Data Loss Prevention

This chapter contains the following sections:

Overview of Data Loss Prevention

The Data Loss Prevention (DLP) feature secures your organization's proprietary information and intellectual property and enforces compliance with government regulations by preventing users from maliciously or unintentionally emailing sensitive data from your network. You define the types of data that your employees are not allowed to email by creating DLP policies that are used to scan outgoing messages for any data that may violate laws or corporate policies.

Overview of the DLP Scanning Process

	Action	More Information
1.	A user in your organization sends an email message to a recipient outside of your organization.	The Email Security appliance is a “gateway” appliance that processes messages that are entering or leaving your network. Messages sent to other users within your network are not scanned.
2.	The Email Security appliance processes the message through the stages of its email “work queue” before it reaches the DLP scanning stage.	Pre-DLP-scanning processes ensure, for example, that the message includes no spam or malware. To see where DLP processing occurs in the workqueue, see the workqueue flow diagram in Email Pipeline Flows.
3.	The appliance scans the message body, header, and attachments for sensitive content that you have identified in DLP Policies.	See How Data Loss Prevention Works , on page 2.
4.	If sensitive content is found, the appliance takes action to protect the data, such as quarantining the message, dropping it, or delivering it with restrictions. Otherwise, the message continues through the appliance's work queue and if no issues are found, the Email Security appliance delivers it to the recipient.	You define the actions to be taken. See Message Actions, on page 20.

How Data Loss Prevention Works

When someone in your organization sends a message to a recipient outside your organization, the appliance determines which outgoing mail policy applies to the sender or recipient of that message, based on rules that you defined. The appliance evaluates the content of the message using the DLP policies that are specified in that outgoing mail policy.

Specifically, the appliance scans the message content (including headers and attachments) for text that matches words, phrases, predefined patterns such as social security numbers, or a regular expression that you identified as sensitive content in an applicable DLP policy.

The appliance also evaluates the context of disallowed content in order to minimize false positive matches. For example, a number matching a credit card number pattern is only a violation if it is accompanied by an expiration date, credit card company name (Visa, AMEX, etc.), or a person's name and address.

If message content matches more than one DLP policy, the first matching DLP policy in the list applies, based on the order that you specified. If an outgoing mail policy has multiple DLP policies that use the same criteria to determine whether content is a violation, all policies use the result from a single content scan.

When potentially sensitive content appears in a message, the appliance assigns a risk factor score between 0 - 100 to the potential violation. This score indicates the likelihood that the message contains a DLP violation.

The appliance then assigns the severity level (such as Critical or Low) that you have defined for that risk factor score, and performs the message action that you have specified for that severity level in the applicable DLP Policy.

System Requirements for Data Loss Prevention

Data Loss Prevention is supported on all supported C-Series and X-Series appliances except appliances using D-Mode licenses.

How to Set Up Data Loss Prevention

Perform these steps in order:

DETAILED STEPS

	Command or Action	Purpose
Step 1	Enable the DLP feature.	Enabling Data Loss Prevention (DLP) , on page 4
Step 2	Define the possible actions that can be taken for messages in which violations are found or suspected. For example, you can quarantine such messages.	Message Actions, on page 20
Step 3	Create DLP policies, which: • identify the content that must not be emailed from your organization, and • specify which actions will be taken for each violation.	Choose a method: • Setting Up DLP Prevention Using a Wizard , on page 5 • Creating a DLP Policy Using a Predefined Template , on page 6 • Creating a Custom DLP Policy (Advanced) , on page 7
Step 4	Set the order of the DLP policies to determine which DLP policy is used to evaluate messages for DLP violations when the content could match more than one DLP policy.	Arranging the Order of the Email DLP Policies for Violation Matching , on page 18
Step 5	Ensure that you have created Outgoing Mail Policies for each group of senders and recipients whose messages will be scanned for DLP violations.	See Mail Policies To further refine permitted and restricted message senders and recipients in individual DLP policies, see Filtering Messages for DLP Policies, on page 17.
Step 6	Specify which DLP policies apply to which senders and recipients by assigning DLP policies to Outgoing Mail Policies.	Associating DLP Policies with Outgoing Mail Policies, on page 19
Step 7	Configure settings for storage of and access to sensitive DLP information.	• Displaying Sensitive DLP Data in Message Tracking , on page 25

	Command or Action	Purpose
		• Controlling Access to Sensitive Information in Message Tracking

Enabling Data Loss Prevention (DLP)

Step 1 Select **Security Services > Data Loss Prevention**.

Step 2 Click **Enable**.

Step 3 Scroll to the bottom of the license agreement page and click **Accept** to accept the agreement.

Note If you do not accept the license agreement, DLP is not enabled on the appliance.

Step 4 Under **Data Loss Prevention Global Settings**, select **Enable Data Loss Prevention**.

Step 5 (Recommended) For now, deselect the other options on this page.
You can change these settings later, following instructions discussed elsewhere in this chapter.

Step 6 Submit and commit your changes.

What to Do Next

See How to Set Up Data Loss Prevention , on page 3.

Policies for Data Loss Prevention

DLP Policy Description

A DLP policy includes:

- a set of conditions that determine whether an outgoing message contains sensitive data, and
- the actions to be taken when a message contains such data.

You specify how message content is evaluated, based on:

- Specific disallowed content or patterns of information. Depending on the policy, you may need to create a regular expression to search for identification numbers. See About Defining Disallowed Content Using Content Matching Classifiers , on page 8.
- A list of specific senders and recipients for filtering messages. See Filtering Messages for DLP Policies, on page 17.

- A list of attachment file types for filtering messages. See Filtering Messages for DLP Policies, on page 17.
- Settings that allow different actions to occur based on the severity of the violation. See About Assessing Violation Severity , on page 18.

You determine the message senders and recipients that each policy applies to when you enable DLP policies in Outgoing Mail Policies.

Predefined DLP Policy Templates

To simplify creation of DLP policies, your appliance includes a large collection of predefined policy templates.

Template categories include:

- **Regulatory Compliance.** These templates identify messages and attachments that contain personally identifiable information, credit information, or other protected or non-public information.
- **Acceptable Use.** These templates identify messages sent to competitors or restricted recipients that contain sensitive information about an organization.
- **Privacy Protection.** These templates identify messages and attachments that contain identification numbers for financial accounts, tax records, or national IDs.
- **Intellectual Property Protection.** These templates identify popular publishing and design document file types that may contain intellectual property that an organization would want to protect.
- **Company Confidential.** These templates identify documents and messages that contain information about corporate accounting information and upcoming mergers and acquisitions.
- **Custom Policy.** This “template” lets you create your own policy from scratch using either pre-defined content matching classifiers or violation identification criteria specified by your organization. This option is considered advanced and should be used only in the rare cases when the predefined policy templates do not meet the unique requirements of your network environment.

Some of these templates require customization.

Setting Up DLP Prevention Using a Wizard

The DLP Assessment Wizard helps you configure commonly-used DLP policies and enable them in the appliance’s default outgoing mail policy.

Note By default, DLP policies added using the DLP Assessment Wizard deliver all messages, regardless of the severity of detected DLP violations. You will need to edit the policies created using the wizard.

Before You Begin

- Remove any existing DLP policies from the appliance. You can only use the DLP Assessment Wizard if there are no existing DLP policies on the appliance.
- If you need to detect messages that include student identification numbers or account numbers other than credit card numbers, US Social Security numbers, and US Drivers License numbers, create a regular

expression that identifies those numbers. For more information, see Regular Expressions for Identifying Identification Numbers , on page 12.

Step 1 Choose **Security Services > Data Loss Prevention**.

Step 2 Click **Edit Settings**.

Step 3 Select the **Enable and configure DLP using the DLP Assessment Wizard** check box.

Step 4 Click **Submit**.

Step 5 Complete the wizard.
Keep the following in mind:

- Any business that operates in California and owns or licenses computerized personally identifying information (PII) data for California residents, regardless of their physical location, is required to comply with **US State Regulations (California SB-1386)**. This law is one of the policy choices in the wizard.
- If you do not enter an email address to receive automatically-generated scheduled DLP Incident Summary report, the report will not be generated.
- When you review your configured settings, if you return to a step to make a change, you must proceed through the remaining steps until you reach the review page again. All settings that you previously entered will be remembered.
- When you complete the wizard, the Outgoing Mail Policies page displays, with your DLP policies enabled in the default outgoing mail policy. A summary of your DLP policy configuration is displayed at the top of the page.

Step 6 Commit your changes.

What to Do Next

- (Optional) To edit these DLP policies, create additional policies, change the overall action on messages, or change the severity level settings, choose **Mail Policies > DLP Policy Manager**. For information, see Creating a DLP Policy Using a Predefined Template , on page 6, Creating a Custom DLP Policy (Advanced) , on page 7, and Adjusting the Severity Scale , on page 18.
- (Optional) To enable existing DLP policies for other outgoing mail policies, see Using Outgoing Mail Policies to Assign DLP Policies to Senders and Recipients , on page 19.

Creating a DLP Policy Using a Predefined Template

Step 1 Select **Mail Policies > DLP Policy Manager**.

Step 2 Click **Add DLP Policy**.

Step 3 Click the name of a category to display a list of the available DLP policy templates.
Note To view descriptions of each template, click **Display Policy Descriptions**.

Step 4 Click **Add** for the DLP policy template that you want to use.

Step 5 (Optional) Change the predefined name and description of the template.

Step 6 If the policy requires or recommends customizing one or more content matching classifiers, enter a regular expression to define the pattern of your organization's identification numbering system and a list of words or phrases related to the identification numbers that identify them as such or are typically associated with them.
For information, see:

About Defining Disallowed Content Using Content Matching Classifiers , on page 8and Regular Expressions for Identifying Identification Numbers , on page 12.

Note You cannot add or remove content matching classifiers for policies based on a predefined template.

Step 7 (Optional) Apply the DLP policy only to messages with specific recipients, senders, attachment types, or previously-added message tags.
For more information, see Filtering Messages for DLP Policies, on page 17.

You can separate multiple entries using a line break or a comma.

Step 8 In the Severity Settings section:

- Choose an action to take for each level of violation severity.For more information, see About Assessing Violation Severity , on page 18.
- (Optional) Click **Edit Scale** to adjust the violation severity scale for the policy. For more information, see Adjusting the Severity Scale , on page 18.

Step 9 Submit and commit your changes.

Creating a Custom DLP Policy (Advanced)

Note Creating custom policies is very complex; create custom policies only if the predefined DLP policy templates do not meet the needs of your organization.

You can create a custom DLP policy from scratch using the Custom Policy template and add either a predefined content matching classifier or a custom classifier to the policy.

Custom policies can return a DLP violation if the content matches a single classifier or all classifiers, depending on how the policy is defined.

Before You Begin

Suggested: Define the criteria that identify a content violation. See Creating a Content Matching Classifier for Custom DLP Policies , on page 11. You can also define these criteria from within this procedure.

Step 1 Select **Mail Policies > DLP Policy Manager**.

Step 2 Click **Add DLP Policy**.

Step 3 Click **Custom Policy**.

Step 4 Click **Add** for the Custom Policy template.

Step 5 Enter a name and description for the policy.

Step 6 Identify the content and context that constitute a DLP violation:

a) Select a content matching classifier.

b) Click **Add**.

- If you selected **Create a Classifier**, see Creating a Content Matching Classifier for Custom DLP Policies , on page 11 .
- Otherwise, the selected classifier is added to the table.

c) (Optional) Add additional classifiers to the policy.
For example, you might be able to eliminate known likely false positive matches by adding another classifier and selecting NOT.

d) If you added multiple classifiers: Choose an option in the table heading to specify whether **any** or **all** of the classifiers must match in order to count the instance as a violation.

Step 7 (Optional) Apply the DLP policy only to messages with specific recipients, senders, attachment types, or previously-added message tags.
For more information, see Filtering Messages for DLP Policies, on page 17.

You can separate multiple entries using a line break or a comma.

Step 8 In the Severity Settings section:

- Choose an action to take for each level of violation severity. For more information, see About Assessing Violation Severity , on page 18.
- (Optional) Click **Edit Scale** to adjust the violation severity scale for the policy. For more information, see Adjusting the Severity Scale , on page 18

Step 9 Submit and commit your changes.

About Defining Disallowed Content Using Content Matching Classifiers

Content matching classifiers define the content that cannot be emailed and optionally the context in which that content must occur in order to be considered a data loss prevention violation.

Suppose you want to prevent patient identification numbers from being emailed from your organization.

In order for the appliance to recognize these numbers, you must specify the patterns of the record numbering system used by your organization, using one or more regular expressions. You can also add a list of words

and phrases that might accompany the record number as supporting information. If the classifier detects the number pattern in an outgoing message, it searches for the supporting information to verify that the pattern is an identification number and not a random number string. Including context matching information results in fewer false positive matches.

For this example, you might create a DLP policy that uses the HIPAA and HITECH template. This template includes the Patient Identification Numbers content matching classifier, which you can customize to detect a patient's identification number. To detect numbers in the pattern of 123-CL456789, you would enter the regular expression [0-9]{3}\-[A-Z]{2}[0-9]{6} for the classifier. Enter "Patient ID" for a related phrase. Finish creating the policy and enable it in an outgoing mail policy. Submit and commit your changes. Now, if the policy detects the number pattern in an outgoing message with the phrase "Patient ID" in close proximity to the number pattern, the DLP policy returns a DLP violation.

About Using Content Matching Classifiers in DLP Policies

Many of the predefined DLP policy templates include content matching classifiers from RSA. Some of these classifiers require customization in order to identify the patterns that are used for data in your organization.

If you create a custom DLP policy you can choose a predefined classifier or create one of your own.

Content Matching Classifier Examples

The following examples show how classifiers match message content:

Credit Card Number

Several DLP policy templates include the Credit Card Number classifier. The credit card number itself is subject to various constraints, such as the pattern of digits and punctuation, the issuer-specific prefix, and the final check digit. The classifier requires additional supporting information to make a match, such as an expiration date, or the name of the card issuer. This reduces the number of false positives.

Examples:

- `378734493671000` (No match because of no supporting information)
- `378734493671000 VISA` (Match)
- `378734493671000 exp: 12/2019` (Match)

US Social Security Number

The US Social Security Number classifier requires a properly formatted number as well as supporting data, such as a date of birth, name, or the string SSN .

Examples:

- `321-02-3456` (No match because of no supporting information)
- `SN: 281234123458` (Match)

ABA Routing Numbers

The ABA Routing Number classifier is similar to the Credit Card Number classifier.

Examples:

- `119999992` (No match because of no supporting information)
- `ABA No.800000080` (Match)

Driver License Numbers (US)

Many policies use a US Drivers License classifier. By default, this classifier searches for drivers licenses issued in the US. US state-specific policies such as California AB-1298 and Montana HB-732 search for their respective state US drivers' licenses only.

The individual state classifiers match against the patterns for that state, and require the corresponding state name or abbreviation, and additional supporting data.

Examples:

- `CA DL: C3452362` (Match because it has the correct pattern for the number and supporting data)
- `California DL: C3452362` (Match)
- `DL: C3452362` (No match because there is not enough supporting data)
- `California C3452362` (No match because there is not enough supporting data)
- `OR DL: C3452362` (Match)
- `OR DL: 3452362` (Match because it is the correct pattern for Oregon)
- `WV DL: D654321` (Match because it is the correct pattern for West Virginia)
- `WV DL: G6543` (Match)

National Provider IDs (US)

The US National Provider Identifier classifier scans for a US National Provider Identifier (NPI) numbers, which is a 10-digit number with a check digit.

Examples:

- `NPI No. 1245319599` (Match for NPI)
- `NPI No. 1235678996` (Match for NPI)
- `3459872347` (No match because of no supporting information)
- `NPI: 3459872342` (No match because of incorrect check digit)

Academic Records (English)

The predefined FERPA (Family Educational Rights and Privacy Act) DLP policy template uses the Student Records classifier. Combine it with a customized Student Identification Number classifier to detect specific student ID patterns for better accuracy.

Example:

- `Fall Semester Course Numbers: CHEM101, ECON102, MATH103` (Match)

Financial Statements (English)

The predefined Sarbanes-Oxley (SOX) policy template uses the Corporate Financials classifier to search for non-public corporate financial information.

Example:

`Gross Profits, Current Assets, and Cash Flow Statement for the Quarter ended June 30, 2016.` (Match)

Creating a Content Matching Classifier for Custom DLP Policies

Custom classifiers that you create are added to the list of classifiers that you can use when creating custom DLP policies.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Understand how content matching classifiers are used to identify potential DLP violations.	See: • About Defining Disallowed Content Using Content Matching Classifiers , on page 8 • Content Matching Classifier Examples, on page 9
Step 2	Select **Mail Policies > DLP Policy Customizations** and click **Add Custom Classifier**. Enter a classifier name and description.	—
Step 3	Enter a proximity and a minimum total score.	See Determiners of the Risk Factor of a Suspected Violation , on page 15
Step 4	Choose one of the following detection rule types and define the associated content matching criteria: • words or phrases • text from a dictionary • a regular expression, or • an existing data loss prevention entity	See: • Classifier Detection Rules for Identifying Sensitive Content (Custom DLP Policies Only) , on page 12 • Using Custom Dictionaries of Sensitive DLP Terms (Custom DLP Policies Only) , on page 14 • Regular Expressions for Identifying Identification Numbers , on page 12
Step 5	(Optional) Add additional rules by clicking **Add Rule**.	For information about Weight and Max Score, see Determiners of the Risk Factor of a Suspected Violation , on page 15.
Step 6	If you include multiple rules, specify whether **All** or **Any** rules must match.	This setting is at the top of the Rules section.
Step 7	Submit and commit your changes.	—

What to Do Next

Use your custom content classifier in a custom DLP Policy. See Creating a Custom DLP Policy (Advanced) , on page 7.

Classifier Detection Rules for Identifying Sensitive Content (Custom DLP Policies Only)

Content matching classifiers require rules for detecting DLP violations in a message or document. Classifiers can use one or more of the following detection rules:

- **Words or Phrases**. A list of words and phrases for which the classifier should look. Separate multiple entries with a comma or line break.
- **Regular Expression**. A regular expression to define a search pattern for a message or attachment. You can also define a pattern to exclude from matching to prevent false positives. See Regular Expressions for Identifying Identification Numbers , on page 12and Examples of Regular Expressions for Identifying Identification Numbers , on page 13for more information.
- **Dictionary**. A dictionary of related words and phrases. Your appliance includes pre-defined dictionaries, or you can create your own. See Using Custom Dictionaries of Sensitive DLP Terms (Custom DLP Policies Only) , on page 14.
- **Entity**. A predefined pattern that identifies common types of sensitive data, such as credit card numbers, addresses, social security numbers, or ABA routing numbers. For descriptions of the entities, go to **Mail Policies > DLP Policy Manager**, click **Add DLP Policy**, click **Privacy Protection**, then click **Display Policy Descriptions**.

Regular Expressions for Identifying Identification Numbers

Some policy templates require customization of one or more content matching classifiers, which involves creating a regular expression to search for identification numbers that may be linked to confidential information, such as a custom account number, patient identification number or Student ID. You can use the **Perl Compatible Regular Expression (PCRE2)** syntax to add regular expressions for content matching classifiers or the DLP policy templates. The regular expressions are validated for PCRE2 compatibility only when the DLP feature is enabled on your appliance.

Note Regular expressions are case sensitive, so they should include upper and lower case, such as `[a-zA-Z]`. If only certain letters are used, you can define the regular expression accordingly.

The less specific the pattern, such as an 8-digit number, the more likely you will want the policy to search for additional words and phrases to distinguish a random 8-digit number from an actual customer number.

Use the following table as a guide for creating regular expressions for classifiers:

Element	Description
Regular expression (abc)	Regular expressions for classifiers match a string if the sequence of directives in the regular expression match any part of the string. For example, the regular expression ACC matches the string ACCOUNT as well as ACCT .

Element	Description
[ ]	Use brackets to indicate a set of characters. Characters can defined individually or within a range. For example, [a-z] matches all lowercase letters from a to z , while [a-zA-Z] matches all uppercase and lowercase letters from A to Z . [xyz] matches only the letters x , y , or z .
Backslash special characters (\ )	The backslash character *escapes* special characters. Thus the sequence \. only matches a literal period, the sequence \$ only matches a literal dollar sign, and the sequence \^ only matches a literal caret symbol. The backslash character also begins tokens, such as \d . **Important Note:** The backslash is also a special escape character for the parser. As a result, if you want to include a backslash in your regular expression, you must use *two* backslashes — so that after parsing, only one "real" backslash remains, which is then passed to the regular expression system.
\d	Token that matches a digit (0 - 9). To match more than one digit, enter an integer in {} to define the length of the number. For example, \d matches only a single digit such as 5 , but not 55 . Using \d{2} matches a number consisting of two digits, such as 55 , but not 5 .
\D	Token that matches any non-digit character. To match more than one non-digit character, enter an integer in {} to define the length.
\w	Token that matches any alphanumeric character and the underscore (a - z , A - Z , 0 - 9 , and _).
Number of repetitions {min,max}	The regular expression notation that indicates the number of repetitions of the previous token is supported. For example, the expression " \d{8} " matches 12345678 and 11223344 but not 8 .
Or (|)	Alternation, or the "or" operator. If A and B are regular expressions, the expression " A|B " will match any string that matches either "A" or "B." Can be used to combine number patterns in a regular expression. For example, the expression " foo|bar " will match either foo or bar , but not foobar .

Examples of Regular Expressions for Identifying Identification Numbers

Simple regular expressions that describe patterns of numbers and letters in identification or account numbers might look like the following:

- An 8-digit number: `\d{8}`
- Identification code with hyphens between sets of numbers: `\d{3}-\d{4}-\d`
- Identification code that begins with a single letter that can be upper or lower case: `[a-zA-Z]\d{7}`
- Identification code that begins with three digits and is followed by nine uppercase letters: `\d{3}[A-Z]{9}`
- Using | to define two different number patterns to search for: `\d{3}[A-Z]{9}|\d{2}[A-Z]{9}-\d`

Using Custom Dictionaries of Sensitive DLP Terms (Custom DLP Policies Only)

AsyncOS comes with a set of predefined dictionaries, but you can also create custom DLP dictionaries to specify terms for the DLP scanning feature to match.

You can create a custom DLP dictionary in several ways:

- Adding Custom DLP Dictionaries Directly , on page 14
- Creating DLP Dictionaries as Text Files , on page 14and then Importing DLP Dictionaries , on page 15.
- Exporting DLP Dictionaries , on page 15 from another Email Security appliance and then Importing DLP Dictionaries , on page 15.

Adding Custom DLP Dictionaries Directly

Step 1 Select **Mail Policies > DLP Policy Manager.**

Step 2 In the **Advanced Settings** section, click the link beside **Custom DLP Dictionaries**.

Step 3 Click **Add Dictionary**.

Step 4 Enter a name for the custom dictionary.

Step 5 Enter new dictionary entries (words and phrases) into the list of terms.
Dictionary terms are case-sensitive and can contain non-ASCII characters.

When entering multiple entries, separate the entries with line breaks.

Step 6 Click **Add**.

Step 7 Submit and commit your changes.

Creating DLP Dictionaries as Text Files

You can create your own dictionary as a text file on your local machine and import it onto the appliance. Use line breaks for each term in the dictionary text file. Dictionary terms are case-sensitive and can contain non-ASCII characters.

Exporting DLP Dictionaries

Note Predefined DLP dictionaries cannot be exported.

Step 1 Select **Mail Policies > DLP Policy Manager**.

Step 2 Click the link for the **Custom DLP Dictionaries** section under Advanced Settings.

Step 3 Click **Export Dictionary**.

Step 4 Select a dictionary to export.

Step 5 Enter a file name for the dictionary.

Step 6 Choose where to save the exported dictionary, either on your local computer or in the configuration directory on the appliance.

Step 7 Select an encoding for the file.

Step 8 Click **Submit** and save the file.

Importing DLP Dictionaries

Before You Begin

If you will import a file that you exported from a non-DLP dictionary on an Email Security appliance, you must first strip the weight values from the text file and convert any regular expressions to words or phrases.

Step 1 Select **Mail Policies > DLP Policy Manager**.

Step 2 In the **Advanced Settings** section, click the link beside **Custom DLP Dictionaries**.

Step 3 Click **Import Dictionary**.

Step 4 Select a file to import from either your local machine or the configuration directory on the appliance.

Step 5 Select an encoding.

Step 6 Click **Next**.
A “Success” message appears and the imported dictionary is displayed in the Add Dictionary page. However, the process is not yet complete.

Step 7 Name and edit the dictionary.

Step 8 Click **Submit**.

Determiners of the Risk Factor of a Suspected Violation

When the appliance scans a message for DLP violations, it assigns a risk factor score to the message. This score indicates the likelihood that the message contains a DLP violation. A score of 0 means the message almost certainly does not contain a violation. A score of 100 means it almost certainly does contain a violation.

For DLP Policies Based On Predefined Templates

You cannot view or modify risk factor scoring parameters for DLP policies created from predefined templates. However, if there are too many false positive matches for a particular DLP policy, you can adjust the severity scale for that policy. See About Assessing Violation Severity , on page 18. For policies based on templates that do not have a content matching classifier, such as the SOX (Sarbanes-Oxley) template, the scanning engine always returns a risk factor value of "75" when a message violates the policy.

For Custom DLP Policies

When you create content matching classifiers for custom DLP policies, you specify values that are used to determine the risk factor score:

- **Proximity**. How close the rule matches must occur in the message or attachment to count as a violation. For example, if a numeric pattern similar to a social security number appears near the top of a long message and an address appears in the sender's signature at the bottom, they are presumed to be unrelated and the data does not count as a match.
- **Minimum Total Score**. The minimum risk factor score required for sensitive content to be labeled a DLP violation. If the score of a message's matches does not meet the minimum total score, its data is not considered sensitive.
- **Weight**. For each custom rule you create, you specify a "weight" to indicate the importance of the rule. A score is obtained by multiplying the number of detection rule matches by the weight of the rule. Two instances of a rule with a weight of 10 results in a score of 20 . If one rule is more important for the classifier than the others, it should be assigned a greater weight.
- **Maximum Score**. A rule's maximum score prevents a large number of matches for a low-weight rule from skewing the final score of the scan.

To calculate the risk factor, the classifier multiplies the number of matches for a detection rule by the weight of the rule. If this value exceeds the detection rule's maximum score, the classifier uses the maximum score value. If the classifier has more than one detection rule, it adds the scores for all of its detection rules into a single value. The classifier maps the detection rules score (10 - 10000) on a scale of 10 -100 using the logarithmic scale shown in the following table to create the risk factor:

Table 1: How Risk Factor Scores Are Calculated From Detection Rule Scores

Rule Scores	Risk Factor
10	18
20	28
30	33
50	41
100	50
150	56
300	65

Rule Scores	Risk Factor
500	72
1000	82
10000	100

Viewing the Policies in Which Custom Content Classifiers are Used

Step 1 Select **Mail Policies > DLP Policy Customizations.**

Step 2 In the **Custom Classifiers** section, click the **Policies** link in the heading of the Custom Classifiers table.

Filtering Messages for DLP Policies

To improve performance or accuracy, you can limit a DLP policy to apply only to certain messages based on the following criteria:

Option	Description
Filtering by Senders and Recipients	You can limit the DLP policy to apply to messages that do or do not include recipients or senders that you specify using one of the following: • Full email address: `user@example.com` • Partial email address: `user@` • All users in a domain: `@example.com` • All users in a partial domain: `@.example.com` Separate multiple entries using a line break or a comma. AsyncOS first matches the recipient or sender of an outgoing message to an outgoing mail policy, then matches the sender or recipient to the sender and recipient filters specified in the DLP policies enabled for that mail policy. For example, you might want to disallow all senders from sending a certain type of information, except to recipients in a partner domain. You would create a DLP policy for that information, including a filter that exempts all users in the partner domain, then include this DLP policy in an Outgoing Mail Policy that applies to all senders.
Filtering by Attachment Types	You can limit the DLP policy to scanning only messages that do or do not include specific attachment types. Choose an attachment category, then a predefined file type, or specify file types that are not listed. If you specify a file type that is not predefined, AsyncOS searches for the file type based on the attachment's extension. You can also limit DLP scanning to attachments with a minimum file size.

Option	Description
Filtering by Message Tag	If you want to limit a DLP policy to messages containing a specific phrase, you can use a message or content filter to search outgoing messages for the phrase and insert a custom message tag into the message. For more information, see Content Filter Actionsand Using Message Filters to Enforce Email Policies

About Assessing Violation Severity

When the DLP scanning engine detects a potential DLP violation, it calculates a risk factor score that represents the likelihood that the instance actually is a DLP violation. The policy compares the risk factor score to the Severity Scale defined in that policy in order to determine the severity level (for example, Low or Critical.) You specify the action to take for violations at each severity level (except Ignore, for which no action is ever taken.) You can adjust the risk factor scores required to reach each severity level.

Adjusting the Severity Scale

All policies have a default severity scale. You can adjust this scale for each policy.

For example, by default, a violation has a severity level of Critical if its risk factor score is between 90 and 100. However, for violations that match a particular policy, you may want increased sensitivity to potential data loss. For this DLP policy, you could change the Critical severity level to any violation with a risk factor score between 75 and 100.

Step 1 Select **Mail Policies > DLP Policy Manager**.
Step 2 Click the name of the policy to edit.
Step 3 In the **Severity Settings** section, click **Edit Scale**.
Step 4 Use the scale's arrows to adjust the scores for the severity levels.
Step 5 Click **Done**.
Step 6 In the Severity Scale table, verify that your scores are as you want them.
Step 7 Click **Submit**.

Arranging the Order of the Email DLP Policies for Violation Matching

If a DLP violation matches more than one of the DLP policies enabled in the outgoing mail policy, only the first matching DLP policy in the list is used.

Step 1 On the DLP Policy Manager page, click **Edit Policy Order**.
Step 2 Click on the row for a policy you want to move and drag it to a new position in the order.
Step 3 Once you have finished reordering the policies, submit and commit your changes.

Associating DLP Policies with Outgoing Mail Policies

Associating DLP Policies with the Default Outgoing Mail Policy

The default outgoing mail policy is used when no other outgoing mail policy matches the sender or a recipient.

Before You Begin

Complete all activities up to this point in the table in How to Set Up Data Loss Prevention , on page 3. For example, ensure that you have created the DLP policies that you want to include in the default Outgoing Mail Policy.

Step 1 Choose **Mail Policies > Outgoing Mail Policies**.

Step 2 In the **Default Policy** row of the table, click the **Disabled** link in the **DLP** column.

Step 3 Select **Enable DLP (Customize Settings)**.

Step 4 Select the DLP policies to enable for the default outgoing mail policy.

Step 5 Submit and commit your changes.

What to Do Next

Choose the DLP policies for additional Outgoing Mail Policies. See Using Outgoing Mail Policies to Assign DLP Policies to Senders and Recipients , on page 19.

Using Outgoing Mail Policies to Assign DLP Policies to Senders and Recipients

Specify which DLP policies apply to which senders and recipients by enabling them in outgoing mail policies. You can use DLP policies only in outgoing mail policies.

Before You Begin

Configure the DLP policy settings for the default Outgoing Mail policy. See Associating DLP Policies with the Default Outgoing Mail Policy , on page 19.

Step 1 Choose **Mail Policies > Outgoing Mail Policies**.

Step 2 Click the link in the DLP column in any row of the table.

Step 3 Select the DLP policies to associate with this outgoing mail policy.

Step 4 Submit your changes.

Step 5 Repeat as needed for other Outgoing Mail Policies.

Step 6 Commit your changes.

Important Information About Editing or Deleting DLP Policies

Action	Information
Editing a DLP policy	If you rename a policy, you must re-enable it in your outgoing mail policies.
Deleting a DLP policy	If you delete a policy, you will receive a notification if the DLP policy is used in one or more outgoing mail policies. Deleting a DLP policy removes it from these mail policies.

Message Actions

You specify primary and secondary actions that the Email Security appliance will take when it detects a possible DLP violation in an outgoing message. Different actions can be assigned for different violation types and severities.

Primary actions include:

- Deliver
- Drop
- Quarantine

Secondary actions include:

- Sending a copy to a policy quarantine if you choose to deliver the message. The copy is a perfect clone of the original, including the Message ID. Quarantining a copy allows you to test the DLP system before deployment in addition to providing another way to monitor DLP violations. When you release the copy from the quarantine, the appliance delivers the copy to the recipient, who will have already received the original message.
- Encrypting messages. The appliance only encrypts the message body. It does not encrypt the message headers.
- Altering the subject header of messages containing a DLP violation.
- Adding disclaimer text to messages.
- Sending messages to an alternate destination mailhost.
- Sending copies (bcc) of messages to other recipients. (For example, you could copy messages with critical DLP violations to a compliance officer's mailbox for examination.)
- Sending a DLP violation notification message to the sender or other contacts, such as a manager or DLP compliance officer. See Drafting DLP Notifications , on page 23.

Note These actions are not mutually exclusive: you can combine some of them within different DLP policies for various processing needs for different user groups. You can also configure different treatments based on the different severity levels in the same policy. For example, you may want to quarantine messages with critical DLP violations and send a notification to a compliance officer, but you may want to deliver messages with low severity levels.

Defining Actions to Take for DLP Violations (Message Actions)

Before You Begin

- Create at least one dedicated quarantine to hold messages (or copies of messages) that violate DLP policies.

  This can be a local quarantine on an Email Security appliance or a centralized quarantine on a Security Management appliance.

  For information, see Centralized Policy, Virus, and Outbreak Quarantines
- If you want to encrypt messages before delivery, make sure you have set up an encryption profile. See Cisco Email Encryption
- To include disclaimer text when delivering messages with DLP violations or suspected violations, specify disclaimer text in **Mail Policies > Text Resources**. For information, see Disclaimer Template
- To send a notification to the sender of a DLP violation or to another person such as a compliance officer, first create the DLP notification template. See Drafting DLP Notifications , on page 23.

Step 1 Select **Mail Policies > DLP Policy Customizations.**

Step 2 In the **Message Actions** section, click **Add Message Action**.

Step 3 Enter a name for the message action.

Step 4 Enter a description of the message action.

Step 5 Choose whether to drop, deliver, or quarantine messages containing DLP violations.

Note If you select Deliver, you can choose to have a copy of the message sent to a policy quarantine. The copy of the message is a perfect clone, including the Message ID.

Step 6 If you want to encrypt the message upon delivery or its release from quarantine, select the **Enable Encryption** check box and select the following options:

- **Encryption Rule**. Always encrypts the message or only encrypt it if an attempt to send it over a TLS connection first fails.
- **Encryption Profile**. Encrypts the message using the specified encryption profile and delivers it if you use a Cisco IronPort Encryption Appliance or a hosted key service.
- **Encrypted Message Subject**. Subject for the encrypted message. Use the value is $Subject to keep the existing message subject.

Step 7 If you select Quarantine as the action, choose the policy quarantine that you want to use for messages containing DLP violations.

Step 8 Click **Advanced** if you want to modify the message using any of the following options:

- Add a custom header
- Modify the message subject
- Deliver it to alternate host
- Send a copy (bcc) to another recipient
- Send a DLP notification message

Step 9 Submit and commit your changes.

Viewing and Editing Message Actions

Step 1 Select **Mail Policies > DLP Policy Customizations.**

Step 2 In the **Message Actions** section, choose an action:

To	Do This
View the mail policies to which each action is assigned	Click the **Policies** link in the heading of the Message Actions table.
View the description that you entered for each action	Click the **Description** link in the heading of the Message Actions table.
View or edit details of a Message Action	Click the name of the Message Action.
Delete a Message Action	Click the trash can icon next to the message action you want to delete. A confirmation message notifies you if the message action is used in one or more DLP policies.
Duplicate a Message Action You can use this feature to create a backup copy of a Message Action before changing it, or to use as a starting point for a new, similar Message Action.	Click the **Duplicate** icon next to the message action that you want to duplicate.

Step 3 Submit and commit any changes.

Drafting DLP Notifications

Use this procedure to create a template for the notification that will be sent when an email message contains information that violates your organization's data loss prevention policies. You can send this notification to the sender of the message that violated DLP policy, or to another address, for example a manager or DLP Compliance officer.

Before You Begin

- Familiarize yourself with the DLP Notification Template Variable Definitions, on page 23. You can use these variables to customize the notification with specific details about each violation.

Step 1 Select **Mail Policies > Text Resources**.

Step 2 Click **Add Text Resource**.

Step 3 For **Type**, select **DLP Notification Template**.
DLP variables are not available for the plain Notification template.

Step 4 Enter notification text and variables.
The notification should inform its recipients that an outgoing message may contain sensitive data that violates your organization's data loss prevention policies.

What to Do Next

Specify this DLP notification template in a Message Action in a DLP policy in the DLP Policy Manager.

DLP Notification Template Variable Definitions

Use the following variables to include specific information about each DLP violation in the notification.

Variable	Substituted With
$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).
$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
$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.
$Reputation	Replaced by the SenderBase 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 Cisco 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 Cisco appliance.
$bodysize	Replaced by the size, in bytes, of the message.
$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.

Variable	Substituted With
$remoteip	Replaced by the IP address of the system that sent the message to the Cisco appliance.
$recvlistener	Replaced by the nickname of the listener that received the message.
$dropped_filenames	Same as $filenames , but displays list of dropped files.
$dropped_filename	Returns only the most recently dropped filename.
$recvint	Replaced by the nickname of the interface that received the message.
$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.
$Time	Replaced by the current time, in the local time zone.
$orgid	Replaced by the SenderBase Organization ID (an integer value).
$enveloperecipients	Replaced by all Envelope Recipients (Envelope To, <RCPT TO>) of the message.
$dropped_filetypes	Same as $filetypes , but displays list of dropped file types.
$dropped_filetype	Returns only the file type of the most recently dropped file.

Displaying Sensitive DLP Data in Message Tracking

DLP deployment offers the option to log the content that violates your DLP policies, along with the surrounding content, which can then be viewed in Message Tracking. This content may include sensitive data such as credit card numbers and social security numbers.

Before You Begin

Enable Message Tracking. See Enabling Message Tracking

Step 1 Select **Security Services > Data Loss Prevention**.

Step 2 Click **Edit Settings**.

Step 3 Select the **Enable Matched Content Logging** check box.

Step 4 Submit and commit your changes.

What to Do Next

Specify which administrative users can view this information. See Controlling Access to Sensitive Information in Message Tracking.

About Updating the DLP Engine and Content Matching Classifiers

Updates for the Cisco DLP engine and the predefined content matching classifiers on your appliance are independent of updates for other security services.

Determining the Current Version of the DLP Engine

Step 1 Select **Security Services > Data Loss Prevention.**

Step 2 Look in the **Current DLP Version Files** section.

Note You can also use the `dlpstatus` CLI command to view the current version of the DLP engine. See the *CLI Reference Guide for AsyncOS for Cisco Email Security Appliances* for more information.

Updating the DLP Engine and Content Matching Classifiers Manually

Before you Begin

See the following:

- (If applicable) DLP Updates on Centralized (Clustered) Appliances , on page 27

Step 1 Select **Security Services > Data Loss Prevention.**

Step 2 Click **Update Now** in the **Current DLP Version Files** section.
This button is available only when there are new updates available for download.

Note You can also use the `dlpupdate` CLI command to update the DLP engine. See the *CLI Reference Guide for AsyncOS for Cisco Email Security Appliances* for more information.

Enabling Automatic Updates (Not Recommended)

Use this procedure to enable the appliance to check for and download updates at a regular interval.

Note Cisco recommends that you do not enable automatic updates. These updates may change the content matching classifiers used in your DLP policies. Instead, manually download DLP updates and test them in a lab environment before updating appliances used in production.

Before You Begin

- On the **Security Settings > Service Updates** page, make sure you have enabled automatic updates and specified an update interval for all service updates.
- See DLP Updates on Centralized (Clustered) Appliances , on page 27.

Step 1 Select **Security Services > Data Loss Prevention**.

Step 2 Click **Edit Settings**.

Step 3 Select the **Enable automatic updates** check box.

Step 4 Submit and commit your changes.

DLP Updates on Centralized (Clustered) Appliances

Note the following:

- You cannot enable automatic DLP updates for appliances in clustered deployments.
- DLP updates are always performed at the machine level, irrespective of DLP configured at the cluster, machine or group level.
- You can only check the status of an appliance's DLP engine using the dlpstatus CLI command at the machine level.

Working with DLP Incident Messages and Data

Note See also the documentation for the Security Management appliance, as applicable to your deployment.

To	Do This
Search for messages containing DLP violations using criteria such as DLP policy name, violation severity, and action taken, and view details of messages found	See Tracking Messages.
View or manage messages that have been quarantined as suspected DLP violations	See Working with Messages in Policy, Virus, or Outbreak Quarantines.
View a summary of DLP incidents	See information about DLP Incident Summary reports in Using Email Security Monitor.
View information about DLP violations discovered in outgoing mail	See information about DLP Incident reports in Using Email Security Monitor.

Troubleshooting Data Loss Prevention

DLP Fails to Detect Violations in Email Attachments

Problem

When using predefined DLP policies, DLP fails to detect violations in email attachments. This can be caused by:

- The small value of the proximity parameter in the predefined DLP policies

Note You cannot change the proximity of a predefined DLP policy.

- The high severity scale parameter defined in the predefined DLP policies

Solution

- Create a custom policy and adjust the proximity as required. See Creating a Custom DLP Policy (Advanced) , on page 7
- Lower the severity scale parameter of the predefined DLP policy. See Adjusting the Severity Scale , on page 18