

Websense Email Security Transition: Policies and Settings

Topic 70052 | TRITON AP-EMAIL | Version 8.0.x | Updated 03-Mar-2015

Part of the Websense® TRITON® APX security suite, Websense TRITON AP-EMAIL is an appliance-based email protection solution that combines on-premises email analysis with world-class Web analytics to provide maximum security against today's sophisticated blended threats. The Email Hybrid Module adds in-the-cloud prefiltering capabilities to the robust analysis capabilities of the on-premises solution. The Email Sandbox Module includes file and URL sandboxing capabilities to analyze and provide feedback regarding suspicious files and attachments.

This solution also offers Websense TRITON AP-DATA data loss protection (DLP) technology to accurately detect the transmission of sensitive data via email. Integration with Websense TRITON AP-WEB or Web Filter & Security allows the email protection system to use that module's master URL database to detect malicious embedded URLs in email.

This paper is for users of the Websense Email Security software solution who want information about making the transition to the TRITON AP-EMAIL on-premises solution. It describes how to configure some common email policies in TRITON AP-EMAIL. Also included is a list of the locations of configuration settings in Websense Email Security and their corresponding locations in the TRITON AP-EMAIL interface.

For a general description of the TRITON AP-EMAIL solution and some suggestions for easing the transition from Websense Email Security, see [Websense Email Security Transition: Overview](#).

Contents:

[Sample email protection policies in TRITON AP-EMAIL](#)

[Configuration Settings](#)

Sample email protection policies in TRITON AP-EMAIL

Rules in Websense Email Security are created from separate, modular components in the Rules Administrator, a graphical drag-and-drop tool. In TRITON AP-EMAIL, you create a policy that applies to a specified set of email senders and recipients, then

determine the rule that defines how messages that match the sender/recipient conditions are handled.

Email DLP policies are configured in the TRITON AP-DATA console and enabled for enforcement in the Email console.

This chapter includes instructions for creating some common, sample policies in TRITON AP-EMAIL. You may already have rules to address these situations in Websense Email Security.

- ◆ *Block a message that contains specific keywords*
- ◆ *Edit or add rules to an email policy*
- ◆ *Disable a rule within a policy*
- ◆ *Configure message and attachment size*
- ◆ *Configure advanced content analysis*
- ◆ *Analyze message attachments*
- ◆ *Configure dictionary threshold limits*

Block a message that contains specific keywords

To create a policy to quarantine an email that contains specific keywords either in the message subject or body, you can configure either a custom content filter for an Email module policy or an email DLP policy in the Data module. A custom content filter is a good option for basic keyword analysis, and a message that triggers this filter is quarantined in an Email module message queue. You can use an email DLP policy for complex rules to quarantine a message in a Data module queue.

For an email custom content filter, perform the following steps in the Email module:

1. Navigate to the **Main > Policy Management > Filters** page and click **Add**.
2. Specify a name and brief description for the filter.
3. Select **Custom Content** in the **Filter type** drop-down list.
4. Select whether to trigger the filter when any defined condition is matched or when all defined conditions are matched.
5. Click **Add** in the Filter Conditions box to open the Add Condition dialog box.
6. In the Message Attribute drop-down list, select **Message subject** or **Message body text**, depending on which element you want analyzed.
7. In the Condition details box, choose an operator (Contains, Does not contain, Matches regular expression, Does not match regular expression).
8. Enter the text you would like the filter to detect.
9. Mark the **Match case** check box if you want to use that option.
10. Click **OK**.

For an email DLP policy, perform the following steps in the Data module:

1. Select **Main > Policy Management > DLP Policies > Email DLP Policy**.
2. Select either the **Outbound** or **Inbound** tab to specify the email direction.

3. Select the **Patterns & phrases** attribute.
4. Add a keyword:
 - a. Select the **Enable attribute** check box.
 - b. Click **Add** to open the Add Pattern or Key Phrase dialog box.
 - c. Select the **Key phrase** option and then enter a word or phrase for which you would like to trigger the policy.
 - d. Select number of matches needed to trigger the policy (default value is 1).
 - e. Specify the email fields you would like searched.
 - f. Click **OK**.
5. Specify the **Severity** (High, Medium, or Low) and set the **Action** to **Quarantine**.
6. Click **OK**.

Edit or add rules to an email policy

You can edit existing policy rules or add a new rule to a policy in the Email module for flexibility in controlling message traffic in your organization.

Edit existing policy rules in the Email module as follows:

1. Select **Main > Policy Management > Policies** and then click **Add**.
2. Define policy properties:
 - a. Specify a name and description for the policy.
 - b. Set the status and assign the policy order.
 - c. Specify the sender/recipient conditions for this policy.
3. Edit an existing policy rule by clicking a rule name.
 - To edit existing filter properties, click **Edit** in the Filter section.
To add new a new filter, select **Add filter** from the Filter name drop-down list.
 - To edit action options, click **Edit** in the Action section.
To add a new action, select **Add action** from the Action name drop-down list.
4. Click **OK** to close the Edit Rule page.
5. Click **OK** to save your policy.

You may add a new rule only in association with a custom content filter. Add a custom rule as follows:

1. Select **Main > Policy Management > Policies** and then click **Add**.
2. Define policy properties:
 - a. Specify a name and description for the policy.
 - b. Set the status and assign the policy order.
 - c. Specify the sender/recipient conditions for this policy.
3. Add a new policy rule by clicking **Add** in the Rules section.

- a. Select a custom content filter in the Filter section. Click **Edit** in the Filter Properties box if you want to add or edit the filter conditions.
To add a new custom content filter, select **Add filter** from the Filter name drop-down list.
 - b. Select an action from the drop-down Action name field. Click **Edit** in the Action section to modify action options.
To add a new action, select **Add action** from the Action name drop-down list.
4. Click **OK** to close the Add Rule page.
 5. Click **OK** to save your policy.

Disable a rule within a policy

You can block rule application within a policy by disabling the rule. Block the application of a rule in an email protection policy as follow:

1. Select **Main > Policy Management > Policies**.
2. Select a policy from the **Inbound**, **Outbound**, or **Internal** list.
3. Click the name of the rule you want to disable.
4. Select the **Disabled** option for the rule status.
5. Click **OK** to save your rule changes.
6. Click **OK** to save your policy changes.

Configure message and attachment size

You can restrict inbound email messages from being delivered if the message data exceeds a specific size. Create a policy to quarantine a message if the message body or an attachment exceeds the specified limit.

Message size and attachment size per connection limits can be set in the Email module or the Data module.

Restrict message and attachment size per connection using the Email module as follows:

1. On the **Settings > Inbound/Outbound > Directory Attacks** page, select the **Limit the number of messages/connections per IP every** option, and then specify a time limit using the drop-down menu.
2. Specify a message limit in the **Maximum number of messages** field.
3. Specify a connection limit using the **Maximum number of connections** options.
4. Click **OK**.

You can also use the message size options available in the following Email module pages:

- ◆ **Settings > Inbound/Outbound > Message Control**
- ◆ **Settings > Inbound/Outbound > Connection Control**

- ◆ **Main > Policy Management > Filters > Add Filter** (add a custom content filter)

For more information about setting message size and attachment limitations in the Email module, see the following email Administrator Help topics:

- ◆ [Configuring message properties](#)
- ◆ [Managing connection options](#)
- ◆ [Creating and configuring a filter](#)

Restrict message and attachment size per connection using Data module settings as follows:

1. On the **Main > Policy Management > DLP Policies > Email DLP Policy** page, select the **Message size** attribute.
2. Select the **Enable attribute** check box and then use the up or down arrow to select the message size to monitor.
3. Specify a **Severity** (High, Medium, Low) and set the **Action** to **Quarantine**.
4. Click **OK**.

Configure advanced content analysis

Advanced content analysis provides a comprehensive examination of message header, message body, and message attachments. It also supports the dynamic evaluation of keyword frequency.

Advanced content analysis can be configured in the Data module. Content analysis settings are available for the following content classifiers:

- ◆ Patterns and phrases
- ◆ File properties
- ◆ Fingerprint
- ◆ Transaction size
- ◆ Number of email attachments
- ◆ Number of email destinations

Configure advanced content analysis for an email message as follows:

1. In the Data module, select **Main > Policy Management > DLP Policies**.
2. Click **Create custom policy** to create a new policy using the custom policy wizard.
3. Complete the **General** tab in the wizard and click **Next** to access the **Condition** tab.
4. Click **Add** and select a content classifier from the drop-down list to configure its advanced settings.

For example, you may want to define a threshold for the content classifier, or impose a limit to the rule so that it searches for specific fields. The advanced settings available depend on the content classifier you select.

5. Click **Next** to continue using the custom policy wizard to create a policy. You should complete the **Severity & Action**, **Source**, and **Destination** tabs.
6. Click **Finish**.

You can also use an Email module custom content filter to analyze various message attributes like message header or body text (**Main > Policy Management > Filters > Add Filter**). See [Creating and configuring a filter](#) in the email protection system Administrator Help for details.

Analyze message attachments

You can block inbound and outbound messages that contain attachments. Configure message attachment analysis as follows:

1. In the Data module, select **Main > Policy Management > DLP Policies > Email DLP Policy**.
2. Click either the **Inbound** or **Outbound** tab, and then select the **Number of attachments** attribute.
3. Specify the attributes for number of attachments.
 - a. Select the **Enable attribute** check box.
 - b. Use the up or down arrow to specify the **Detect email messages with at least *n* attachments** condition.
 - c. Specify the **Severity** (High, Medium, Low) and set the **Action** to **Quarantine**.
4. Click **OK**.

You can also use file sandboxing capabilities to analyze attachments that may contain security threats. The Email Sandbox Module add-on is required for this capability. See [Creating and configuring a filter](#) in the email protection system Administrator Help for details about configuring file sandbox analysis.

Configure dictionary threshold limits

You can set a threshold value for words or phrases in a dictionary. This value determines whether a message should be blocked based on the keyword frequency within the message.

Configure a dictionary and its threshold limits as follows:

1. In the Data module, select **Main > Policy Management > DLP Policies**.
2. Click **Create custom policy** to open the custom policy wizard.
3. Complete the **General** tab and then click **Next**.
4. On the **Condition** tab, select **Add > Patterns & Phrases**.
 - a. On the **General** tab in the Select a Content Classifier dialog box, select **New > Dictionary**.
 - b. In the **Add Dictionary** dialog, name your dictionary and define the properties for the dictionary classifier and then click **OK**.

For more information about creating dictionary classifiers, refer to the Data Security Manager Help topic titled [Adding a dictionary classifier](#).

5. Click **Next**.
6. Specify the **Severity** (High, Medium, Low) and set the **Action** to **Quarantine**.
You can also define **Advanced** conditions for the rule to change severity and action when specific conditions are met.
7. Specify a **Source** filter range and then click **Next**.
8. Specify a **Destination** filter range and then click **Next**.



Note

The **Destination** settings and the **Source** destination settings must be the same.

9. Click **Finish**.

Configuration Settings

Migrating your Websense Email Security settings to Websense TRITON AP-EMAIL is a manual process. Determining the correct settings and their location in the Email module can be a time-consuming operation.

Printing your Websense Email Security configuration settings can streamline the transition process. See [Websense Email Security Transition: Overview](#) for information about printing the configuration settings.

The following table lists Websense Email Security configuration settings and the user interface location of the corresponding settings in TRITON AP-EMAIL.

Websense Email Security setting	TRITON AP-EMAIL module location
Dashboard	Main > Status > Dashboard Main > Status > Alerts
Email Connection Management	
Protected Domains	Settings > Users > Domain Groups
Mail Relays	Settings > Inbound/Outbound > Relay Control
Blacklist	Main > Policy Management > Always Block/Permit Settings > Inbound/Outbound > Connection Control
Reverse DNS lookup	Settings > Inbound/Outbound > Connection Control

Websense Email Security setting	TRITON AP-EMAIL module location
Reputation/DNS blacklist	Settings > Inbound/Outbound > Connection Control
Directory Harvest Detection	Settings > Inbound/Outbound > Directory Attacks
Denial of Service Detection	Settings > Inbound/Outbound > Connection Control
Remote User Authentication	Settings > Users > User Authentication
SPF check	Settings > Inbound/Outbound > Relay Control
Receive Service	Settings > Inbound/Outbound > Connection Control Settings > Inbound/Outbound > Message Control
SMTP Properties	Settings > General > System Settings Settings > Inbound/Outbound > Connection Control
Connections	Settings > Inbound/Outbound > Message Control Settings > Inbound/Outbound > Connection Control
ESMTP Commands	Settings > Users > User Authentication Settings > Inbound/Outbound > Enforced TLS Connections Settings > Inbound/Outbound > Encryption
Rules Service	Main > Policy Management > Policies Main > Policy Management > Filters Main > Policy Management > Actions Note: You can also configure an email DLP policy in the Data module.

Websense Email Security setting	TRITON AP-EMAIL module location
Configuration	Settings > Inbound/Outbound > Connection Control Settings > Inbound/Outbound > Message Control Settings > Inbound/Outbound > Mail Routing Settings > Inbound/Outbound > TLS Certificate Settings > Administrators > Delegated Administrators Main > Policy Management > Policies Main > Policy Management > Filters Main > Policy Management > Actions Note: You can also configure an email DLP policy in the Data module.
Queue Management	Main > Message Management > Message Queues Main > Message Management > Blocked Messages Main > Message Management > Delayed Messages
Send Service	Settings > General > System Settings Settings > Inbound/Outbound > Connection Control Settings > Inbound/Outbound > Mail Routing Settings > Inbound/Outbound > Non-Delivery Options
SMTP Properties	To set the SMTP greeting text: Settings > General > System Settings To set the SMTP greeting delay interval: Settings > Inbound/Outbound > Connection Control
Connections	Settings > Inbound/Outbound > Connection Control
Routing	Settings > Inbound/Outbound > Mail Routing Settings > Inbound/Outbound > IP Groups Settings > Inbound/Outbound > Non-Delivery Options
Smart Host Routing	Settings > Inbound/Outbound > Encryption Main > Policy Management > Policies Main > Policy Management > Filters Main > Policy Management > Actions

Websense Email Security setting	TRITON AP-EMAIL module location
Requeuing Scheme	Settings > Inbound/Outbound > Non-Delivery Options
Domain Substitution	Settings > Inbound/Outbound > Address Rewriting
Logging	Main > Status > Logs Main > Status > Real-Time Monitor
Administrator Alerts	Settings > Alerts > Enable Alerts Settings > Alerts > Alert Events
Message Administrator	Main > Message Management > Message Queues Main > Message Management > Blocked Messages Main > Message Management > Delayed Messages Main > Status > Logs Main > Status > Real-Time Monitor
True Source IP	Settings > Inbound/Outbound > True Source IP
Administration Service	Settings > General > System Settings Settings > Administrators > Delegated Administrators Note: Administrator accounts are created in TRITON Manager settings. A Super Administrator can manage those created accounts in the Delegated Administrators page.
Accounts	TRITON Manager settings Settings > Administrators > Delegated Administrators Settings > Administrators > Roles
Certificate Management	Settings > Inbound/Outbound > TLS Certificate Settings > Personal Email > SSL Certificate
Dictionary Management	Main > Policy Management > Filters > Add custom content filter In the Data module: Main > Policy Management > DLP Policies > Create custom policy
Monitor	Main > Status > Real-Time Monitor

Websense Email Security setting	TRITON AP-EMAIL module location
Scheduler	For database downloads: Settings > General > Database Downloads For database maintenance tasks: Settings > Reporting > Log Database
Database Management	Settings > Reporting > Log Database Settings > Reporting > Log Server Settings > Reporting > Preferences
Virtual Learning Agent	In the Data module: Main > Policy Management > Content Classifiers > Machine Learning
Personal Email Manager	Settings > Personal Email > Notification Message Settings > Personal Email > User Accounts Settings > Personal Email > End-user Portal Settings > Personal Email > SSL Certificate
Report Central	Settings > Reporting > Preferences Main > Status > Presentation Reports

