Content Filters

This chapter contains the following sections:

Overview of Content Filters

Use content filters to customize handling of messages beyond the standard routine handling by the other content security features such as anti-virus scanning or DLP. For example, you can use a content filter if the content warrants quarantining for later examination, or because corporate policy requires certain messages to be encrypted before delivery.

How Content Filters Work

Content filters are similar to message filters, except that they are applied later in the email pipeline — after message filtering, after a message has been "splintered" into a number of separate messages for each matching mail policy, (see Message Splintering for more information), and after the message has undergone anti-spam and anti-virus scanning.

A content filter scans either incoming or outgoing messages. You cannot define a filter that scans both types of messages. The email gateway has a separate "primary list" of content filters for each type of message. The primary list also determines in which order the appliance runs the content filters. However, each individual mail policy determines which particular filters will be executed when a message matches the policy.

Content filters scan messages on a per-user (sender or recipient) basis.

Content filters have the following components:

- *conditions* that determine when the email gateway uses a content filter to scan a message (optional)
- *actions* that the email gateway takes on a message (required)
- *action variables* that the email gateway can add to a message when modifying it (optional)

Related Topics

- How to Scan Message Content Using a Content Filter, on page 2
- Content Filter Conditions, on page 2
- Content Filter Actions, on page 10
- Action Variables, on page 18

How to Scan Message Content Using a Content Filter

Procedure

	Command or Action	Purpose
Step 1	(Optional) Define the supporting features for the content filter.	Create any of the following items that you want to use with your content filter: • Encryption Profile • Disclaimer template • Notification template • Policy quarantine • URL allowed lists
Step 2	Define the incoming or outgoing content filter.	A content filter may be comprised of: • Content Filter Conditions, on page 2 (optional) • Content Filter Actions, on page 10 • Action Variables, on page 18 (optional) Creating a Content Filter, on page 20
Step 3	Define the group of users for whom you want to set up content security rules.	Create an incoming or outgoing mail policy.
Step 4	Assign the content filter to the group of user whose incoming or outgoing messages you want to use the filter for.	See Mail Policies

Content Filter Conditions

A condition is a “trigger” that determines whether the email gateway uses the filter on a message that matches the associated mail policy. Specifying conditions for a content filter is optional. Content filters without a condition are applied to all messages that match the associated mail policy.

In the content filter conditions, when you add filter rules that search for certain patterns in the message body or attachments, you can specify the minimum threshold for the number of times the pattern must be found. When AsyncOS scans the message, it totals the “score” for the number of matches it finds in the message and attachments. If the minimum threshold is not met, the regular expression does not evaluate to true. You can specify this threshold for text, smart identifiers, or content dictionary terms.

Multiple conditions may be defined for each filter. When multiple conditions are defined, you can choose whether the conditions are tied together as a logical OR ("Any of the following conditions...") or a logical AND ("All of the following conditions").

Table 1: Content Filter Conditions

Condition	Description
(no conditions)	Specifying conditions in content filters is optional. If no conditions are specified, a true rule is implied. The true rule matches all messages, and the actions are always performed.
Message Body or Attachments	**Contains text:** Does the message body contain text or an attachment that matches a specific pattern? **Contains smart identifier:** Does content in the message body or attachment match a smart identifier? • Credit card numbers • U.S. Social Security numbers • CUSIP (Committee on Uniform Security Identification Procedures) numbers • ABA (American Banking Association) routing numbers **Contains smart identifier prefix**: Does content in the message body or attachment match a smart identifier with a prefix ('credit,' 'ssn,' 'cusip,' or 'aba')? **Contains term in content dictionary:** Does the message body contain any of the regular expressions or terms in the content dictionary named <*dictionary name*> ? For this option to be enabled, the dictionary must already have been created. See Content Dictionaries. **Note** The dictionary-related conditions are only available if you have one or more dictionaries enabled. For information about creating content dictionaries, see Content Dictionaries. **Number of matches required**. Specify the number of matches required for the rule to evaluate to true. You can specify this threshold for text, smart identifiers, or content dictionary terms. This includes delivery-status parts and associated attachments.

Condition	Description
Message Body	**Contains text:** Does the message body contain text that matches a specific pattern? **Contains smart identifier:** Does content in the message body match a smart identifier? Smart identifiers can detect the following patterns: • Credit card numbers • U.S. Social Security numbers • CUSIP (Committee on Uniform Security Identification Procedures) numbers • ABA (American Banking Association) routing numbers **Contains smart identifier prefix**: Does content in the message body match a smart identifier with a prefix (‘credit,' 'ssn,' 'cusip,' or 'aba’)? **Contains term in content dictionary:** Does the message body contain any of the regular expressions or terms in the content dictionary named <*dictionary name*> ? For this option to be enabled, the dictionary must already have been created. See Content Dictionaries. **Note** The dictionary-related conditions are only available if you have one or more dictionaries enabled. For information about creating content dictionaries, see Content Dictionaries. **Number of matches required**. Specify the number of matches required for the rule to evaluate to true. You can specify this threshold for text or smart identifiers. This rule applies to the body of the message only. It does not include attachments or headers.
URL Category	See Filtering by URL Reputation or URL Category: Conditions and Rules and About URL Categories.
Message Size	Is the body size within a specified range? Body size refers to the size of the message, including both headers and attachments. The body-size rule selects those messages where the body size compares as directed to a specified number.
Macro Detection	Does the incoming or outgoing message contain macro-enabled attachments? You can use the Macro Detection condition to detect macro-enabled attachments in messages for the selected file type(s).

Condition	Description
Attachment Content	**Contains text.** Does the message contain an attachment that contains text or another attachment that matches a specific pattern? This rule is similar to the body-contains() rule, but it attempts to avoid scanning the entire “body” of the message. That is, it attempts to scan only that which the user would view as being an attachment. **Contains a smart identifier.** Does content in the message attachment match the specified smart identifier? **Contains smart identifier prefix**: Does content in the message attachment match a smart identifier with a prefix (‘credit,' 'ssn,' 'cusip,' or 'aba’)? **Contains terms in content dictionary.** Does the attachment contain any of the regular expressions or terms in the content dictionary named <*dictionary name*> ? To search for dictionary terms, the dictionary must already have been created. See Content Dictionaries. **Note** The dictionary-related conditions are only available if you have one or more dictionaries enabled. For information about creating content dictionaries, see Content Dictionaries. **Number of matches required**. Specify the number of matches required for the rule to evaluate to true. You can specify this threshold for text, smart identifier, or content dictionary matches.

Condition	Description
Attachment File Info	**Filename.** Does the message have an attachment with a filename that matches a specific pattern? **Filename contains term in content dictionary.** Does the message have an attachment with a filename that contains any of the regular expressions or terms in the content dictionary named <*dictionary name*> ? For this option to be enabled, the dictionary must already have been created. See Content Dictionaries. **Note** The dictionary-related conditions are only available if you have one or more dictionaries enabled. For information about creating content dictionaries, see Content Dictionaries. **File type**. Does the message have an attachment of a file type that matches a specific pattern based on its fingerprint (similar to a UNIX file command)? **MIME type**. Does the message have an attachment of a specific MIME type? This rule is similar to the attachment-type rule, except only the MIME type given by the MIME attachment is evaluated. (The email gateway does not try to "guess" the type of the file by its extension if there is no explicit type given.) **File Hash List.** Does the message have an attachment that matches a specific file SHA-256 value? Select the required file hash list from the drop-down list. **Note** You can only select a file hash list that contains the SHA-256 file hash type. **Image Analysis.** Does the message have an image attachment that matches the image verdict specified? Valid image analysis verdicts include: *Suspect, Inappropriate, Suspect or Inappropriate, Unscannable* , or *Clean.* **External Threat Feeds**: Does the file match the threat information from the selected external threat feed source(s)? **Select a File Hash Exception List**: (Optional) Select the list of allow listed file hashes that you do not want the email gateway to detect for threats. For more information, see Configuring Email Gateway to Consume External Threat Feeds. **Attachment is Corrupt.** Does this message have an attachment that is corrupt? **Note** A corrupt attachment is an attachment that the scanning engine cannot scan and identified as corrupt.
Attachment Protection	**Contains an attachment that is password-protected or encrypted.** (For example, use this condition to identify attachments that are potentially unscannable.) **Contains an attachment that is NOT password-protected or encrypted.**

Condition	Description
Subject Header	**Subject Header:** Does the subject header match a certain pattern? **Contains terms in content dictionary**: Does the subject header contain any of the regular expressions or terms in the content dictionary <*dictionary name*> ? To search for dictionary terms, the dictionary must already have been created. See Content Dictionaries. **Note** The dictionary-related conditions are only available if you have one or more dictionaries enabled. For information about creating content dictionaries, see Content Dictionaries.
Other Header	**Header name**: Does the message contain a specific header? **Header value:** Does the value of that header match a certain pattern? **Header value contains terms in the content dictionary.** Does the specified header contain any of the regular expressions or terms in the content dictionary named <*dictionary name*> ? To search for dictionary terms, the dictionary must already have been created. See Content Dictionaries **Note** The dictionary-related conditions are only available if you have one or more dictionaries enabled. For information about creating content dictionaries, see Content Dictionaries. For an example showing how this option can be used, see Using Custom Headers to Redirect URLs in Suspected Spam to the Cisco Web Security Proxy: Configuration Example.
Envelope Sender	**Envelope Sender.** Does the Envelope Sender (i.e., the Envelope From, <MAIL FROM>) match a given pattern? **Matches LDAP group**. Is the Envelope Sender, i.e., the Envelope From, <MAIL FROM>) in a given LDAP group? **Contains term in content dictionary.** Does the envelope sender contain any of the regular expressions or terms in the content dictionary named <*dictionary name*> ? To search for dictionary terms, the dictionary must already have been created. See Content Dictionaries. **Note** The dictionary-related conditions are only available if you have one or more dictionaries enabled. For information about creating content dictionaries, see Content Dictionaries.

Condition	Description
Envelope Recipient	**Envelope Recipient**. Does the Envelope Recipient, (i.e. the Envelope To, <RCPT TO>) match a given pattern? **Matches LDAP group**. Is the Envelope Recipient, (i.e. the Envelope To, <RCPT TO>) in a given LDAP group? **Contains term in content dictionary.** Does the envelope recipient contain any of the regular expressions or terms in the content dictionary named <*dictionary name*> ? To search for dictionary terms, the dictionary must already have been created. See Content Dictionaries. **Note** The dictionary-related conditions are only available if you have one or more dictionaries enabled. For information about creating content dictionaries, see Content Dictionaries. The Envelope Recipient rule is message-based. If a message has multiple recipients, only one recipient has to be found in a group for the specified action to affect the message to all recipients. Is the Envelope Sender (i.e., the Envelope From, <MAIL FROM>) in a given LDAP group?
Receiving Listener	Did the message arrive via the named listener? The listener name must be the name of a listener currently configured on the system.
Remote IP	Was the message sent from a remote host that matches a given IP address or IP block? The Remote IP rule tests to see if the IP address of the host that sent that message matches a certain pattern. This can be an Internet Protocol version 4 (IPv4) or version 6 (IPv6) address. The IP address pattern is specified using the allowed hosts notation described in Sender Group Syntax, except for the SBO, IPR, dnslist notations and the special keyword ALL.
Reputation Score	What is the sender's IP Reputation Score? The Reputation Score rule checks the IP Reputation Score against another value.
DKIM Authentication	Did DKIM authentication pass, partially verify, return temporarily unverifiable, permanently fail, or were no DKIM results returned?

Condition	Description
Forged Email Detection	Is the sender address of the message forged? The rule checks if the From: header in the message is similar to any of the users in the content dictionary. Select a content dictionary and enter the threshold value (1 through 100) for considering a message as potentially forged. The Forged Email Detection condition compares the From: header with the users in the content dictionary. During this process, depending on the similarity, the email gateway assigns similarity score to each of the users in the dictionary. The following are some examples: • If the From: header is <j0hn.sim0ns@example.com> and the content dictionary contains a user 'John Simons,' the email gateway assigns a similarity score of 82 to the user. • If the From: header is <john.simons@diff-example.com> and the content dictionary contains a user 'John Simons,' the email gateway assigns a similarity score of 100 to the user. The higher the similarity score, the higher the probability that the message is forged. If the similarity score is greater than or equal to the specified threshold value, the filter action is triggered. If you want to skip the Forged email detection filter for messages from specific senders, choose the address list from the **Exception List** drop-down list. **Note** You can choose only the address lists that are created using the full email addresses. For more information, refer to Using a List of Sender Addresses for Incoming Connection Rules. For more information, see Forged Email Detection.
SPF Verification	What was the SPF verification status? This filter rule allows you to query for different SPF verification results. For more information about SPF verification, see the "Email Authentication" chapter. **Note** If you have configured an SPF verification content filter condition without an SPF identity and if a message contains different SPF identities with different verdicts, the condition is triggered if one of the verdicts in the message matches the condition.
S/MIME Gateway Message	Is the message S/MIME signed, encrypted, or signed and encrypted? For more information, see S/MIME Security Services
S/MIME Gateway Verified	Is the S/MIME message successfully verified, decrypted, or decrypted and verified? For more information, see S/MIME Security Services

Condition	Description
Message Language	Is the message (subject and body) in one of the selected languages? This condition will not check for the language in attachments and headers. **How does language detection work?** The email gateway uses the built-in language detection engine to detect the language in a message. The email gateway extracts the subject and the message body and passes it to the language detection engine. The language detection engine determines the probability of each language in the extracted text and passes it back to the email gateway. The email gateway considers the language with the highest probability as the language of the message. The email gateway considers the language of the message as 'undetermined' in one of the following scenarios: • If the detected language is not supported by email gateway • If the email gateway is unable to detect the language of the message • If the total size of the extracted text sent to the language detection engine is less than 50 bytes.
Duplicate Boundaries Verification	Does the message contain duplicate MIME boundaries? If you want to take actions on messages that contain duplicate MIME boundaries, use this condition. **Note** Attachment-based conditions (for example, Attachment Content) or actions (for example, Strip Attachment by Content) will not work on malformed messages (with duplicate MIME boundaries).
Geolocation	Does the message originate from the selected countries? You can use the Geolocation condition to handle incoming messages from particular countries that you select. **Note** Enable the Anti-Spam engine on your email gateway before you use the Geolocation content filter.
Domain Reputation	Does the sender domain match the specified criteria? • Sender Domain Reputation • External Threat Feeds For more information, see Configuring Email Gateway to Consume External Threat Feeds or Sender Domain Reputation Filtering

Content Filter Actions

The action is what the email gatewaydoes with a message that matches the content filter's condition. Many different types of actions are available, including modifying the message, quarantining it, or dropping it. A "final action" performed on a message, delivering or dropping it, forces the Email Security appliance to perform the action immediately and forgo all further processing, such as Outbreak Filter or DLP scanning.

At least one action must be defined for each content filter.

Actions are performed in order on messages, so consider the order of actions when defining multiple actions for a content filter.

When you configure a quarantine action for messages that match Attachment Content conditions, Message Body or Attachment conditions, Message body conditions, or the Attachment content conditions, you can view the matched content in the quarantined message. When you display the message body, the matched content is highlighted in yellow. You can also use the $MatchedContent action variable to include the matched content in the message subject. For more information, see the Text Resources chapter.

Only one final action may be defined per filter, and the final action must be last action listed. Bounce, deliver, and drop are final actions. When entering actions for content filters, the GUI and CLI will force final actions to be placed last.

See also Action Variables, on page 18.

Table 2: Content Filter Actions

Action	Description
Quarantine	**Quarantine**. Flags the message to be held in one of the policy quarantine areas. **Duplicate message**: Sends a copy of the message to the specified quarantine and continues processing the original message. Any additional actions apply to the original message.
Encrypt on Delivery	The message continues to the next stage of processing. When all processing is complete, the message is encrypted and delivered. **Encryption rule**: Always encrypts the message or only encrypts it if an attempt to send it over a TLS connection first fails. See Using a TLS Connection as an Alternative to Encryption for more information. **Encryption Profile.** Once processing is complete, encrypts the message using the specified encryption profile, then delivers the message. This action is for use with a Cisco Encryption Appliance or a hosted key service. **Subject**. Subject for the encrypted message. By default, the value is `$Subject` .

Action	Description
Strip Attachment by Content	**Attachment contains.** Drops all attachments on messages that contain the regular expression. Archive files (zip, tar) will be dropped if any of the files they contain match the regular expression pattern. **Contains smart identifier.** Drops all attachments on a message that contains the specified smart identifier. **Attachment contains terms in the content dictionary.** Does the attachment contain any of the regular expressions or terms in the content dictionary named *<dictionary name>* ? **Number of matches required**. Specify the number of matches required for the rule to evaluate to true. You can specify this threshold for text, smart identifier, or content dictionary matches. **Replacement message.** The optional comment serves as the means to modify the text used to replace the attachment that was dropped. Attachment footers simply append to the message.

Action	Description
Strip Attachment by File Info	**File name**. Drops all attachments on messages that have a filename that match the given regular expression. Archive file attachments (zip, tar) will be dropped if they contain a file that matches. **File size**. Drops all attachments on the message that, in raw encoded form, are equal to or greater than the size (in bytes) given. Note that for archive or compressed files, this action does not examine the uncompressed size, but rather the size of the actual attachment itself. **File type**. Drops all attachments on messages that match the given "fingerprint" of the file. Archive file attachments (zip, tar) will be dropped if they contain a file that matches. **MIME type**. Drops all attachments on messages that have a given MIME type. **File Hash List**. Drops all attachments on messages that match the file SHA-256 value in the selected file hash list. Select the required file hash list from the drop-down list. **Note** You can only select a file hash list that contains the SHA-256 file hash type. **Image Analysis Verdict**. Drops attachments for image attachments that match the image verdict specified. Valid image analysis verdicts include: *Suspect, Inappropriate, Suspect or Inappropriate, Unscannable* , or *Clean* . **External Threat Feeds**. Drops all message attachments on messages whose files are categorized as malicious by the ETF engine. **Select a File Hash Exception List**. (Optional) Select the list of allow listed file hashes that you do not want the Cisco Email Security Gateway to detect for threats. For more information, see Configuring Email Gateway to Consume External Threat Feeds. **Replacement message.** The optional comment serves as the means to modify the text used to replace the attachment that was dropped. Attachment footers simply append to the message.

Action	Description
Strip Attachment with Macro	Drops all macro-enabled attachments of the specified file type. **Note** If an archive or embedded file contains macros, the parent file is dropped from the message. **Custom Replacement Message (Optional)**: By default, a system generated message is added to the bottom of the message body when an attachment is dropped. The following is a sample system generated message when a macro-enabled attachment is dropped from the message: `A MIME attachment of type <application/vnd.ms-excel> was removed here by a drop-macro-enabled-attachments filter rule on the host <mail.example.com>.` The custom message that you enter in the **Custom Replacement Message** field replaces the system-generated message.
URL Reputation	See Modifying URLs in Messages: Using URL Reputation and URL Category Actions in Filters and Creating Allowed Lists for URL Filtering. Use "No Score" to specify an action for URLs for which a reputation cannot be determined. **Note** The email gateway considers a message signed if it is encrypted using S/MIME or it contains an S/MIME signature.
URL Category	See Modifying URLs in Messages: Using URL Reputation and URL Category Actions in Filters and About URL Categories. **Note** The email gateway considers a message signed if it is encrypted using S/MIME or it contains an S/MIME signature.
Add Disclaimer Text	**Above**. Add disclaimer above message (heading). **Below.** Add disclaimer below message (footer). **Note:** You must have already created disclaimer text in order to use this content filter action. See Disclaimer Template for more information.
Bypass Outbreak Filter Scanning	Bypass Outbreak Filter scanning for this message.
Bypass DKIM Signing	Bypass DKIM signing for this message.
Send Copy (Bcc:)	**Email addresses**. Copies the message anonymously to the specified recipients. **Subject**. Add a subject for the copied message. **Return path (optional).** Specify a return path. **Alternate mail host (optional).** Specify an alternate mail host.

Action	Description
Notify	**Notify.** Reports this message to the specified recipients. You can optionally notify the sender and recipients. **Subject**. Add a subject for the copied message. **Return path (optional).** Specify a return path. **Use template**. Select a template from the templates you created. **Include original message as an attachment**. Adds the original message as an attachment.
Change Recipient to	**Email address**. Changes the recipient of the message to the specified email address.
Send to Alternate Destination Host	**Mail host**. Changes the destination mail host for the message to the specified mail host. **Note** This action prevents a message classified as spam by an anti-spam scanning engine from being quarantined. This action overrides the quarantine and sends it to the specified mail host.
Deliver from IP Interface	**Send from IP interface.** Send from the specified IP Interface. The Deliver from IP Interface action changes the source host for the message to the source specified. The source host consists of the IP interface that the messages should be delivered from.
Strip Header	**Header name.** Remove the specified header from the message before delivering.
Add/Edit Header	**Inserts a new header into the message or modifies an existing header.** **Header name**. Name of new or existing header. **Specify value of new header.** Inserts a value for the new header into the message before delivering. **Prepend to the Value of Existing Header.** Prepends the value to the existing header before delivering. **Append to the Value of Existing Header.** Appends the value to the existing header before delivering. **Search & Replace from the Value of Existing Header**. Enter a search term to find the value you want to replace in the existing header in the **Search for** field. Enter the value you want to insert into the header in the **Replace with** field. You can use a regular expression to search for the value. Leave the **Replace with** field empty if you want to delete the value from the header.
Forged Email Detection	Strips the From: header from the forged message and replaces it with the Envelope Sender. See Forged Email Detection.

Action	Description
Add Message Tag	Inserts a custom term into the message to use with DLP policy filtering. You can configure a DLP policy to limit scanning to messages with the message tag. The message tag is not visible to recipients. For information on using messages tags in a DLP policy, see Policies for Data Loss Prevention.
Add Log Entry	Inserts customized text into the IronPort Text Mail logs at the INFO level. The text can include action variables. The log entry also appears in message tracking.
Add CEF Log Entry	Inserts customized text into the Consolidated Event Logs. The text can include action variables. **Note** You can use this content filter action only when you configure the 'Consolidated Event Logs' log subscription in your email gateway. **Label**: Add a label for the Consolidated Event Logs entry. **Note** The label must not contain more than 64 characters. **Value**: Add a message for the Consolidated Event Logs entry. **Note** The message must not contain more than 1024 characters. **Note** In your email gateway, there is a limit of 65535 characters for a CEF log line when using Consolidated Event Logs through the Syslog Push method. Your external SIEM solution may also have a defined limit on the number of characters allowed for a CEF log file. Make sure you configure the customized texts to be logged and the Consolidated Event Logs subscription fields accordingly based on the number of characters allowed in your email gateway and the SIEM solution. The CEF log entry appears in Consolidated Event Logs when you configure the 'Consolidated Event Logs' log subscription with "Custom Log Entries" present in "Selected Log Fields." **For Example**: If you enter ‘label1’ in the ‘Label’ field and ‘value20' in the ‘Value’ field, then the following field is added in Consolidated Event Logs: `ESACustomLogs={'label1': ['value20']}`
S/MIME Sign/Encrypt on Delivery	Performs an S/MIME signing or encryption of the message during the delivery. This means that the message continues to the next stage of processing, and when all processing is complete, the message is signed or encrypted and delivered. **S/MIME Sending Profile**: Performs an S/MIME signing or encryption using the specified S/MIME sending profile. See Managing S/MIME Sending Profiles.

Action	Description
Encrypt and Deliver Now (Final Action)	Encrypts and delivers the message, skipping any further processing. **Encryption rule**: Always encrypts the message or only encrypts it if an attempt to send it over a TLS connection first fails. See Using a TLS Connection as an Alternative to Encryption for more information. **Encryption Profile.** Encrypts the message using the specified encryption profile, then delivers the message. This action is for use with a Cisco Encryption Appliance or a hosted key service. **Subject**. Subject for the encrypted message. By default, the value is `$Subject` .
S/MIME Sign/Encrypt (Final Action)	Performs an S/MIME signing or encryption and delivers the message, skipping any further processing. **S/MIME Sending Profile**: Performs an S/MIME signing or encryption using the specified S/MIME sending profile. See Managing S/MIME Sending Profiles.
Bounce (Final Action)	Sends the message back to the sender.
Skip Remaining Content Filters (Final Action)	Delivers the message to the next stage of processing, skipping any further content filters. Depending on configuration, this may mean deliver the message to recipient(s), quarantine, or begin Outbreak Filters scanning.
Drop (Final Action)	Drops and discards the message.
Safe Print	Use the 'Safe Print' content filter action to safe print a message attachment. You can use the Safe Print content filter action in any one of the following ways: • **Safe print matching attachments**: Use this option to safe print all message attachments that match a configured content filter condition. • **Safe print all attachments**: Use this option to safe print all message attachments when the configured content filter condition is true Select **Yes** to strip a message attachment that is marked as unscannable. **Note** By default, a system generated message is added as an attachment text file when an attachment is unscannable. You can enter a custom message in the **Custom Replacement Message** field. For more information, see How to Configure Email Gateway to Safe Print Message Attachments.

Related Topics

- Action Variables, on page 18

Action Variables

Headers added to messages processed by content filters can contain variables that will be automatically replaced with information from the original message when the action is executed. These special variables are called *action variables.* Your email gateway supports the following set of action variables:

Table 3: Action Variables

Variable	Syntax	Description
All Headers	`$AllHeaders`	Replaced by the message headers.
Body Size	`$BodySize`	Replaced by the size, in bytes, of the message.
Date	`$Date`	Replaced by the current date, using the format MM/DD/YYYY.
Dropped File Name	`$dropped_filename`	Returns only the most recently dropped filename.
Dropped File Names	`$dropped_filenames`	Same as $filenames , but displays list of dropped files.
Dropped File Types	`$dropped_filetypes`	Same as $filetypes , but displays list of dropped file types.
Envelope Sender	`$envelopefrom` or `$envelopesender`	Replaced by the Envelope Sender (Envelope From, <MAIL FROM>) of the message.
Envelope Recipients	`$EnvelopeRecipients`	Replaced by all Envelope Recipients (Envelope To, <RCPT TO>) of the message.
File Names	`$filenames`	Replaced with a comma-separated list of the message's attachments' filenames.
File Sizes	`$filesizes`	Replaced with a comma-separated list of the message's attachment's file sizes.
File Types	`$filetypes`	Replaced with a comma-separated list of the message's attachments' file types.
Filter Name	`$FilterName`	Replaced by the name of the filter being processed.
GMTimeStamp	`$GMTimeStamp`	Replaced by the current time and date, as would be found in the Received: line of an email message, using GMT.
HAT Group Name	`$Group`	Replaced by the name of the sender group the sender matched on when injecting the message. If the sender group had no name, the string " >Unknown< " is inserted.
Mail Flow Policy	`$Policy`	Replaced by the name of the HAT policy applied to the sender when injecting the message. If no predefined policy name was used, the string " >Unknown< " is inserted.

Variable	Syntax	Description
Matched Content	`$MatchedContent`	Replaced by the value (or values) that triggered a content-scanning filter. Matched content can be a content dictionary match, a smart identifier, or a match to a regular expression.
Header	`$Header['string']`	Replaced by the value of the quoted header, if the original message contains a matching header. Note that double quotes may also be used.
Hostname	`$Hostname`	Replaced by the hostname of the email gateway.
Internal Message ID	`$MID`	Replaced by the Message ID, or "MID" used internally to identify the message. Not to be confused with the RFC822 "Message-Id" value (use $Header to retrieve that).
Receiving Listener	`$RecvListener`	Replaced by the nickname of the listener that received the message.
Receiving Interface	`$RecvInt`	Replaced by the nickname of the interface that received the message.
Remote IP Address	`$RemoteIP`	Replaced by the IP address of the system that sent the message to the email gateway.
Remote Host Address	`$remotehost`	Replaced by the hostname of the system that sent the message to the email gateway.
SenderBase Reputation Score	`$Reputation`	Replaced by the SenderBase Reputation score of the sender. If there is no reputation score, it is replaced with " None ".
Subject	`$Subject`	Replaced by the subject of the message.
Time	`$Time`	Replaced by the current time, in the local time zone.
Timestamp	`$Timestamp`	Replaced by the current time and date, as would be found in the Received: line of an email message, in the local time zone.

How to Filter Messages Based on Content

Related Topics

- Creating a Content Filter, on page 20
- Enabling Content Filters for All Recipients by Default, on page 21
- Applying the Content Filter to Messages for a Certain User Group, on page 21
- Notes on Configuring Content Filters in the GUI, on page 22

Creating a Content Filter

Before You Begin

- If you want to encrypt a message that matches the content filter, create an encryption profile.
- If you want to add a disclaimer to a matching message, create a disclaimer template to use for generating disclaimers.
- If you want to send a notification message to a user due to a matching message, create a notification template for generating notifications.
- If you want to quarantine a message, you create a new policy quarantine for these messages or use an existing one.

Procedure

Step 1 Click **Mail Policies > Incoming Mail Policies**

or

Mail Policies > Outgoing Mail Policies.

Step 2 Click **Add Filter**.

Step 3 Enter a name and description for the filter.

Step 4 (X-REF) 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 5 (Optional) Add a condition for triggering the filter.

a) Click Add Condition.
b) Select the condition type.
c) Define the condition's rules.
d) Click **OK**.
e) Repeat these steps for any additional conditions you want to add to the filter. 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.

Note If you do not add a condition, the email gateway will perform the content filter's action to any message that matches one of the mail policies associated with the filter.

Step 6 Add an action for the email gateway to take on a message that matches the filter's condition.

a) Click Add Action.
b) Select the action type.
c) Define the action.
d) Click **OK**.
e) Repeat the previous steps for any additional actions you want the email gateway to take.
f) For multiple actions, arrange the actions in the order that you want the email gateway to apply them to the message. There can only be one "final" action per filter, and AsyncOS automatically moves the final action to the end of the order.

Step 7 Submit and commit your changes.

What to do next

- You can enable the content filter in a default incoming or outgoing mail policy.
- You can enable the content filter in a mail policy for a specific group of users.

Enabling Content Filters for All Recipients by Default

Procedure

Step 1 Click **Mail Policies > Incoming Mail Policies**

or

Mail Policies > Outgoing Mail Policies.

Step 2 Click the link for the Content Filters security service 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 , on page 1) are displayed on this page. When you change the value to "Enable Content Filters (Customize settings)," the checkboxes for each filter become enabled.

Step 4 Check the **Enable** checkbox for each content filter you want to enable.

Step 5 Submit and commit your changes.

Applying the Content Filter to Messages for a Certain User Group

Before You Begin

- Create an incoming or outgoing mail policy for the group of users whose messages for which you want to use the content filter. See Creating a Mail Policy for a Group of Senders and Recipients for more information.

Procedure

Step 1 Click **Mail Policies > Incoming Mail Policies**

or

Mail Policies > Outgoing Mail Policies.

Step 2 Click the link for the Content Filters security service (the Content Filters column) for the mail policy to which you want to apply the content filter.

Step 3 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)."

Step 4 Select the checkboxes for the content filters you want to use.

Step 5 Submit and commit your changes.

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 condition 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 the "Common Administrative Tasks" chapter for more information on delegated administrators and content filters.
- Administrators and operators can view and edit all content filters on the email gateway, 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*"

- 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 Email Security Manager 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 email gateway. 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 email gateway (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.

- 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.