Text Resources

This chapter contains the following sections:

- Overview of Text Resources, on page 1
- Content Dictionaries, on page 2
- Using and Testing the Content Dictionaries Filter Rules, on page 7
- Understanding Text Resources, on page 9
- Overview of Text Resource Management, on page 10
- Using Text Resources, on page 13

Overview of Text Resources

This chapter discusses creating and managing various text resources, such as content dictionaries, disclaimers, and templates.

Related Topics

- Content Dictionaries, on page 1
- Text Resources, on page 2
- Message Disclaimer Stamping, on page 2
- Using Custom Dictionaries of Sensitive DLP Terms (Custom DLP Policies Only)

Content Dictionaries

Content dictionaries are groups of words or entries that work in conjunction with the Body Scanning feature on the appliance and are available to both content and message filters. Use the dictionaries you define to scan messages, message headers, and message attachments for terms included in the dictionary in order to take appropriate action in accordance with your corporate policies. For example, you could create a list of confidential or profane words, and, using a filter rule to scan messages that contain words in the list, drop, archive, or quarantine the message.

The AsyncOS operating system includes the ability to define a total of 100 content dictionaries using the GUI (Mail Policies > Dictionaries) or the CLI's **`dictionaryconfig`** command. You can create, delete, and view dictionaries; add and delete entries from a dictionary; and import and export entire dictionaries.

You can use content dictionaries to scan messages against message or content filters in order to take appropriate action in accordance with your corporate policies. You can create, delete, and view dictionaries; add and

delete entries from a dictionary; and import and export entire dictionaries. You can also determine case sensitivity and word boundary detection for each dictionary. For example, you could create a list of confidential or profane words, and, using a filter rule to scan messages for words in the list, drop or archive messages containing matching words. And you can add a "weight" terms in a dictionary so that certain terms trigger a filter action more easily.

Dictionaries can contain non-ASCII characters.

Note that, for efficient processing, the following content dictionary entries are treated as words:

- Entries containing only alphanumeric characters
- Email addresses containing the following characters: 0-9, A-Z, a-z, dot, underscore, hyphen, and at symbol
- Domain names containing the following characters: 0-9, A-Z, a-z, dot, underscore, hyphen, and at symbol

If you want the appliance to treat such a word as a regular expression, enclose the word in parenthesis, for example, (user@example.com) .

Related Topics

- Dictionary Content, on page 3
- Importing and Exporting Dictionaries as Text Files, on page 4
- Adding Dictionaries, on page 5
- Deleting Dictionaries, on page 6
- Importing Dictionaries, on page 6
- Exporting Dictionaries, on page 7

Text Resources

Text resources are text objects, such as disclaimers, notification templates, and anti-virus templates. You can create new objects for use in various components of AsyncOS. You can import and export text resources.

Message Disclaimer Stamping

Message disclaimer stamping allows you to add a disclaimer text resource to messages. For example, you could append a copyright statement, promotional message, or disclaimer to every message sent from within your enterprise.

Content Dictionaries

Content dictionaries are groups of words or entries that work in conjunction with the Body Scanning feature on the appliance and are available to both content and message filters. Use the dictionaries you define to scan messages, message headers, and message attachments for terms included in the dictionary in order to take appropriate action in accordance with your corporate policies. For example, you could create a list of confidential or profane words, and, using a filter rule to scan messages that contain words in the list, drop, archive, or quarantine the message.

The AsyncOS operating system includes the ability to define a total of 100 content dictionaries using the GUI (Mail Policies > Dictionaries) or the CLI's **`dictionaryconfig`** command. You can create, delete, and view dictionaries; add and delete entries from a dictionary; and import and export entire dictionaries.

You can use content dictionaries to scan messages against message or content filters in order to take appropriate action in accordance with your corporate policies. You can create, delete, and view dictionaries; add and delete entries from a dictionary; and import and export entire dictionaries. You can also determine case sensitivity and word boundary detection for each dictionary. For example, you could create a list of confidential or profane words, and, using a filter rule to scan messages for words in the list, drop or archive messages containing matching words. And you can add a "weight" terms in a dictionary so that certain terms trigger a filter action more easily.

Dictionaries can contain non-ASCII characters.

Note that, for efficient processing, the following content dictionary entries are treated as words:

- Entries containing only alphanumeric characters
- Email addresses containing the following characters: 0-9, A-Z, a-z, dot, underscore, hyphen, and at symbol
- Domain names containing the following characters: 0-9, A-Z, a-z, dot, underscore, hyphen, and at symbol

If you want the appliance to treat such a word as a regular expression, enclose the word in parenthesis, for example, (user@example.com) .

Related Topics

- Dictionary Content, on page 3
- Importing and Exporting Dictionaries as Text Files, on page 4
- Adding Dictionaries, on page 5
- Deleting Dictionaries, on page 6
- Importing Dictionaries, on page 6
- Exporting Dictionaries, on page 7

Dictionary Content

Words in dictionaries are created with one text string per line, and entries can be in plain text or in the form of regular expressions. Dictionaries can also contain non-ASCII characters. Defining dictionaries of regular expressions can provide more flexibility in matching terms, but doing so requires you to understand how to delimit words properly. For a more detailed discussion of Python style regular expressions, consult the Python Regular Expression HOWTO, accessible from

http://www.python.org/doc/howto/

Note To use the special character # at the beginning of a dictionary entry, you can use a character class [#] to prevent it being treated as a comment.

For each term, you specify a "weight," so that certain terms can trigger filter conditions more easily. When AsyncOS scans messages for the content dictionary terms, it "scores" the message by multiplying the number of term instances by the weight of term. Two instances of a term with a weight of three would result in a score of six. AsyncOS then compares this score with a threshold value associated with the content or message filter to determine if the message should trigger the filter action.

You can also add smart identifiers to a content dictionary. Smart identifiers are algorithms that search for patterns in data that correspond to common numeric patterns, such as social security numbers and ABA routing numbers. These identifiers can useful for policy enforcement. For more information about regular expressions,

see “Regular Expressions in Rules” in the “Using Message Filters to Enforce Email Policies” chapter. For more information about smart identifiers, see “Smart Identifiers” in the “Using Message Filters to Enforce Email Policies” chapter.

Note Dictionaries containing non-ASCII characters may or may not display properly in the CLI on your terminal. The best way to view and change dictionaries that contain non-ASCII characters is to export the dictionary to a text file, edit that text file, and then import the new file back into the appliance . For more information, see Importing and Exporting Dictionaries as Text Files, on page 4.

Related Topics

- Word Boundaries and Double-byte Character Sets, on page 4

Word Boundaries and Double-byte Character Sets

In some languages (double-byte character sets), the concepts of a word or word boundary, or case do not exist. Complex regular expressions that depend on concepts like what is or is not a character that would compose a word (represented as “\w” in regex syntax) cause problems when the locale is unknown or if the encoding is not known for certain. For that reason, you may want to disable word-boundary enforcement.

Importing and Exporting Dictionaries as Text Files

The content dictionary feature also includes, by default, the following text files located in the configuration directory of the appliance :

- `config.dtd`
- `profanity.txt`
- `proprietary_content.txt`
- `sexual_content.txt`

These text files are intended to be used in conjunction with the content dictionaries feature to aid you in creating new dictionaries. These content dictionaries are weighted and use smart identifiers to better detect patterns in data and trigger filters when the patterns indicate compliance issues.

Note Importing and exporting dictionaries does not preserve the Match Whole Words and Case Sensitive settings. This settings are only preserved in the configuration file.

See FTP, SSH, and SCP Access for more information accessing on the configuration directory.

You can also create your own dictionary files and import them onto the appliance . The best way to add non-ASCII characters to dictionaries is to add the terms into the dictionary in a text file off the appliance , move that file onto the appliance , and then import that file as a new dictionary. For more information about importing dictionaries, see Importing Dictionaries, on page 6. For information about exporting dictionaries, see Exporting Dictionaries, on page 7.

Caution These text files contain terms that some persons may consider obscene, indecent or offensive. If you import terms from these files into your content dictionaries, the terms will be displayed when you later view the content dictionaries you have configured on the appliance .

Adding Dictionaries

Procedure

Step 1 Navigate to the **Mail Policies** > **Dictionaries page**.

Step 2 Click **Add Dictionary**.

Step 3 Type a name for the dictionary.

Step 4 (Optional) Configure Advanced Matching.

Note AsyncOS preserves the **Match Whole Words** and **Case Sensitive** settings when you save them in the configuration file. AsyncOS does not preserve these settings when importing and exporting dictionaries.

Step 5 (Optional) Add a smart-identifier to the dictionary.

Smart identifiers are algorithms that search for patterns in data that correspond to common numeric patterns, such as social security numbers and ABA routing numbers. For more information about smart identifiers, see the “Using Message Filters to Enforce Email Policies” chapter.

Step 6 Enter new dictionary entries into the list of terms.

If you have multiple new entries to add, and you want them to be equally likely trigger a filter action, put each new term on its own line.

Note Content dictionary entries with the regular expression: “ .* ” at the beginning or end will cause the system to lock if a match for the “word” MIME part is found. Cisco Systems recommends you do not use “ .* ” at the beginning or end of a content dictionary entry.

Step 7 Specify a weight for the term(s).

You can “weight” a dictionary term so that it is more likely than other terms to trigger a filter action. For more information about how this weight is used to determine filter actions, see “Threshold Scoring for Content Dictionaries” in the “Using Message Filters to Enforce Email Policies” chapter.

Step 8 Click **Add**.

Step 9 Submit and commit your changes.

What to do next

Related Topics

- Dictionary Content, on page 3.

Deleting Dictionaries

Before You Begin

Be aware that AsyncOS marks any message filter that references the deleted dictionary as invalid. AsyncOS leaves any content filter that references the deleted dictionary enabled, but will evaluate them to false.

Procedure

Step 1 Navigate to the **Mail Policies** > **Dictionaries page**.

Step 2 Click the trash can icon next to the dictionary to delete in the dictionary listing.

A confirmation message lists any filters that are currently referencing the dictionary.

Step 3 Click **Delete** in the confirmation message.

Step 4 Commit your changes.

Importing Dictionaries

Before You Begin

Verify that the file to import is present in the configuration directory on the appliance .

Procedure

Step 1 Navigate to the **Mail Policies** > **Dictionaries** page.

Step 2 Click **Import Dictionary**.

Step 3 Select the location to import from.

Step 4 Select the file to import.

Step 5 Select the default weight to use for dictionary terms.

AsyncOS will assign a default weight to any terms with unspecified weights. You can edit the weights after importing the file.

Step 6 Select an encoding.

Step 7 Click **Next**.

Step 8 Name and edit the dictionary.

Step 9 Submit and commit your changes.

Exporting Dictionaries

Procedure

Step 1 Navigate to the **Mail Policies** > Dictionaries page.

Step 2 Click **Export Dictionary**.

Step 3 Select the dictionary to export.

Step 4 Enter a file name for the exported dictionary.

This is the name of the file that will be created in the configuration directory on the appliance .

Step 5 Select the location to export to.

Step 6 Select an encoding for the text file.

Step 7 Submit and commit your changes.

Using and Testing the Content Dictionaries Filter Rules

Dictionaries can be used along with the various dictionary-match() message filter rules and with content filters.

Related Topics

• Dictionary Match Filter Rule, on page 7

Dictionary Match Filter Rule

The message filter rule named `dictionary-match`(< *dictionary_name* >) (and its counterparts) evaluates to true if the message body contains any of the regular expressions in the content dictionary named *dictionary_name* . If that dictionary does not exist, the rule evaluates to false.

Note that the `dictionary-match()` rule functions similarly to the `body-contains()` body scanning rule: it only scans the body and attachments of messages, and not the headers.

For scanning headers, you can use the appropriate *`-dictionary-match()` -type rule (there are rules for specific headers, such as `subject-dictionary-match()` and a more generic rule, `header-dictionary-match()` , in which you can specify any header including custom headers). See “Dictionary Rules” in the “Using Message Filters to Enforce Email Policies” chapter for more information about dictionary matching.

Table 1: Message Filter Rules for Content Dictionaries

Rule	Syntax	Description
Dictionary Match	`dictionary-match (<dictionary_name>)`	Does the message contain a word that matches all the regular expressions listed in the named dictionary?

In the following example, a new message filter using the `dictionary-match()` rule is created to blind carbon copy the administrator when the appliance scans a message that contains any words within the dictionary

named “secret_words” (created in the previous example). Note that because of the settings, only messages that contain the whole word “ `codename` ” matching the case exactly will evaluate to true for this filter.

```
bcc_codenames:

if (dictionary-match ('secret_words'))

{

bcc('administrator@example.com');

}
```

In this example, we send the message to the Policy quarantine:

```
quarantine_codenames:

if (dictionary-match ('secret_words'))

{

quarantine('Policy');


}
```

Related Topics

- Example Dictionary Entries, on page 8
- Testing Content Dictionaries, on page 8

Example Dictionary Entries

Table 2: Example Dictionary Entries

Description	Example
Wildcard	
Anchors	Ends with: foo $ Begins with: ^ foo
Email address(Do not escape the period)	**foo@example.com**, **@example.com** **example.com$** (ends with)**@example.***
Subject	**An email subject**(keep in mind when using the ^ anchor in email subjects that subjects are often prepended with “RE:” or “FW:” and the like)

Testing Content Dictionaries

The `trace` function can provide quick feedback on message filters that use the `dictionary-match()` rule. See Debugging Mail Flow Using Test Messages: Trace for more information. You can also use the `quarantine()` action to test filters, as in the `quarantine_codenames` filter example above.

Understanding Text Resources

Text resources are text templates that can be attached to messages or sent as messages. Text resources can be one of the following types:

- **Message disclaimers —** Text that is added to messages. For more information, see Disclaimer Template, on page 13.
- **Notification templates —** Messages that are sent as notifications, used with the notify() and notify-bcc() actions. For more information, see Notification Templates, on page 18.
- **Anti-virus Notification templates —** Messages that are sent as notifications when a virus is found in a message. You can create a template for a container (which appends the original message), or as a notice that is sent without the appended message. For more information, see Anti-Virus Notification Templates, on page 19.
- **Bounce and Encryption Failure Notification templates —** Messages that are sent as notifications when a message is bounced or message encryption fails. For more information, see Bounce and Encryption Failure Notification Templates, on page 21.
- **Encryption Notification Templates —** Messages that are sent when you configure the appliance to encrypt outgoing email. The message notifies recipients that they have received an encrypted message and provides instructions for reading it. For more information, see Encryption Notification Templates, on page 22.

You can use the CLI (**`textconfig`**) or the GUI to manage text resources, including: adding, deleting, editing, importing, and exporting. For information on managing text resources using the GUI, see Overview of Text Resource Management, on page 10.

Text resources can contain non-ASCII characters.

Note Text resources containing non-ASCII characters may or may not display properly in the CLI on your terminal. To view and change text resources that contain non-ASCII characters, export the text resource to a text file, edit that text file, and then import the new file back into the appliance . For more information, see Importing and Exporting Dictionaries as Text Files, on page 4.

Related Topics

- Importing and Exporting Dictionaries as Text Files, on page 4

Importing and Exporting Text Resources as Text Files

You must have access to the configuration directory on the appliance . Imported text files must be present in the configuration directory on the appliance . Exported text files are placed in the configuration directory.

See FTP, SSH, and SCP Access for more information on accessing the configuration directory.

To add non-ASCII characters to text resources, add the terms into the text resource in a text file off the appliance , move that file onto the appliance , and then import that file as a new text resource. For more information about importing text resources, see Importing Text Resources, on page 11. For information about exporting text resources, see Exporting Text Resources, on page 11.

Overview of Text Resource Management

You can manage text resources using either the GUI or the CLI. This section focuses on the GUI.

Manage text resources from the CLI using the **`textconfig`** command.

Text resource management includes these tasks:

- Adding
- Editing and deleting
- Exporting, and importing
- Defining plain text messages for all text resource types
- Defining HTML-based messages for some text resource types

Related topics

- Adding Text Resources, on page 10
- Deleting Text Resources, on page 10
- Exporting Text Resources, on page 11
- Importing Text Resources, on page 11
- Overview of HTML-Based Text Resources, on page 12.

Adding Text Resources

Procedure

Step 1 Navigate to **Mail Policies** > **Text Resources**

Step 2 Click **Add Text Resource**.

Step 3 Enter a name for the text resource in the **Name** field.

Step 4 Select the type of text resource from the **Type** field.

Step 5 Enter the message text in either the **Text** or the **HTML and Plain Text** field.

If the text resource allows only plain text messages, use the **Text** field. If the text resource allows both HTML and plain text messages, use the **HTML and Plain Text** fields.

Step 6 Submit and commit your changes.

What to do next

Related topics

- Overview of HTML-Based Text Resources, on page 12.

Deleting Text Resources

Before you begin

Note the impact of deleting text resources:

- Any message filters that reference the deleted text resource are marked as invalid.
- Any content filters that reference the deleted text resource are left enabled, but will evaluate to false.

Procedure

Step 1 On the **Mail Policies** > **Text Resources** page, click the trash can icon under the Delete column for the text resource you want to delete. A confirmation message is displayed.

Step 2 Click **Delete** to delete the text resource.

Note You cannot delete a text resource that is referenced in any of the content or message filter configurations.

Step 3 Commit your changes.

Importing Text Resources

Before you begin

Ensure that the file to import is in the configuration directory on the appliance .

Procedure

Step 1 On the **Mail Policies** > **Text Resources** page, click **Import Text Resource**.

Step 2 Select a file to import.

Step 3 Specify an encoding.

Step 4 Click **Next**.

Step 5 Choose a name, edit, and select the text resource type.

Step 6 Submit and commit your changes.

Exporting Text Resources

Before you begin

Be aware that when you export a text resource, a text file is created in the configuration directory on the appliance .

Procedure

Step 1 On the **Mail Policies** > **Text Resources** page, click **Export Text Resource**.

Step 2 Select a text resource to export.

Step 3 Enter a file name for the text resource.

Step 4 Select an encoding for the text file.

Step 5 Click **Submit** to create the text file containing the text resource in the configuration directory.

Overview of HTML-Based Text Resources

You can create some text resources with both HTML-based and plain text messages, such as Disclaimers. When a text resource containing both HTML-based and plain text messages is applied to an email message, the HTML-based text resource message is applied to the text/html part of the email message, and the plain text message is applied to the text/plain part of the email message.

When you add or edit an HTML-based text resource, the GUI includes a rich text edit that allows you to enter rich text without having to manually write HTML code.

Consider the following information when adding and editing an HTML-based text resource:

- You can choose to have the plain text version of the message to be automatically generated based on the HTML version, or you can define the plain text version independently.
- You can switch between the rich text editor and HTML code by clicking the **Code View** button.
- To enter HTML code that is not supported in the rich text editor in the GUI, switch to code view and manually enter HTML code. For example, you might want to do this to insert a reference to an image file located on an external server using the **<img src>** HTML tag.

Related Topics

- Importing and Exporting HTML-Based Text Resources, on page 12

Importing and Exporting HTML-Based Text Resources

You can export to and import from a text file HTML-based text resources. When you export an HTML-based text resource to a file, the file contains the following sections for each version of the text resource:

- `[html_version]`
- `[text_version]`

The order of these sections does not matter.

For example, an exported file might contain the following text:

```
[html_version]
 <p>Sample <i>message.</i></p>
 [text_version]
 Sample message.
```

Consider the following rules and guidelines when exporting and importing HTML-based text resources:

- When you export an HTML-based text resource whose plain text message is automatically generated from the HTML version, the exported file does not contain the `[text_version]` section.
- When you import from a text file, any HTML code under the [html_version] section is converted to the HTML message in the created text resource if the text resource type supports HTML messages. Similarly, any text under the `[text_version]` section is converted to the plain text message in the created text resource.

- When you import from a file that contains an empty or nonexistent `[html_version]` section to create a HTML-based text resource, the appliance creates both an HTML and plain text message using the text in the `[text_version]` section.

Using Text Resources

All types of text resources are created in the same way, using the Text Resources page or the textconfig CLI command. Once created, each type is used in a different way. Disclaimers and notification templates are used with filters and listeners, while anti-virus notification templates are used with mail policies and anti-virus settings.

Related Topics

- Disclaimer Template, on page 13
- Disclaimer Stamping and Multiple Encodings, on page 16
- Notification Templates, on page 18
- Anti-Virus Notification Templates, on page 19
- Bounce and Encryption Failure Notification Templates, on page 21
- Encryption Notification Templates, on page 22

Disclaimer Template

The appliance can add a default disclaimer above or below the text (heading or footer) for some or all messages received by a listener. You can add disclaimers to messages on the appliance using the following methods:

- Via a listener, using the GUI or the `listenerconfig` command (see Adding Disclaimer Text via a Listener, on page 14).
- Using the content filter action, `Add Disclaimer Text` (see Content Filter Actions).
- Using the message filter action, `add-footer()` (see the "Using Message Filters to Enforce Email Policies" chapter).
- Using a data loss prevention profile (see Data Loss Prevention).
- Using message modification for Outbreak Filters to alert the user that the message may be an attempt at phishing or malware distribution (see Modifying Messages). Disclaimers added for this type of notification are added above the text.

For example, you can append a copyright statement, promotional message, or disclaimer to every message sent from within your enterprise.

Prior to using disclaimer text you have to create the disclaimer template. Use the Text Resources page in the GUI (see Adding Text Resources, on page 10) or the `textconfig` command (see the CLI Reference Guide for AsyncOS for Cisco Email Security Appliances) to create and manage a set of text strings to be used.

Related Topics

- Adding Disclaimers via Filters, on page 14
- Adding Disclaimer Text via a Listener, on page 14
- Disclaimers and Filter Action Variables, on page 14

Adding Disclaimer Text via a Listener

Once you have disclaimer text resources created, select which text strings will be appended to messages received by the listener. You can add disclaimer text above or below a message. This feature is available on both public (inbound) and private (outbound) listeners.

If you send a message that consists of text and HTML (Microsoft Outlook calls this type of message a "multipart alternative"), the appliance will stamp the disclaimer on both parts of the message. However, if your message has signed content, the content will not be modified because the modification will invalidate the signature. Instead, a new part is created with a disclaimer stamp that says " Content-Disposition inline attachment ." For more information on multipart messages, see "Message Bodies vs. Message Attachments" in the "Using Message Filters to Enforce Email Policies" chapter.

Adding Disclaimers via Filters

You can also append specific, predefined text strings to the disclaimers of messages using the filter action `add-footer()` or the content filter action "Add Disclaimer Text." For example, the following message filter rule appends the text string named `legal.disclaimer` to all messages sent from users in the LDAP group "Legal:"

```
Add-Disclaimer-For-Legal-Team:

if (mail-from-group == 'Legal')

{

add-footer('legal.disclaimer');

}
```

Disclaimers and Filter Action Variables

You can also use message filter action variables (see "Action Variables" in the "Using Message Filters to Enforce Email Policies" chapter for more information).

The following variables are available for the Disclaimer Template:

Table 3: Anti-Virus Notification Variables

Variable	Substituted With
$To	Replaced by the message To: header (not the Envelope Recipient).
$From	Replaced by the message From: header (not the Envelope Sender).
$Subject	Replaced by the subject of the original message.
$Date	Replaced by the current date, using the format MM/DD/YYYY.
$Time	Replaced by the current time, in the local time zone.
$GMTimestamp	Replaced by the current time and date, as would be found in the Received: line of an email message, using GMT.
$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).

Variable	Substituted With
$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.
$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.
$Reputation	Replaced by the IP Reputation score of the sender. If there is no reputation score, it is replaced with "None".
$filenames	Replaced with a comma-separated list of the message's attachments' filenames.
$filetypes	Replaced with a comma-separated list of the message's attachments' file types.
$filesizes	Replaced with a comma-separated list of the message's attachment's file sizes.
$remotehost	Replaced by the hostname of the system that sent the message to the appliance .
$AllHeaders	Replaced by the message headers.
$EnvelopeFrom	Replaced by the Envelope Sender (Envelope From, <MAIL FROM>) of the message.
$Hostname	Replaced by the hostname of the appliance .
$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.
$enveloperecipients	Replaced by all Envelope Recipients (Envelope To, <RCPT TO>) of the message.
$bodysize	Replaced by the size, in bytes, of the message.
$FilterName	Returns the name of the filter being processed.
$MatchedContent	Returns the content that triggered a scanning filter rule (including filter rules such as body-contains and content dictionaries).
$DLPPolicy	Replaced by the name of the email DLP policy violated.
$DLPSeverity	Replaced by the severity of violation. Can be "Low," "Medium," "High," or "Critical."
$DLPRiskFactor	Replaced by the risk factor of the message's sensitive material (score 0 - 100).
$threat_category	Replaced with the type of Outbreak Filters threat, such as phishing, virus, scam, or malware.
$threat_type	Replaced by a subcategory of the Outbreak Filters threat category. For example, can be a charity scam, a financial phishing attempt, a fake deal, etc.
$threat_description	Replaced by a description of the Outbreak Filters threat.
$threat_level	Replaced by the message's threat level (score 0 - 5).

Variable	Substituted With
$threat_verdict	Replaced by Yes or No, depending on the Message Modification Threat Level threshold. If the viral or non-viral threat level of a message is greater than or equal to the message modification threat level threshold, the value of this variable is set to Yes.

To use message filter action variables in disclaimers, create a message disclaimer (via the Text Resource page in the GUI or the **textconfig** command), and reference the variable:

The add-footer() action supports non-ASCII text by adding the footer as an inline, UTF-8 coded, quoted printable attachment.

Disclaimer Stamping and Multiple Encodings

AsyncOS includes a setting used to modify the way disclaimer stamping with different character encodings works. By default, AsyncOS attempts to place the disclaimers it attaches within the body part of an email message. You can use a setting configured within the `localeconfig` command to configure the behavior if the encodings of the body part and the disclaimer are different. To understand this setting, it is helpful to view an email message as consisting of several parts:

To: joe@example.com From: mary@example.com Subject: Hi!	Headers
<blank line>	
Hello!	Body part
This message has been scanned...	First attachment part
Example.zip	Second attachment part

The message body after the first blank line may contain many MIME parts. The second and following parts are often called “attachments,” while the first is often called the “body” or “text.”

A disclaimer can be included in an email as either an attachment (above) or as part of the body

To: joe@example.com From: mary@example.com Subject: Hi!	Headers
<blank line>	
Hello!	Body part
This message has been scanned...	Disclaimer now included in body part

Example.zip	First attachment part

Typically, when there is an encoding mismatch between the message body and a disclaimer, AsyncOS attempts to encode the entire message in the same encoding as the message body so that the disclaimer will be included in the body ("inline") and not included as a separate attachment. In other words, the disclaimer will be included inline if the encoding of the disclaimer matches that of the body, or if the text in the disclaimer contains characters that can be displayed inline (in the body). For example, it is possible to have a ISO-8859-1 encoded disclaimer that only contains US-ASCII characters; consequently, this will display "inline" without problems.

However, if the disclaimer cannot be combined with the body, you can use the `localeconfig` command to configure AsyncOS to attempt to promote, or convert, the body text to match the encoding of the disclaimer so that the disclaimer can be included in the body of the message:

```
example.com> localeconfig

Behavior when modifying headers: Use encoding of message body
Behavior for untagged non-ASCII headers: Impose encoding of message body
Behavior for mismatched footer or heading encoding: Try both body and footer or heading
encodings
Behavior when decoding errors found: Disclaimer is displayed as inline content and the
message body is added as an attachment.

Choose the operation you want to perform:
- SETUP - Configure multi-lingual settings.
[]> setup

If a header is modified, encode the new header in the same encoding as the message body?
(Some MUAs incorrectly handle headers encoded in a different encoding than the body.
However, encoding a modified header in the same encoding as the message body may cause
certain
characters in the modified header to be lost.) [Y]>

If a non-ASCII header is not properly tagged with a character set and is being used or
modified,
impose the encoding of the body on the header during processing and final representation
of the message?
(Many MUAs create non-RFC-compliant headers that are then handled in an undefined way.
Some MUAs handle headers encoded in character sets that differ from that of the main body
in an incorrect way.
Imposing the encoding of the body on the header may encode the header more precisely.
This will be used to interpret the content of headers for processing, it will not modify
or rewrite the
header unless that is done explicitly as part of the processing.) [Y]>

Disclaimers (as either footers or headings) are added in-line with the message body whenever
 possible.
However, if the disclaimer is encoded differently than the message body, and if imposing a
 single encoding
will cause loss of characters, it will be added as an attachment. The system will always
try to use the
message body's encoding for the disclaimer. If that fails, the system can try to edit the
message body to
use an encoding that is compatible with the message body as well as the disclaimer. Should
 the system try to
re-encode the message body in such a case? [Y]>

If the disclaimer that is added to the footer or header of the message generates an error
when decoding the message body,
it is added at the top of the message body. This prevents you to rewrite a new message
content that must merge with
the original message content and the header/footer-stamp. The disclaimer is now added as
```

```
an additional MIME part
that displays only the header disclaimer as an inline content, and the rest of the message
 content is split into
separate email attachments. Should the system try to ignore such errors when decoding the
message body? [N]>

Behavior when modifying headers: Use encoding of message body
Behavior for untagged non-ASCII headers: Impose encoding of message body
Behavior for mismatched footer or heading encoding: Try both body and footer or heading
encodings
Behavior when decoding errors found: Disclaimer is displayed as inline content and the
message body
is added as an attachment.

Choose the operation you want to perform:
- SETUP - Configure multi-lingual settings.
[]>
```

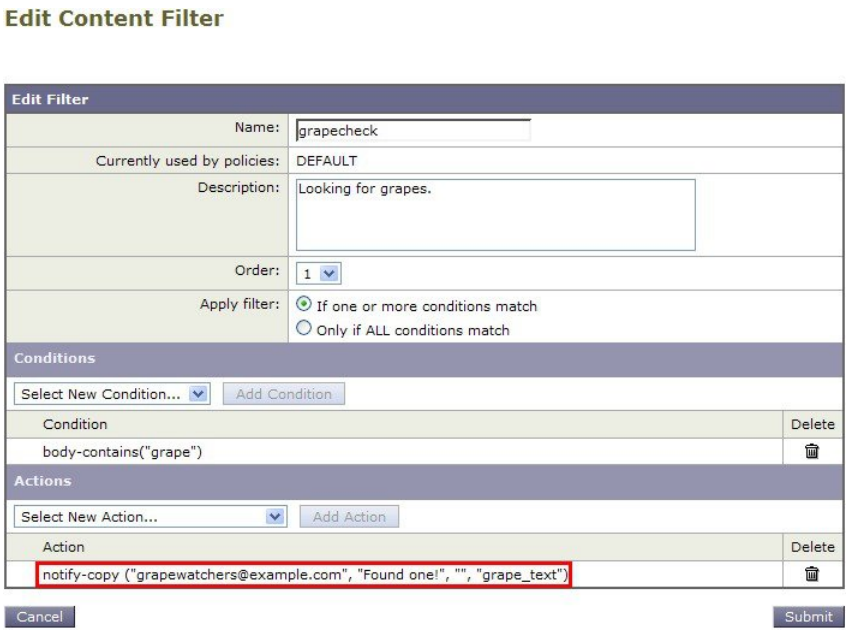
For more information about the `localeconfig` command, see the "Configuring the Appliance to Receive Mail" chapter.

Notification Templates

Notification templates are used with the **`notify()`** and **`notify-copy()`** filter actions. Notification templates may contain non-ascii text and action variables (see "Action Variables" in the "Using Message Filters to Enforce Email Policies" chapter), including the anti-virus-related variables used by anti-virus notifications. For example, you could use the **`$Allheaders`** action variable to include the headers from the original message. You can configure the From: address for notifications, see Configuring the Return Address for Appliance Generated Messages.

Once you have created a notification template, you can refer to it in content and message filters. The following figure shows a content filter where the **`notify-copy()`** filter action is set to send the "grape_text" notification to "grapewatchers@example.com:"

Figure 1: Notify Example in a Content Filter



Anti-Virus Notification Templates

There are two types of anti-virus notification templates:

- **anti-virus notification template**. The anti-virus notification template is used when the original message is not attached to the virus notification.
- **anti-virus container template**. The container template is used when the original message is sent as an attachment.

Anti-virus notification templates are used in basically the same way as notification templates except that they are used with the anti-virus engine instead of filters. You can specify a custom notification to send while editing a mail policy. You can configure the From: address for anti-virus notifications. For information, see Configuring the Return Address for Appliance Generated Messages.

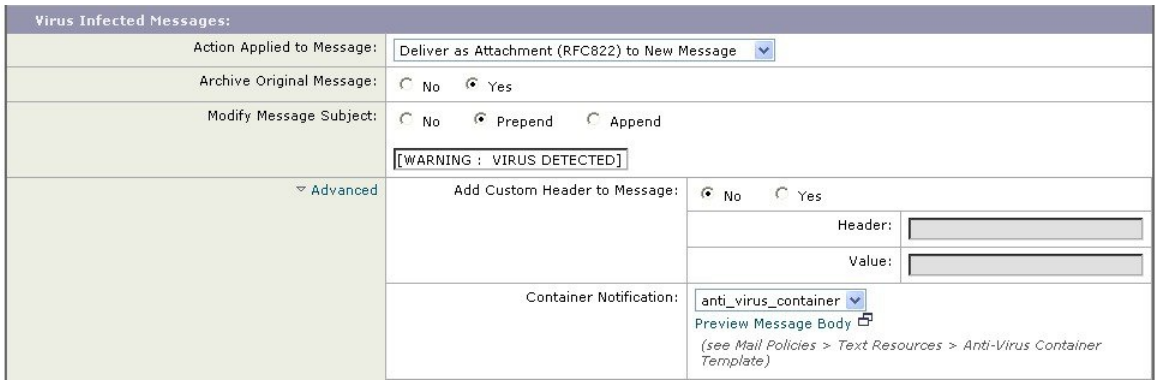
Related Topics

- Custom Anti-Virus Notification Templates, on page 19

Custom Anti-Virus Notification Templates

The following figure shows a mail policy where a custom anti-virus notification is specified.

Figure 2: Anti-Virus Container Template Notification Example in a Mail Policy



Related Topics

- Anti-Virus Notification Variables, on page 19

Anti-Virus Notification Variables

When creating an anti-virus notification, you can use any of the notification variables listed in the following table:

Table 4: Anti-Virus Notification Variables

Variable	Substituted With
$To	Replaced by the message To: header (not the Envelope Recipient).
$From	Replaced by the message From: header (not the Envelope Sender).
$Subject	Replaced by the subject of the original message.

Variable	Substituted With
$AV_VIRUSES	Replaced by the list of all the viruses found anywhere in the message: “Unix/Apache.Trojan”, “W32/Bagel-F”
$AV_VIRUS_TABLE	Replaced by the table of MIME-Part/Attachment names and viruses in each part: “HELLO.SCR” : “W32/Bagel-F” <unnamed part of the message> : “Unix/Apache.Trojan”
$AV_VERDICT	Replaced by the anti-virus verdict.
$AV_DROPPED_TABLE	Replaced by the table of attachments that were dropped. Each row is composed of a part or filename followed by the list of viruses associated with that part: “HELLO.SCR” : “W32/Bagel-f”, “W32/Bagel-d” “Love.SCR” : “Netsky-c”, “W32/Bagel-d”
$AV_REPAIRED_VIRUSES	Replaced by the list of all the viruses found and repaired.
$AV_REPAIRED_TABLE	Replaced by the table of all parts and viruses found and repaired: “HELLO.SCR” : “W32/Bagel-F”
$AV_DROPPED_PARTS	Replaced by the list of filenames that were dropped: “HELLO.SCR”, “CheckThisOut.exe”
$AV_REPAIRED_PARTS	Replaced by the list of filenames or parts that were repaired.
$AV_ENCRYPTED_PARTS	Replaced by the list of filenames or parts that were encrypted.
$AV_INFECTED_PARTS	Replaced by a comma-separated list of filenames for the files that contained a virus.
$AV_UNSCANNABLE_PARTS	Replaced by the list of filenames or parts that were unscannable.
$Date	Replaced by the current date, using the format MM/DD/YYYY.
$Time	Replaced by the current time, in the local time zone.
$GMTimestamp	Replaced by the current time and date, as would be found in the Received: line of an email message, using GMT.
$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).
$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.
$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	Substituted With
$Reputation	Replaced by the IP Reputation score of the sender. If there is no reputation score, it is replaced with “None”.
$filenames	Replaced with a comma-separated list of the message’s attachments’ filenames.
$filetypes	Replaced with a comma-separated list of the message's attachments' file types.
$filesizes	Replaced with a comma-separated list of the message’s attachment’s file sizes.
$remotehost	Replaced by the hostname of the system that sent the message to the appliance .
$AllHeaders	Replaced by the message headers.
$EnvelopeFrom	Replaced by the Envelope Sender (Envelope From, <MAIL FROM>) of the message.
$Hostname	Replaced by the hostname of the appliance .

Note Variable names are not case-sensitive. For example, specifying “$to” is equivalent to specifying “$To” in the text resource. If an “AV_” variable is empty in the original message, the string <None> is substituted.

After the text resource has been defined, use the **Mail Policies** > **Incoming/Outgoing Mail Policies** > **Edit Anti-Virus Settings** page or the **`policyconfig -> edit -> antivirus`** command to specify that the original message is to be included as an RFC 822 attachment for Repaired, Unscannable, Encrypted, or Virus Positive messages. See Send Custom Alert Notification for more information.

Bounce and Encryption Failure Notification Templates

Bounce and encryption failure notification templates are used in basically the same way as notification templates except that they are used with bounce notifications and message encryption failure notifications. You can specify a custom bounce notification to send while editing a bounce profile and a custom message encryption failure notification while editing an encryption profile.

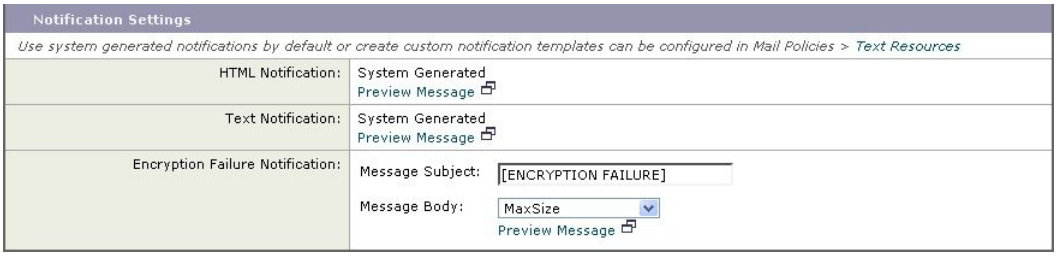
The following figure shows a bounce notification template specified in a bounce profile.

Figure 3: Bounce Notification Example in a Bounce Profile

Note You must use RFC-1891 DSNs to use custom templates.

The following figure shows an encryption failure template specified in an encryption profile.

Figure 4: Encryption Failure Notification Example in an Encryption Profile



Related Topics

- Bounce and Encryption Failure Notification Variables, on page 22

Bounce and Encryption Failure Notification Variables

When creating a bounce or encryption failure notification, you can use any of the notification variables listed in the following table:

Table 5: Bounce Notification Variables

Variable	Substituted With
$Subject	The subject of the original message.
$Date	Replaced by the current date, using the format MM/DD/YYYY.
$Time	Replaced by the current time, in the local time zone.
$GMTimeStamp	Replaced by the current time and date, as would be found in the Received: line of an email message, using GMT.
$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).
$BouncedRecipient	Bounced recipient address
$BounceReason	Reason for this notification
$remotehost	Replaced by the hostname of the system that sent the message to the appliance .

Encryption Notification Templates

Encryption notification templates are used when you configure Cisco Email Encryption to encrypt outbound email. The notification informs recipients that they have received an encrypted message and provides

instructions for reading it. You can specify a custom encryption notification to send with encrypted messages. You specify both an HTML and a text encryption notification when you create an encryption profile. Therefore, if you want to create a custom profile, you should create both text and HTML notifications.