to a URL's reputation that can occur after the message is initially scanned.

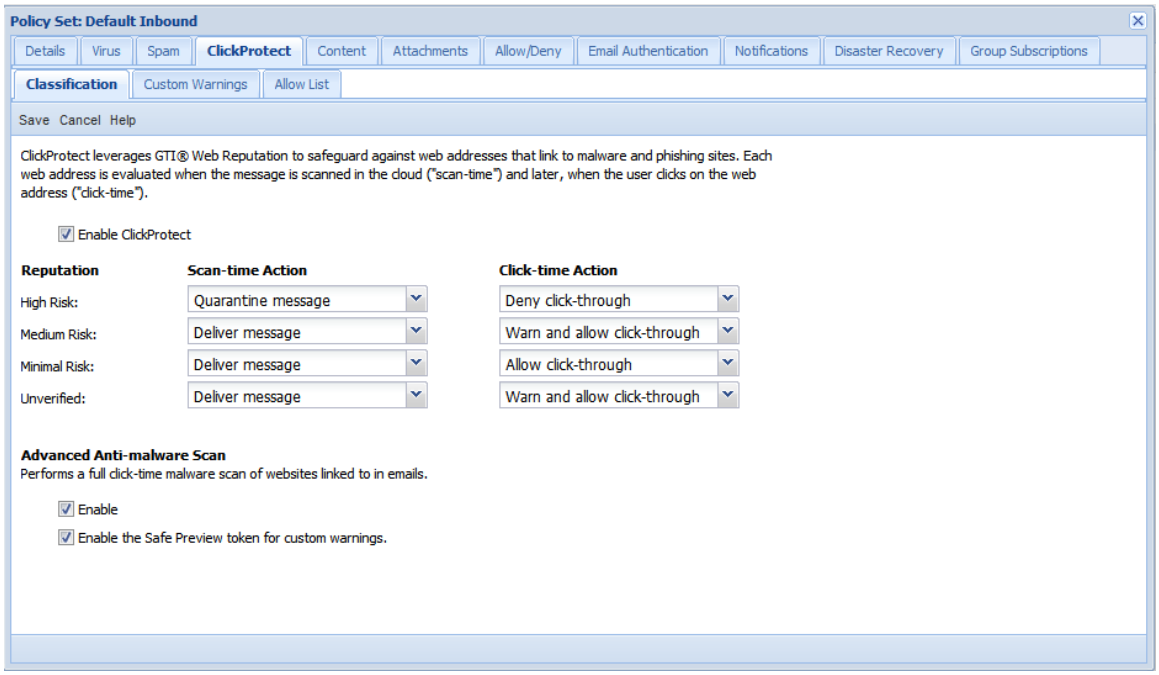

Figure 5-1 New ClickProtect tab in the inbound policy window

Update ClickProtect options for an inbound policy set

Configure ClickProtect to take specific scan-time and click-time actions that protect your users from risky URL links in inbound email messages.

Task

For option definitions, click **Help** in the interface.

1 Select **Email Protection** | **Policies** | **Inbound Policies**

2 Highlight a custom policy or select the Default Inbound policy, click **Edit**.

3 In the **Policy Set** window, select **ClickProtect**.

4 Select **Enable ClickProtect**.

5 Select scan-time and click-time actions for each reputation type.

6 Under **Advanced Anti-malware Scan**, select malware scan options as necessary.

7 Click **Save**.

Once ClickProtect is active, you can customize the warning messages your users see as well as update the list of approved URLs.

Classification tab

Use the **Classification** tab to configure ClickProtect scan-time and click-time actions.

Table 5-9 Classification tab option definitions

Option	Definition
Save	Click to save changes.
Cancel	Click to reset without saving changes.
Enable ClickProtect	Select to enable ClickProtect and configure your scan-time and click-time actions.
Reputation	Displays the risk categories: • **High Risk** — Specifies a URL that exhibits detrimental behavior. For example, the site is known to host malware. • **Medium Risk** — Specifies a URL that exhibits questionable behavior that may be detrimental to the user. • **Minimal Risk** — Specifies a URL that exhibits appropriate behavior or that is verified as trusted. • **Unverified** — Specifies a URL for which no reputation information has been calculated.
Scan-time Action	Specifies the action to take at scan-time, for each reputation type. • **Deliver message** • **Quarantine message** • **Deny message** • **Tag subject**
Click-time Action	Specifies the action to take at click-time, for each reputation type. • **Allow click-through** — Select to immediately redirect the user to the website. • **Warn and allow click-through** — Select to display a warning message in a browser and give the user the option to continue to the requested website. • **Deny click-through** — Select to display a block message in a browser and explain why the website was denied. You can customize the warning and blocked message pages in the **Custom Warnings** tab.
Advanced Anti-malware Scan	Specifies whether or not you want to scan email links for malware at click-time. • **Enable** — Select to enable the anti-malware scan. • **Enable the Safe Preview token for custom warnings** — Select to enable the **Safe Preview** option in the **Custom Warnings** tab. You can customize the warning message page in the **Custom Warnings** tab.

Custom Warnings tab

The **Custom Warnings** tab allows you to customize the warning page that displays when a website risk is detected at click-time. Each text field allows you to enter and format the text using the toolbar options. You can also add tokens to display specific information about a link.

Table 5-10 Custom Warnings tab option definitions

Option	Definition
Save	Click to save the text, tokens, and HTML formatting.
Cancel	Click to discard your changes and restore the previously saved text.

Table 5-10 Custom Warnings tab option definitions *(continued)*

Option	Definition
Warn-and-allow	Specifies the text that displays when you select **Warn and allow click-through** as the click-time action for a risk level. This page typically warns the user of the risk and gives them the option to continue or abandon the link.
Deny Click-through	Specifies the text that displays when you select **Deny click-through** as the click-time action for a risk level. This page typically warns the user of the risk and provides and explanation for why the website was blocked.
Malware Found	Specifies the text that displays when you enable the **Advanced Anti-malware Scan** option and malware is found.
Error Occured	Specifies the text that displays when an error occurs. For example, a URL's reputation cannot be checked, or a website cannot be scanned for malware.

Custom Warnings tokens

Use these tokens to include specific details about a link in the text of your custom warning message.

Table 5-11 Tokens definitions

Add this token	To display
%URL%	The URL that the user clicked. Recommended for the **Warn-and-allow** warning message only.
%URL_REPUTATION%	The risk level of the website based on its reputation. • Minimal • Medium • High • Unverified
%URL_CATEGORY%	The category of the website.

%IMAGE_PREVIEW%	A safe preview of the website.
	In certain situations, the image preview may not display. This can happen when:
	• Access to the page is denied due to the %URL_REPUTATION% value. For example, **High Risk** is set to **Deny click-through**.
	• The malware scan detected a virus.
	• Safe preview is not enabled for the **Advanced Anti-malware Scan**.
	• The %URL_CATEGORY% value includes sexual or violent content.
	  • Extreme
	  • Gruesome Content
	  • Incidental Nudity
	  • Nudity
	  • Pornography
	  • Provocative Attire
	  • Sexual Materials
	• An error occurs during the preview scan, or the preview scan takes longer than 20 seconds.

%FROM_ADDRESS%	The email address that sent the email with the website URL.

Table 5-11 Tokens definitions *(continued)*

Add this token	To display
%DATE_TIME%	The timestamp of the email.
%SUBJECT%	The subject line of the email.
%MESSAGE_ID%	The message ID of the email.
%MALWARE_NAME%	The name of the malware threat.

Custom Warning token examples

- The website you requested is considered %URL_REPUTATION% risk.
- The link was sent to you by %FROM_ADDRESS% on %DATE_TIME%.
- The email subject line was %SUBJECT%.
- This website, %URL%, is associated with the %URL_CATEGORY% category.

Allow List tab

The **Allow List** tab allows you to configure the list of domains, IP addresses, and URLs that ClickProtect should always allow in an email. For example, a website that you want to exclude from URL rewrite, or an internal website that ClickProtect is unable to access.

Table 5-12 Allow List tab option definitions

Option	Definition
Save	Click to save changes.
Cancel	Click to restore previous settings.
Domain, IP Address, or URL	Enter a domain, IP address, or URL to add it to the **Allow List**. • Maximum of 256 characters for each address. • Wild cards can be used with domains and IP addresses. • Maximum of 200 addresses.
Options	• **Add >>** — Click to add a new address to the list. • **<< Remove** — Select an address in the list and click **<< Remove** to delete it. • **<< Remove All** — Click to delete all addresses from the list. Click **Save** to keep your changes.
Allow List	Displays the list of allowed domains, IP addresses, and URLs.

More Options	Specifies additional options for managing the allow list.
	• **Upload list (appends):** — Upload addresses in a text file and add them to the list. To use this option, create a file with one item per line. Uploading adds new entries to the existing list. It will not delete existing items.
	  • **Browse** — Click to select a file to upload.
	  • **Upload** — Click to upload the file and update the list. Click **Save** to keep your changes.
	• **Download list (be sure to save changes first):** — Download the current allow list in a .csv file.
	  • **Download** — Click to download the list.
	• **Subscribe to the Default Inbound policy ClickProtect List** — Select to use the allow list associated with the default inbound policy.

Content

Email Protection has default inbound and outbound mail filters to block and clean malicious email and to quarantine malicious email. The filters are configured by using policies, which are the parameters for the filters default policies, are automatically assigned to each of your domains.The content filtering is controlled by comparing the content of an email against predefined lists of keywords or phrases (content groups).

The **Content Groups** subtab for the default inbound policy's page, allows you to configure how the system reacts if it receives an email that contains text that violated the content policies.

If the content group is enabled, then email is filtered for the following content.

- Profanity
- Racially Insensitive
- Sexual Overtones

Email Protection also provides predefined content groups that contain valid and acceptable personal identifiable information that is allowed in email messages due to specific policies. You cannot edit these content groups, but can designate whether or not they are used. Following are the two types of predefined content groups.

- Credit Card Number
- Social Security Number

The credit cards that are supported include AMEX, VISA, MC and, DISC.

Credit card numbers and social security numbers can be represented or formatted in various ways and Email Protection may not be able to capture all messages that contain this information.

Actions for Inbound Policy Content Groups

The way in which custom policies are applied to your users varies depending on whether you are classified as a service-provider or an enterprise-customer. If you are a service-provider, each domain can have one custom policy. If you are an enterprise-customer, a single default policy applies to all domains. Thus, for an enterprise-customer, you must create a group or groups of users, and for each group, you can create a custom policy. A group can be created according to domain membership or according to any other user characteristics that may apply across multiple domains

Task

1 Select the content group to modify, click **Edit**.

2 In the **Group Name** field, enter the custom content group.

The **Content** field is disabled for content groups.

3 From the **Action** drop-down list, select one of the following options.

Option	Description
None	The email is forwarded to the recipient email address.
Quarantine	The email is sent to the recipient's content quarantine area.
Deny	The email is denied delivery.
Allow	The email is sent to the recipient email address.
Tag the message subject	The phrase "[CONTENT]" is added to the subject line of the email at the beginning of the subject text and the email is sent to the recipient email address.

4 If you want to send a copy of the email to a separate address, select a predefined distribution list from the **Silent Copy** drop-down list.

5 Select **Enable** to enact the filtering for that document.

6 Click **Save**.

Outbound Policy Content Groups

Additional **Outbound Policy Content Groups** scan designated triggers within messages using predetermined policy dictionary keywords. A library of predefined compliance rules is provided.

> **Before you begin**
>
> This function is available to outbound policies only who have subscribed to Email Encryption. If a customer or domain subscribes to Email Encryption, then selecting this option can be used to enforce Email Encryption if the outbound message contains the word [encrypt]. The word, [encrypt] can reside in the message subject line or the body of the outbound message.

Task

1 The following options are available.

Option	Description
Expand All	Click to view and select from the list of extended dictionaries.
Collapse All	Click to close the extended list.
Encrypt Message	Available for outbound content groups, if the customer has subscribed to encryption.

The combination for a maximum encrypted message size including the message header, body and attachment, cannot exceed 30 MB for encrypted messages.

2 Click **Launch Validator** to open the **Regular Expression Validation** window.

3 Enter the **Regular Expression**.

Copy the sample text in the **Sample Text** field.

4 Click **Test**. If your regular expression is found within the sample text, it is selected within the **Result: Match** field.

COPY YOUR REGULAR EXPRESSION to the content field before closing out the **Regular Expression Validation** window. The information does not automatically populate to the content field. You will lose your information.

Content group names for outbound policies

Choose from these options to configure content groups for your outbound policy. These settings ensure that your outbound email messages conform to both international regulatory compliance rules as well as your corporate operating compliance rules.

Table 5-13 Group name definitions

Category	Option Definitions
Acceptable Use	• **Confidential Internal Memos** — Terms commonly found in internal company memos. Commonly used terms for expressing confidentiality. • **Controlled Substances** — Terms relating to illegal substances. • **Discrimination** — Terms relating to racism and bigotry. • **Gambling** — Terms relating to gambling activities. • **Offensive Language** — Terms relating to profanity. • **Threatening Language** — Terms commonly found to be related to weapons or harmful chemicals.
Australia Policy	• **NSW Drivers Licence** — Commonly used expressions supporting drivers Licence numbers. Patterns related to New South Wales Drivers Licence. • **Queensland Drivers Licence** — Commonly used expressions supporting drivers Licence numbers. Patterns related to Queensland Drivers Licence. • **Tax File Number** — Patterns related to Australia Tax File Number. • **Victoria Drivers Licence** — Commonly used expressions supporting drivers Licence numbers. Patterns related to Victoria Drivers Licence.
Austria Policy	• **Austria IBAN** — Numerical patterns related to Austrian IBAN.
Banking and Financial Sector	• **ABA Routing Number** — ABA Routing Number with check sum and keyword validation.
Brazil Policy	• **Brazil CEP** — Patterns related to Brazil CEP. • **Brazil CNPJ** — Patterns related to Cadastro Nacional de Pessoas Juridicas. • **Brazil CPF** — Patterns related to Brazil Cadastro de Pessoas Fisicas. • **Brazil Placa de Carro** — Patterns related to Brazil Placa de Carro.

Table 5-13 Group name definitions *(continued)*

Category	Option Definitions
Canada Policy	• **Alberta Drivers License** — Commonly used expressions supporting drivers license numbers. Numerical patterns related to Alberta Drivers License. • **Alberta Health** — Numerical patterns related to Alberta Health Card. • **Canada Passport** — Numerical patterns related to Ontario Health Card. • **Manitoba Drivers License** — Commonly used expressions supporting drivers license numbers. Patterns related to Manitoba Drivers License. • **Manitoba Health** — Numerical patterns related to Manitoba Health Card. • **Ontario Drivers License** — Commonly used expressions supporting drivers license numbers. Numerical patterns related to Ontario Drivers License. • **Ontario Health** — Numerical patterns related to Ontario Health Card. • **Quebec Drivers License** — Commonly used expressions supporting drivers license numbers. Numerical patterns related to Quebec Drivers License. • **Quebec Health** — Numerical patterns related to Quebec Health Card. • **Saskatchewan Drivers License** — Commonly used expressions supporting drivers license numbers. • **Saskatchewan Health** — Numerical patterns related to Quebec Health Card. • **Social Insurance Number** — Numerical patterns related to Canadian Social Insurance Number.
China Policy	• **Chinese Passport** — Patterns related to Chinese Passport.
Chinese Hong Kong Policy	• **Hong Kong ID** — Patterns related to Hong Kong ID.
Chinese Taiwan Policy	• **Citizen ID** — Patterns related to Taiwan Citizen ID Number.
Competitive Edge	• **Board Meeting Minutes** — Terms commonly found in documents detailing board meeting activities. • **Pricing Information** — Terms found frequently in price lists.
Employee Discontent	• **Disgruntled Employee Communications** — Terms commonly used by someone expressing discontent with their job or other. • **Executive Job Search** — Terms found in executive job searches. • **Resume** — Terms often found in a person's resume or curriculum vitae. • **Tax Return or Related Data** — Commonly used expression for employer identification number.
Entertainment Industry IP	• **Registered Programming Schedules** — Terms commonly found in entertainment or broadcast program schedules.
FERPA Compliance	• **Social Security Numbers and Ethnicities** — Social Security Number with SSA Check and Keyword Check. Terms describing a person's ethnic background. • **Social Security Numbers and Grades** — Social Security Number with SSA Check and Keyword Check. Terms frequently found adjacent to student grade information.

Table 5-13 Group name definitions *(continued)*

Category	Option Definitions
Financial and Security Compliance	• **Financial Audit Documents** — Terms related to financial audits. • **Financial Report Documents** — Terms and expressions commonly used in financial reports. • **Financial Statement Documents** — Terms commonly found in financial statements.
FISMA Compliance	• **FIPS High Impact Rating** — FIPS Classification of System with High Impact Rating. • **FIPS Low Impact Rating** — FIPS Classification of System with Low Impact Rating. • **FIPS Medium Impact Rating** — FIPS Classification of System with Medium Impact Rating.
France Policy	• **France IBAN** — Numerical patterns related to French IBAN. • **INSEE** — Numerical patterns related to French INSEE Code.
German Policy	• **German IBAN** — Numerical patterns related to German IBAN.
GLBA Compliance	• **ABA Routing Number** — ABA Routing Number with check sum and keyword validation. • **Credit Card Number Violations** — Credit Card Number with keyword check. • **Credit Report Violations** — Terms commonly found within a credit report. • **Social Security Numbers Violations** — Social Security Number with SSA Check and Keyword Check.
HIPAA Compliance	• **Credit Card Numbers and Medical Terms** — Credit Card Number with keyword check. Terms commonly found adjacent to a medical diagnosis. • **Personal Health Info- Admission/Discharge Data** — Patient admission and discharge related information. • **Personal Health Info- Contains Social Security Numbers** — Patient admission and discharge related information. Social Security Number with SSA Check and Keyword Check. • **Personal Health Info- Diagnosis Data** — Terms commonly found adjacent to a medical diagnosis. • **Social Security Numbers and Medical Terms** — Social Security Number with SSA Check and Keyword Check. Terms commonly found adjacent to a medical diagnosis.
India Policy	• **India PAN** — Patterns related to Indian Permanent Account Number.
Israel Policy	• **Israel IBAN** — Text patterns related to Israeli Identification. • **Israel Identification** — Numerical patterns related to Israeli Identification.
Korean Policy	• **Residents Registration Number** — Patterns related to Korean Resident's Registration Number.
Legal	• **Attorney Client Communications** — Terms often found in Attorney Client Communications. • **Lawsuit and Legal Matters** — Terms often found in Legal Documents.
Mexico Policy	• **Mexico CURP** — Patterns related to Mexican Clave Única de Registro de Población. • **Mexico NSS** — Patterns related to Mexican Número del seguro Social. • **Mexico RFC** — Patterns related to Mexican Registro Federal de Contribuyentes. • **Mexico CLABE** — Patterns related to Mexican CLABE.

Table 5-13 Group name definitions *(continued)*

Category	Option Definitions
Netherlands Policy	• **Netherlands IBAN** — Numerical patterns related to Dutch IBAN.
North America PII	• **Bulk Social Insurance Number Violations** — Numerical patterns related to Canadian Social Insurance Number. • **Bulk Social Security Number Violations** — Social Security Number with SSA Check and Keyword Check. Numerical Threshold for SSN Numbers. Default is set to greater than 100. • **Canada Personal Identifiable Information Violations** — Numerical patterns related to Canadian Social Insurance Number. • **Employer ID Number Violations** — Commonly used expression for employer identification number. • **Social Insurance Number Violations** — Numerical patterns related to Canadian Social Insurance Number. • **Social Security Number ONLY Violations** — Social Security Number with SSA Check only, no keywords required. • **Social Security Number Violations** — Social Security Number with SSA Check and keyword check. • **Unencrypted Credit Card Number Violations** — Credit Card Number with keyword check. • **United States Personal Identifiable Information Violations** — Social Security Number with SSA Check and keyword check.
Payment Card Industry	• **Bulk Credit Card Number Violations** — Credit Card Number with keyword check. Numerical Threshold for Credit Card Numbers. Default is set to greater than 100 credit card numbers. • **Credit Card Number Violations** — Credit Card Number with keyword check.
Poland Policy	• **Numer PESEL** — Numerical patterns related to Polish PESEL. • **Numer NIP** — Numerical patterns related to Polish NIP. • **Numer Paszportu** — Numerical patterns related to Polish Numer Paszportu. • **Numer Regon** — Numerical patterns related to Polish Regon ID. • **Poland IBAN** — Numerical patterns related to Polish IBAN.
Russia Policy	• **Russia Pension Fund** — Patterns related to Russian Pension Fund Individual Number. • **Russia Personal Tax ID** — Patterns related to Russian Personal Tax ID. • **Russia External Passport** — Patterns related to Russian External Passport. • **Russia Internal Passport** — Patterns related to Russian Internal Passport.
Singapore Policy	• **Bank Account Pattern** — Terms relating to bank account information. Patterns related to Singapore Bank Account. • **NRIC** — Patterns related to Singapore National Registration Identity Card. • **Sofinummer** — Numerical patterns related to Dutch Sofinummer.

Table 5-13 Group name definitions *(continued)*

Category	Option Definitions
SOX Compliance	• **Board Meeting Minutes** — Terms commonly found in documents detailing board meeting activities. Terms commonly found that are sensitive to Sarbanes-Oxley. • **Compensation and Benefits** — Terms pertaining to compensation and benefits. Terms commonly found that are sensitive to Sarbanes-Oxley. • **Compliance Reports** — Terms commonly found in compliance reports. Terms commonly found that are sensitive to Sarbanes-Oxley. • **Financial Reports** — Terms and expressions commonly used in financial reports. Terms commonly found that are sensitive to Sarbanes-Oxley. • **Financial Statement Disclosures** — Terms commonly found in financial statements. Terms commonly found that are sensitive to Sarbanes-Oxley. • **Merger and Acquisition** — Terms commonly used in merger or acquisition scenarios. Terms commonly found that are sensitive to Sarbanes-Oxley. • **Profit and Loss Statements** — Terms often used in profit and loss statements. Terms commonly found that are sensitive to Sarbanes-Oxley. • **Projected Earnings** — Terms found frequently in projected earnings information. Terms commonly found that are sensitive to Sarbanes-Oxley. • **Sales Forecast** — Terms commonly found in a sales forecast. Terms commonly found that are sensitive to Sarbanes-Oxley. • **Suspicious Activity Reports** — Terms commonly found within a suspicious activity report. Terms commonly found that are sensitive to Sarbanes-Oxley.
Spain Policy	• **Spain DNI** — Patterns related to Spanish Documento Nacional de Identidad. • **Spain IBAN** — Patterns related to Spanish IBAN.
State Privacy Laws	• **California Drivers License Law** — Commonly used expressions supporting drivers license numbers. • **Social Security Number** — Social Security Number with SSA Check and keyword check.
Turkey Policy	• **Turkey Citizen Number** — Patterns related to Turkish Citizen Number. • **Turkey IBAN** — Patterns related to Turkish IBAN.
UK Policy	• **NHS Number** — Patterns related to UK National Health Service Number. • **NINO** — Patterns related to UK National Insurance Number. • **SEDOL** — Patterns related to UK SEDOL. • **UK IBAN** — Patterns related to UK IBAN.
Uncategorized Groups	• **China Policy China National ID** — Patterns related to Chinese National ID. • **Sexual Content** — Terms relating to sex.

Custom Content Groups

The **Custom Content Groups** subtab allows administrators to define their own custom content keyword group and assist in monitoring their email. By configuring a content group, the administrator can

determine how the system reacts if it receives an email that contains text that violated that content policy. Administrators can also define a different action for each content group.

Before you begin

If the content group is enabled, then email will be filtered for that content.

Task

1 Select the content group to modify, click **Edit**.

2 In the **Group Name** field, type the custom content group.

3 In the **Content** field, list the content keywords needed to define your custom content group.

4 From the **Action** drop-down list, select one of the following options.

Option	Description
None	The email is forwarded to the recipient email address.
Quarantine	The email is sent to the recipient's content quarantine area.
Deny	The email is denied delivery.
Allow	The email is sent to the recipient email address.
Tag the message subject	The phrase "[CONTENT]" is added to the subject line of the email at the beginning of the subject text and the email is sent to the recipient email address.
Encrypt Message	Is available for outbound content groups if the user has subscribed to encryption.

The combination for maximum encrypted message size includes the message header, body and attachment cannot exceed 30 MB for encrypted messages.

5 If you want to send a copy of the email to a separate address, select a predefined distribution list from the **Silent Copy** drop-down list.

6 Select **Enable** to enact the filtering for that document.

7 Click **Save**.

Apply actions to your registered document

After you have uploaded your registered documents, you may assign an appropriate action to those documents.

Before you begin

The **Apply Actions** option is only available on the outbound policy content group page if you have encryption enabled.

Task

1 Select the content group to modify, click **Edit**.

2 In the **Action** drop-down field, select one of the following options.

Option	Description
None	The email is forwarded to the recipient email address.
Quarantine	The email is sent to the recipient's content quarantine area.
Deny	The email is denied delivery.
Allow	The email is sent to the recipient email address.
Tag the message subject	The phrase "[CONTENT]" is added to the subject line of the email at the beginning of the subject text and the email is sent to the recipient email address.
Encrypt Message	Is available for outbound content groups if the user has subscribed to encryption.

The combination for maximum encrypted message size includes the message header, body and attachment cannot exceed 30 MB for encrypted messages.

3 If you want to send a copy of the email to a separate address, select a predefined distribution list from the **Silent Copy** drop-down list.

4 Select **Enable** to enact the filtering for that document.

5 Click **Save**.

Content Notifications

The Notifications subtab allows you to configure whether the sender or recipient is notified if an email violates a specific email filtering policy, other than spam policies, and a specific action is applied to it.

HTML Shield tab

HTML Shield allows you to apply an additional layer of security to HTML formatted emails by eliminating varying levels of potentially harmful HTML content. This is useful for blocking potential *zero-hour threats*, or threats that target previously unknown vulnerabilities, that may be hidden in HTML code. HTML Shield is particularly useful for users who have received dangerous emails in the past.

Table 5-14 HTML Shield options

Option	Definition
Save	Click to save changes.
Cancel	Click to cancel changes.

Table 5-14 HTML Shield options *(continued)*

Option	Definition
HTML Shield Protection	Specifies the level of protection: • **Low** — Addresses the most common HTML-based sources of potential exploits by removing malicious HTML tags. • **Medium** — Adds additional security options by disabling Javascript, Java, and ActiveX as well as removing threats that may be hidden in HTML comments or invalid HTML attributes. • **High** — Provides the highest level of protection by removing all HTML content. • **None** — HTML Shield Protection is not active.
Options for Low and Medium settings	Specifies additional options you can set when selecting Low or Medium HTML Shield protection.

Attachments

Attachment filtering provides the ability to control the types and sizes of allowed attachments entering your email network.

The following explains the different attachment types of filters applicable to this system.

- **Attachment Filtering by File Type** — Enable or disable filtering of attachments by file type. File type is determined using the file extension, MIME content type, and binary composition.
- **Attachment Filtering by Size** — Designate a maximum allowed size for each enabled attachment type.
- **Custom Attachment Rules by Filename** - Configure custom rules using filenames that override the global settings for an attachment file type. You can designate that the rule use the entire filename or any part of the filename.
- **Filtering for Files Contained within a Zip File Attachment** — Configure custom rules to cause Email Protection to analyze the files within a zip file attachment, if possible, to determine if a file in the zip file violates attachment policies. If the zip file cannot be analyzed, designate the email action to be applied.
- **Encrypted or "High Risk" Zip File Attachment Rules** — Configure custom rules for emails with encrypted zip files and/or zip files that are considered high risk (too large, too many nested levels, etc.).

File Types

The **File Types** subtab allows you to configure how the system reacts if it receives an email of a specified attachment type or if an attachment violates attachment policies.

> **Before you begin**
>
> By default, all attachments which are not on the allow list will be filtered with the selected action. Attachments are scrutinized by filename, MIME content type and binary composition.

Attachment File Types

Allowed attachment file types and their files extensions.

Table 5-15 File Types that are allowed.

Allowed File Types	File Extensions
Microsoft Word documents	*.doc, *.dot, *.rtf, *.wiz
Microsoft PowerPoint documents	*.pot, *.ppa, *.pps, *.ppt, *.pwz
Microsoft Excel documents	*.xla, *.xlb, *.xlc, *.xlk, *.xls, *.xlt, *.xlw

Table 5-15 File Types that are allowed. *(continued)*

Allowed File Types	File Extensions
Microsoft Access files	*.adp, *.ldb, *.mad, *.mda, *.mdb, *.mdz, *.snp
Other Microsoft Office files	*.cal, *.frm, *.mbx, *.mif, *.mpc, *.mpd, *.mpp, *.mpt, *.mpv, *.win, *.wmf
Office Word 2007 XML documents	*.docx
Office Word 2007 XML macro-enabled document	*.docm
Office Word 2007 XML template	*.dotx
Office Word 2007 XML macro-enabled template	*.dotm
Office Excel 2007 XML workbook	*.xlsx
Office Excel 2007 XML macro-enabled workbook	*.xlsm
Office Excel 2007 XML template	*.xltx
Office Excel 2007 XML macro-enabled template	*.xltm
Office Excel 2007 binary workbook (BIFF12)	*.xlsb
Office Excel 2007 XML macro-enabled add-in	*.xlam
Office PowerPoint 2007 XML presentation	*.pptx
Office PowerPoint 2007 macro-enabled XML presentation	*.pptm
Office PowerPoint 2007 XML template	*.potx
Office PowerPoint 2007 macro-enabled XML template	*.potm
Office PowerPoint 2007 macro-enabled XML add-in	*.ppam
Office PowerPoint 2007 XML show	*.ppsx
Office PowerPoint 2007 macro-enabled XML show	*.ppsm
Adobe Acrobat (PDF) Files	*.abf, *.atm, *.awe, *.fdf, *.ofm, *.p65, *.pdd, *.pdf
Macintosh Files	*.a3m, *.a4m, *.bin, *.hqx, *.rs_
Compressed or Archived Files	*.arj, *.bz2, *.cab, *.gz, *.gzip, *.jar, *.lah, *.lzh, *.rar, *.rpm, *.tar, *.tgz, *.z, *.zip
Audio Files	*.aff, *.affc, *.aif, *.aiff, *.au, *.m3u, *.mid, *.mod, *.mp3, *.ra, *.rmi, *.snd, *.voc, *.wav
Video/Movie Files	*.asf, *.asx, *.avi, *.lsf, *.lsx, *.m1v, *.mmm, *.mov, *.movie, *.mp2, *.mp4, *.mpa, *.mpe, *.mpeg, *.mpg, *.mpv2, *.qt, *.vdo
Image Files	*.art, *.bmp, *.dib, *.gif, *.ico, *.jfif, *.jpe, *.jpeg, *.jpg, *.png, *.tif, *.tiff, *.xbm
Executables Defaults to **Disallow**	*.bat, *.chm, *.class, *.cmd, *.com, *.dll, *.dmg, *.drv, *.exe, *.grp, *.hlp, *.lnk, *.ocx, *ovl, *.pif, *.reg, *.scr, *.shs, *.sys, *.vdl, *.vxd
Scripts Defaults to **Disallow**	*.acc, *.asp, *.css, *.hta, *.htx, *.je, *.js, *.jse, *.php, *.php3, *.sbs, *.sct, *.shb, *.shd, *.vb, *.vba, *.vbe, *.vbs, *.ws, *.wsc, *.wsf, *.wsh, *.wst

Table 5-15 File Types that are allowed. *(continued)*

Allowed File Types	File Extensions
ASCII Text Files	*.cfm, *.css, *.htc, *.htm, *.html, *.htt, *.htx, *.idc, *.jsp, *.nsf, *.plg, *.txt, *ulx, *.vcf, *.xml, *.xsf
Postscript Files	*.cmp, *.eps, *.prn, *.ps

Filename Policies

The **Filename Policies** subtab designates the rules for specific filenames. The structure allows you to specify *custom* rules that override the global rules defined in the file types tab.

Before you begin

Attachment filtering policies are applied in the following order.

1 **Filename** policies

2 **Additional** policies

3 **File Types** policies

Task

1 From the filter drop-down list, select one of the following.

Option	Description
Is	Email Protection filters for file names that have an exact match to the text in the value field. For example, if you want to filter for the file name config.exe and no others, you must select Is and then type config.exe in the value field. For this example, the *Is* option has the meaning *File name IS config.exe.*
Contains	Email Protection filters for file names that contain the text in the value description anywhere within the filename string. For example, if you want to filter for any file that contains config in its name, like postconfig or config.ini, select this option.
Ends with	Email Protection filters for file names that end with the text in the value description. For example, if you want to filter for any executable files ending with .exe, select this option.

In the **Value** field, type the name or partial name with which Email Protection should search incoming email.

2 From the **Action** drop-down list, select one of the following options.

Option	Description
Quarantine	The email is sent to the recipient's content quarantine area.
Deny	The email is denied delivery.
Allow	The email is sent to the recipient email address.
Strip	Email Protection strips the attachment from the email and the email is sent to the recipient. Text is inserted into the email notifying the recipient that an attachment has been stripped.
Encrypt Message	Is available for outbound content groups, if the user has subscribed to encryption.

The combination for maximum encrypted message size includes the message header, body and attachment cannot exceed 30 MB for encrypted messages.

3 If you want to send a copy of the email to a separate address, select a predefined distribution list from the **Silent Copy** drop-down list.

4 Click **Save**.

Additional Policies

The **Additional Policies** subtab designates the additional rules for predefined file types. These rules allow you to refine the policies for allowed file types. These rules override the rules defined in the **File Type Policies** tab.

Additional Policies Details

From the drop-down lists, select the appropriate settings for each of the following.

Table 5-16 Additional messages

Option	Description
Message contains a high risk zip attachment:	A zip file is an archive file that contains other files and folders, typically in a compressed format. There are several ways in which an attacker can create a zip file that when delivered in an email message, poses a threat to the recipient. These threats include driving a recipient's mailbox over-quota, running the recipient's computer out of storage space, locking up or crashing the recipient's computer. A zip attachment will be considered high risk if it violates any of the following rules: • The zip file itself is too large >. • A file contained in the zip file is too large >. • The zip file contains too many files >. • The compression rate is too high > % compressed. • The zip file contains too many levels of nesting > levels.
Message contains an encrypted zip attachment:	An encrypted zip attachment is a zip archive file that is password protected and encrypted. Encrypted zip attachments in an email message pose a threat to the recipient because they can be infected with viruses that may not be detected by virus software.
File in zip attachment violates attachment policy:	A zip file is an archive file that contains other files and folders, typically in a compressed format. A zip archive contains an index which lists each file included in the archive by name. The filenames listed in the archive index are scanned to determine if an attachment type or attachment filename policy has been violated. If so, you determine what action is taken on the zip attachment. You may choose to do nothing or choose to have the action associated with the violated attachment policy to be taken. Attachment-filtering policies are applied in the following order. 1 **Filename** policies 2 **Attachment** policies 3 **File Type** policies
Deny messages where the total size exceeds:	• An inbound message can be denied if it exceeds a maximum capacity anywhere from 5 MB to MB System Maximum. • An outbound message can be denied if it exceeds a maximum capacity anywhere from 10 MB to MB System Maximum. Notifications are not sent to the sender or recipient for maximum message size violations.

Notifications for Attachments

The Notifications subtab allows you to configure whether the sender or recipient is notified if an email violates a specific email filtering policy, other than spam policies, and a specific action is applied to it.

Allow Deny

Allow / deny allows you to define lists of domains, email addresses or IP addresses that are always *denied* (blacklists) or always *accepted* (whitelists) at multiple levels.

The administrator-level lists override the user-level lists in a top-down manner: global lists first, policy set lists next, and lastly user-level lists. For example, if the same address is added to a user-level allow list and the policy set deny list, the address is always denied.

At the same level, the allow list overrides the deny-list. For example, if you designate a range of email addresses (for example, by designating an entire domain) in the deny list, but then designate a single email address from that domain in the allow list, the email from that single address will always be accepted while the email from any other address in the domain in the deny list will always be denied.

The same address string cannot be added multiple times in the same list or added to both the allow or deny lists.

Be aware that emails that have been quarantined by Email Protection may not need to be added to deny lists because they are already being blocked from entering your email network.

Sender Allow

The **Sender Allow** subtab allows you to define a list of sender email addresses whose email will be accepted for delivery without email filtering for content and spam, but filters for viruses. To enter values into the sender allow list complete the following information.

The setup for **Sender Allow** is only available to certain user roles, when a user-defined policy set is selected. If you want to include the values listed for the default inbound policy set, select the checkbox located beneath the list.

Task

1 Enter an address into the **Domain, Email Address, or IP Address**: field. Use one of the following formats.

Option	Description
An email address - for example:	• user@example.com • user@sub.example.com • user@example.*.com
A domain name - for example:	• example.com • *.example.com • example.* • mysubdomain.*.*
An IP address - IP addresses must contain 4 octets; Each octet must be numeric, between 0 and 255, OR a wildcard.	• 10.20.0.4 • 10.20.*.4 • 10.*.*.* • *.20.*.16 • 10.0.62.0/24

Wildcards and numbers cannot be mixed in an octet.

Examples include:

2 Click **Add**.

3 Click **Save**.

4 Click **Download** to download a csv file that can be opened in Microsoft Excel.

The SPF setting (enable or disable) does not appear in the download list file.

Tasks

- *Subscribe to Default Inbound Sender Allow List* on page 50
  Selecting the subscription to the Default Inbound Sender Allow default list adds the default domain policy to your customized inbound sender allow list. The default list can be viewed by clicking the default inbound selection under the policies tab.
- *Validate SPF* on page 50
  Sender Policy Framework (SPF) is a method that prevents sender address forgery. After you have added an entry to the allow list, you have the ability to add an SPF verification setting for that sender.
- *Bulk Upload* on page 50
  To upload a file with a predefined list, complete the following steps.

Subscribe to Default Inbound Sender Allow List

Selecting the subscription to the Default Inbound Sender Allow default list adds the default domain policy to your customized inbound sender allow list. The default list can be viewed by clicking the default inbound selection under the policies tab.

If the default list changes, your subscription to the default is updated to reflect those changes.

Validate SPF

Sender Policy Framework (SPF) is a method that prevents sender address forgery. After you have added an entry to the allow list, you have the ability to add an SPF verification setting for that sender.

Before you begin

The SPF verification does not apply to IP addresses.

To add an SPF verification to an existing address complete the following.

Task

1 Select the address you wish to add under the **Validate SPF** table. This will activate the **Require SPF Validation** and **Remove SPF Validation** buttons.

2 Select **Require SPF Validation**. A green check mark will display next to your selection.

3 Click **Save**.

4 Select **Remove SPF Validation** to remove your SPF selections. A red X will display next to your removed selection.

When the **Require SPF Validation** feature is enabled, then an SPF result of softfail or permfail will cause the allow list entry to be ignored.

Bulk Upload

To upload a file with a predefined list, complete the following steps.

Before you begin

The predefined list must be in the following format.

- Must be a text file
- One email address per line
- File must be available for your browser to access

Task

1 To **Upload** a file with a predefined list of domains, click **Browse** and select a file to upload. After you select the file, click **Upload**. The file is added to the domain list.To remove a value from the list, select it in the list box and click **Remove**. Select **Remove All** to remove all entries.

2 Click **Save**.

The maximum number of values allowed in any list is . Any duplicate or invalid values are discarded automatically.

Sender Deny

The **Sender Deny** allows you to define a list of sender email addresses whose email will not be accepted for delivery. If an email address is entered here, users will not be able to override this setting even if the email address is entered in their user-level allow list.

To enter values into the **Sender Deny List** complete the following information.

Task

1 Enter an address into the**Domain, Email Address, or IP Address:** field. Use one of the following formats.

Option	Description
An email address - for example:	• user@example.com • user@sub.example.com • user@example.*.com
A domain name - for example:	• example.com • *.example.com • example.* • mysubdomain.*.*
An IP address - IP addresses must contain 4 octets; Each octet must be numeric, between 0 and 255, OR a wildcard.  **Wildcards and numbers cannot be mixed in an octet.** **Examples include:**	• 10.20.0.4 • 10.20.*.4 • 10.*.*.* • *.20.*.16 • 10.0.62.0/24

2 Click **Add**.

3 Click **Save**.

Tasks

- *If the Sender is on the Sender Deny List* on page 52
  To select one of the available message disposition options complete the following.
- *Bulk Upload* on page 52
  To upload a file with a predefined list, complete the following steps.

If the Sender is on the Sender Deny List

To select one of the available message disposition options complete the following.

Click one of the available message disposition options (the selection will also apply to an end-users' deny list).

- **Deny delivery** — Senders in the policy set's deny list receive a notification that the message was denied by the intended recipient.
- **Accept and silently discard the message** - Senders in the policy set's deny list are *not* sent a notification that their messages were never sent to the intended recipient.

Task

- **Subscribe to Default Inbound Sender Deny List** —Select the subscription to the **Default Inbound Sender Deny** default list to add the default domain policy to a customized inbound sender deny list. The default list can be viewed by selecting the default inbound selection under the policies tab.

  If the default list changes, your subscription to the default is updated to reflect those changes.

Bulk Upload

To upload a file with a predefined list, complete the following steps.

> **Before you begin**
>
> The predefined list must be in the following format.
>
> - Must be a text file
> - One email address per line
> - File must be available for your browser to access

Task

1. To **Upload** a file with a predefined list of domains, click **Browse** and select a file to upload. After you select the file, click **Upload**. The file is added to the domain list.To remove a value from the list, select it in the list box and click **Remove**. Select **Remove All** to remove all entries.
2. Click **Save**.

The maximum number of values allowed in any list is . Any duplicate or invalid values are discarded automatically.

Recipient Shield

The **Recipient Shield** allows you to define a list of recipient email addresses and designate an action for any emails sent to that recipient. Emails received for all alias email addresses for the designated user

account will also be included in the recipient shield processing. For example, you can designate that emails received to an ex-employee's user account are always denied.

For service-provider customers, the email addresses you enter apply only to the domain you are configuring. For enterprise-customers, the email addresses you enter apply to all domains within the enterprise. However, if groups are administered, enterprise-customers can create a unique recipient list within a custom policy set and then assign one or more groups to that policy set.

Task

1 Enter an address into the **Email Address** field.

Email address must contain a valid domain from the current customer.

2 Click **Add**.

3 Click **Save**.

Tasks

- *If the Recipient is on the Recipient Shield List* on page 53
  To select the desired action to be applied when an email is received for one of the addresses in the Recipient Shield List box, complete the following steps.
- *Bulk Upload* on page 53
  To upload a file with a predefined list, complete the following steps.

If the Recipient is on the Recipient Shield List

To select the desired action to be applied when an email is received for one of the addresses in the Recipient Shield List box, complete the following steps.

Task

1 Select the desired action to be applied when an email is received for one of the addresses in the **Recipient Shield List** field. Valid values include the following.

Option	Description
Accept and silently discard the message	The email is accepted, but is discarded without notification.
Deny delivery	The email is denied delivery.
Do nothing	The email is forwarded to the recipient email address with no processing applied.

2 Subscribe to **Default Inbound Recipient Shield List**.

Select the subscription to the **Default Inbound Recipient Shield** default list to add the default domain or group policy to your customized inbound recipient shield list. The default list can be viewed by selecting the default inbound selection under the policies tab.

If the default list changes, your subscription to the default is updated to reflect those changes.

Bulk Upload

To upload a file with a predefined list, complete the following steps.

Before you begin

The predefined list must be in the following format.

- Must be a text file
- One email address per line
- File must be available for your browser to access

Task

1 To **Upload** a file with a predefined list of domains, click **Browse** and select a file to upload. After you select the file, click **Upload**. The file is added to the domain list.To remove a value from the list, select it in the list box and click **Remove**. Select **Remove All** to remove all entries.

2 Click **Save**.

The maximum number of values allowed in any list is . Any duplicate or invalid values are discarded automatically.

Email Authentication

Email Authentication features help verify the validity of email senders and protect their contents in transit. This is useful for identifying and blocking some types of forged messages or phishing attempts.

Email Authentication features include:

- Enforced TLS
- Enforced SPF
- Enforced DKIM

Enforced TLS

Transport Layer Security (TLS) is used to encrypt inbound and outbound emails. **Enforced TLS** can require that TLS is used to receive an inbound email from or, deliver an outbound email to the specified domains. If Enforced TLS is specified and TLS cannot be negotiated, the message is denied and notifications can optionally be sent to the sender, recipient, or both.

If an Enforced TLS subscriber wants to send and receive email to or from partners that also use TLS, a certificate generated by a recognized certificate authority (CA) is generated.

Encryption subscribers must enforce TLS to ensure that their email is encrypted.

The following recognized global list of trusted CAs includes:

- AddTrust
- Comodo
- DigiCert Inc
- DST - Digital Signature Trust
- Entrust.net
- Equifax
- GlobalSign
- Go Daddy
- GeoTrust
- RSA Data Security
- SecureNet
- StartCom
- TC TrustCenter
- Thawte
- Trustis FPS
- Valicert
- Usertrust
- Verisign

- GTE CyberTrust
- IPS Servidores
- Netlock
- Network Solutions
- QuoVadis
- Tata
- Starfield Tech
- SwissSign
- SecureTrust /Trustwave

Add an Enforced TLS

Add a **Sender/Inbound** or a **Recipient/Outbound** domain or sub-domain to an enforced TLS list, to specify that TLS is enforced on mail from that sender/recipient's domain or sub-domain.

Before you begin

Enforced TLS requires a negotiation between our mail transfer agent and yours to be successful. You must have TLS turned on at your end to accommodate this transaction. Refer to your MTA software manual on how to enable/turn-on TLS to ensure TLS is implemented in your system prior to setting up your domain lists.

Task

1 Enter a domain in the **Domain** field. Click **Add**.

To enter values for the TLS domain list, enter the full address of the sender domain and/or sub-domain, or use part of the domain using wildcards. Specifying a sender domain does not automatically include any sub-domains of that domain. The following list demonstrates different examples of entries using a wildcard (*).

Table 5-17 Wildcard Examples

Domain Example	Matches
*.example.com	*subdomain1.example.com* and *subdomain2.example.com*
example.*	*example.com* and *example.net*
subdomain.*.*	*subdomain.example.com* and *subdomain.someplace.com*
subdomain.*.example.com	*subdomain.something.example.com* and *subdomain.else.example.com*

If the subdomain is not going to be entered using the wildcard character, the sub-domain must be explicitly defined.

The maximum number of values allowed in the **Domain** list is. Any duplicate or invalid values are discarded automatically.

2 To remove a value from the list, select it in the list box and click **Remove**. Select **Remove All** to remove all entries.

3 To generate a CA validation on existing domains, select the domain requiring the CA and click **Validate CA**

4 Click **More Options**.

Option	Description
Upload Enforced TLS List (appends to existing list):	To **Upload** a file with a predefined list of domains, click **Browse** and select a file to upload. After you select the file, click **Upload**. The file is added to the domain list.
Download Enforced TLS List (be sure to save changes first):	To download the domain list to a CSV file, click **Download**.

5 Click **Save**.

Select the **Subscribe to Default Inbound policy Enforced TLS List** to include the Enforced TLS list from the default policy with the current policy.

If the Enforced TLS settings in the default policy change, the subscription automatically updates any subscribed policies.

Enforce SPF

Sender Policy Framework (SPF) can be used by email recipients to determine if the messages they receive were sent from an IP address authorized by the domain owner, which can help detect spoofing. SPF can only help detect spoofing when domain owners implement and maintain SPF records in Domain Name Server (DNS).

To implement SPF, domain owners must create special DNS entries which list the IP addresses that are authorized to send email from their domain. Email recipients must compare an email's source IP address to the IP address in the domain owner's DNS SPF records. If they match, it is reasonable to assume that the message was sent by the domain owner or an authorized third party. If they don't match, the recipient should be suspicious of the message because it might be a cleverly masked phishing attempt.

Important SPF information:

- Many domain owners have not implemented SPF, including many well-known commercial domains, since SPF implementation is voluntary.
- Even those that have implemented SPF might have outdated or inaccurate records, resulting in false positives. The only way to resolve this is to contact the domain owner and ask them to correct the issue.
- Nothing prevents spammers and hackers from implementing SPF, so it is not a reliable spam indicator.
- Many organizations allow third parties to send email on behalf of their domain (authorized spoofing). The IP addresses of these third parties must be included in the domain owner's SPF records in order for recipients to be able to successfully validate these types of messages.
- Hosted email providers often give the same SPF records to all their domain owners, making it impossible to distinguish one domain owner from another, thus reducing usefulness of the technology.
- Even when SPF is implemented and enforced, it is still possible for spammers to create very convincing emails coming from domains that are similar to, but not exactly the same, as the domain normally used by the organization being spoofed; therefore, continued user training and caution is advised.

You can enable Enforced SPF in two distinct ways; for specific domains and for all domains.

Create an enforced SPF domain

To require SPF validation for specific domains, complete the following.

To enable Enforced SPF for specific domains, add them to the domain list. Domains in the list must pass an SPF check or the message is denied.

Require SPF validation for specific domains

Task

1 Enter a domain in the **Domain** field. Click **Add**.

To enter values for the SPF domain list, enter the full address of the sender domain and/or sub-domain, or use part of the domain using wildcards. Specifying a sender domain does not automatically include any sub-domains of that domain. The following list demonstrates different examples of entries using a wildcard (*).

Table 5-18 Wildcard Examples

Domain Example	Matches
*.example.com	*subdomain1.example.com* and *subdomain2.example.com*
example.*	*example.com* and *example.net*
subdomain.*.*	*subdomain.example.com* and *subdomain.someplace.com*
subdomain.*.example.com	*subdomain.something.example.com* and *subdomain.else.example.com*

If the subdomain is not going to be entered using the wildcard character, the sub-domain must be explicitly defined.

The maximum number of values allowed in the **Domain** list is. Any duplicate or invalid values are discarded automatically.

2 To remove a value from the list, select it in the list box and click **Remove**. Select **Remove All** to remove all entries.

3 **More Options**

Option	Description
Upload Enforced SPF List (appends to existing list):	To **Upload** a file with a predefined list of domains, click **Browse** and select a file to upload. After you select the file, click **Upload**. The file is added to the domain list.
Download Enforced SPF List (be sure to save changes first):	To download the domain list to a CSV file, click **Download**.

4 Click **Save**.

Select the **Subscribe to Default Inbound policy Enforced SPF List** to include the Enforced SPF list from the default policy with the current policy.

If the Enforced SPF settings in the default policy change, the subscription automatically updates any subscribed policies.

Enforce SPF for all domains not on the list

Select actions to apply to *all other* domains, not in the domain list, by using the drop-down lists. For domains not added to a domain list, the following actions can be applied.

If a domain is listed, the action is *deny if the SPF fails* or *allow if the SPF passes*.

Task

1 Select the appropriate SPF action (deliver, deny, tag subject) using the drop-down lists under the **For Domains not in the list** option, for the following criteria:

- when SPF is available but validation fails – the domain owner has implemented SPF but the message did not come from an IP address included in the SPF record
- when SPF is not available – the domain owner has not implemented SPF, it is not possible to SPF verify the message
- when SPF is available and validation succeeds

When the action is *tag subject*, tags are applied to the end of the subject. The tags are:

- [WARNING: SPF validation failed]
- [WARNING: SPF validation unavailable]
- [SPF verified]

2 Click **Save**.

When domains are present in the domain list and actions are specified for all other domains, the domain list action of deny takes preference over the actions that apply to all other domains.

Enforced DKIM

DomainKeys Identified Mail (DKIM) is part of the Email Authentication suite designed to verify the email sender and the message integrity. The DomainKeys specification has adopted aspects of identified internet mail to create an enhanced protocol called DomainKeys Identified Mail.

Create an enforced DKIM domain

To require DKIM validation for specific domains, complete the following.

Task

1 Enter a domain in the **Domain** field. Click **Add**.

To enter values for the DKIM domain list, enter the full address of the sender domain and/or sub-domain, or use part of the domain using wildcards. Specifying a sender domain does not automatically include any sub-domains of that domain. The following list demonstrates different examples of entries using a wildcard (*).

Table 5-19 Wildcard Examples

Domain Example	Matches
*.example.com	*subdomain1.example.com* and *subdomain2.example.com*
example.*	*example.com* and *example.net*
subdomain.*.*	*subdomain.example.com* and *subdomain.someplace.com*
subdomain.*.example.com	*subdomain.something.example.com* and *subdomain.else.example.com*

If the subdomain is not going to be entered using the wildcard character, the sub-domain must be explicitly defined.

The maximum number of values allowed in the **Domain** list is. Any duplicate or invalid values are discarded automatically.

2 To remove a value from the list, select it in the list box and click **Remove**. Select **Remove All** to remove all entries.

3 **More Options**

Option	Description
Regardless of Sender Domain	From the drop-down lists, select the appropriate DKIM action (deliver, deny, tag subject) for the following criteria: • when a DKIM signature is present but is not valid. • when no DKIM signature is present. • when a valid DKIM signature is present. When the action is tag subject, tags are applied to the end of the subject. The tags are: WARNING: DKIM validation failed, DKIM verified, WARNING: DKIM validation unavailable .
Upload Enforced DKIM List (appends to existing list):	To **Upload** a file with a predefined list of domains, click **Browse** and select a file to upload. After you select the file, click **Upload**. The file is added to the domain list.

Option	Description
Download Enforced DKIM List (be sure to save changes first):	To download the domain list to a CSV file, click **Download**.

4 Click **Save**.

Select the **Subscribe to Default Inbound policy Enforced DKIM List** subscription to add the appropriate inbound/outbound default domain policy to your customized Enforced DKIM policy. The default list can be viewed by selecting the corresponding inbound/outbound default selection under the policies tab. This option is only available in custom (non-default) policy sets.

If the default list changes, your subscription to the default is updated to reflect those changes.

Enforce DKIM for all domains not on the list

Select actions to apply to *all other* domains, not in the domain list, by using the drop-down lists. For domains not added to a domain list, the following actions can be applied.

If a domain is listed, the action is *deny if the DKIM fails* or *allow if the DKIM passes*.

Task

1 Select the appropriate DKIM action (deliver, deny, tag subject) using the drop-down lists under the **For Domains not in the list** option, for the following criteria:

- when a DKIM signature is present but is not valid
- when no DKIM signature is present
- when a valid DKIM signature is present

When the action is *tag subject*, tags are applied to the end of the subject. The tags are:

- [WARNING: DKIM validation failed]
- [WARNING: DKIM validation unavailable]
- [DKIM verified]

2 Click **Save**.

When domains are present in the domain list and actions are specified for all other domains, the domain list action of deny takes preference over the actions that apply to all other domains.

Email Authentication Notifications

The Notifications subtab allows you to configure whether the sender or recipient is notified if an email violates a specific email filtering policy, other than spam policies, and a specific action is applied to it.

Notifications

Use the **Notifications** setup information to send notification emails to the recipient or sender when an email is filtered because it contained a known virus, compromised content, attachment or you may also setup your own enforced TLS template. You can see the content of notifications and change it in the notifications tabs.

Notification Variables for a Virus

Within the notification emails, there are available variables that will automatically insert content from the system. For example, the variable $(DATE) will insert the date when the notification email was sent. You must manually type the variables as shown below and the variables are case-sensitive.

Variable syntax requires $({name_of_variable}), where {name_of_variable} is replaced with the predefined variable name (without the curly braces).

Table 5-20 Variables include the following:

Variable	Description
$(SUBJECT)	Inserts a variable that automatically indicates the subject of the email that violated the policy.
$(FROM)	Inserts a variable that automatically indicates the sender's email address (From: address) from the email that violated the policy. This variable inserts the From: address that is displayed in the email.
$(SENDER)	Inserts a variable that automatically indicates the sender's email address (From: address) from the email that violated the policy. This variable inserts the SMTP envelope From: address received from the sending email server.
$(TO)	Inserts a variable that automatically indicates the recipient's email address (To: address) from the email that violated the policy.
$(DATE)	Inserts a variable that automatically indicates the date when the email was received that violated the policy.
$(REASON)	Inserts a variable that automatically indicates the reason why the email violated the policy.
$(ACTION)	Inserts a variable that automatically indicates the action that was applied to the email that violated the policy.
$(DOMAIN)	Inserts a variable that automatically indicates the Domain that received the email that violated the policy.
$(MSG_HEADER)	Inserts a variable that automatically indicates the email header information from the email that violated the policy.
$(SIZE)	Inserts a variable that automatically indicates the size, including attachments, of the email that violated the policy.
$(POSTMASTER)	Inserts "postmaster@" and then your configured domain.

Set Up Notifications for a Virus

The **Virus** subtab allows you to write a notification email in a template that will alert a sender or recipient to a policy violation.

You must define one notification email template for each combination of sender, recipient, and email action for emails that violated the policy (for example, define one notification template for the combination of the destination being the sender email address and the email action of quarantine, and a different notification template for the combination of the destination being the recipient email address and the email action of quarantine).

Task

1 Select the subject you want to modify, then click **Edit**.

2 In the appropriate field, type or edit the information you want to change.

Option	Description
From	Type the address of the sender of the who will receive the notification.
Reply-to	Type the address of the recipient of the notification.
Subject	Include a header in the notification email for both sender or recipient when applicable.
Body	Give a brief description of why the party is being notified.

3 Click **Save**.

Notification Variables for Content

Within the notification emails, there are available variables that will automatically insert content from the system. For example, the variable $(DATE) will insert the date when the notification email was sent. You must manually type the variables as shown below and the variables are case-sensitive.

Variable syntax requires $({name_of_variable}), where {name_of_variable} is replaced with the predefined variable name (without the curly braces).

Table 5-21 Variables include the following:

Variable	Description
$(SUBJECT)	Inserts a variable that automatically indicates the subject of the email that violated the policy.
$(FROM)	Inserts a variable that automatically indicates the sender's email address (From: address) from the email that violated the policy. This variable inserts the From: address that is displayed in the email.
$(SENDER)	Inserts a variable that automatically indicates the sender's email address (From: address) from the email that violated the policy. This variable inserts the SMTP envelope From: address received from the sending email server.
$(TO)	Inserts a variable that automatically indicates the recipient's email address (To: address) from the email that violated the policy.
$(DATE)	Inserts a variable that automatically indicates the date when the email was received that violated the policy.
$(REASON)	Inserts a variable that automatically indicates the reason why the email violated the policy.
$(ACTION)	Inserts a variable that automatically indicates the action that was applied to the email that violated the policy.
$(DOMAIN)	Inserts a variable that automatically indicates the Domain that received the email that violated the policy.
$(MSG_HEADER)	Inserts a variable that automatically indicates the email header information from the email that violated the policy.
$(SIZE)	Inserts a variable that automatically indicates the size, including attachments, of the email that violated the policy.
$(POSTMASTER)	Inserts "postmaster@" and then your configured domain.

Set Up Notifications for a Content

The **Content** subtab allows you to write a notification email in a template that will alert a sender or recipient to a policy violation.

You must define one notification email template for each combination of sender, recipient, and email action for emails that violated the policy (for example, define one notification template for the combination of the destination being the sender email address and the email action of quarantine, and a different notification template for the combination of the destination being the recipient email address and the email action of quarantine).

Task

1 Select the subject you want to modify, then click **Edit**.

2 In the appropriate field, type or edit the information you want to change.

Option	Description
From	Type the address of the sender of the who will receive the notification.
Reply-to	Type the address of the recipient of the notification.
Subject	Include a header in the notification email for both sender or recipient when applicable.
Body	Give a brief description of why the party is being notified.

3 Click **Save**.

Notification Variables for an Attachment

Within the notification emails, there are available variables that will automatically insert content from the system. For example, the variable $(DATE) will insert the date when the notification email was sent. You must manually type the variables as shown below and the variables are case-sensitive.

Variable syntax requires $({name_of_variable}), where {name_of_variable} is replaced with the predefined variable name (without the curly braces).

Table 5-22 Variables include the following:

Variable	Description
$(SUBJECT)	Inserts a variable that automatically indicates the subject of the email that violated the policy.
$(FROM)	Inserts a variable that automatically indicates the sender's email address (From: address) from the email that violated the policy. This variable inserts the From: address that is displayed in the email.
$(SENDER)	Inserts a variable that automatically indicates the sender's email address (From: address) from the email that violated the policy. This variable inserts the SMTP envelope From: address received from the sending email server.
$(TO)	Inserts a variable that automatically indicates the recipient's email address (To: address) from the email that violated the policy.
$(DATE)	Inserts a variable that automatically indicates the date when the email was received that violated the policy.
$(REASON)	Inserts a variable that automatically indicates the reason why the email violated the policy.
$(ACTION)	Inserts a variable that automatically indicates the action that was applied to the email that violated the policy.
$(DOMAIN)	Inserts a variable that automatically indicates the Domain that received the email that violated the policy.
$(MSG_HEADER)	Inserts a variable that automatically indicates the email header information from the email that violated the policy.

Table 5-22 Variables include the following: *(continued)*

Variable	Description
$(SIZE)	Inserts a variable that automatically indicates the size, including attachments, of the email that violated the policy.
$(POSTMASTER)	Inserts "postmaster@" and then your configured domain.

Set Up Notifications for an Attachment

The **Attachment** subtab allows you to write a notification email in a template that will alert a sender or recipient to a policy violation.

You must define one notification email template for each combination of sender, recipient, and email action for emails that violated the policy (for example, define one notification template for the combination of the destination being the sender email address and the email action of quarantine, and a different notification template for the combination of the destination being the recipient email address and the email action of quarantine).

Task

1 Select the subject you want to modify, then click **Edit**.

2 In the appropriate field, type or edit the information you want to change.

Option	Description
From	Type the address of the sender of the who will receive the notification.
Reply-to	Type the address of the recipient of the notification.
Subject	Include a header in the notification email for both sender or recipient when applicable.
Body	Give a brief description of why the party is being notified.

3 Click **Save**.

Notification Variables for an Email Authentication

Within the notification emails, there are available variables that will automatically insert content from the system. For example, the variable $(DATE) will insert the date when the notification email was sent. You must manually type the variables as shown below and the variables are case-sensitive.

Variable syntax requires $({name_of_variable}), where {name_of_variable} is replaced with the predefined variable name (without the curly braces).

Table 5-23 Variables include the following:

Variable	Description
$(SUBJECT)	Inserts a variable that automatically indicates the subject of the email that violated the policy.
$(FROM)	Inserts a variable that automatically indicates the sender's email address (From: address) from the email that violated the policy. This variable inserts the From: address that is displayed in the email.
$(SENDER)	Inserts a variable that automatically indicates the sender's email address (From: address) from the email that violated the policy. This variable inserts the SMTP envelope From: address received from the sending email server.
$(TO)	Inserts a variable that automatically indicates the recipient's email address (To: address) from the email that violated the policy.
$(DATE)	Inserts a variable that automatically indicates the date when the email was received that violated the policy.
$(REASON)	Inserts a variable that automatically indicates the reason why the email violated the policy.

Table 5-23 Variables include the following: *(continued)*

Variable	Description
$(ACTION)	Inserts a variable that automatically indicates the action that was applied to the email that violated the policy.
$(DOMAIN)	Inserts a variable that automatically indicates the Domain that received the email that violated the policy.
$(MSG_HEADER)	Inserts a variable that automatically indicates the email header information from the email that violated the policy.
$(SIZE)	Inserts a variable that automatically indicates the size, including attachments, of the email that violated the policy.
$(POSTMASTER)	Inserts "postmaster@" and then your configured domain.

Set Up Notifications for Email Authentication

The **Email Authentication** subtab allows you to write a notification email in a template that will alert a sender or recipient to a policy violation.

You must define one notification email template for each combination of sender, recipient, and email action for emails that violated the policy (for example, define one notification template for the combination of the destination being the sender email address and the email action of quarantine, and a different notification template for the combination of the destination being the recipient email address and the email action of quarantine).

Task

1 Select the subject you want to modify, then click **Edit**.

2 In the appropriate field, type or edit the information you want to change.

Option	Description
From	Type the address of the sender of the who will receive the notification.
Reply-to	Type the address of the recipient of the notification.
Subject	Include a header in the notification email for both sender or recipient when applicable.
Body	Give a brief description of why the party is being notified.

3 Click **Save**.

Disaster Recovery

Disaster Recovery allows you to specify what actions to take when email cannot be delivered.

A customer administrator or higher must be enabled to make changes to this window.

- Defer to domain-based Email Continuity access control configured under **Disaster Recovery Setup**. Select this option to use the configuration settings from the **Disaster Recovery Setup** window.
- Allow users to use the Email Continuity webmail client. Select this option to allow users to use the **Email Continuity** webmail client when email cannot be delivered.
- Do not allow users to use the Email Continuity webmail client. Select this option if you do not want to allow users to use the Email Continuity webmail client when email cannot be delivered.

Group Subscriptions

Group Subscriptions allow you to apply a policy set to one or more of the user groups you create in Account Management.

Add a group subscription

Subscribe groups to the current policy set.

Task

For option definitions, click **Help** in the interface.

1 Select one or more groups from the **Available Groups** list.

Press and hold the Ctrl key to select multiple groups.

2 Click **Add** to add the group to the **Groups Subscribed to this Policy Set** list.

3 Click **Save**.

To remove a value from the list, select the group and click **Remove**.

6 Setup

Email Protection filters email destined for your inbound Simple Mail Transfer Protocol (SMTP) email server or servers. Your provisioner should have already defined one or more SMTP servers in the Control Console.

Contents

Inbound Servers

Email Protection filters email destined for your inbound SMTP email servers. Some inbound servers are configured when you are provisioned in the system, but you can also add additional servers as needed. You must add all email servers that receive inbound email for a given domain.

Contents

Verify setup of inbound servers

If you are new to Email Protection, your provisioner has already set up SMTP servers for you. Before continuing, you should verify that these settings are correct.

Task

For option definitions, click **Help** in the interface.

1. In Email Protection, select **Setup**.
2. In the **Setup** tab, check that you are viewing the correct domain. Click the link to select a different domain.
3. Review the SMTP settings for each server in the list to verify that it is correct.
4. Click **Save**.

Set up an inbound server

Add additional inbound servers for a domain to ensure that all servers in a domain receive inbound email.

Task

For option definitions, click **Help** in the interface.

1. In Email Protection, select **Setup**.
2. If necessary, click the domain link to change domains.
3. Click **Add New Host**.
4. In the **SMTP Host Address** field, enter the IP address or fully qualified domain name of the server host.

   CIDR notation is not allowed. If you don't have a valid DNS name for your email servers, you must use the IP address.
5. Enter the value for the **Port**.

   The default value is 25.
6. Enter a value to rank the **Preference** of the server relative to the other servers.
7. Select **Active**.

   At least one server must be selected as active.
8. Click **Save**.

Email Protection immediately routes email to the active servers.

Delete an inbound server

Remove any server entries that are no longer used by a domain.

Task

For option definitions, click **Help** in the interface.

1. In Email Protection, select **Setup**.
2. If necessary, click the domain link to change domains.
3. Find the inbound server you want to remove, select **Delete**.
4. Click **Save**.

Inbound Servers page

Use the **Inbound Servers** page to configure proper delivery to inbound SMTP servers. For each SMTP host, specify an address, port, and preference value.

Table 6-1 Inbound Server Setup option definitions

Option	Description
Domain link	Specifies the current domain. Click to select a different domain.
Save	Click to save all changes.
Cancel	Click to restore previously saved settings.

Table 6-1 Inbound Server Setup option definitions *(continued)*

Option	Description
SMTP Host list	• **SMTP Host Address** — Specifies the host that delivers inbound SMTP traffic. Enter either an IP address or a fully qualified hostname that is registered in DNS. For example, `mycompany.com`. Required field. • **Port** — Specifies the SMTP port. Typically, the value is 25. Required field. • **Preference** — Specifies the MX preference for this server. When delivering mail, the service delivers to the lowest numbered servers first. If delivery fails, the service will then deliver to the SMTP host address with the next highest number, and so on. Required field. • **Enforce TLS** — Specifies whether or not the email connection to the server is encrypted using TLS. If you select **Enforce TLS**, and your inbound mail server does not have TLS enabled, all inbound messages to the mail server will be denied. • **Active** — Specifies whether or not the SMTP host address is currently accepting traffic. • **Delete** — Select to delete the specified SMTP host.
Add New Host	Click to add a new IP address or hostname to the list.
Test Connectivity	Click to test the server connection status for all active SMTP host addresses.

Outbound Servers

Email Protection allows you to filter outbound messages sent from your email servers. If your service includes outbound filtering, use the **Outbound Servers Setup** page to configure the IP addresses for your servers.

Contents

Configure outbound servers

Enable outbound filtering by adding and configuring the IP addresses your email server uses to send email to the service.

Task

For option definitions, click **Help** in the interface.

1 In Email Protection, select **Setup** | **Outbound Servers**.

2 If necessary, click the domain link to change domains.

3 Click **Add New Address**.

4 In the **Server IP Address Range** field, enter the IP address or addresses for all outbound mail servers. CIDR notation is acceptable, up to /24.

5 If necessary, select **Enforce TLS**.

Encryption should select this option to ensure that their email is encrypted.

6 If necessary, select **More Options** to view and configure additional options.

- Select options to **Allow filtering email from** Microsoft Office 365 or Google Apps for Business.
- Configure an **Alternate Outbound Delivery Server**.

After a message is delivered to the alternate outbound delivery server, Email Protection is no longer associated with the message.

7 Click **Save**.

Wait at least 15 minutes for your new settings to take effect.

Delete an outbound server

Remove an outbound server if the range of addresses is no longer used.

Task

For option definitions, click **Help** in the interface.

1 In Email Protection, select **Setup**.

2 If necessary, click the domain link to change domains.

3 Find the outbound server you want to remove, select **Delete**.

4 Click **Save**.

Configuring your email to "smart host" or "relay" all outbound email

After you set up your outbound server addresses, you should configure the outbound "smart host" or "relay" address on your email servers. Use the address that is specified for you in the **Outbound Server Setup** page.

Email Protection uses the "smart host" or "relay" address to ensure that your outbound email is filtered. This is accomplished by routing all of your outbound email through Email Protection before it continues on to its final destination.

Outbound Servers Setup page

Use the **Outbound Servers** page to configure filtering for outbound servers. You can configure individual IP addresses, or a range of addresses using CIDR notation. Email Protection also provides support for Microsoft Office 365 and Google Apps for Business.

Table 6-2 Outbound Servers Setup option definitions

Option	Definition
Domain link	Specifies the current domain. Click to select a different domain.
Save	Click to save all changes.

Table 6-2 Outbound Servers Setup option definitions *(continued)*

Option	Definition
Outbound servers list	• **Server IP Address Range** — Enter an IP address or address range. CIDR notation is acceptable, up to /24. • **Enforce TLS** — Specifies whether or not the email connection to the server is encrypted using TLS. • **Delete** — Select to delete the specified SMTP host.
Add New Address	Click to add a new address or address range.
More Options...	Click to view additional options.
Allow filtering email from	• **Microsoft Office 365** — Select to enable support for Microsoft Office 365. • **Google Apps for Business** — Select to enable support for Google Apps for Business.
Alternate Outbound Delivery Server	• **Server IP or Hostname** — Specifies the host for alternate outbound delivery. Enter either an IP address or a fully qualified hostname. • **Port** — Specifies the SMTP port. Typically, the value is 25. • **Enforce TLS** — Specifies whether or not the email connection to the server is encrypted using TLS. • **Active** — Specifies whether or not the server is currently active.

Outbound Disclaimer

You can create text that will be appended to all outgoing emails.

Contents

Add an outbound email disclaimer

The **Outbound Disclaimer Setup** actions configure disclaimer text for each domain that appears in all outbound emails.

Task

For option definitions, click **Help** in the interface.

1 In Email Protection, select **Setup** | **Outbound Disclaimer**.

2 If necessary, click the domain link to change domains.

3 Select **Display disclaimer in outbound email messages** to enable the text area.

4 Enter your **Disclaimer Text**.

You should limit your text to a maximum of 2000 characters.

5 Click **Save**.

Outbound Disclaimer page

Customize the text you want to appear in all outbound emails.

Table 6-3 Outbound Disclaimer Setup option definitions

Option	Definition
Save	Click to save your changes.
Cancel	Click to restore previously saved settings.
Disclaimer Message Action	• **No disclaimer** — Specifies that no disclaimer is attached to outbound emails. • **Display disclaimer in outbound email messages** — Specifies that your custom text is attached to outbound emails. • **Disclaimer text** — Specifies the text you want to appear in all outbound emails. Limit your text to 2000 characters.

Disaster Recovery

Email Protection's disaster recovery services allows you to temporarily store your email remotely when communication with your email servers is unexpectedly interrupted.

Contents

Disaster recovery services

Disaster recovery includes two services, Fail Safe and Email Continuity.

Fail Safe

- Fail Safe saves messages for later delivery if your mail server becomes unavailable.
- When your mail server becomes available, Fail Safe delivers the messages.
- Users cannot access their messages while messages are in Fail Safe only.
- Fail Safe has an unlimited amount of storage capacity but removes messages that have been in Fail Safe storage for more than 5 days.

Email Continuity

- Email Continuity saves messages for later delivery if your mail server becomes unavailable.
- When your mail server becomes available, Email Continuity delivers the messages.
- Users can access their messages through a Web-based interface while messages are in Email Continuity only.
- Email Continuity also has unlimited storage capacity and removes messages that have been in Email Continuity storage for more than 60 days.

Set up automatic spooling for disaster recovery

You can set up disaster recovery to automatically begin storing, or spooling, your email after a specified number of minutes of downtime.

Task

For option definitions, click **Help** in the interface.

1. In Email Protection, select **Setup**.
2. If necessary, click the domain link to change domains.
3. Under **Configuration Settings**, select **Automatic**.
4. Select a value for the number of minutes of downtime the system should wait before automatically starting spooling.
5. If applicable, select **Allow users to use Email Continuity**.
6. Click **Save**.

Start and stop spooling for disaster recovery manually

You can manually start or stop spooling whenever you know that your email servers are down.

Task

For option definitions, click **Help** in the interface.

1. In Email Protection, select **Setup**.
2. If necessary, click the domain link to change domains.
3. Under **Configuration Settings**, select **Manual**.
4. Select an option from the drop-down.
   - Select **Start Spooling** to begin manual spooling.
   - Select **Stop Spooling** to end manual spooling.
5. Optionally, select **Deliver spooled mail when connectivity is available**.
6. If applicable, select **Allow users to use Email Continuity**.
7. Click **Save**.

Set up notifications of disaster recovery

Specify one or more email addresses that should be notified when disaster recovery events occur.

Task

For option definitions, click **Help** in the interface.

1. In Email Protection, select **Setup**.
2. If necessary, click the domain link to change domains.
3. Under **Notifications**, enter a **Recipient Email Address**.

4 Click **Add** to update the list.

You can add up to four email addresses.

5 Click **Save**.

Disaster Recovery page

The following information explains how to set up disaster recovery services.

Table 6-4 Disaster Recovery Setup option definitions

Option	Definition
Status	Specifies the current spooling status, including: • Whether spooling is on or off • If applicable, how long messages have been spooling • If applicable, the amount of messages that have been spooled, in kilobytes The animated graphic is a visual aid that indicates current spooling status, where: • **Filtering Solution** — the Email Protection filtering servers. • **Stored Mail** — Email Continuity spooling servers. • **Customer Server** — your mail servers. Click **Test Connectivity** to test connectivity with each active SMTP host address listed on the **Inbound Servers** window. When Email Continuity is active and email is spooling, a second information icon displays for **Non-Local Email Accounts**. Non-local emails occur when users are not provisioned in your system. These emails are put into a different queue. Click the link **View Non-Local Email Accounts now** to launch the non-local email inbox and identify unprovisioned users.
Configurations and Settings	• **Automatic** —Configures the system to automatically spool all incoming email when the system detects a loss of connectivity with your email server for a specified period of time. Be aware that it may take several minutes to determine that your inbound server is unavailable. During this time, and during the time delay, received emails can fail if your inbound server is unavailable. • **Manual** — You can start and stop **Disaster Recovery** spooling manually for planned email server outages such as server maintenance. • **Start Spooling** initiates manual spooling • **Stop Spooling** stop manual spooling. It may take a few minutes for manual spooling of incoming mail to start and stop. Select the **Deliver spooled email when connectivity is available** option to deliver spooled email when connectivity to the email server is restored. • **Allow users to use Email Continuity** —Allows users in the selected domain to use Email Continuity. This is for Email Continuity only and allows the user access when connectivity is disabled.
Notifications	Notifications are automatically delivered to all listed recipients when the following **Disaster Recovery** events occur: • Automatic spooling starts • Automatic unspooling starts • Automatic or manual unspooling completes In order to minimize the possibility that **Disaster Recovery** notifications cannot be delivered to listed recipients, McAfee recommends that notifications be sent to email addresses associated with mobile devices.

MX records

A mail exchange record (MX record) is a resource record in DNS that specifies the mail server that is responsible for accepting email on behalf of a domain. Each MX record specifies a host name and preference value that prioritizes mail delivery when multiple servers are available. You must configure your MX records to point to the Email Protection service in order for email to be correctly routed and filtered. Conversely, if your MX records are invalid or out-of-date, you run the risk of losing your email or limiting the effectiveness of the service.

- Complete the Inbound Servers set up process for each domain before redirecting your MX records.
- Configure the MX records for each of your domains by clicking on the name of the current domain in the menu bar.

Contents

Redirecting your MX Records

Your MX records must be configured as fully qualified domains names and then redirected to point to Email Protection. This change allows Email Protection to filter your email and route it to your mail servers. Your network administrator or domain registrar is typically the individual responsible for updating the MX records.

The information necessary for your company to make these changes is provided in the *Email Protection Activation Guide*.

It may take several days for your MX record redirect to propagate to all the email servers that send messages to your email server. During that time, your email server may still receive email directly from those email servers.

Select a region to review MX records

Select a region to use its MX records for email filtering.

Before you begin

Before changing your MX records, you must first complete the inbound servers setup process.

Task

For option definitions, click **Help** in the interface.

1 Select **Email Protection** | **Setup** | **MX Records**

2 Under **Region**, select an option to update the page.

3 Review the information under **Recommended Configuration**, **Current Configuration**, and **Lock Down**.

Use this information to configure your MX records so that mail is routed through the Email Protection service. The Lock Down information allows you to configure your email servers to only accept connections from the service.

MX Records Setup page

The **MX Records Setup** page allows you to determine what MX records to use based on your region, whether or not your MX records are configured correctly, and provides you with IP addresses that you can use to prevent attackers from bypassing the service.

Table 6-5 MX Record Setup page option definitions

Option	Definition
Region	Specifies the location of your email servers. Selecting a region determines the set of MX records you should use.
Recommended Configuration	Displays the recommended MX records for your selected region. Use these records to redirect your email to the Email Protection service. To avoid delivery issues, you should replace your current configuration with the full set of MX records.
Current Configuration	Displays the current set of MX records based on a query to your authoritative DNS provider. Each record includes the following status information: • **Invalid** — The record is unrecognized and unable to route email to the Email Protection service. • **Valid** — The record is recognized and able to route email to the Email Protection service. • **Outdated** — The record is recognized, but does not match the current recommended MX records displayed under **Recommended Configuration**. You should update your records to match what is displayed. Recheck your current configuration: • **Check Again** — Click to query your authoritative DNS provider. • **Use this DNS server** — Enter the hostname of an alternative DNS server and click **Check Again**.
Lock Down	Displays a list of files that you can use to limit SMTP connections and prevent attackers from bypassing Email Protection. Each file contains the list of IP addresses that you should allow from Email Protection. All others should be blocked. There are four different formats. Select the one that will work best with your environment: • **CIDR /21 notation** — Contains two /21 IP blocks. • **CIDR /24 notation** — Contains a list of /24 IP blocks. • **Individual IPs** — Contains a list of individual IP addresses. • **Optimized for Microsoft Office 365** — For Microsoft Office 365 users, this file contains a list of IP addresses that are formatted for use when creating an Inbound Connector in Forefront Online Protection for Exchange (FOPE).

User Creation Settings page

The user creation settings page configures the method that is used to create user accounts (email addresses) in Email Protection and designates an action to take when the recipient email address is invalid.

Table 6-6 User Creation Settings option definitions

Option	Definition
User Creation Mode	• **SMTP Discovery** — Specifies that users are created automatically based on SMTP transactions. In this mode, a user account is automatically created when several messages have been successfully delivered to a recipient who does not already have a user account. The number of delivered messages required to trigger a user creation event varies due to system-related factors. Only messages delivered to recipient email addresses in a primary domain are counted for the purpose of user creation. Messages sent to recipient email addresses in alias domains are not counted. • **Explicit** — Specifies that only the manual creation and deletion methods are enabled in Email Protection. If Email Protection receives an email that does not have an existing user account, it will perform the action designated in the **When a Recipient is Invalid** area. When the action is **Deny delivery**, the email is rejected and an error message is displayed to the sender. • **Invalid Recipient Handling** (limited to select users) — Specifies that users must explicitly define email addresses and aliases using settings under account management. After these settings are defined, users may use the link to force users to explicitly define email addresses and aliases.
When a Recipient is Invalid	• **Accept and silently discard the message** — The email is accepted, but is discarded without notification. • **Deny delivery** — The email is denied delivery. • **Do nothing** — The email is denied delivery if the customer MTA permfailed the email as invalid recipient and the user creation method is set to **Explicit**.

Registered Documents

Registering your confidential document files prevents them from being distributed outside your company using outbound emails. This feature is an enhancement to the Data Loss Prevention (DLP) package.

Contents

How registering documents prevents distribution of proprietary documents

In order to protect your sensitive documents from being sent out in emails, you should register those documents with Email Protection. Registering the document creates a fingerprint that the system can use to identify the text and filter the email before it is sent to its destination.

When you upload a file to register it, the document is broken down into smaller parts. Each individual part creates a unique fingerprint. A registered document can result in hundreds or even thousands of such fingerprints.

When a document is sent in outbound email by a user, it is also broken down in the same manner. The fingerprints of the outbound email are then compared to the ones stored in the system. If enough of the fingerprints match, the policy action you specify is taken.

- In order for a registration to be effective, the system must have a substantial amount of text content that it can fingerprint and store. Therefore, very short documents may be rejected during the registration process because there isn't enough content for the system to use.
- Registering compressed formats like zip files may not produce accurate matches.

Add a registered document

Register your sensitive documents by creating a digital fingerprint.

> **Before you begin**
> You must enable encryption to use the registered documents feature.

Task

For option definitions, click **Help** in the interface.

1. In Email Protection, select **Setup**.
2. If necessary, click the domain link to change domains.
3. Click **New** to add a file.
4. Click **Browse** and select a file on your local machine.
5. Enter a **Description**.
6. Click **Save**.

After the file uploads, the document will be in a pending status. Wait for a few minutes and then click **Refresh** to confirm that the document is registered.

Registered Documents page

The **Registered Documents** page allows you to manage the documents that you do not want distributed outside your company.

Table 6-7 Registered Documents page option definitions

Option	Definition
New	Click to register a new document.
Edit	Click to edit the description of an existing document.
Delete	Click to delete the selected document.
Refresh	Click to refresh the page and update the status of a document.

Table 6-7 Registered Documents page option definitions *(continued)*

Option	Definition
Registered Documents list	• **Filename** — The filename of the document. • **Description** — The summary of the document. • **Size** — The file size of the document. • **Registration Date** — The date the document was registered. • **Expiration Date** — The date the document expires.
New/Edit options	• **Registered Document** — Specifies the filename of the document. • **Browse** — Click to select the document on your local machine that you want to register. • **Description** — Specifies a summary of the document. Enter any relative details in the description. • **Save** — Click to save the description and upload the file if registering a new document. • **Cancel** — Click to close the options without saving your changes.

DKIM Setup

DomainKeys Identified Mail (DKIM) allows you to associate your domain name to your email messages by adding a DKIM-Signature to the message header. Doing so allows you to easily identify legitimate email and can help make phishing attacks easier to detect.

Contents

Set up DKIM

To configure DKIM for your outbound mail, you should add DKIM keys to DNS.

Before you begin

DKIM is only available if an outbound package has been associated with the domain.

Configure your outbound servers.

Task

For option definitions, click **Help** in the interface.

1 In Email Protection, select **Setup** | **DKIM Setup**.

2 If necessary, click the domain link to change domains.

3 Click **Generate Keys**.

4 Before continuing, create a DNS TXT record for the specified hostname.

5 Copy and paste the DKIM keys into the new file.

6 Once the DKIM keys have been added to DNS, click **Validate**.

7 When the record validates successfully, click **Activate**.

A DKIM-signature is attached to the message header of all outbound emails.

DKIM Setup page

The **DKIM Setup** page allows you to add DKIM signatures to outbound mail.

Table 6-8 DKIM Setup page option definitions

Option	Definition
Generate Keys	Click to generate a key pair. This is the first step in the process.
Validate	Click to ensure that the DNS entry is correct. If the DNS entry does not validate, go back and make sure that you entered the value correctly.
Activate	Click to activate your DKIM signature.
Deactivate	Click to delete your active DKIM signature.

7 Message Audit

Message Audit provides a basic self-service message audit capability that allows you to research message disposition information as well as blocked IP addresses.

Message Audit has the following capabilities:

- Message Search
- Perimeter Block Search
- Search History

Contents

Viewing message disposition information

Message audit provides a self-service message audit capability that allows you to research message disposition information.

Message disposition information describes the *disposition* of a message which can include the following.

- Whether or not the message was delivered successfully.
- If it was read.
- If it was blocked or quarantined.

Search by Message ID

Use search in the message ID option to find message disposition information based on the unique message ID of an email message.

Task

To search by message id, complete the following steps.

1 Under Email Protection, select **Message Audit**.

2 Click **Message Search**.

This option is selected by default.

3 Select **Search by Message ID**.

4 Enter the unique email ID in the **Message ID** field.

5 Click **Search**.

The results appear in the **Search Results** window.

6 View and download search results.

To...	Use these steps...
Download all Results	Click **Download** in the **Search Results** window.
Preview a result	Select an item to view it in the **Audit Details Preview** window.
View result details	Double-click an item to view it in a new **Audit Details** tab.
Download an individual result	Double-click an item to view it in a new **Audit Details** tab and click **Download**.

Search by header

Use the Search by Header option to find message disposition information based on the message header of an email message.

Task

To search by header, complete the following steps.

1 Under Email Protection, select **Message Audit**.

2 Click **Message Search**.

This option is selected by default.

3 Select **Search by Header**.

4 Enter an email header into the **Header** field.

Header search does not support wildcards.

5 Click **Search**.

The results appear in the **Search Results** window.

6 View and download search results.

To...	Use these steps...
Download all Results	Click **Download** in the **Search Results** window.
Preview a result	Select an item to view it in the **Audit Details Preview** window.
View result details	Double-click an item to view it in a new **Audit Details** tab.
Download an individual result	Double-click an item to view it in a new **Audit Details** tab and click **Download**.

Disposition Definitions

Use disposition definitions to understand each disposition, its description, and suggested actions you can take in response.

Recipient Status Disposition Descriptions

A single email may have numerous recipients. A recipient status disposition records the status for an individual recipient of the email.

The following dispositions are not included: email continuity (new, replied, forwarded, outbound, system generated messages).

Table 7-1 Recipient Disposition Description

Recipient Disposition	Description	Suggested Actions if necessary
250 Backend; Mode: normal	Message was accepted for delivery.	
250 Backend; (Mode: exempt)	Recipient is exempt from filtering.	Contact your customer administrator to remove exemption if desired.
250 OK	Successfully delivered. The user name who released the email from Quarantine may be listed in the audit details window.	
250 OK silent discard for recipient shield	Due to the recipient shield, the message had a silent discard but the recipient received an OK message.	Contact your customer administrator to allow delivery.
250 Deferred; (Mode: normal)	The sender of the message receives a successfully delivered confirmation, but a copy or notification of the message is sent to a designated recipient due to a policy violation.	Contact your customer administrator if this is in error.
521 outbound.logi.com must use TLS (Mode: normal)	Enforced TLS is enabled but the server denies the email.	Contact your email server administrator. The outbound email server may not have TLS configured
551 Sender is on domain's block list (Mode: normal)	The policy settings determine the message has a permanent failure and will not be retried.	For Users - Log on to the Control Console, under Email Protection select **Policies** | **select the policy** | **Allow/Deny** to reset the domain block list. Please allow up to 15 minutes for changes to take effect.
551 Mailhost is on a global block list	The mail host is sending a high percentage of spam.	Try again in 2 hours. If it fails again, it means the IP address is continuing to send spam. Contact your mail administrator if this is in error.
551 Mailhost is on our global block list	Due to prior abuse, the sender or recipient is being blocked.	Contact your customer administrator to appeal this status.
551 Sender is on domain's block list	This sender is not allowed to send messages per policy settings.	Contact your customer administrator if this is in error.
552 Message size exceeds fixed maximum	This sender has sent a message which exceeds a policy setting maximum.	Contact your customer administrator if this is in error.

Table 7-1 Recipient Disposition Description *(continued)*

Recipient Disposition	Description	Suggested Actions if necessary
553 Mailbox is restricted	The message was sent to an address that is rejected by a recipient shield.	Contact your customer administrator.
553 Sender is on user deny list	User has added sender to his/her deny list.	Log on to the Control Console and under Email Protection select **Policies** | **Policies Set** | **Allow/Deny** to reset and remove the sender from your deny list.
553 Invalid recipient (Mode: normal)	The message was rejected because user creation was set to deny.	Contact your customer administrator. if this is in error.
554 Denied IPR	The sending IP address has recently seen a high percentage of spam.	Try again in 2 hours. If it fails again, it means the IP address is continuing to send spam. Contact your mail administrator if this is in error.
554 Denied Spamhaus	Spamhaus is a 3rd party block listing service.	Contact www.spamhaus.org to see block list or log on to the Control Console and under Email Protection select **Policies** | **select the inbound policy** | **Spam** | **More Options** | **uncheck Enable Real-time Blackhole List**.
592 Recipient does not accept mail	Recipient's email address is questionable.	Escalate to your customer administrator.

Data Status Disposition Descriptions

Data status dispositions record the status of an email in reference to the body of that email.

The following dispositions are not included: email continuity (new, replied, forwarded, outbound, system generated messages).

Table 7-2 Message Disposition Description

Message Disposition	Description	Suggested Action if necessary
250 Delivered Replied	Successful Delivery.	
250 Failsafe	Message has been accepted and is stored in failsafe.	Notify recipient their mail server is down.
250 Queued	Message is in the queue. Each message is handled differently due to policy. The queue information may be listed in the audit details window.	
250 OK qk	Message was quarantined because message contained a keyword that is rejected by your customer administrator policy. The keyword may be listed in the audit details window.	Contact your customer administrator.
250 OK qs	Message contained spam.	Contact your customer administrator if necessary.
250 OK qa	Message was quarantined because message contained an attachment that is rejected by your customer administrator policy. The attachment title may be listed in the audit details window.	Contact your customer administrator if necessary.

Table 7-2 Message Disposition Description *(continued)*

Message Disposition	Description	Suggested Action if necessary
250 OK qv	Message might contain a virus and is being quarantined. The virus name may be listed in the Audit Details window.	Contact your customer administrator if necessary.
250 OK, Silent Deny	Sender believes delivery to be successful but message was dropped by policy.	Contact your customer administrator to turn on or off silent deny.
250 encrypted	Message was delivered via the encryption inbox.	Contact your customer administrator if this is in error.
451 No Recipients	Message is received but the system is unable to verify if recipients can receive mail. Will first retry sending the message. If this is unsuccessful, will stop trying to send the message after a specified amount of time (typically 5 days).	Notify recipient.
521 Could not deliver message over TLS for domain	Enforced TLS is enabled but the server denies the email.	Contact your email server administrator. The inbound email server may not have TLS configured
551 Denied IVF	There is a high risk of viruses and worms so this type of message is automatically denied. The virus name may be listed in the Audit Details window.	Escalate to your customer administrator.
551 Denied SPAM	This type of message is automatically denied due to a spam content. The spam title may be listed in the Audit Details window.	Escalate to your customer administrator.
551 Message contains an encrypted ZIP File	This policy denies attachments that cannot be scanned.	Escalate to your customer administrator to allow.
552 message size exceeds fixed maximum message size of {whatever} (Mode: normal)	Sender believes delivery to be successful but the message exceeded maximum policy size and was discarded.	Contact your customer administrator if this is in error.
554 Denied	This policy does not allow a specific keyword. The keyword may be listed in the Audit Details window.	Escalate to your customer administrator to quarantine or Allow content.
554 Denied SPAM	This policy determined this type of message to be spam. The spam title may be listed in the Audit Details window.	Contact your customer administrator to allow.
554 Content filter will not allow this message	This policy contains an spam content group that blocked this message. The spam keyword may be listed in the Audit Details window.	Contact your customer administrator.
554 This message contains a virus	This policy denies an attachment containing this virus or this virus can not be cleaned. The virus name may be listed in the Audit Details window.	Contact your customer administrator.
554 Message Denied: Restricted attachment	The policy setting denies these attachments due to type or size. The attachment name may be listed in the Audit Details window.	Contact your customer administrator to quarantine and strip the attachment or try to clean the attachment.

Table 7-2 Message Disposition Description *(continued)*

Message Disposition	Description	Suggested Action if necessary
554 Denied, restricted attachment (contains two restricted attachments)	The policy setting denies these attachments due to type or size. The attachment name may be listed in the Audit Details window.	Contact your customer administrator to allow.
554 must use TLS (Mode normal)	TLS is not enforced.	Coordinate with the mail administrator of the failed domain to ensure TLS is enabled on both mail servers.
554 Error: SPF validation failed because no SPF records available	Denied due to an enforced SPF policy violation.	Contact your customer administrator if this policy is in error.

Search by message details

Use the message details option to view message disposition information based on specific parts of the message (for example, the sender or the subject line).

Task

To search by message details, complete the following steps.

1 Under Email Protection, select **Message Audit**.

2 Click **Message Search**.

This option is selected by default.

3 Select **Search by Message Details**.

This option is selected by default.

4 Select your search criteria by completing one or more of the following.

A valid to or from email address is required.

- From the drop-down list, select the correct **Domain** associated with the chosen customer.
- Enter the domain address in the **From** field.

You may use wildcards for this search. Examples include:

- (*) wildcard to represent zero or any number of alphanumeric values.
- (?) wildcard to represent a single instance of an alphanumeric value - Example: b?b@domain.*.
- A blank field will also prompt a search.

- Enter the domain address in the **To** field.

You may use wildcards for this search. Examples include:

- (*) wildcard to represent zero or any number of alphanumeric values.
- (?) wildcard to represent a single instance of an alphanumeric value - Example: b?b@domain.*.
- A blank field will also prompt a search.

- Enter the start date.
- Enter the start time.
- Enter the end date.
- Enter the end time.
- Enter the text of the subject line.
- Select *All of the words*, *Any of the words*, or *Exact phrase* to refine a subject line search.
- Enter the **Sender IP**.

5 Click **Search**.

The results appear in the **Search Results** window.

6 View and download search results.

To...	Use these steps...
Download all Results	Click **Download** in the **Search Results** window.
Preview a result	Select an item to view it in the **Audit Details Preview** window.
View result details	Double-click an item to view it in a new **Audit Details** tab.
Download an individual result	Double-click an item to view it in a new **Audit Details** tab and click **Download**.

Viewing blocked IP addresses

The **Perimeter Block Search** allows the user to search and review which IPs have been blocked based on the history of the sender IP.

If there is a question with the results of your IP search do one of the following.

- If an IP has been blocked in error, you should submit an IP research request by going to postmaster.mcafee.com and clicking on the link that reads **click here to submit an IP Research Request** to fill out the form and submit it for review.
- If the IP was allowed, but message audit was unable to track it, then escalate this information to your customer administrator for further research.
- If message audit is unable to trace the IP, escalate this information to your customer administrator.

Perimeter Block Search window

The Perimeter Block Search window allows you to search for and review IPs that have been blocked.

Table 7-3 Search Criteria window

Option	Definition
Sender IP	Type the complete sender IP. Wildcard searches are not allowed.
Start Date	Type a start date using a range within the last 14 days. The date is based on your time zone. Click the calendar icon to select a date from the calendar window.
Start Date	Type an end date using a range within the last 14 days. The date is based on your time zone. Click the calendar icon to select a date from the calendar window.
Search	Click to run your search.

Table 7-4 Search Results window

Option	Definition
Timestamp	The time and date that the IP address was blocked or allowed.
Sender IP	The IP address being reviewed.
Status	Indicates whether that IP address was blocked or allowed.
Download	Click to generate a csv file containing the search details.

Run a Perimeter Block Search

Use the Perimeter Block Search form to search and review IPs that have been blocked based on the history of the sender IP.

Task

To run a perimeter block search, complete the following steps.

1 Under Email Protection, select **Message Audit**.

2 Click **Perimeter Block Search**.

3 Enter the sender IP address.

This is a required field. Use a fully qualified IP address. Wildcard searches are not allowed.

4 Enter a start date.

5 Enter or select an end date.

6 Click **Search**.

The results appear in the **Search Results** window.

7 Click **Download** in the **Search Results** window to download all results.

Viewing Search History

The search history tool allows you to view the history of users who have searched in message audit during the previous 14 days.

Search History window

The Search History window allows you to view information on past searches.

To change domains, or if appropriate, to change customers, you can click the link for your current domain/customer in the upper right of the window. In the **Select** window that opens, begin entering the name of the entity you want and select that entity when a list of entities appears.

Input information is not case sensitive.

Search criteria, search by message ID, and search by message header are collapsible panes. Simply click the header you want to use to open that window.

Table 7-5 Search criteria

Option	Definition
Start Date	Type a start date using a range within the last 60 days. The date is based on your time zone. Click the calendar icon to select a date from the calendar window.
End Date	Type an end date using a range within the last 60 days. The date is based on your time zone. Click the calendar icon to select a date from the calendar window.
Search	Click to run your search.

Table 7-6 Search Results

Option	Definition
Timestamp	The timestamp provides the recording of the IP address that was either blocked or allowed based on the time criteria selected.
User	The user who performed the search.
Search Type	The type of search (message or perimeter block)
Search Criteria	The fields and search criteria used in the search.
Download	Click to generate a .csv file containing the search details.

The Preview window and Details tab both provide additional information and options for an individual search result.

Table 7-7 Preview window and details

Option	Description
UserIP	The IP address for the user who performed the search.
Results Count	The number of results returned by the search.
Download	In the **Details** tab, click to generate a .csv file containing the search details.

Review Search History

Use the search form to find search history results based on a date range.

Task

To review your search history, complete the following steps.

1 Under Email Protection, select **Message Audit**.

2 Click **Search History**.

3 Enter a start date.

4 Enter an end date.

5 Click **Search**.

The results appear in the **Search Results** window.

6 View and download search results.

To	Use these steps
Download all Results	Click **Download** in the **Search Results** window.
Preview a result	Select an item to view it in the **Preview** window.
View result details	Double-click an item to view it in a new **Details** tab.
Download an individual result	Double-click an item to view it in a new **Details** tab and click **Download**.

Message Audit window

Message Audit is a self-service audit capability which allows a partner administrator or higher to research specific message disposition information based on the message details, message ID or message header.

Input information is not case sensitive.

Search criteria, search by message ID, and search by message header are collapsible windows. Click the header you want to use to open that window.

Table 7-8 Search by Message Details

Option	Definition
From	If you are using the *From* field as your primary search field, then you may use a wildcard for your search. For example: • (*) wildcard to represent zero or any number of alphanumeric values • (?) wildcard to represent a single instance of an alphanumeric value - Example: b?b@domain.* • A blank field will also prompt a search.
To	If you are using the *To* field as your primary search field, then you may use a wildcard for your search. For example: • (*) wildcard to represent zero or any number of alphanumeric values • (?) wildcard to represent a single instance of an alphanumeric value - Example: b?b@domain.*
Start Date	Type a start date from the last 14 days. The date is based on your time zone. Click the calendar icon to select a date from the calendar window.
Start Time	Select the start time on the start date to further narrow the date and time range. The drop-down lists the time of day in 15 minute intervals.
End Date	Type an end date from the last 14 days. The date is based on your time zone. Click the calendar icon to select a date from the calendar window.

Table 7-8 Search by Message Details *(continued)*

Option	Definition
End Time field	Select the end time on the end date to further narrow the date and time range. The drop-down lists the time of day in 15 minute intervals.
Subject	Type the subject of the email you are searching. Select either *all of the words*, *any of the words*, or an *exact phrase* from the drop-down to narrow this search. You may use an asterisk (*) wildcard for your search.
Sender IP	Type the complete Sender IP. Wildcard searches are not allowed.

Table 7-9 Search by Message ID

Option	Definition
Message ID	Type the complete message ID of the email.

Table 7-10 Search by Header

Option	Definition
Message Header	Type or copy the message header of the email into the text box. Wildcard searches are not allowed.

Table 7-11 Search Results

Option	Definition
From	The *From* email address.
To	The*To* email address.
Subject	The subject line.
Direction	Describes whether the email was sent or received: **Inbound** — An email sent to a recipient on a domain provisioned on the filtering service. **Outbound** — An email sent from a domain provisioned on the filtering service to an external recipient.
Received	The date the email was received.
Download	Click to download all of the search results in a csv file.

The **Audit Details Preview** window and **Audit Detail** tabs display the details of an email and its delivery contents.

Table 7-12 Audit Details Preview window and Audit Detail

Option	Description
From	The *From* email address.
To	The *To* email address.
Subject	The subject line.
Size	The file size of the email.
Message ID	The unique message ID.
Tracking ID	The unique tracking ID.
Sender IP	The IP address of the sender.
Direction	Describes whether the email was sent (outbound) or received (inbound).
Spam Score	The likelihood that the email is spam.
Download	Click to download the audit details in a csv file.

Table 7-13 Event details

Option	Description
Timestamp	The date and time fo the event.

Event	Provides details on each event, including:
	• A blank field will also prompt a search.
	• Frontend/backend Transport Layer Security (TLS) — yes/no.
	• Backend IP — the attempted destination the IP Server was sent.
	• User Name — who released the email from quarantine.
	• Tags for quarantined messages include:
	  • qv — Quarantine Virus
	  • qk — Quarantine Content Keyword
	  • qs — Quarantined Spam
	  • qa — Quarantined Attachment
	  If your message was deleted from quarantine, you may view who deleted the message. For example: Detail: deleted from quarantine by: global@kt2.com .

8 Reports

Email Protection provides a large number of reports with which to monitor your service.

Contents

Reports definition overview

Email Protection provides a large number of reports with which to monitor your service. The following table offers the list of reports available and an overview of their functions.

Table 8-1 Reports Overview

Report	Description
Traffic Overview	Information about all inbound and outbound email traffic and bandwidth for the designated domain during the selected date or date range.
Threat: TLS	Information about all TLS inbound and outbound email traffic, percentages and bandwidth for the designated domain during the selected date or date range.
Traffic Encryption	Information about all outbound email traffic, percentages and bandwidth for the designated domain during the selected date or date range sent out to be encrypted.

Table 8-1 Reports Overview *(continued)*

Report	Description
Threats: Overview	Information about email violations by policy type for the designated domain during the selected date or date range.
Threats: Viruses	Information about all inbound and outbound emails that violated the virus policies for the designated domain during the selected date or date range.
Threats: Spam	Information about emails that violated the spam policies for the designated domain during the selected date or date range.
Threats: Content	Information about emails that violated the content keyword policies for the designated domain during the selected date or date range.
Threats: Attachments	Information about emails that had attachments that violated the attachment policies for the designated domain during the selected date or date range.
Enforced TLS Details	Information about all enforced TLS inbound and outbound email traffic, including the number of messages and bandwidth for the designated domain during a selected time frame. The report also includes a count of inbound and outbound messages that were denied due to an enforced TLS policy violation.
Enforced SPF	Information about all enforced SPF inbound email traffic, including the designated domain during a selected time frame. The report also includes a count of messages that were denied due to an Enforced SPF Policy violation.
ClickProtect: Overview	Information about ClickProtect processing. ClickProtect processing tracks web hyperlinks received in emails that can be clicked and followed by the user or that can be blocked, depending on the ClickProtect policy configurations for the designated domain during the selected date or date range.
ClickProtect: Click Log	Information about Web hyperlinks in emails that were clicked by the recipient for the designated domain during the selected date or date range.
Quarantine: Release Overview	Information about emails that were quarantined and released from all quarantine areas within the Email Protection for the designated domain during the selected date or date range.
Quarantine: Release Log	Information about emails that were released from all quarantine areas within the Email Protection for the designated domain during the selected date or date range.
User Activity	Information about all inbound and outbound email traffic and bandwidth for the designated domain during the selected date or date range.
Event Log	Displays messages that have had actions performed based on the content, spam content, virus, or attachment policy definitions. Messages can be sorted per domain, and inbound direction, outbound direction or both. Messages that are identified as threats by the Email Protection are also included.
Audit Trail	Displays the audit log items for all actions performed by users at report manager, or higher-level, roles within the Control Console for the designated domain during the selected date or date range, including sign ins and configuration changes.
Inbound Server Connections	Displays information about the connections made to the inbound email servers during processing.
Disaster Recovery: Overview	Information about emails that were spooled and unspooled by the disaster recovery service for the designated domain during the selected date or date range.
Disaster Recovery: Event Log	Displays the event log items for actions performed within the disaster recovery service. Included are actions performed automatically by the Email Protection and performed manually by the administrator.

Set up your customer or domain and timezone

For all reports, select your customer or your domain to manage.

Task

1 Select the customer report.

2 Depending on how your system is configured, you may run a report for a primary domain, a domain alias, or a public domain. A public domain is a registered domain with a public MX record that is used for uniform email addresses across multiple primary domains. A public domain name will have the primary domain appended to it with brackets [primary domain], and a Domain Alias is appended with brackets [alias]. The following examples demonstrate this feature:

- acme.com [acme-denver.com] is the public domain [primary domain] respectively
- acme.com [alias]

Traffic Overview

The**Traffic Overview** report contains various charts and summarized text to provide you with an overall understanding of the traffic and bandwidth trends for the specified time period. The **Download** button at the top of the window allows you to download all the report information to a spreadsheet.

Traffic Overview Report Information

To review your email traffic overview report, simply click the icons on the top right corner of each bar graph to view it in an alternate format. Pie charts cannot be changed.

Field	Description
Traffic Summary	Summarizes in text form the data displayed in the charts.
Data Volume Summary	Summarizes in text form the data displayed in the charts.
Allowed Traffic Requests	Displays the aggregates of allowed requests by users over a specified time period. These numbers include one or more hits on a single visit to a Web page
Blocked Traffic Trends	Displays the aggregates of blocked requests for the specified time period. These numbers include one or more content requests on a single visit to a web page.
Data Volume In Trends	Displays inbound bandwidth usage.
Data Volume Out Trends	Displays outbound bandwidth usage.

Traffic TLS

The**Traffic: TLS Report** window displays information about all TLS inbound and outbound email traffic, percentages and bandwidth for the designated domain during the selected date or date range.

The Reporting Period: All report data is viewable on either a day, week, or month basis for the current month, or the previous month.

The **Download** button at the top of the window allows you to download all the report information to a spreadsheet.

Traffic TLS Report Overview

The TLS report identifies inbound and outbound email messages that were delivered via a TLS connection and any email messages that were denied due to an enforced TLS policy violation.

The following table lists the TLS connections that were delivered.

You can click the icons on the top right corner of each bar graph to view it in an alternate format. Pie charts cannot be changed.

Table 8-2 Traffic Summary

Title	Description
TLS Inbound Messages	The total of TLS inbound messages that were processed via a TLS connection.
% Inbound Messages sent via TLS	The percentage of incoming email messages process via a TLS connection.
Inbound Messages blocked by Enforced TLS	The total of inbound email messages blocked by an enforced TLS policy.
TLS Outbound Messages	The total of TLS outbound messages that were processed via a TLS connection.
% Outbound Messages sent via TLS	The percentage of outgoing email messages processed via a TLS connection.
Outbound Messages blocked by Enforced TLS	The total of outgoing email messages blocked by an enforced TLS policy.

Table 8-3 Bandwidth Summary

Title	Description
TLS Inbound Total Bandwidth	The quantity of data transferred via TLS, measured in bytes.
% Inbound Bytes sent via TLS	The percentage of inbound mail sent via TLS, measured in bytes.
Outbound Total Bandwidth	The quantity of data transferred via TLS, measured in bytes.
% Outbound Bytes sent via TLS	The percentage of outbound mail sent via TLS, measured in bytes.

Traffic Encryption

The **Traffic: Encryption Report** window displays information about all **Outbound Email Traffic**, percentages and bandwidth for the designated domain during the selected date or date range sent out to be encrypted.

Reporting Period: All report data is viewable on either a day, week, or month basis for the current month, or the previous month.

Traffic Encryption Report Overview

Email Encryption Trends identify outbound email messages that delivered encrypted email messages.

The following table lists the encryption reports that were detected.

You can click the icons on the top right corner of each bar graph to view it in an alternate format. Pie charts cannot be changed.

Table 8-4 Email Encryption Summary

Title	Description
Outbound Encrypted Messages	The total outbound messages to be delivered for encryption.
% Outbound Messages sent via Encryption	The percentage of outgoing email messages sent out to be encrypted.

Table 8-5 Email Encryption Bandwidth Summary

Title	Description
Outbound Total Bandwidth	The total bandwidth of outgoing email messages sent for encryption.
% Outbound Bytes Messages sent via Encryption	The percentage of outgoing bytes messages sent out to be encrypted.

Threats Overview

The **Threats: Overview** report window displays information about email violations by policy type for the designated domain during the selected date or date range

The Reporting Period: All report data is viewable on either a day, week, or month basis for the current month, or the previous month.

The **Download** button at the top of the window allows you to download all the report information to a spreadsheet.

Threats Overview Report Details

The **Threats Overview** report provides an at-a-glance view of inbound and outbound threats spam, viruses, spam beacons, content violations, and attachment violations being filtered by the Email Protection before they can reach the customer network. Administrators can use the reports to quickly gauge the effectiveness and value of the Email Protection.

The **Threats: Overview** indicates the total number of inbound and outbound emails that violated each policy type for the designated domain and date range. Data for each policy type is color-coded as indicated in the legend below the graph. Your policy types and policy configuration determine the contents of this report.

Inbound Total messages categorized as: spam, viruses, content, and attachments. Total outbound messages categorized as: viruses, content, and attachments.

Note: The numbers in the *Inbound Threat Summary* are included to give you an overall picture of what the Email Protection is doing to protect your company. The numbers will likely not add up to 100% because the following utilities are used to scan email:

- Several different virus engines
- Software that identifies multiple viruses in a single email
- Software that resolves several domain names and aliases at your site
- Utilities that identify spam and viruses in a single email

Table 8-6 Inbound Threat Summary

Title	Description
Total Viruses	All Inbound emails that contained known viruses.
Infection Rate	The number of emails with viruses / all Inbound emails. Expressed in this notation: 0/407 In this example, the notation means "0" infected emails out of a total of "407" emails received.
Total Spam Identified	All Inbound emails found to have potential spam.
Spam Volume	The percentage of Inbound emails that were found to have potential Spam.
Spam Beacons Detected	All Spam Beacons detected in Inbound emails. Each email may contain multiple spam beacons and all beacons are counted. Definition: Spam beacons, typically a transparent, 1x1 pixel graphic embedded in HTML content, can reveal user activity to spammers while flagging the recipient's address as active.
Content Keyword Violations	All Inbound emails that violated the content keyword policies.
Attachment Policy Violations	All Inbound emails that had attachments that violated the attachment policies.

Table 8-7 Outbound Threat Summary

Title	Description
Total Viruses	All outbound emails that contained known viruses.
Infection Rate	The percentage of outbound emails that contained known viruses.
Content Keyword Violations	All outbound emails that violated the content keyword policies.
Attachment Policy Violations	All outbound emails that had attachments that violated the attachment policies.

Threats Virus

The **Threats: Viruses** report measures the number of inbound and outbound virus-infected emails filtered by the service and provides information on their disposition cleaned or stripped per customer preference. The report also includes the names of known viruses filtered out.

Threat Virus Report Details

Indicates the total number of inbound and outbound emails that contained known viruses as well as the names and number of occurrences of the most frequently encountered viruses. Your policy types and policy configuration determine the contents of this report.

Table 8-8 Virus Detection Summary

Field	Description
Total Viruses Inbound	The total number of inbound emails that contained known viruses ("infected emails").
Inbound Infection Rate	The percentage of infected inbound emails vs. the total number of received inbound emails.
Total Viruses Outbound	The total number of infected outbound emails.
Outbound Infection Rate	The percentage of infected outbound emails vs. the total number of sent outbound emails.

Table 8-8 Virus Detection Summary *(continued)*

Field	Description
Disinfected (cleaned)	The total number of infected emails that had their viruses successfully removed and the emails were forwarded to their destinations.
Stripped	The total number of infected emails that had the infected attachments stripped and then were forwarded to their destinations.

Table 8-9 Virus Policy Actions

Field	Description
Deny	The percentage of emails that were infected and had policy actions applied to them. Delivery is denied.
Quarantine	The percentage of emails that were infected and had policy actions applied to them. The email is sent to the recipient's quarantine area.

Table 8-10 Top Inbound Viruses

Field	Description
{ name }	The name(s) of the most frequently encountered viruses in inbound emails, in order of most frequent to less frequent.
{ number}	The quantity of the most frequently encountered viruses in inbound emails, in order of most frequent to less frequent.

Table 8-11 Top Outbound Viruses

Field	Description
{ name }	The name(s) of the most frequently encountered viruses in outbound emails, in order of most frequent to less frequent.
{ number}	The quantity of the most frequently encountered viruses in outbound emails, in order of most frequent to less frequent.

Threats Spam

The **Threats: Spam** report window displays information about emails that violated the spam policies for the designated domain during the selected date or date range.

Administrators can easily gauge the impact of the most prevalent email threat spam within this report, which includes three key measurements:

- Total Inbound Spam Identified
- Inbound Spam Volume
- Invalid Email Detected

Threats Spam Report Details

The **Threat: Spam** report indicates the total number of inbound and outbound emails that violated spam policies and the percentage of policy actions (for example, quarantine) applied to emails that violated spam policies.

Table 8-12 Spam Detection Summary

Field	Description
Total Inbound Spam Identified	The total number of inbound emails that violated spam policies.
Inbound Spam Volume	The percentage of inbound emails that violated spam policies vs. the total number of received inbound emails.
Invalid Email Detected	Displays the number of messages classified as invalid mail. Invalid email is defined as either email sent from invalid senders or email sent to invalid recipients.
Spam Beacons Detected	All spam beacons detected in inbound emails. Each email may contain multiple Spam Beacons all beacons are counted. DEFINITION: Spam beacons, typically a transparent, 1x1 pixel graphic embedded in HTML content, can reveal user activity to spammers while flagging the recipient's address as active.
Real-time Blackhole Lists	Displays the number of messages identified as suspect by reputation-based DNSBL filtering.
Bounce Messages Denied	Displays the total number of messages that were denied. These totals are not included in the spam volume totals, Total Inbound spam identified totals, or spam policy action graphs.

Table 8-13 Spam Policy Actions

Field	Description
Deny	The percentage of emails that violated spam policies and had policy actions applied to them. Delivery is denied.
Quarantine	The percentage of emails that violated spam policies and had policy actions applied to them. The email is sent to the recipient's quarantine area.
Tag	The percentage of emails that violated spam policies and had policy actions applied to them. The email is sent to the recipient with the tag of [SPAM].
Other	The percentage of emails that fall under all other policies (for example; Do Nothing) and had policy actions applied to them. The email is either sent to the recipient with the appropriate action applied or the email is denied.

Threats Content

The **Threats: Content** report indicates the total number of Inbound and outbound emails that violated the keyword content policies and the percentage of policy actions (for example, quarantine) applied to emails that violated the keyword content policies during the selected date or date range.

Threats Content Report Details

Both the top inbound content group violations and the top outbound content group violations reports measure the number of messages found to violate the top ten inbound / outbound customer email

content policies for both global policies and custom policies. The following table lists the Top Ten content policies that may be reported.

Table 8-14 Top Inbound / Outbound Content Group Violations

Field	Description
Credit Card	The total number of emails that contained keywords and phrases from the credit card predefined content group.
Profanity	The total number of emails that contained keywords and phrases from the profanity predefined content group.
Racially Insensitive	The total number of emails that contained keywords and phrases from the racially insensitive predefined content group.
Sexual Overtones	The total number of emails that contained keywords and phrases from the sexual overtones predefined content group.
Social Security	The total number of emails that contained keywords and phrases from the social security predefined content group.
Acceptable Use - Offensive Language	The total number of emails that contained keywords and phrases from the offensive language predefined content group.
Acceptable Use - Discrimination	The total number of emails that contained keywords and phrases from the discrimination predefined content group.
North America PII - Social Security Number Violations	The total number of emails that contained keywords and phrases from the social security number violations predefined content group.
North America PII - Unencrypted Credit Card Number Violations	The total number of emails that contained keywords and phrases from the credit card number violations predefined content group.
Sexual Content	The total number of emails that contained keywords and phrases from the sexual content predefined content group.
{ custom }	The total number of emails that contained keywords and phrases from a {custom} content group created by you. You may have multiple {custom} content groups, each with a unique name.

Table 8-15 Content Policy Actions

Field	Description
Deny	The percentage of emails that violated content keyword policies and had policy actions applied to them. Delivery is denied.
Quarantine	The percentage of emails that violated content keyword policies and had policy actions applied to them. The email will be viewable in the domain's Message quarantine / Content quarantine area.
Allow	The percentage of emails that did not violate content keyword policies. The email is forwarded to the recipient email address with no processing applied.
Tag	The percentage of emails that violated content keyword policies and had policy actions applied to them. The email is sent to the recipient email address with the word "[CONTENT]" added to the subject line.
Encrypt	The percentage of outbound emails that violated any encrypted policies.

Threats Attachment

With the **Threats: Attachment** report, administrators can view the number of inbound and outbound messages found in violation of customer attachment policies. The report includes message totals by file type blocked, including executables, scripts, documents, audio, image, and compressed files.

Threats Attachment Report Details

Threats: Attachment reports the total of messages with attachments processed that have violated an attachment policy and the percentage of policy actions (for example, *quarantine*) applied to emails that violated the attachment policies.

Table 8-16 Attachment Summary

Field	Description
Average Attachment Size	The average size (in KB) of attachments encountered in emails.
Executables	The total number of executable files (for example, *.exe) received as attachments.
Scripts	The total number of script files received as attachments.
Office Documents	The total number of Microsoft Office documents (for example, *.doc or *.xls files, etc.) received as attachments.
Audio	The total number of audio files (for example, *.wav or *.mp3 files, etc.) received as attachments.
Images	The total number of graphic files (for example, *.gif or *.bmp files, etc.) received as attachments.
Compressed Archives	The total number of archive files (for example, *.zip or *.tar files, etc.) received as attachments.

Table 8-17 Attachment Policy Actions

Field	Description
Deny	The percentage of emails that violated attachment policies and had policy actions applied to them. Delivery is denied.
Quarantine	The percentage of emails that violated attachment policies and had policy actions applied to them. The email will be viewable in the domain's message quarantine / attachment quarantine area.
Encrypt	The percentage of outbound emails that violated any encrypted policies.
Strip	The percentage of emails that have had text stripped from an attachment.

Enforced TLS Details

The **Enforced TLS Details** report displays information about all Enforced TLS inbound and outbound email traffic, including the number of messages and bandwidth for the designated domain during a selected time frame. The report also includes a count of inbound and outbound messages that were denied due to an enforced TLS policy violation.

Enforced TLS Details Report

The **Enforced TLS Details** report identifies inbound and outbound email messages that were delivered via a TLS connection and any email messages that were denied due to an enforced TLS policy violation.

Table 8-18 Traffic Summary

Field	Description
Enforced TLS Accepted - Inbound Messages	The total number of TLS inbound messages that were processed via an enforced TLS connection for a given domain.
Enforced TLS Accepted - Outbound Messages	The total number of TLS outbound messages that were processed via an enforced TLS connection for a given domain.

Table 8-18 Traffic Summary *(continued)*

Field	Description
Enforced TLS Accepted - Inbound Bandwidth	The quantity of data transferred via enforced TLS for inbound messages, measured in bytes, for a given domain.
Enforced TLS Accepted - Outbound Bandwidth	The quantity of data transferred via enforced TLS for outbound messages, measured in bytes for a given domain.
Enforced TLS Denied - Inbound Messages	The total of incoming email messages blocked by an enforced TLS policy for a given domain.
Enforced TLS Denied - Outbound Messages	The total of outgoing email messages blocked by an enforced TLS policy for a given domain.

Enforced SPF Report

The **Enforced SPF** report displays all enforced SPF inbound email traffic, including the information about number of messages and validations for the designated domains, during a selected time frame. The report also includes a percentage of incoming email messages that were denied, validated or unavailable due to an enforced SPF policy violation.

SPF Message Summary

The **Enforced SPF** report identifies inbound email messages that were delivered or denied due to an enforced SPF policy violation.

Table 8-19 SPF Report Summary

Field	Description
Top Enforced SPF Denied Domains	The total number of email messages, including the top ten defined domains, that were denied by an enforced SPF policy because their SPF record could not be validated.  Data in the report table does not display unless an enforced SPF policy has been created with a *deny* action or domains have been added to the list for the enforced SPF policy.
SPF Message Summary	Summarizes in text form the totals and percentages of enforced SPF emails that were successful, unavailable or failed.

ClickProtect: Overview report

The ClickProtect Overview report provides you with the results of your ClickProtect implementation including counts of messages affected and the number of user clicks that were allowed and denied.

Table 8-20 ClickProtect Statistics

Field	Description
Messages with links	The total number of email messages that contained a link.
Messages with multiple links	The total number of email messages that contained more than one linke.
Total clicks	The total number of times that recipients clicked links in their email.
Total allowed click-throughs	The total number of times that recipients were allowed to access the website after clicking the link.

Table 8-20 ClickProtect Statistics *(continued)*

Field	Description
Total warn-and-allow click-throughs	The total number of times that recipients were taken to the warning page before being allowed to access the website.
Total click-throughs denied due to reputation	The total number of times that recipients were denied access to a website because of the site's reputation.
Total click-throughs denied due to malware	The total number of times that recipients were denied access to a website because the site contained malware.
Number of individual users that clicked	The total number of recipients that attempted to click a link in an email.
Spam messages with click-throughs	The total number of spam emails that contained links clicked by recipients.
Messages with links on the ClickProtect Allow list	The total number of emails that contained links that are listed in the ClickProtect allow list.

ClickProtect: Click Log report

The ClickProtect Click Log report provides details on each email link that is scanned for potential risks as well as the resulting action.

Table 8-21 ClickProtect: Click Log options

Field	Description
Timestamp	Displays the date and time.
From	Displays the email address of the sender.
To	Displays the email address of the recipient.
Subject	Displays the subject line of the email.
URL	Displays the full URL of the link.
Reputation	Displays the reputation of the website. • **High Risk** — Specifies a URL that exhibits detrimental behavior. For example, the site is known to host malware. • **Medium Risk** — Specifies a URL that exhibits questionable behavior that may be detrimental to the user. • **Minimal Risk** — Specifies a URL that exhibits appropriate behavior or that is verified as trusted. • **Unverified** — Specifies a URL for which no reputation information has been calculated.
Category	When available, displays the category associated with the website.
Malware	When found, displays the name of the malicious software.
Action	The action taken at click-time. • **Denied-malware** • **Denied-reputation** • **Warn and allow** • **Allowed**
Score	Displays the spam likelihood score assigned to the email as a graphical bar. The spam score ranges from 0-100% (green to red), with 100% (or red) being the highest likelihood that the email is spam.

Quarantine Release Overview

The **Quarantine: Release Overview** report provides an at-a-glance overview of inbound message activity within message quarantine. Administrators can view the total number of messages quarantined or released in four categories: spam, viruses, content violations, and attachment violations. Detailed statistics are provided for each category as to what was identified, what was released, the percentage released, and the number of individuals that had released emails from that category.

Quarantine Release Overview Report Details

The **Quarantine: Release Overview** report indicates the total number of Inbound emails that were quarantined and then released from all quarantine areas spam, virus, attachment, and content. Data for each quarantine type is color-coded as indicated in the legend below the graph.

Table 8-22 Inbound Spam Release Summary

Field	Description
Total Spam Identified	The total number of quarantined emails that were identified as spam.
Total Spam Released	The total number of emails released from spam quarantine.
Release Percent	The percent of emails released from the spam quarantine vs. the total number of emails that were quarantined as potential spam.
Total # of Individuals	The total number of user accounts that had emails released from the spam quarantine.

Table 8-23 Inbound Virus Release Summary

Field	Description
Total Viruses Identified	The total number of viruses detected in incoming emails that were quarantined.
Total Viruses Released	The total number of emails released from the virus quarantine.
Release Percent	The percent of emails released from the virus quarantine vs. the total number of emails that were quarantined because of viruses.
Total # of Individuals	The total number of user accounts that had emails released from the virus quarantine.

Table 8-24 Inbound Content Release Summary

Field	Description
Total Content Identified	The total number of quarantined emails that violated content policies.
Total Content Released	The total number of emails released from the content quarantine.
Release Percent	The percent of emails released from the content quarantine vs. the total number of emails that was quarantined because of content.
Total # of Individuals	The total number of user accounts that had emails released from the content quarantine.

Table 8-25 Inbound Attachment Release Summary

Field	Description
Total Attachment Identified	The total number of quarantined emails that violated attachment policies.
Total Attachment Released	The total number of emails released from the attachment quarantine.
Release Percent	The percent of emails released from the attachment quarantine vs. the total number of emails that were quarantined because of attachments.
Total # of Individuals	The total number of user accounts that had emails released from the attachment quarantine.

Quarantine Release Log

This report provides a list of all messages released from the message quarantine areas: spam, viruses, attachments, and content. You can view quarantined released email from 1-30 days. Within this log, you can search for released mail by day, week, or month.

Users can actively manage their individual spam quarantines, by adding appropriate email addresses to their allow lists to reduce the number of messages quarantined as spam and subsequently released.

Display field

Use the drop-down list to designate which type of quarantine release events to display:

- **All Events:** release events for all quarantines.
- **Spam:** release events for the spam quarantine.
- **Viruses:** release events for the virus quarantine.
- **Attachments:** release events for the attachment quarantine.
- **Content:** release events for the content quarantine.

Log Item Pop-up Window

Hover the cursor over a log item and a pop-up window appears displaying additional information about the item, such as the **Sender IP** address.

Quarantine Release Log Report Details

The **Quarantine: Release Log** report includes details about each Inbound email that was quarantined and then released from all quarantine areas spam, virus, attachment, content.

Table 8-26 Quarantine: Release Log Summary

Field	Description
Type	The reason why this email was quarantined: **spam:** email violated the spam policies, **virus:** email contained a known virus, **attachment:** email's attachment violated the attachment policies, **content:** email contained content that violated the content policies, including keywords and HTML.
From	The email address that sent the email.
To	The recipient email address.
Subject	The text in the subject line of the email.
Release Date	The date, time, and time zone when this email was released from quarantine from the Email Protection.
Size	The total file size of this email, including all attachments.

User Activity

The **User Activity** report displays a list of the top Inbound and the top outbound user email addresses per domain within your organization. Also displayed for each user email address are the total number of messages received or sent and the total file size of all of the messages for that user.

User Activity Report Details

The **User Activity** report indicates data about the user accounts that receive the highest number of inbound emails and the user accounts that send the highest number of outbound emails.

Table 8-27 Top Inbound Users

Field	Description
Email Address	The recipient email addresses that received the most Inbound email, in order of volume.
Messages	The total number of emails received by each email address.
Size	The total size in bytes (KB or MB) of all emails, including attachments, received by each email address.

Table 8-28 Top Outbound Users

Field	Description
Email Address	The sender email addresses that sent the most outbound email, in order of volume. If a sender email address was not created in the Email Protection system, you may see an address in this list formatted as either "<unknown>@xyz.com" or "@xyz.com" where "xyz.com" can be any domain related to the customer account.
Messages	The total number of emails sent by each email address.
Size	The total size in bytes (KB or MB) of all emails, including attachments, sent by each email address.

Event Log

The **Event Log** report window displays messages that have had actions performed based on the content, spam content, virus, attachment, enforced TLS or enforced SPF policy definitions. Messages can be sorted per domain, and inbound direction, outbound direction or both. Messages that are identified as threats by the Email Protection are also included.

Administrators can find detailed information on each inbound or outbound message that triggered a virus, attachment, content, enforced TLS or enforced SPF policy. The Administrator can specify a date range based on the current day, a week, or a month.

Display field (policy types)

Use the drop-down list to designate which type of event to display:

- **All Events**: policy enforcement events for viruses, spam keywords, attachments, and content.
- **Spam Keyword**: policy enforcement events for spam keywords (for inbound messages only).
- **Viruses**: policy enforcement events for viruses.
- **Attachments**: policy enforcement events for attachments.
- **Content**: policy enforcement events for content.
- **Enforced TLS**: policy enforcement events for enforced TLS.
- **Enforced SPF**: policy enforcement events for enforced SPF (for inbound messages only).

Direction field

Use the drop-down list to choose whether event gog items are displayed for inbound or outbound emails:

- **Inbound Only**: only inbound emails are displayed.
- **Outbound Only**: only outbound emails are displayed.
- **Inbound & Outbound**: both inbound and outbound emails are displayed.

Log Item Pop-up Window

Hover the cursor over a log item and a pop-up window appears displaying additional information about the item, such as the **Sender IP** address.

Event Log Report Details

The **Event Log** report logs items for actions performed for emails that were determined to violate content, spam content, virus, attachment, enforced TLS, or enforced SPF policies for the designated domain and date range, including actions performed automatically by Email Protection and performed manually by the users.

Table 8-29 Event Log Details

Field	Description
Type	The policy type that the filtered email violated.
Timestamp	The date, time, and time zone when the action was performed on the filtered email.
From	The email address that sent the email.
To	The recipient email address.
Subject	The text in the subject line of the email.
Details	The reason for the action. - If the email contained a virus, the "virus name" is shown. - If the email contained a policy enforced spam keyword, the "keyword" is shown. - If the email contained policy enforced content, the "content" is shown. - If the email contained policy enforced attachment, the "attachment type" is shown. - If the email was denied for enforced tls policy, the denied "domain" is shown
Action	The action applied to the email (for example, quarantined, denied, and none).

Audit Trail

The **Audit Trail** report window displays the audit log items for all actions performed by users at report manager, or higher level, roles within the Control Console for the designated domain during the selected date or date range, including sign ins and configuration changes.

This report provides detailed information about activity within the Control Console, including:

- An audit of successful/unsuccessful sign in attempts.
- Any changes made to the domain such as users or group creation.
- Any changes to inbound IP settings, policy sets, and filters.
- Any changes to customer provisioning.
- Any other changes from the user-level up to the domain-level.

Audit Trail Report Details

The **Audit Trail** report indicates the audited items for actions performed in the Control Console for the designated domain and date range.

Table 8-30 Audit Trail Details

Field	Description
Timestamp	The date, time, and time zone when the action was performed in the Control Console.
Domain	The domain where the action was performed.
Details	A description of the action that was performed, including the role and user account of the person that performed the action.

Inbound Server Connection

The **Inbound Server Connections** report window displays information about the connections made to the Inbound email servers (customer MTAs) during processing. The report includes data for server volume trends and details about connection successes or failures. The server IP address is resolved at the time of report generation, to match event data. Non-configured servers are also shown, including deleted or inactive servers.

This report outlines the overall success and fail rates for connections to the customers inbound email server(s). Administrators can use this report to pinpoint connection failures on a particular server by viewing the status of the inbound IP connection, failure rate %, and success or fail.

The customer administrator can quickly view the connection status here.

Display Volume Trends For

Use the drop-down list to display:

- **All Servers:** information for all Inbound servers configured for the selected domain.
- **{ specific server }:** information about the selected Inbound server only.

Overall Failure Rate

The percentage of connection failures to the designated server.

Total Successes

The total number of successful connections to the designated server. Each email message delivered equals one successful connection.

Total Failures

The total number of unsuccessful attempts to connect to the designated server.

Inbound Server Connection Report Details

This report outlines the overall Success and Fail rates for connections to the customers inbound email server. Administrators can use this report to pinpoint connection failures on a particular server by viewing the status of the inbound IP connection, failure rate %, and success or fail.

Table 8-31 Inbound Server Connection Details

Field	Description
Server : Port	The server address and port number.
IP Address	The IP address of the server.
Status	Whether the server is currently active, inactive, or deleted.
Preference	MX Preference for this server. When delivering email, the service will attempt to deliver to the lowest numbered server first.
Failure Rate %	The percentage of connection failures to this server and port.
Success	The total number of successful connections to this server and port. Each email message delivered equals one successful connection.
Fail	The total number of unsuccessful attempts to connect to the selected server and port.

Disaster Recovery Overview

The **Disaster Recovery: Overview** report window displays information about emails that were spooled and unspooled by the Disaster Recovery Service for the designated domain during the selected date or date range. This report details message activity within either **Email Continuity** or the **Fail Safe Service**, including the number of messages spooled or unspooled by the email disaster recovery services.

Disaster Recovery Overview Report Details

The **Disaster Recovery: Overview** report indicates the total number of spooled and unspooled emails processed by disaster recovery and the total size processed in bytes over the designated time period.

Table 8-32 Disaster Recovery Summary - Messages

Field	Description
Spooled Messages	The number of emails that were spooled, either automatically or manually.
Unspooled Messages	The number of emails that were unspooled, either automatically or manually.

Table 8-33 Disaster Recovery Summary - Bytes

Field	Description
Spooled Bytes	The amount of spool storage used by spooling emails during an outage.
Unspooled Bytes	The amount of spool storage freed by unspooling emails after an outage.

Disaster Recovery Event Log

The **Disaster Recovery: Event Log** report window displays the event log items for actions performed within the disaster recovery service. Included are actions performed automatically by the Email Protection and performed manually by the administrator. Includes data about automatic and manual spooling and unspooling of email messages during an outage within the selected domain. The **Disaster Recovery Event Log** includes events from both **Disaster Recovery** and from **Email Continuity**.

Disaster Recovery Event Log Details

This report provides a detailed listing of message spooling activity within time periods determined by the administrator.

Table 8-34 Disaster Recovery: Event Log

Field	Description
Timestamp	The date, time, and time zone when the action was performed in disaster recovery mode.
Event	The event log items for disaster recovery actions performed for the designated domain and date range.
Initiated By	The responsible party that performed the disaster recovery action. If an action was manually performed, indicates the role and user account of the person who performed the action. All actions performed by the Email Protection will be listed under the *system* users.

Index