Example of Mail Policies and Content Filters

This appendix contains the following sections:

Overview of Incoming Mail Policies

The following example demonstrates the features of mail policies by illustrating the following tasks:

1. Editing the anti-spam, anti-virus, Outbreak Filter, and Content Filters for the default Incoming Mail Policy.
2. Adding two new policies for different sets of users — the sales organization and the engineering organization — and then configuring different email security settings for each.
3. Creating three new content filters to be used in the Incoming Mail Overview policy table.
4. Editing the policies again to enable the content filters for some groups, but not for others.

This example is meant to show the power and flexibility with which you can manage different recipient-based settings for anti-spam, anti-virus, Outbreak Filter, and Content Filters for mail policies. This example assigns these a custom user role called “Policy Administrator” that has mail policy and content filters access privileges. For more detailed information about how anti-spam, anti-virus, Outbreak filters, and delegated administration work, refer to the chapters following this one:

- Managing Spam and Graymail
- Anti-Virus
- Outbreak Filters
- Distributing Administrative Tasks

Accessing Mail Policies

You can access incoming and outgoing mail policies by using the Mail Policies menu.

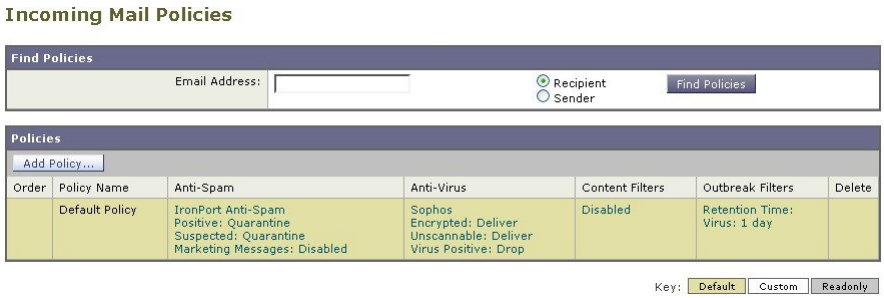
On brand new systems, if you completed all steps in the system setup wizard and you chose to enable Anti-Spam, Sophos or McAfee Anti-Virus, and Outbreak Filters, the Incoming Mail Policies Page will resemble in the following figure.

By default, these settings are enabled for the default Incoming Mail Policy:

- Anti-Spam (if the Spam Quarantine is enabled): Enabled
    - Positively-identified spam: quarantine, prepend the message subject
    - Suspected spam: quarantine, prepend the message subject

    - Marketing email: scanning not enabled
- Anti-Spam (if the Spam Quarantine is not enabled): Enabled
    - Positively-identified spam: deliver, prepend the message subject
    - Suspected spam: deliver, prepend the message subject
    - Marketing email: scanning not enabled
- Anti-Virus: Enabled, Scan and Repair viruses, include an X-header with anti-virus scanning results
    - Repaired messages: deliver, prepend the message subject
    - Encrypted messages: deliver, prepend the message subject
    - Unscannable messages: deliver, prepend the message subject
    - Virus infected messages: drop
- Outbreak Filters: Enabled
    - No file extensions are excepted
    - Retention time for messages with suspect viral attachments is 1 day
    - Message modification is not enabled
- Content Filters: Disable

Figure 1: Incoming Mail Policies Page: Defaults for a Brand New Appliance



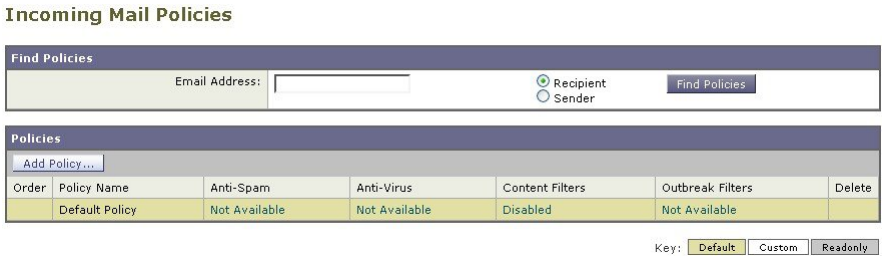
Note In this example, the Incoming Mail Policy will use the default anti-spam settings for when the Spam Quarantine is enabled.

Enabled, Disabled, and "Not Available"

The columns in a mail policy table (either incoming or outgoing) display links for the state of the security service for each policy name. If a service is enabled, the word "Enabled" or a summary of the configuration is displayed. Similarly, the word "Disabled" is displayed if a service is disabled.

"Not Available" is displayed as a link if the license agreement for a service has not been accepted yet or a service has expired. In these cases, clicking the "Not Available" link will display the global page within the Security Services tab, rather than the page where you can configure per-policy settings for a service. An alert is displayed to let you know that your page has changed to a different tab. See the following figure.

Figure 2: Security Services Not Available



Configuring the Default Anti-Spam Policies for Incoming Messages

Each row in the mail policy table represents a different policy. Each column represents a different security service.

- To edit the default policy, click any of the links for a security service in the bottom row of the incoming or outgoing mail policy table.

In this example, you will change the anti-spam settings for the default policy for incoming mail to be more aggressive. The default value is to quarantine positively identified and suspected spam messages, with marketing email scanning disabled. This example shows how to change the setting so that positively identified spam is dropped. Suspected spam continues to be quarantined. Marketing email scanning is enabled, with marketing messages being delivered to the intended recipients. The subjects of marketing messages will be prepended with the text [MARKETING] .

Step 1 Click the link for the anti-spam security service.

Note For default security service settings, the first setting on the page defines whether the service is enabled for the policy. You can click “Disable” to disable the service altogether.

Step 2 In the “Positively Identified Spam Settings” section, change the “Action to apply to this message” to Drop.

Step 3 In the “Marketing Email Settings” section, click **Yes** to enable marketing email scanning.

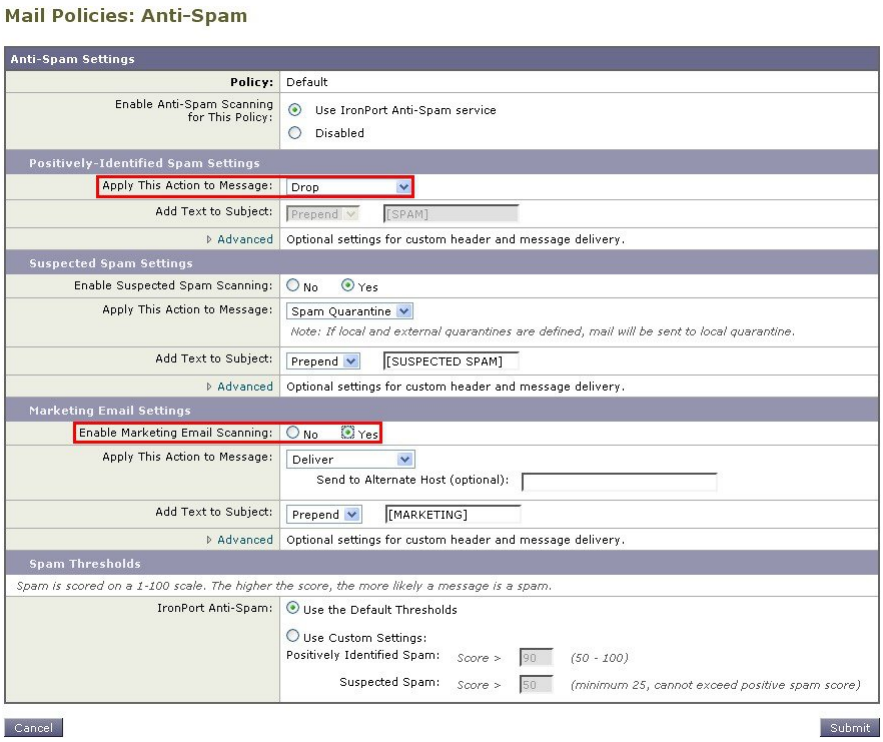
If enabled, the default action is to deliver legitimate marketing messages while prepending the subject with the text [MARKETING] .

The “Add text to message” field only accepts US-ASCII characters.

Step 4 Click **Submit**. Note that the summary link for the anti-spam security service in the Incoming Mail Policies table has changed to reflect the new values.

Similar to the steps above, you can change the default anti-virus and virus outbreak filter settings for the default policy.

Figure 3: Anti-Spam Settings Page



Creating a Mail Policy for a Group of Sender and Recipients

In this part of the example, you will create two new policies: one for the sales organization (whose members will be defined by an LDAP acceptance query), and another for the engineering organization. Both policies will be assigned to the Policy Administrator custom user role to make delegated administrators belonging to this role responsible for managing these policies. You will then configure different email security settings for each.

Step 1 Click the **Add Policy** button to begin creating a new policy.

Step 2 Define a unique name for and adjust the order of the policy (if necessary).

The name of the policy must be unique to the Mail Policies table (either incoming or outgoing) in which it is defined.

Remember that each recipient is evaluated for each policy in the appropriate table (incoming or outgoing) in a top-down fashion.

Step 3 Click the Editable by (Roles) link and select the custom user roles for the delegated administrators who will be responsible for managing the mail policy.

When you click the link, AsyncOS displays the custom roles for delegated administrators that have edit privileges for mail policies. Delegated administrators can edit a policy's Anti-Spam, Anti-Virus, and Outbreak Filters settings and enable or disable content filters for the policy. Only operators and administrators can modify a mail policy's name or its

senders, recipients, or groups. Custom user roles that have full access to mail policies are automatically assigned to mail policies.

See the Distributing Administrative Tasks for more information on delegated administration.

Step 4 Define users for the policy.

You define whether the user is a sender or a recipient. (See Examples of Policy Matching for more detail.) The form shown in the following figure defaults to recipients for incoming mail policies and to senders for outgoing mail policies.

Users for a given policy can be defined in the following ways:

- Full email address: user@example.com
- Partial email address: user@
- All users in a domain: @example.com
- All users in a partial domain: @.example.com
- By matching an LDAP Query

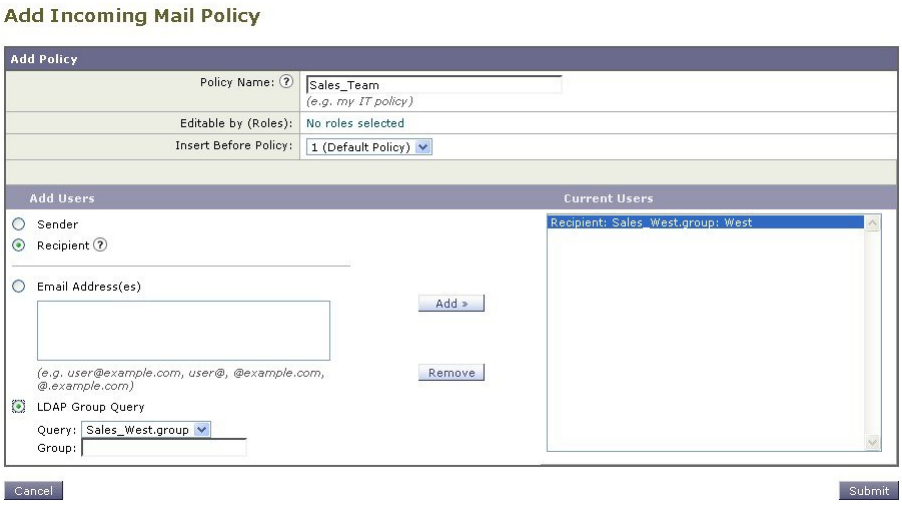
Note Entries for users are case-insensitive in both the GUI and CLI in AsyncOS. For example, if you enter the recipient Joe@ for a user, a message sent to joe@example.com will match.

If you store user information within LDAP directories in your network infrastructure — for example, in Microsoft Active Directory, SunONE Directory Server (formerly known as "iPlanet Directory Server"), or Open LDAP directories — you can configure the appliance to query your LDAP servers for the purposes of accepting recipient addresses, rerouting messages to alternate addresses and/or mail hosts, masquerading headers, and determining if messages have recipients or senders from specific groups.

If you have configured the appliance to do so, you can use the configured queries to define users for a mail policy.

See LDAP Queries for more information.

Figure 4: Defining Users for a Policy



Step 5 Click the **Add** button to add users into the Current Users list.

Policies can contain mixtures of senders, recipients, and LDAP queries.

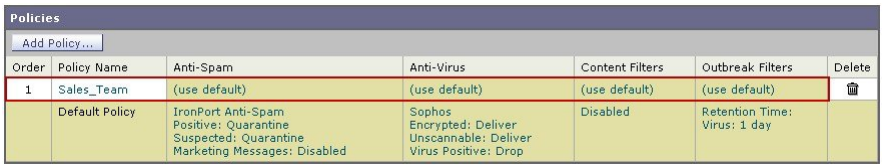
Use the **Remove** button to remove a defined user from the list of current users.

Step 6 When you are finished adding users, click **Submit**.

Example of Mail Policies and Content Filters

Note that all security services settings are set to use the default values when you first add a policy.

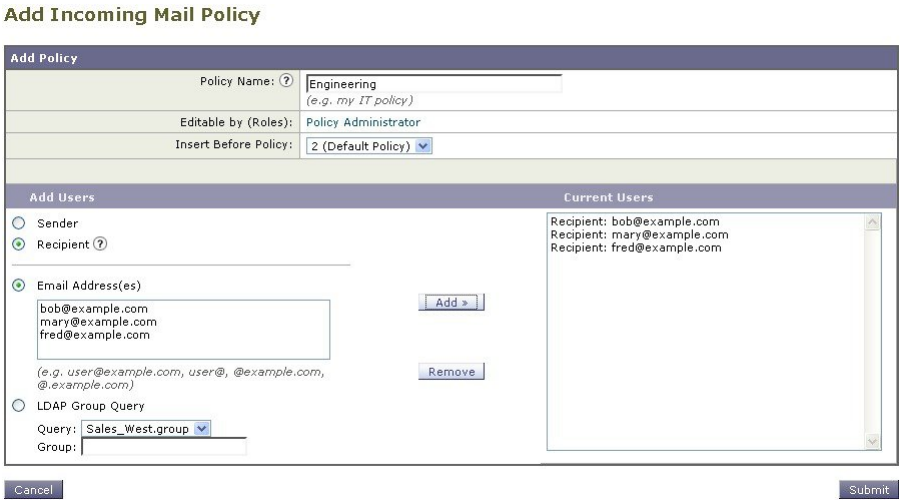
Figure 5: Newly Added Policy — Sales Group



Step 7 Click the **Add Policy** button again to add another new policy.

In this policy, individual email addresses for members of the engineering team are defined:

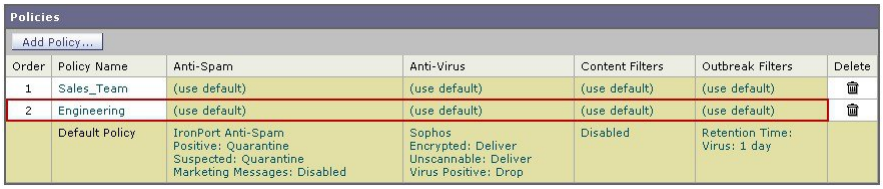
Figure 6: Creating a Policy for the Engineering Team



Step 8 When you are finished adding users for the engineering policy, click **Submit**.

Step 9 Commit your changes.

Figure 7: Newly Added Policy — Engineering Team



Note At this point, both newly created policies have the same settings applied to them as those in the default policy. Messages to users of either policy will match; however, the mail processing settings are not any different from the default policy. Therefore, messages that match users in the “Sales_Group” or “Engineering” policies will not be processed any differently than the default policy.

Default, Custom, and Disabled

The key at the bottom of the table shows how the color coding of cells for specific policies relates to the policy defined for the default row:

- Yellow shading shows that the policy is using the same settings as the default policy.
- No shading (white) shows that the policy is using different settings than the default policy.
- Grey shading shows that the security service has been disabled for the policy.

Creating Mail Policies for Different Groups of Senders and Recipients

In this part of the example, you will edit the two policies just created in the previous section.

- For the sales group, you will change the anti-spam settings to be even more aggressive than the default policy. (See Configuring the Default Anti-Spam Policies for Incoming Messages, on page 3.) The default policy of dropping positively identified spam messages will be kept. However, in this example, you will change the setting for marketing messages so that they will be sent to the Spam quarantine.

  This aggressive policy has the effect of minimizing unwanted messages being sent to sales team inboxes.

  See Managing Spam and Graymail for more information on anti-spam settings.

- For the engineering team, customize the Outbreak Filters feature setting so that it will modify the URLs in suspicious messages, except for links to example.com. Attachment files with the extension "dwg" will be bypassed by the Outbreak Filter scanning.

  See Outbreak Filters for more information on configuring Outbreak Filters.

  To edit the anti-spam settings for the sales team policy:

Step 1 Click the link for the Anti-Spam security service (the Anti-Spam) column in the sales policy row.

Because the policy was just added, the link is named: (use default) .

Step 2 On the anti-spam security service page, change the value for "Enable Anti-Spam Scanning for this Policy" from "Use Default Settings" to "Use Anti-Spam service."

Choosing "Use Anti-Spam service" here allows you to override the settings defined in the default policy.

Step 3 In the "Positively-Identified Spam Settings" section, change the "Apply This Action to Message" to "Drop."

Step 4 In the "Suspected Spam Settings" section, click **Yes** to enable suspected spam scanning.

Step 5 In the "Suspected Spam Settings" section, change the "Apply This Action to Message" to "Spam Quarantine."

Note Selecting the Spam quarantine forwards mail according to the settings defined in the Spam Quarantine chapter.

Step 6 In the "Add text to subject" field, click **None**.

Messages delivered to the Spam quarantine will have no additional subject tagging.

Step 7 In the "Marketing Email Settings" section, click **Yes** to enable scanning for marketing mail from legitimate sources.

Step 8 In the "Apply This Action to Message" section, select "Spam Quarantine."

Step 9 Submit and commit your changes.

Not that the shading shows that the policy is using different settings than the default policy.

At this point, any message that is suspected spam and whose recipient matches the LDAP query defined for the sales team policy will be delivered to the Spam Quarantine.

Creating Mail Policies for Different Groups of Senders and Recipients

To edit the Outbreak Filter settings for the engineering team policy:

Step 1 Click the link for the Outbreak Filters feature security service (the Outbreak Filters column) in the engineering policy row.

Because the policy was just added, the link is named: (use default) .

Step 2 On the Outbreak Filters feature security service page, change the scanning setting for the policy to "Enable Outbreak Filtering (Customize settings)."

Choosing "(Customize settings)" here allows you to override the settings defined in the default policy.

Doing so will also enable the contents of the rest of the page to allow you to select different settings.

Step 3 In the "Bypass Attachment Scanning" section of the page, type **dwg** in the in the file extension field.

The file extension " dwg " is not in the list of known file type that the appliance can recognize by its fingerprint when attachment scanning.

Note You do not need to type the period (.) before the three letter filename extension.

Step 4 Click **Add Extension** to add .dwg files to the list of file extensions that will bypass Outbreak Filters feature scanning.

Step 5 Click **Enable Message Modification**.

Enabling message modification allows the appliance to scan for targeted threats, such as phishing and scams, and URLs to suspicious or malicious websites. The appliance can rewrite links in messages to redirect the user through the Cisco Security proxy if they attempt to access the website.

Note Anti-spamming scanning must be enabled on the mail policy in order for Outbreak Filters to scan for targeted, non-viral threats.

Step 6 Select for **Enable for Unsigned Messages**.

This allows the appliance to rewrite URLs in signed messages. You must enable URL rewriting to be able to configure other Message Modification settings and the length of time that messages found to be non-viral threats stay in the quarantine before being released. This example uses the default retention time of 4 hours.

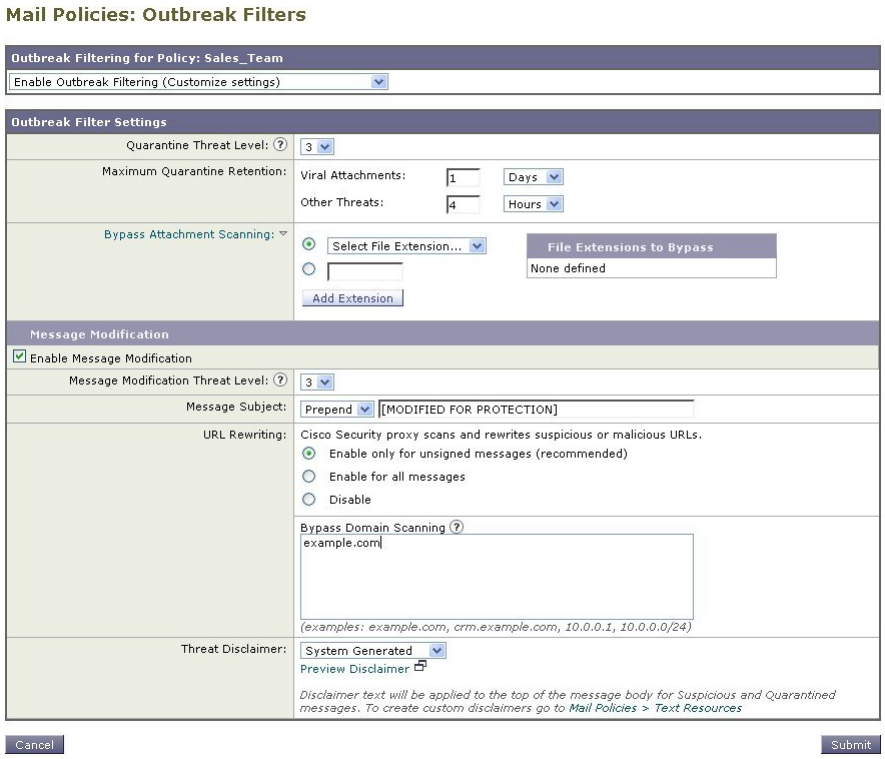
Step 7 Enter example.com in the **Bypass Domain Scanning** field.

The appliance will not modify links to example.com.

Step 8 Select System Generated for the **Threat Disclaimer**.

The appliance can insert a disclaimer above the message body to warn the user about the message's contents. The following example uses the system generated threat disclaimer.

Figure 8: Outbreak Filters Settings



Step 9 Submit and commit your changes.

Note that the shading shows that the policy is using different settings than the default policy.

At this point, any message that contains an attachment whose file extension is dwg — and whose recipient matches the recipients defined for the engineering team policy — will bypass the Outbreak Filter scanning and continue processing. Messages that contain links to the example.com domain will not have their links modified to redirect through the Cisco Security proxy and will not be considered suspicious.

Finding Senders or Recipients in Mail Policies

Use the “Find Policies” button to search for users already defined in policies defined in the Incoming or Outgoing Mail Policies pages.

For example, typing joe@example.com and clicking the Find Policies button will display results showing which policies contain defined users that will match the policy.

Click the name of the policy to jump to the Edit Policy page to edit the users for that policy.

Note that the default policy will always be shown when you search for any user, because, by definition, if a sender or recipient does not match any other configured policies, it will *always* match the default policy.

Managed Exceptions

Using the steps shown in the two examples above, you can begin to create and configure policies on a *managed exception* basis. In other words, after evaluating your organization's needs you can configure policies so that the majority of messages will be handled by the default policy. You can then create additional "exception" policies for specific users or user groups, managing the differing policies as needed. In this manner, message splintering will be minimized and you are less likely to impact system performance from the processing of each splinter message in the work queue.

You can define policies based on your organizations' or users' tolerance for spam, viruses, and policy enforcement. The following table outlines several example policies. "Aggressive" policies are designed to minimize the amount of spam and viruses that reach end-users mailboxes. "Conservative" policies are tailored to avoid false positives and prevent users from missing messages, regardless of policies.

Table 1: Aggressive and Conservative Mail Policy Settings

	Aggressive Settings	**Conservative Settings**
Anti-Spam	Positively identified spam: Drop Suspected spam: Quarantine Marketing mail: Deliver and prepend " [Marketing] " to the subject messages	Positively identified spam: Quarantine Suspected spam: Deliver and prepend " [Suspected Spam] " to the subject of messages Marketing mail: Disabled
Anti-Virus	Repaired messages: Deliver Encrypted messages: Drop Unscannable messages: Drop Infectious messages: Drop	Repaired messages: Deliver Encrypted messages: Quarantine Unscannable messages: Quarantine Infectious messages: Drop
Virus Filters	Enabled, no specific filename extensions or domains allowed to bypass Enable message modification for all messages	Enabled with specific filename extensions or domains allowed to bypass Enable message modification for unsigned messages

Filtering Messages Based on Content

In this part of the example, you will create three new content filters to be used in the Incoming Mail Policy table. All of these content filters will be editable by delegated administrators belonging to the Policy Administration custom user role. You will create the following:

1. "scan_for_confidential"

   This filter will scan messages for the string "confidential." If the string is found, a copy of the message will be sent to email alias hr@example.com , and the message will be sent to the Policy quarantine area.

2. "no_mp3s"

   This filter will strip MP3 attachments and notify the recipients that an MP3 file was stripped.

3. "ex_employee"

This content filter will scan for messages sent to a specific envelope recipient address (an ex-employee). If the message matches, a specific notification message will be sent to the sender of the message and then the message will be bounced.

After creating the content filters, you will then configure each of the policies (including the default policy) to enable the specific content filters in differing combinations.

Quarantining Message with “Confidential” in the Subject

The first example content filter contains one condition and two actions.

Step 1 Click the Mail Policies tab.

Step 2 Click Incoming Content Filters.

Step 3 Click the **Add Filter** button.

Step 4 In the Name field, type scan_for_confidential as the name of the new filter.

Filter names can contain ASCII characters, numbers, underscores or dashes. The first character of a content filter name must be a letter or an underscore.

Step 5 Click the **Editable By (Roles)** link, select the Policy Administrator and click **OK**.

Delegated administrators who belong to the Policy Administrator user role will be able to edit this content filter and use it in their mail policies.

Step 6 In the Description field, type the description. For example: scan all incoming mail for the string ‘confidential’ .

Step 7 Click Add Condition.

Step 8 Select Message Body.

Step 9 Type confidential in the Contains text: field and click **OK**.

The Add Content Filter page shows the condition added.

Step 10 Click Add Action.

Step 11 Select Send Copy To (Bcc:).

Step 12 In the Email Addresses field, type hr@example.com .

Step 13 In the Subject field, type [message matched confidential filter] .

Step 14 Click **OK**.

The Add Content Filter page shows the action added.

Step 15 Click Add Action.

Step 16 Select Quarantine.

Step 17 In the drop-down menu, select the Policy quarantine area.

Step 18 Click **OK**.

The Add Content Filter page shows the second action added.

Step 19 Submit and commit your changes.

At this point, the content filter is not enabled for any incoming Mail Policy; in this example, you have only added a new content filter to the primary list. Because it has not been applied to any policy, no email processing by the appliance will be affected by this filter.

Stripping MP3 Attachments from Messages

The second example content filter contains no conditions and one action.

Step 1 Click the **Add Filter** button.
Step 2 In the Name field, type no_mp3s as the name of the new filter.
Step 3 Click the **Editable By (Roles)** link, select the Policy Administrator and click **OK**.
Step 4 In the Description field, type the description. For example: strip all MP3 attachments .
Step 5 Click Add Action.
Step 6 Select Strip Attachment by File Info.
Step 7 Select File type is .
Step 8 In the drop-down field, select -- mp3 .
Step 9 Enter a replacement message if desired.
Step 10 Click **OK**.
Step 11 Submit and commit your changes.

Note It is not necessary to specify a condition when creating a content filter. When no condition is defined, any actions defined will always apply in the rule. (Specifying no condition is equivalent to using the true() message filter rule — all messages will be matched if the content filter is applied to a policy.)

Bouncing Messages Sent to a Former Employee

The third content filter example uses one condition and two actions.

Step 1 Click the **Add Filter** button.
Step 2 In the Name: field, type **`ex_employee`** as the name of the new filter.
Step 3 Click the **Editable By (Roles)** link, select the Policy Administrator and click **OK**.
Step 4 In the Description: field, type the description. For example: **`bounce messages intended for Doug`** .
Step 5 Click **Add Condition**.
Step 6 Select **Envelope Recipient**.
Step 7 For the envelope recipient, select **`Begins with`** , and type **`doug@`** .
Step 8 Click **OK**.

The Content Filters page refreshes to show the condition added. Note that you could create an LDAP directory containing the email addresses of former employees. As ex-employees are added to that directory, this content filter would be dynamically updated.

Step 9 Click Add Action.

Step 10 Select Notify.

Step 11 Select the checkbox for Sender and, in the **Subject** field, type message bounced for ex-employee of `example.com` .

Step 12 In the Use template section, select a notification template.

Note Some sections of the content filter rule builder will not appear in the user interface if the resource has not been preconfigured. For example, content dictionaries, notification templates, and message disclaimers will not appear as options if they have not been configured previously via the **Mail Policies > Dictionaries** page (or the `dictionaryconfig` command in the CLI). For more information about creating dictionaries, see Content Dictionaries.

Step 13 Click **OK**.

The Add Content Filters page shows the action added.

Step 14 Click Add Action.

Step 15 Select Bounce (Final Action) and click OK.

You can only specify one final action for a content filter. If you try to attempt to add more than one final action, the GUI displays an error.

Adding this action may will cause senders of messages to this ex-employee to potentially receive two messages: one for the notification template, and one for the bounce notification template.

Step 16 Submit and commit your changes.

Applying Individual Content Filters to Different Groups of Recipients

In the examples above, you created three content filters using the Incoming Content Filters pages. The Incoming Content Filters and Outgoing Content filters pages hold the “primary lists” of all possible content filters that can be applied to a policy.

Figure 9: Incoming Content Filters: Three Filters Created

In this part of the example, you will apply the three new content filters to be used in the Incoming Mail Policy table.

- The default policy will receive all three content filters.
- The engineering group will *not* receive the no_mp3s filter.
- The sales group will receive the content filters as the default incoming mail policy.

Enabling Content Filters for All Recipients by Default

Click the links to enable and select content filters for individual policies.

Step 1 Click Incoming Mail Policies to return to the Incoming Mail Policy table.

The page is refreshed to show the default policy and the two policies added in Creating a Mail Policy for a Group of Sender and Recipients, on page 4. Note that content filtering is disable by default for all policies.

Step 2 Click the link for the Content Filters security service (the Content Filters column) in the default policy row.

Step 3 On the Content Filtering security service page, change the value Content Filtering for Default Policy from "Disable Content Filters" to "Enable Content Filters (Customize settings)."

The content filters defined in the primary list (which were created in Overview of Content Filters using the Incoming Content Filters pages) are displayed on this page. When you change the value to "Enable Content Filters (Customize settings)," the checkboxes for each filter change from disabled (greyed out) to become enabled.

Step 4 Check the **Enable** checkbox for each content filter.

Step 5 Click **Submit**.

The table on the Incoming Mail Policies page shows the names of the filters that have been enabled for the default policy.

Allowing MP3 Attachments for Recipients in Engineering

To disable the "no_mp3s" content filters for the "engineering" policy:

Step 1 Click the link for the Content Filters security service (the Content Filters column) in the engineering team policy row.

Step 2 On the Content Filtering security service page, change the value for Content Filtering for Policy: Engineering from "Enable Content Filtering (Inherit default policy settings)" to "Enable Content Filtering (Customize settings)."

Because this policy was using the default values, when you change the value from "Use Default Settings" to "Yes," the checkboxes for each filter change from disabled (greyed out) to become enabled.

Step 3 Deselect the checkbox for the "no_mp3s" filter.

Step 4 Click **Submit**.

The table on the Incoming Mail Policies page shows the names of the filters that have been enabled for the engineering policy.

Step 5 Commit your changes.

What to do next

At this point, incoming messages that match the user list for the engineering policy will not have MP3 attachments stripped; however, all other incoming messages will have MP3 attachments stripped.

Notes on Configuring Content Filters in the GUI

- It is not necessary to specify a condition when creating a content filter. When no action is defined, any actions defined will always apply in the rule. (Specifying no action is equivalent to using the true() message filter rule — all messages will be matched if the content filter is applied to a policy.)

- If you do not assign a custom user role to a content filter, the content filter is public and can be used by any delegated administrator for their mail policies. See Distributing Administrative Tasks for more information on delegated administrators and content filters.
- Administrators and operators can view and edit all content filters on an appliance , even when the content filters are assigned to custom user roles.
- When entering text for filter rules and actions, the following meta characters have special meaning in regular expression matching: . ^ $ * + ? { [ ] \ | ( )

  If you do not wish to use regular expression you should use a '\' (backslash) to escape any of these characters. For example: "*Warning*"

- When you define more than one Condition for a content filter, you can define whether *all* of the defined actions (that is, a logical AND) or any of the defined actions (logical OR) need to apply in order for the content filter to be considered a match.
- You can test message splintering and content filters by creating “benign” content filters. For example, it is possible to create a content filter whose only action is “deliver.” This content filter will not affect mail processing; however, you can use this filter to test how the mail policy processing affects other elements in the system (for example, the mail logs).
- Conversely, using the “primary list” concept of the Incoming or Outgoing Content Filters, it is possible to create very powerful, wide-sweeping content filters that will immediately affect message processing for all mail handled by the appliance . The process for this is to:
  - Use the Incoming or Outgoing Content Filters page to create a new content filter whose order is 1.
  - Use the Incoming or Outgoing Mail Policies page to enable the new content filter for the default policy.
  - Enable the content filter for all remaining policies.
- The Bcc: and Quarantine actions available in Content Filters can help you determine the retention settings of quarantines you create. (See Policy, Virus, and Outbreak Quarantines) You can create filters that would simulate mail flow into and out of your policy quarantines so that messages are not released too quickly from the system (that is, the quarantine areas do not fill their allotted disk space too quickly).
- Because it uses the same settings as the Scan Behavior page or the scanconfig command, the “Entire Message” condition does not scan a message’s headers; choosing the “Entire Message” will scan only the message body and attachments. Use the “Subject” or “Header” conditions to search for specific header information.
- Configuring users by LDAP query will only appear in the GUI if you have LDAP servers configured on the appliance (that is, you have configured the appliance to query specific LDAP servers with specific strings using the ldapconfig command).
- Some sections of the content filter rule builder will not appear in the GUI if the resource has not been preconfigured. For example, notification templates and message disclaimers will not appear as options if they have not been configured previously using the Text Resources page or the textconfig command in the CLI.
- Content filters features will recognize, can contain, and/or scan for text in the following character encodings:
  - Unicode (UTF-8)
  - Unicode (UTF-16)
  - Western European/Latin-1 (ISO 8859-1)
  - Western European/Latin-1 (Windows CP1252)
  - Traditional Chinese (Big 5)

- Simplified Chinese (GB 2312)
- Simplified Chinese (HZ GB 2312)
- Korean (ISO 2022-KR)
- Korean (KS-C-5601/EUC-KR)
- Japanese (Shift-JIS (X0123))
- Japanese (ISO-2022-JP)
- Japanese (EUC)

You can mix and match multiple character sets within a single content filter. Refer to your web browser's documentation for help displaying and entering text in multiple character encodings. Most browsers can render multiple character sets simultaneously.

Figure 10: Multiple Character Sets in a Content Filter

- On the Incoming or Outgoing Content Filters summary pages, use the links for "Description," "Rules," and "Policies" to change the view presented for the content filters:
  - The **Description** view shows the text you entered in the description field for each content filter. (This is the default view.)
  - The **Rules** view shows the rules and regular expressions build by the rule builder page.
  - The **Policies** shows the policies for which each content filter is enabled.