Email DLP Quick Start

TRITON - Email Security is automatically configured to work with TRITON - Data Security. The Email Security module registers with the Data Security Management Server when you install it, and Data Security policies are enabled by default in TRITON - Email Security.

**Important**

You must click **Deploy** in TRITON - Data Security to complete the registration process.

A quick-start email data loss prevention (DLP) policy is provided. You just need to configure it.

**To get started with your email DLP policy**

1. Define user directories for Data Security users and other policy resources such as devices and networks. (See *Configuring user directory server settings*, page 2.)
2. Set up email properties for alerts (See *Setting up email properties*, page 3.)
3. Select and enable the attributes to monitor in outgoing email messages—for example message size or attachment type. Configure properties for those attributes. When the settings you configure are matched, the policy is triggered. (See *Select the attributes to monitor for outbound and inbound email*, page 4.)
4. Select and enable the attributes to monitor in inbound email messages—for example questionable images. Configure properties for those attributes.

**Note**

If you want to monitor internal email messages, you must create a custom policy. On the Destination tab of the policy wizard, select **Network** or **Endpoint Email**, then select **Direction > Internal**.

5. Identify an owner or owners for the policy. See *Defining policy owners*, page 8 for instructions.
6. Identify trusted domains if any. See *Identifying trusted domains*, page 8 for more information.

---

**Note**

You cannot delete or rename your email policy, but you can enable or disable attributes.

In this section, you define inbound and outbound email attributes. You define Internal DLP email through the custom policy wizard.

---

7. Deploy your settings. (See *Deploying your settings*, page 9.)

### Configuring user directory server settings

To resolve user details during analysis and enhance the details displayed in reporting, you need to first configure user directory server settings.

In the TRITON Console, you define the LDAP user directory to use *when adding and authenticating TRITON administrators* with network accounts. (Select *TRITON Settings* from the TRITON toolbar, then select *User Directories*.)

On the Data Security tab, you define the user directory to use *for Data Security users and other policy resources* such as devices and networks.

1. Select *Settings > General > System*.
2. Click the *User Directories* option in the System pane.
3. Click *New* in the toolbar.
4. In the Add User Directory Server screen, complete the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the user directory server.</td>
</tr>
<tr>
<td>Type</td>
<td>Select the type of directory from the pull-down menu: Active Directory, Domino, ADAM, or CSV file.</td>
</tr>
<tr>
<td><strong>Connection Settings</strong></td>
<td></td>
</tr>
<tr>
<td>IP address or host name</td>
<td>Enter the IP address or host name of the user directory server.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the port number of the user directory server.</td>
</tr>
<tr>
<td>User distinguished name</td>
<td>Enter a user name that has access to the directory server.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password for this user name.</td>
</tr>
</tbody>
</table>
5. Click **OK** to save your changes.

**Note**
If you select CSV as the file type in the Add User Directory Server, you won’t see the IP address, port, and SSL fields. You need to supply the full path for the CSV files, along with a user name and password. The Test Connection functionality is the same.

There are no Directory usage fields associated with CSV files.

---

### Setting up email properties

Set up the email properties, such as SMTP mail server, to be used for system alerts.

1. Select **Settings > General > System**.
2. Select the **Alerts** option in the System pane.
3. On the **General** tab select the conditions on which you want to trigger alerts.
4. On the **Email Properties** tab, complete the fields as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sender name</td>
<td>When an alert is sent to administrators, from whom should it be coming?</td>
</tr>
<tr>
<td>Sender email address</td>
<td>Enter the email address of the person from whom the alert is coming.</td>
</tr>
</tbody>
</table>

5. To define or edit the **Outgoing mail server**, click Edit (the pencil icon). Complete the fields as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address or host name</td>
<td>Enter the IP address or host name of the outgoing SMTP mail server to use for scheduled alert notifications.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the port number of the mail server to use.</td>
</tr>
</tbody>
</table>

6. Complete the remaining fields as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subject</td>
<td>Enter a subject for alerts. Click the right-arrow to select a variable to include in the subject, such as %Severity%.</td>
</tr>
<tr>
<td>Recipients</td>
<td>Click Edit to select the recipients to whom alerts should be sent.</td>
</tr>
</tbody>
</table>

7. Click **OK** to save your changes.

**Note**

The same outgoing mail server is used for alerts, notifications, and scheduled tasks. The settings you use here apply to the other cases, and if you change the settings for one, it affects the others.

---

**Select the attributes to monitor for outbound and inbound email**

Configure the attributes that you want to monitor for outbound and inbound email messages.

1. In TRITON - Data Security, select **Main > Policy Management > DLP Policies > Email DLP Policy**.
2. On the Outbound tab, check one or more email attributes to include in the policy for outbound email messages. To define properties for an attribute, highlight it and enter information in the right pane. (Refer to the following table for a description of each attribute.)

a. If you want to send notifications when there is a violation of a particular attribute setting, select the **Send Notification** check box. You can configure who receives the notifications by clicking the name of the notification, “Email policy violation.” Click this option to define the mail server, email subject, and message body, as well as other required properties.

By default, for inbound messages, policy owners receive notifications. For outbound messages, both policy owners and message senders receive them.

b. For each attribute, indicate how **severe** a breach would be (low, medium, or high severity), and what **action** should be taken if a breach is detected. The default severity levels and available actions are shown below for each attribute.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message size</td>
<td>Select the size of email messages to monitor. For example, choose 25 MB if you want Data Security to analyze and enforce messages exceeding 25 MB, but you’re not concerned about messages smaller than 25 MB, even if there is a match. The default size is 10 MB. Default severity: <strong>low</strong>. Available actions: <strong>quarantine</strong> (default), <strong>permit</strong>.</td>
</tr>
<tr>
<td>Regulatory &amp; compliance</td>
<td>Select the regulatory and compliance rules you need to enforce. These are applied to the regions you selected with the regulatory &amp; compliance option.</td>
</tr>
<tr>
<td></td>
<td>• Personally Identifiable Information (PII)</td>
</tr>
<tr>
<td></td>
<td>• Private Health Information (PHI)</td>
</tr>
<tr>
<td></td>
<td>• Payment Card Industry (PCI)</td>
</tr>
<tr>
<td></td>
<td>If you have not selected regions, an error pops up. Click “Select regions” to fix this.</td>
</tr>
<tr>
<td></td>
<td>Default severity: <strong>high</strong>.</td>
</tr>
<tr>
<td></td>
<td>Available actions: <strong>quarantine</strong> (default), <strong>permit</strong>.</td>
</tr>
<tr>
<td>Attachment name</td>
<td>One by one, enter the names of the exact files that should be monitored when they’re attached to an email message. Include the filename and extension. Click <strong>Add</strong> after each entry.</td>
</tr>
<tr>
<td></td>
<td>For example, add the file named <strong>confidential.docx</strong>. When that file is attached to an email message, Data Security detects it and either permits or blocks the message, or drops the attachment and sends the remaining message.</td>
</tr>
<tr>
<td></td>
<td>Note that Drop Attachments applies only to the TRITON - Email Security module. If your email is being monitored by the protector or SMTP agent and you select this option, it will be quarantined when a policy is triggered.</td>
</tr>
<tr>
<td></td>
<td>Default severity: <strong>low</strong>.</td>
</tr>
<tr>
<td></td>
<td>Available actions: <strong>quarantine</strong>, <strong>permit</strong>, <strong>drop attachments</strong> (default)</td>
</tr>
</tbody>
</table>
### Email DLP Quick Start

#### Attachment type
Click **Add** to specify the types of files that should be monitored when attached to an email message, for example Microsoft Excel files.

From the resulting dialog box, select the type or types of files to monitor. If there are more file types than can appear on the page, enter search criteria to find the file type you want. Data Security searches in the file type group, description, and file type for the data you enter.

If the file type does not exist, specify exact files of this type using the **Attachment name** attribute instead.

Default severity: **low**.

Available actions: **quarantine, permit, drop attachments** (default).

**Note:**
Drop Attachments applies only to the TRITON - Email Security module. If your email is being monitored by the protector or SMTP agent and you select this option, it will be quarantined when a policy is triggered.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attachment type</td>
<td>Click <strong>Add</strong> to specify the types of files that should be monitored when attached to an email message, for example Microsoft Excel files. From the resulting dialog box, select the type or types of files to monitor. If there are more file types than can appear on the page, enter search criteria to find the file type you want. Data Security searches in the file type group, description, and file type for the data you enter. If the file type does not exist, specify exact files of this type using the <strong>Attachment name</strong> attribute instead. Default severity: <strong>low</strong>. Available actions: <strong>quarantine, permit, drop attachments</strong> (default). <strong>Note:</strong> Drop Attachments applies only to the TRITON - Email Security module. If your email is being monitored by the protector or SMTP agent and you select this option, it will be quarantined when a policy is triggered.</td>
</tr>
<tr>
<td>Patterns &amp; phrases</td>
<td>Click <strong>Add</strong> to define key phrases or regular expression (RegEx) patterns that should be monitored. RegEx patterns are used to identify alphanumeric strings of a certain format. On the resulting dialog box, enter the precise phrase (for example “Internal Only”) or RegEx pattern (for example ~ m/H.?e/) to include. Select how many phrase matches must be made for the policy to trigger. The default number of matches is 1. Define whether to search for the phrase or RegEx pattern in all email fields, or in one or more specific fields. For example, you may want to search only in an attachment, or skip searching in To and CC fields. Default severity: <strong>medium</strong>. Available actions: <strong>quarantine</strong> (default), <strong>permit</strong>. <strong>Note:</strong> Although you do not define whether to search for only unique strings, the system will use the following defaults: Key phrase: non-unique - all matches will be reported. Regular expression: unique - only unique matches will be reported as triggered values.</td>
</tr>
</tbody>
</table>
Acceptable use

Select the dictionaries that define unacceptable use in your organization. For example, if you want to prevent adult language from being exchanged by email, select Adult.

Data Security includes dictionaries in 9 languages. Select the languages to enforce. Only terms in these languages are considered a match. For example, if you select the Adult dictionary and Hebrew, adult terms in English are not considered an incident.

Note that false positives (unintended matches) are more likely to occur when you select multiple languages. For this reason, exercise caution when selecting the languages to enforce.

You cannot add or delete terms from predefined dictionaries, but you can exclude them from detection if you are getting unintended matches. Select Main > Content Classifiers > Patterns & Phrases, select the dictionary to edit, then enter the phrases to exclude.

By default the policy is triggered by a single match from the dictionary or dictionaries you select.

Default severity: medium.
Available actions: quarantine (default), permit.

Questionable images

Select this attribute to prevent pornographic images from entering your organization. (This feature requires a special Data Security Image Analysis subscription). Pornographic images pose a legal liability to organizations in many countries.

Data Security judges images based on the amount of flesh tone they contain.

Default severity: low.
Available actions: quarantine, permit, drop attachments (default).

Number of attachments

Specify the number of attachments to detect. Email messages with this number of attachments (or more) trigger the policy.

The default number of attachments is 20.

Default severity: low.
Available actions: quarantine (default), permit

Number of destination domains

This option is available for outbound messages only. Sometimes you may want to block messages sent to multiple destination domains, because this may indicate spam.

Specify the number of destination domains to detect. Email messages sent to this number of domains (or more) trigger the policy. The default number of domains is 25.

Also, select which email fields to monitor (To, Cc, Bcc). To and Cc are selected by default.

Default severity: low.
Available actions: quarantine (default), permit.

3. Click the Inbound tab and repeat step 2 to define the attributes to include in the policy for inbound email messages. Note that number of destination domains does not apply to inbound messages.
Defining policy owners

Policy owners can view and modify a policy and, if configured, receive notifications of breaches. Notifications must be enabled in one or more of the policy’s attributes for notifications to be sent.

To define an owner or owners for this email DLP policy:

1. Select the Policy Owners tab.
2. Click Edit.
3. Select one or more owners from the resulting box.
4. Click OK.

If you would like notifications to be sent to policy owners:

1. Select Main > Policy Management > Resources.
2. Click Notifications in the Remediation section of the page.
3. Select an existing notification or click New to create a new one.
4. Under Recipients, select Additional email addresses.
5. Click the right arrow then select the variable, %Policy Owners%.
6. Click OK.

Identifying trusted domains

Trusted domains are, simply, those that you trust, such as the domain of a company you just acquired. Trusted domains do not need to be monitored, so they do not get analyzed by Data Security.

Note

Trusted domains apply to outbound email traffic only.

If you have domains that you do not want enforced:

1. On the Outbound tab, select Enable trusted domains.
2. Click Edit.
3. Browse for the domain or domains you trust.
4. Click OK.
Deploying your settings

The settings you configured in this chapter must be deployed to the Email Security module and other system components to begin monitoring your email. To deploy settings:

1. Click **OK** on the email DLP policy page.
2. Click **Deploy** in the TRITON - Data Security toolbar.

Your email DLP policy is now functioning!