websense

Websense Email Security Transition Guide

Websense® Email Security Gateway

v7.6

10240 Sorrento Valley Rd., San Diego, CA 92121, USA

R140611760

Published August 2011
Printed in the United States of America and Ireland.

Every effort has been made to ensure the accuracy of this manual. However, Websense Inc., makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. Websense Inc. shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or the examples herein. The information in this documentation is subject to change without notice.

Contents

1 Introduction

Websense® Email Security Gateway Anywhere is the next generation of email security that provides maximum protection against spam and viruses, and more sophisticated modern threats.

Unlike other email security solutions that rely exclusively on antispam, antivirus, reputation analysis, and URL filtering, Email Security Gateway combines these features with world-class Web analytics to protect against blended attacks. This Web-based application even offers market-leading, enterprise-class Data Loss Prevention (DLP) technology to accurately detect confidential data loss that goes through email. And it's all tied together in the first unified management console for email, Web, and data security across on-premises and in-the-cloud platforms.

Email Security Gateway Anywhere is a variation of Email Security Gateway that also integrates with the Websense hybrid service, blending the benefits of on-premises and in-the-cloud security by filtering spam and viruses before they reach your organization.

In addition to Email Security Gateway, Websense has 2 other email security solutions: SurfControl RiskFilter and Websense Email Security. This guide is designed for users of Websense Email Security who are considering making the transition to Email Security Gateway or Email Security Gateway Anywhere. It provides guidance and is intended to make the transition between the products easier.

In it, you will:

- Learn key concepts, such as the differences between the products'
  - *System architecture*
  - *Log and report system*
  - *Message management*
  - *Policies, filters, actions, and rules*, and more.
- Learn how to *Make the Move* to Email Security Gateway or Email Security Gateway Anywhere.

✓ **Note**

Unless otherwise noted, all material in this guide pertains to both Email Security Gateway and Email Security Gateway Anywhere.

2 Key Concepts

Email Security Gateway is a functional replacement for Websense Email Security. However, some fundamental differences between these products need to be considered when planning a transition project, including the following:

- Differences in the *System architecture* and *Components*
- Differences in managing *Administration, licensing, and accounts*
- Differences in managing *Policies, filters, actions, and rules*
- Enhancements to the *Log and report system*
- Enhancements to the filter technology
- Ability to *Integrate the hybrid service*
- *Data Security integration*

System architecture

Email Security Gateway is an integrated module of Websense® TRITON Enterprise - a unified content security solution that lets you manage Web Security, Data Security, and Email Security from the same management console. As a TRITON module, Email Security Gateway communicates directly with the server. It operates on a Websense V-Series appliance (V10000 G2 or V5000 G2) and the Email Security management component is installed on a separate Windows machine. Email Security Gateway also requires an installation of Microsoft SQL Server. The back-end of Email Security Gateway is based on Linux, the front-end is based on Java, and the log database is based on Windows Server.

There are 2 administrator interfaces in Email Security Gateway:

- **TRITON - Email Security** - for functional and configuration management
- **Appliance Manager -** for hardware-related management (such as CPU, memory and disk usage)

Being part of a multi-function system, Email Security Gateway consists of appliance and management components. The appliance can be configured as dual mode (Email Security Gateway and Websense Web Security) or Email Security Gateway only.

The TRITON management server can host the TRITON infrastructure, the TRITON Unified Security Center (Email Security and Data Security modules enabled, Web

Security module optional), and the Email Security Log Server. Log Database can reside on a separate Microsoft SQL Server box.

Websense Email Security on the other hand is a stand-alone, software-based product. Since it is a platform native tool, it communicates with the administrator Web service. The front-end and back-end are both installed on Windows Server.

Administration, licensing, and accounts

Administrator accounts work differently in Email Security Gateway than in Websense Email Security. Because Email Security Gateway is a part of the TRITON architecture, the administrator account management is unified across all TRITON modules (Web, email, data). You must, however, have an Email Security Gateway subscription for the unified administrator to access this module. In addition, Websense Email Security Gateway has a role called Network Account that lets you can add one or more administrators from the LDAP user directory.

In Email Security Gateway there are 4 levels of administrator privileges, and each administrator level has predefined permissions that cannot be edited:

- Super Administrator
- Reporting Administrator
- Quarantine Administrator
- Auditor

Administrators are created in the TRITON settings, and managed in the Email Security Gateway Administrator Accounts page, **Settings > General > Administrator Accounts**.

In Websense Email Security, there are 7 administration accounts, and each account has different permission levels:

- Rules administration
- Message administration
- System administration
- Dashboard administration
- User management
- Dashboard access
- Dictionary management

Components

TRITON - Email Security is displayed on a single, unified interface. It has similar core components as Websense Email Security:

- *Dashboard*
- *Rules administrator*
- *Message administrative functionality*

Dashboard

The Today and History dashboards display alert messages and graphical charts that show the current state of your email scanning software, focusing on email traffic activity in your network. The charts on this page cover the 24-hour period beginning at 12:01 a.m. according to the time set on the Log Database machine. The History page displays a 30-day summary of the same data.

To access the Dashboard service in Email Security Gateway, go to **Main** > **Status** > **Today** or **Main** > **Status** > **History**.

Rules administrator

The Websense Email Security Rules Administrator is comparable to the Email Security Gateway Policy Management function. You define the policies that are applied to specified sets of email senders and recipients. You can create multiple policies for different sets of users in your organization and apply different rules in each policy. Policy rules comprise the filters and the filter actions that determine how a message that matches a policy's sender/recipient conditions is handled.

To access rule and policy services, go to **Main** > **Policy Management**.

Message administrative functionality

To control and manage connections and messages in Email Security Gateway, you can configure message properties and settings either via the Receive/Send function, or Message Management function.

To access these settings:

Go to **Settings > Receive/Send** to configure message size, volume limits, and the number of connections Email Security Gateway accepts, and how many at a time.

Go to **Main > Message Management** to create and manage message queues for blocked and delayed email messages.

Database management

The Log Database is the repository where logs, rules, filters, and services are stored.

In Email Security Gateway you need to install an external log server and a log database on a Windows Server. The main database, **esglogdb76**, stores all the log information. You can also configure the main database to create partitions. Database partitions provide flexibility and performance advantages.

Websense Email Security requires access to SQL Server. You can use an instance of SQL Server on a different machine; or you can install Microsoft SQL Server either on the same server where Websense Email Security is installed, or on a separate, dedicated server.

Message management

Mail flow

Mail flow refers to the flow of inbound and outbound email messages in an organization.

Email Security Gateway monitors the flow of email messages in real time, and has a Message Log where you can view records of inbound messages (**Main > Status > Logs**). Email Security Gateway defines mail flow based on mail direction. The mail direction is based on the sender and recipient’s message address.

- **Inbound** - The sender address is not from a protected domain, and the recipient address is in a protected domain.
- **Outbound** - The sender address is from a protected domain and the recipient address is not in a protected domain.
- **Internal** - Both the sender and recipient addresses are in a protected domain.

Mail routing

Mail routing is the process of directing an email message to a recipient's host where inbound email messages can be sorted based on the recipient’s domain name.

Domain-based routing uses the recipient's email domain to make a routing decision. It can use either a DNS or SMTP IP address or host name (Smart Host) for next hop. Domain-based routing includes the default domain route which cannot be deleted and is used for routing all domains that are not protected.

Quarantined messages

Messages can be isolated (quarantined) instead of dropped so that administrators and end users can decide what to do with them.

In Email Security Gateway, sensitive messages can be stored either in local or remote queue storage in the quarantine system. You can use predefined default queues or create custom queues.

For queue management, go to **Main** > **Message Management** > **Blocked Messages**.

Policies, filters, actions, and rules

Policies

Policies tell Websense software how and when to filter inbound and outbound email messages.

In TRITON - Email Security you define policies that apply to specific sender/recipient groups. You then specify the rule (the filter and action pair) that determines how a message that matches a sender/recipient condition is scanned and ultimately handled.

Policies are a reflection of mail flow split, and in Email Security Gateway there are 3 policies, one for each mail direction: inbound, outbound, and internal.

Policy order is important in Email Security Gateway. You can specify policy order only for user-created policies. Default policies are always applied last, and you cannot change their order. If one policy is matched, then the rest are skipped. You can assign a maximum of 32 filters per policy.

✓ **Note**

When a policy is created, it contains the default rules. Default rules can only be edited but not deleted.

Websense Email Security, on the other hand, lets you define rules instead of policies. It has a graphical drag-and-drop tool that lets you create a rule to check mail. All rules are stored in the configuration database.

To create your own policies in Email Security Gateway, go to **Main** > **Policy Management** > **Policies**.

Filters

An email filter defines what Email Security Gateway is scanning for (virus or spam). A filter action determines the final disposition of a message that triggers the filter (deliver, drop, or isolate).

Email filters apply actions (permit, restrict, or block) to inbound or outbound email messages.

There are 3 default filters in Email Security Gateway:

- Antivirus filter (on by default)
- Antispam filter (on by default)
- Disclaimer filter (off by default)

Email Security Gateway uses the concepts of filters, actions, and rules to define the scanning logic.

- **Filter** is an object that defines the scanning logic. Email Security Gateway has 3 predefined default filter types: antivirus, antispam, and disclaimer. You can create new filters based on 3 filter types.
- **Action** is an object that defines what Email Security Gateway should do if a filter is matched. There are 2 default actions, and you can also create new actions.
- **Rules** link the filter and action to the policy so that the filter and action can take effect. Three rules are predefined for each policy to apply 3 type of filters. You cannot create new rules or remove the predefined rules, but you can disable and enable these rules.

Antispam filter

A variety of antispam tools are available in Email Security Gateway to let you filter spam more effectively. Email Security Gateway uses a combination of 4 antispam filters, and the scans are performed in the following order:

1. URL scanning
2. Digital Fingerprinting scanning
3. LexiRules scanning
4. Heuristics scanning

✓ **Note**

These scans may not be performed if hybrid service has already scanned the email and sent its “spam score” to Email Security Gateway.

Below are the key differences in antispam filter technology between Email Security Gateway and Websense Email Security:

- **Scanning order -** In Websense Email Security, the order of the scanning is flexible and customizable. In Email Security Gateway, it is fixed.

- **URL scanning -** When performing a URL scan, Email Security Gateway needs to connect to a remote Websense Web Security server for the URL categorization. Websense Email Security does not need to connect to a server and uses local implementation instead. There are also slight differences in the category names due to the use of different scanning engines.
- **Digital Fingerprinting scanning** – In Email Security Gateway, digital fingerprinting scans include all spam categories. In Websense Email Security, you can customize category selections.
- **Heuristics scanning** – Email Security Gateway does not have a Header-only mode. In Websense Email Security, you can set the scanning level to header only (scans the header only), or to full scan (scans the header and message body).

Antivirus filter

The antivirus filter in Email Security Gateway is a Websense-enhanced Authentium engine that handles Internet-related threats more effectively.

The Antivirus filter in Websense Email Security uses either McAfee or the original Authentium engine.

Scheduler

The scheduler is a mechanism that lets you schedule events for regular activities (such as database maintenance and reporting activities).

In Email Security Gateway, you configure database maintenance and database downloads in 2 different locations.

- For database download scheduling, use the **Settings > General > Database Downloads** page.
- For database maintenance tasks, go to **Settings > Reporting > Log Database**.

In Websense Email Security, all database maintenance and download scheduling tasks are configured in 1 place: **Start > Programs (or All Programs) > Websense Email Security > Scheduler**.

Log and report system

In Email Security Gateway, the log and reporting systems are message-driven rather than event-driven.

In a message-driven environment, the scanned results of messages (clean or spam), and delivery status (delivered or deferred) are written to the Message Log rather than in separate logs. A message with multiple recipients has only 1 log entry, which contains the scan result and delivery status of each recipient. Only when the message has been delivered to all recipients is the overall message delivery status Delivered.

In an event-driven environment, as in Websense Email Security, separate logs are created for each message state. If a message has multiple recipients, it has multiple message logs.

Logging

In Email Security Gateway, the service logging data is stored in the database. The database and scheduler logging data is stored in Windows event log. This differs from Websense Email Security where the service logging data is stored in the database, log file, and Windows event log.

In addition to the Message Log, mentioned previously, Email Security Gateway has the following 3 logs:

- **Audit** - is for changes to Email Security Gateway policies and settings
- **System** - is for recording system events
- **Console** - is for recording TRITON Console events

To access the Message Log in Email Security Gateway, go to **Main** > **Status** > **Logs** and view the Message tab.

Reporting

Mirroring the Websense Web Security reporting solution, Email Security Gateway generates presentation reports of email traffic and system activities. The presentation reporting function loads report data directly from the Email Security Gateway log database. The Email Security Gateway reporting system provides a summary of the overall message, spam and virus, message transfer, and system capacity. The reporting function also provides data for the charts on the Today and History pages.

To access the reporting system in Email Security Gateway, go to **Main** > **Status** > **Presentation Reports**.

Websense Email Security uses Report Central as a subsystem to generate and present reports. Report Central copies the log database from Websense Email Security and uses that copy to generate reports. All reports are based on the private database.

Historical reports

Email archiving is a common compliance requirement for many companies. Email Security Gateway does not support importing historical data from Websense Email Security. Therefore, to access historical reports generated within the old system, you'll need to keep the legacy system running. Both the database and the report generator of the previous Websense email system need to be maintained.

For report generation purposes, the recommended length of time to maintain the legacy system should be equal to the length of time defined in the email retention policy. This way, if you need to generate a report from archived email messages, you can still use the old reporting system.

Websense Email Security uses Report Central to create activity reports. To access historical reports generated within this system, you should maintain both the Websense Email Security software and the Report Central reporting tool.

For full instructions on how to generate reports in Report Central, refer to the Report Central Administrator's Guide.

Data Security integration

Data Security analyzes email content and provides content filtering to prevent sensitive data from leaving the organization. It filters all content outside of antispam and antivirus scanning.

Email Security Gateway is tightly integrated with Websense Data Security and requires the TRITON - Data Security manager to operate. It does not require a separate Data Security subscription, and leverages Data Security rules, dictionary, fingerprinting, and filter technology.

The Data Loss Prevention (DLP) policies in Email Security Gateway are enabled by default, and you can apply a number of filters to them, such as message size, attachment name, attachment type, acceptable use, and number of attachments.

Registration with the Data Security server is automatic if you add an appliance to the TRITON Unified Security Center from the Email Security Gateway interface. Otherwise you need to manually register with Data Security through **Settings > General > Data Security**. After you register with the Data Security management server, you need to click the **Data Security** tab and then click **Deploy** to deploy Data Security policies on Email Security Gateway. For more information about Data Security registration, see Data Security registration information.

On the other hand, with Websense Email Security, you have to manually install a Data Security component (an agent) on the SMTP server, and manually register it with Data Security.

Data Loss Prevention (DLP)

TRITON - Data Security has its own policy framework, which incorporates email policies, Web policies, and other DLP policies.

The Data Security acceptable use and data loss prevention policies are defined in the TRITON - Data Security module. You can configure custom policies or rules, or apply granular controls to users and groups using the Data Security Rule Wizard. Messages in violation of the email DLP policy are quarantined on the TRITON management machine instead of the Email Security Gateway appliance.

To customize DLP policies for Email Security, you must first enable DLP policies in the TRITON - Email Security module.

To enable DLP policies in Email Security Gateway, go to **Main > Policy Management > Policies (for Inbound, Outbound, and Internal)**.

To configure DLP policies, switch to the Data Security module, then select **Main > Policy Management > DLP Policies > Email DLP Policy**.

For more information on how to configure Email Data Loss Prevention Policy, refer to the Data Security Help section Configuring the Email Data Loss Prevention Policy. or refer to the Quick Email DLP document.

Domain group and IP group

The concept of domain group and IP group are new in Email Security Gateway. These groups are common objects that can be used in several locations in Email Security Gateway. A collection of domain names or IP addresses can be defined in a single group.

For example, you can define a domain group to establish domain-based delivery options, or you can define an IP address group for which Reputation Service, Real-time Blacklist (RBL), or directory attack prevention scans are not performed.

You may create or delete a domain or IP address group. The default groups (Protected Domain, Trusted IP Addresses, and Encryption Gateway) cannot be deleted. Most of the Email Security Gateway configurations are for the whole domain group or IP group, or individual domains or IP addresses.

To configure groups in Email Security Gateway, go to **Settings > General > Domain Groups,** or **Settings > General > IP Groups**.

Personal Email Manager

For Websense Email Security, Personal Email Manager is an optional facility for end users to manage their blocked messages. The component needs to be launched separately. The tool includes a My Junk Email page for managing blocked messages. It lets end users maintain personal Always Allowed and Always Deleted lists.

In Email Security Gateway, personal email management is integrated and the interface is hosted in the appliance address (on the V10000 G2 and V5000 G2, it is port 9449 by default). By default, it is enabled, but notification message contents and end user authorization for maintaining block and permit lists must be set by the administrator in the **Settings > Personal Email** pages.

3 Make the Move

There are several steps involved when making the transition from Websense Email Security to Email Security Gateway.

This section provides instructions that will help you make a smooth transition to Email Security. It includes the following topics:

1. What you need to do *Before you begin* the transition
2. How to *Install Email Security Gateway*
3. How to *Get started with Email Security Gateway*

Before you begin

Before you make the transition to the Email Security Gateway system, Websense recommends you perform the following steps:

1. *Meet the system requirements*

   Check that your system (network, hardware, software, server, and other elements) meets the minimum hardware and operating system requirements for Email Security Gateway.

2. *Back up your existing system*

   To safeguard your system while you prepare your Email Security Gateway deployment, back up your existing email system. You will continue to run your existing system in production while you set up and test the new system.

3. *Archive log database*

   You cannot migrate existing email logs from Websense Email Security to Email Security Gateway. If you want to retain records from your existing system, you can archive your existing email logs.

4. *Determine existing settings*

   There are several settings you must configure manually when you make the transition to Email Security Gateway, such as mail relays, block lists, routing, and SMTP properties. To simplify this manual process, print your existing settings.

Meet the system requirements

To successfully deploy Email Security Gateway, you need to ensure your system meets the minimum requirements so that it operates effectively.

Refer to the Deployment and Installation Center for details on the system resources required to support your deployment.

Back up your existing system

Before you transition to Email Security Gateway, you should back up the configuration settings of your existing email system so that you can replicate the same settings on another server.

To back up the system settings in Websense Email Security:

1. From the Database Tools menu, select **Configuration Database Management**. The Configuration Database wizard opens.
2. Select **Backup database to a file**. The SQL/MSDE Server details screen displays.
3. Specify the location of the server that contains the database to be backed up.
   - To connect to the server through a trusted connection, select the **Use trusted connection** check box.
   - To connect to the server using the username and password you specify, clear the **Use trusted connection** check box and enter the username and password.
4. Click **Next**. The Configuration Database Backup Details dialog box displays.
5. Select the database from the drop-down list. Default = STEMConfig
6. Enter or browse to the location of the file where the database is to be saved. Default = Program files\Websense Email Security\Database\STEMConfig_<date>.bak
7. Click **Next**. A summary of your options displays.
8. If you need to change any details, click **Back**. If the options are correct, click **Next**.
9. A progress bar displays. A confirmation screen displays when the backup is complete. Click **Finish**.

Archive log database

You can archive log databases to retain a record of your log data since you cannot migrate existing log information to Email Security Gateway.

To archive the log database to a file in Websense Email Security:

1. From the Database Tools menu, select **Log Database**. The Database wizard opens.

2. Select **Archive the log database to a file** and click **Next**. The MSDE/SQL Server Details screen displays.
3. From the **Server** drop-down list, select the server that contains the log database.
4. Connect to the server using either:
   - A trusted connection
   - A username and password you supply
5. Click **Next**.
6. Select the log database to archive.
7. Browse to the location where you want the archive file to be stored and click **Next**. A summary of your options displays.
   - If the options are correct, click **Next**.
   - If you need to change any details, click **Back**.
8. A confirmation screen displays when the log database has been successfully archived. Click **Finish**.

Determine existing settings

Websense recommends that you manually configure your email security settings in the Email Security Gateway environment, because the default settings may not be the same as they were in Websense Email Security. You should capture existing configuration settings before you make the move to Email Security Gateway.

Refer to Appendix*: Configuration Settings* to see the list of configured settings in Websense Email Security, and their corresponding locations in Email Security Gateway.

Install Email Security Gateway

You can install Email Security Gateway on a Websense V-Series appliance (V5000 G2 or V10000 G2).

Installation instructions for both appliances are described in the Deployment and Installation Center.

- Email Security Gateway Installation (V5000 G2)
- Email Security Gateway installation (V10000 G2)

In addition, you also need to install the TRITON management server and the SQL Server.

- Creating TRITON management server
- Obtaining SQL Server

Get started with Email Security Gateway

1. *Configure new settings*

   To prepare Email Security Gateway for use, you must enter the TRITON – Email Security user interface and configure basic settings. When you open Email Security Gateway for the first time, the Configuration Wizard can help you configure some initial settings.

2. *Migrate existing settings*

   This section includes a list of recommended migration settings that you should reconfigure as part of the transition process.

3. *Integrate the hybrid service*

   Applies only to Email Security Gateway Anywhere. With the proper subscription, you can configure Email Security Gateway to use the Websense hybrid email service, so spam can be filtered in the cloud before it reaches your organization.

4. *Enable or disable policies*

   When you first install Email Security Gateway, the default policies are enabled to protect you against email threats. You can modify the default policies to suit your requirements.

5. *Create custom policies*

   Creating new policies can add flexibility in controlling how messages are filtered and executed. You can define your own rules and policy execution order, and apply these custom policies to specific groups according to your requirements.

6. *Create custom filters*

   You can create custom filters and control the filtering sensitivity levels to suit your requirements. Custom filters can be created based on 1 of the existing predefined filter types: spam, virus, and disclaimer.

7. *Generate reports*

   Reports provide a graphical representation of statistical data captured by Email Security Gateway. As an indicator of good policy implementation, you can capture statistical data about incoming and outgoing messages, spam and virus activities, system capacity, and information about Data Security policies and users. You can also get reports of hybrid service activity.

8. *Test that your email system works*

   Testing the email system is an important step to ensure your email security system is correctly configured to protect your network from spam and viruses.

Configure new settings

You need to assess whether default settings in Email Security Gateway need to be reconfigured so that the settings are consistent with the previous email system, and the transition to Email Security Gateway is steady.

To configure the new settings in Email Security Gateway:

1. If this is your first time using Email Security Gateway, then the Configuration Wizard appears. The Configuration Wizard is available only the first time you open Email Security Gateway, and it can help guide you through configuring some initial settings.
2. Ensure you have captured your existing settings. Refer to Appendix*: Configuration Settings* to see the list of configured settings in Websense Email Security, and their corresponding location in Email Security Gateway.
3. Determine the settings to be modified and then configure them manually. Use the table in the Appendix: *Configuration Settings*, page 53 as a guide to help you locate and configure settings in the new environment.

   For example, if you wish to update the Routing information (**Send Service > Routing**), then you would go to **Settings > Receive/Send > Mail Routing** in Email Security Gateway to configure the settings.

Migrate existing settings

It is recommended that you record data about certain settings. As you proceed with the transition process, you will need to re-enter these settings so you are properly protected against email threats. The following section lists settings that should be reconfigured in Email Security Gateway.

- Mail Relay
- Routing
- User Directories

  In Websense Email Security, this information is found in LDAP Connections, (under Directory Harvest Detection).
- User Authentication

  Websense Email Security uses Directory Harvest Detection to validate users.
- Personal Email Manager
- Queue Management

Note

In Websense Email Security, the **User Directories** and **User Authentication** details are found in Directory Harvest Detection (DHD). DHD uses Lightweight Directory Access Protocol (LDAP) to check the validity of email addresses and domains

To find out where to access these settings in Websense Email Security and in Email Security Gateway, refer to the table *Mapped settings in Websense Email Security*, page 53.

Integrate the hybrid service

This section applies only to customers with an Email Security Gateway Anywhere subscription.

Email Security Gateway Anywhere deployments include a hybrid service. The hybrid service lets you integrate on-premises Email Security Gateway with Websense in-the-cloud email filtering. Hybrid service detects infected email traffic before it reaches the on-premises infrastructure, thereby reducing considerable load from the Email Security Gateway internal systems.

Using the hybrid service is optional in Email Security Gateway and is not enabled by default. To enable the hybrid service, you need to register for the hybrid service and then activate it.

To integrate the hybrid service, follow these steps:

1. *Enter a valid subscription key*
2. *Open firewall ports*
3. *Activate the hybrid service*
4. *Enable or disable the hybrid service*

See the TRITON - Email Security Help section, "Registering for the hybrid service" for detailed instructions on how to configure the email hybrid service.

Enter a valid subscription key

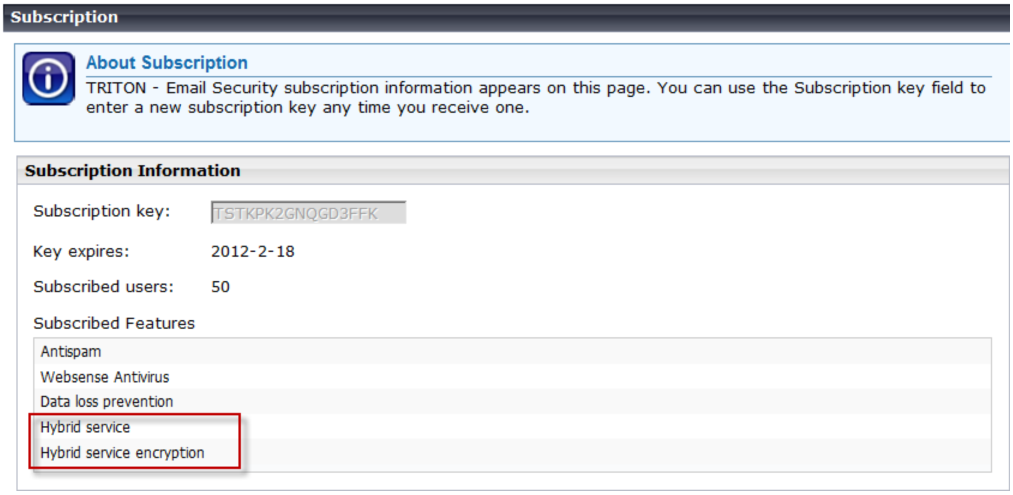
Ensure you have entered a valid Email Security Gateway Anywhere subscription key. This subscription key allows you to configure the hybrid service. You obtain the subscription key when you purchase TRITON - Email Security.

An Email Security Gateway Anywhere key includes the hybrid service and hybrid service encryption. If you want to use hybrid service encryption, be sure the encryption option is included in your subscription to the email hybrid service. The hybrid service lets you use hybrid filtering for inbound messages. The hybrid service encryption license gives you the added functionality to encrypt outbound messages.

If you did not enter the subscription key the first time you opened Email Security Gateway, you can follow these steps to enter the key:

1. Select **Settings** > **General** > **Subscription**.
2. Enter a subscription key in the **Subscription Information** panel and then click **OK**.

Depending on your Email Security Gateway Anywhere license, the Subscription Information panel (**Settings > General > Subscription Information**) displays the features included in your subscription.



Subscription

About Subscription

TRITON - Email Security subscription information appears on this page. You can use the Subscription key field to enter a new subscription key any time you receive one.

Subscription Information

Subscription key: TSTKPK2GNQGD3FFK

Key expires: 2012-2-18

Subscribed users: 50

Subscribed Features

Antispam

Websense Antivirus

Data loss prevention

Hybrid service

Hybrid service encryption

Open firewall ports

You should configure firewall ports so that Email Security Gateway can successfully connect to the server to send and receive messages.

By default, some ports used by Email Security Gateway are blocked by the firewall application, and attempts to connect to Email Security Gateway fail. You need to open the ports so that the firewall can bypass the connection limitation to allow incoming and outgoing traffic to Email Security Gateway.

- For outbound traffic, you need to open the following ports in your firewall: 25, 53, 80, and 443.
- For inbound traffic you need to open port 25.

For instructions on how to configure the firewall ports, refer to the Help file in the firewall application you are using.

Activate the hybrid service

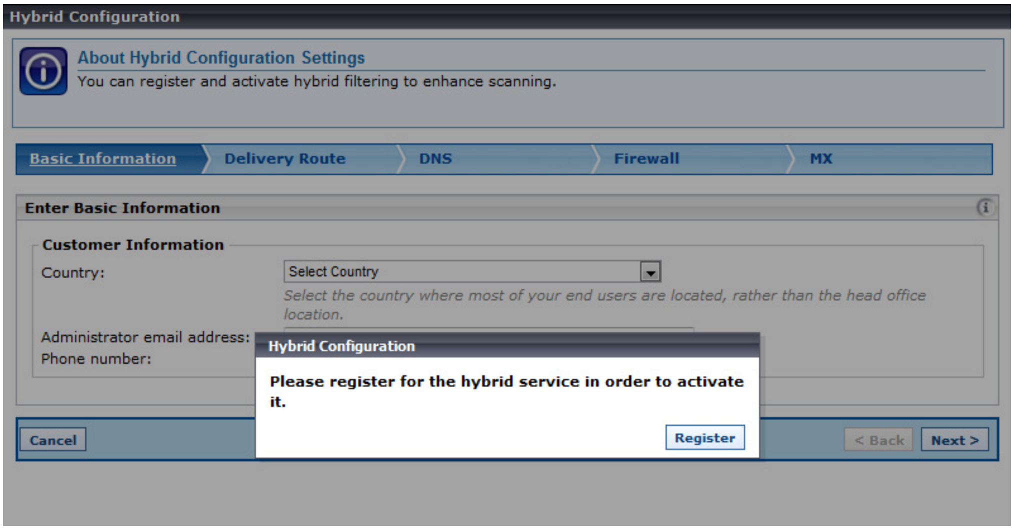
You need to perform 5 main steps to activate your hybrid service account:

1. *Enter your Basic Information*
2. *Define a Delivery Route*
3. *Configure your DNS*
4. *Configure your firewall*
5. *Configure your MX records*

To begin the activation process, follow these steps:

1. Select **Settings** > **General** > **Hybrid Configuration**.

   If you have successfully entered a valid subscription key, a dialog appears prompting you to register for the hybrid service. This dialog appears only when you set up your hybrid account for the first time.



You can register and activate hybrid filtering to enhance scanning.

Select the country where most of your end users are located, rather than the head office location.

Please register for the hybrid service in order to activate it.

2. Click **Register** to start the activation process.

Enter your Basic Information

1. On the **Basic Information** page, enter some basic personal information.
   - **Country** – Select your country where most of the end-users are located. The country you select also provides the system with time zone information.
   - **Administrator email address** – Specify a legitimate email address. The token and password information are sent to this address so it's important to specify a valid email address.
   - **Phone number** – Enter a valid phone number.
2. Click **Next** to continue.

Define a Delivery Route

1. On the **Delivery Route** page, click **Add** to define a route.
2. Specify a delivery route.
    a. Enter a descriptive **Delivery route name**.
    b. Under **Protected Domains,** enter the domain name that you want to protect in the **Domain Address** field.
    c. Specify whether the delivery route should apply to all subdomains in the domain.
    d. To add multiple domains, click **Add** to define a domain name, and specify whether a subdomain is applied.

> ✓ **Note**
>
> When specifying a **Protected Domain**, you must also add it to the Protected Domain Groups list (**Settings > General > Domain Groups)**, otherwise the registration will fail.

3. Click **Add** to define an **SMTP Inbound Server Address** so that you can securely receive messages from hybrid service.
    a. Enter the IP address or name of your Email Security Gateway server. This must be the external IP address or name, visible from outside your network.
    b. To add more servers, click **Add** again.
4. Click **Add** to define an **SMTP Outbound Server Address** so that you can securely encrypt outgoing messages.

> ✓ **Note**
>
> You are required to define the **SMTP Outbound Server Address** if you have a hybrid service encryption license. This step is not required for a hybrid service license without encryption.

    a. Enter the IP address or name of your Email Security Gateway server. This must be the external IP address or name, visible from outside your network.
    b. To add more servers, click **Add** again.

> ✓ **Note**
>
> If a security device (such as a firewall) sits in front of Email Security Gateway, then you must enter the external IP address of the device when defining the inbound or outbound SMTP Server Address.

5. Click **Next** to continue.

Configure your DNS

To configure your Domain Name System (DNS) server, you must create a CNAME record for each domain in your DNS so that Email Security Gateway can verify that you have ownership of the protected domain(s).

Use the Alias and Associated domain information on the DNS page to create a CNAME record. The CNAME is created by your DNS manager - usually your Internet Service Provider (ISP). Contact your DNS manager and ask them to set up a CNAME record for each of your protected domains.

Once you have obtained a CNAME record, click **Next** to continue.

Configure your firewall

The Firewall page shows IP addresses that should be allowed to pass through the firewall. Check your firewall settings to ensure access requests from these addresses are allowed.

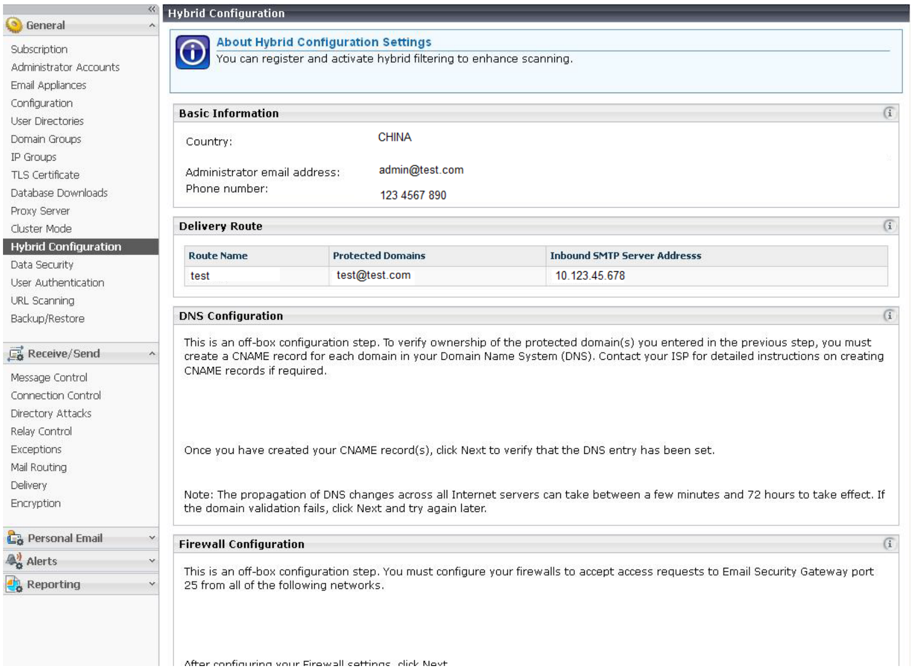
Configure your MX records

An MX record is an entry in a DNS database that defines the host willing to accept mail for a given machine. Your MX records must route inbound email through the hybrid service to Email Security Gateway.

Your MX records, which end in in.mailcontrol.com, are listed on the MX page. Contact your DNS manager (usually your Internet service provider) and ask them to set up or replace your current MX records for each protected domain you have specified with the customer-specific records on the MX page.

Click **Finish** to complete your hybrid configuration.

After you have successfully activated the hybrid service, a page displays showing the summary of your hybrid service configuration settings.



Hybrid Configuration

About Hybrid Configuration Settings

You can register and activate hybrid filtering to enhance scanning.

Basic Information

Country: CHINA

Administrator email address: admin@test.com

Phone number: 123 4567 890

Delivery Route

Route Name	Protected Domains	Inbound SMTP Server Addresss
test	test@test.com	10.123.45.678

DNS Configuration

This is an off-box configuration step. To verify ownership of the protected domain(s) you entered in the previous step, you must create a CNAME record for each domain in your Domain Name System (DNS). Contact your ISP for detailed instructions on creating CNAME records if required.

Once you have created your CNAME record(s), click Next to verify that the DNS entry has been set.

Note: The propagation of DNS changes across all Internet servers can take between a few minutes and 72 hours to take effect. If the domain validation fails, click Next and try again later.

Firewall Configuration

This is an off-box configuration step. You must configure your firewalls to accept access requests to Email Security Gateway port 25 from all of the following networks.

After configuring your Firewall settings, click Next

Enable or disable the hybrid service

Once the hybrid service is successfully activated, it is enabled by default. You can choose to disable the hybrid service at any time.

✓ **Note**

The encryption option is available only if you have the hybrid service encryption license.

To activate or deactivate hybrid service filtering:

1. Select **Main > Policy Management > Filters**.
2. Under **Filters**, select (to enable) or clear (to disable) the **Use hybrid service scanning results** check box.

To activate or deactivate hybrid service encryption:

1. Select **Settings > Receive/Send > Encryption**.
2. Under **Encryption Options**, select (to enable) or deselect (to disable) **Hybrid service** and then click **OK**.

Enable or disable policies

Email Security Gateway has 3 types of policies, depending on the mail flow of the messages—inbound, outbound, or internal. For each email direction, there is 1 predefined default policy. There is also a default Data Security policy for each direction.

By default, predefined policies in Email Security Gateway and default Data Security policies are enabled. You cannot change the order of, or delete default policies (which are always applied last), but you can enable or disable them.

To enable or disable policies:

1. Select **Main** > **Policy Management** > **Policies**.
2. Click the policy you want to modify.
3. For the Status, select either the **Enabled** or **Disabled** option and then click **OK**.

> **Important**
>
> Data Security policies can only be enabled or disabled in Email Security Gateway. If you want to use the email DLP policies, you need to configure them in the Data Security module of TRITON Unified Security Center. See the TRITON - Data Security Help section, "Configuring the Email DLP Policy" for more information.

> **Tip**
>
> To protect yourself from email threats, you should make sure the spam and antivirus policies are enabled (default status).

Create custom policies

Policies tell Websense software how and when to filter inbound and outbound email messages.

To create your own inbound, outbound, or internal policy in Email Security Gateway:

1. Select **Main** > **Policy Management** > **Policies**.
2. Click **Add** to open the Add Policy page and enter a unique Policy name. The policy name must be between 4 and 50 characters long. Use of the following special characters in the policy name is not recommended:

   < > { } ~ ! $ % & @ # . " | \ & + = ? / ; : ,

   Policy names can include spaces, dashes, and apostrophes.
3. Enter a clear and concise **Description** of the policy.

   The special character recommendations that apply to policy names also apply to descriptions.

4. Define the order in which this policy is applied in the **Order** field.

   By default the new policy is placed at the top of the list. You cannot have multiple policies with the same order number. If you select a number that is already in use, the policy that currently has that number and all those below it move down 1 place in the list.

5. Define 1 or more **Sender/Recipient Conditions**.

   By default, each new policy contains 1 sender/recipient condition that applies the policy to all email senders and recipients. Click **Add** to configure additional sender/recipient conditions

6. Edit the available **Rules** to tailor the filters and actions to this policy. Click a rule name to edit its properties.
7. Click **OK** to save your policy.

Create custom filters

You can create custom filters in Email Security Gateway, but they need to be based on 1 of the existing 3 predefined default filter types: spam, virus, or disclaimer.

To create a custom filter:

1. Select **Main** > **Policy Management** > **Filters**.
2. Click **Add**.
3. Set the properties of your new filter.
   a. Type a **Filter name**.
   b. Add a **Description** about the filter.
   c. Select the **Filter Type** you want to use. The filter type you choose determines the filter settings you can configure.
4. Click **OK**.

For more information on how to create custom filters, refer to the TRITON - Email Security Help section “Working with Filters and Policies”.

> **Note**
>
> To retain custom filters or rules created in Websense Email Security, you need to migrate them as a policy or rule to Data Security and then manage them from there.
>
> For instructions on how to migrate custom filters or rules, refer to *Add custom rules to a policy*, page 35.
>
> For more information on managing policies in Data Security, refer to the TRITON - Data Security Help section “Policies Overview”.

Generate reports

You can use templates from the Report Catalog to generate graphical charts and tabular reports based on the current database.

Note

If you want to generate a report from a database in a previous Websense email system, you need to run both the old and new email system in parallel. For further information about this, refer to the section *Historical reports*, page 8.

To generate a report in Email Security Gateway:

1. Select **Main > Status > Presentation Reports**.
2. From the Report Catalog, select the report you want to create and then click **Run** to open the Run Report dialog box.
3. Specify a **Report start date** and **Report end date** for the report.
4. Select a **Report output format** from the drop-down list.

Note

Ensure you have the appropriate software installed to support the format of the report to be generated. For example, to generate a PDF report, you need to have Adobe Reader v7.0 or later installed. To generate an XLS report, you need to have Microsoft Excel 2003 or later installed.

5. Specify how you want the report to be generated:
   - Select **Run the report in the background** (default) to have the report run immediately as a scheduled job. Optionally, you can provide an email address to receive a notification message when the report is complete or cannot be generated. (You can also monitor the job queue for report status.)

     If you run the report in the background, a copy of the completed report is automatically saved, and a link to the report appears on the Review Reports page.
   - Deselect **Run the report in the background** to have the report run in the foreground. In this case, the report is not scheduled, and does not appear on the Review Reports page.

     If you run the report in the foreground, the report is not automatically saved when you close the application used to view the report (Microsoft Excel, Adobe Reader, or a Web browser, for example). You must save the report manually.
6. Click **Run** to generate the report.

For additional instructions on working with reports, see the TRITON - Email Security Help section, Working with presentation reports.

Test that your email system works

After successfully configuring Email Security Gateway, it's important to test the functionality of the email system to ensure that policies are applied correctly so you are properly protected from spam and viruses.

You can perform the following steps to test that the email system functions correctly:

1. *Create a staging environment*
2. *Specify the server on which you want to test the email system*
3. *Create new user accounts*
4. *Test administrator privileges*
5. *Define always block and always permit lists*
6. *Perform tasks to test the email system*
7. *Test that the policies, rules, and alerts work correctly*

Create a staging environment

The staging environment acts as a mirror of the actual environment. You should create a staging environment so that you have a temporary location in which to test the email security system.

Choose 1 of the following options:

- **Create an internal domain**

  You can create an internal domain that lives within the company or within the lab (with its own DNS servers, Exchange server, and Active Directory). When creating an internal domain you need to put Email Security Gateway in the front to manage the email messages.

- **Register a new domain**

  If you register a new domain, ensure it includes MX records.

Specify the server on which you want to test the email system

You can choose to test the email system on a separate Exchange Server, or on the existing company server.

Create new user accounts

For best practice, set up an additional account in the existing email client that points to the test server.

Alternatively, you can create a new user account in the new domain.

Test administrator privileges

Set up multiple users with different permission levels to test whether administrator privileges in Email Security Gateway work.

Define always block and always permit lists

You cannot directly migrate existing lists of addresses that are always blocked or always permitted from another email security system into Email Security Gateway. This data needs to be entered manually.

1. Go to **Main** > **Policy Management** > **Always Block/Permit**
   - Click **Always Block** and add IP or email addresses that you would like to always block.
   - Click **Always Permit** and add IP or email addresses that you would like to always permit.
2. Click **OK**.

Perform tasks to test the email system

Write and send messages
Write messages that intentionally breach policy and then send them to the email address. For example, you may want to include content that contains spam or sensitive data.

Send attachments
Send email messages with attachments that include spam or virus content.

Confirm that the mail is flowing in the right direction
Check the transaction volume in Email Security Gateway.

Test that the policies, rules, and alerts work correctly

If you have correctly configured the system, Email Security Gateway should be able to properly detect and block infected messages based on policy conditions (standard Email Security policies and DLP policies).

Check the logs regularly

Go to the Today page (**Main** > **Status** > **Today**) to view the current state of the email system. This page should correctly reflect email traffic activities that have occurred within the past 24 hours.

Set up SNMP monitoring and alert

1. Go to **Settings** > **Alerts** > **Enable Alerts**.
2. In the SNMP Alerts section, select the **Enable SNMP alerts** check box.
3. Specify the **Community name** on your SNMP Trap server, the **Server IP or nam**e of the Trap server, and the **Port** number the message uses.

Set up a script

Set up a script to send email messages at predefined time intervals.

Check the filtering

If the policies are set up correctly, Email Security Gateway should properly detect and filter messages based on policy conditions.

- Check your inbox to see if legitimate email messages are correctly filtered.
- View the blocked messages to see if email messages are appropriately quarantined; go to **Main > Message Management > Blocked Messages.**

4 Policy migration samples

To ensure that you are properly protected against email threats, you should configure the policy settings in Websense Email Security Gateway so that email traffic can be properly and securely monitored.

The concept of creating a rule from separate, modular components, as in Websense Email Security, does not exist in Email Security Gateway. You create an Email Security Gateway 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.

✓ **Note**

For Data Security policies to be applied to email, ensure you are registered with the Data Security Management Server. In the Email Security module, select **Settings** > **General** > **Data Security**.

This chapter includes instructions for replicating some sample Websense Email Security rules in Email Security Gateway.

Block messages without sender's address

Some spam email messages are sent from senders who are able to conceal their email addresses; therefore these messages do not contain envelope sender information and appear to be sent without a sender's address. You can create a policy to quarantine inbound email messages whose envelope sender address is null.

- *Websense Email Security environment*, page 30
- *Email Security Gateway environment*, page 31

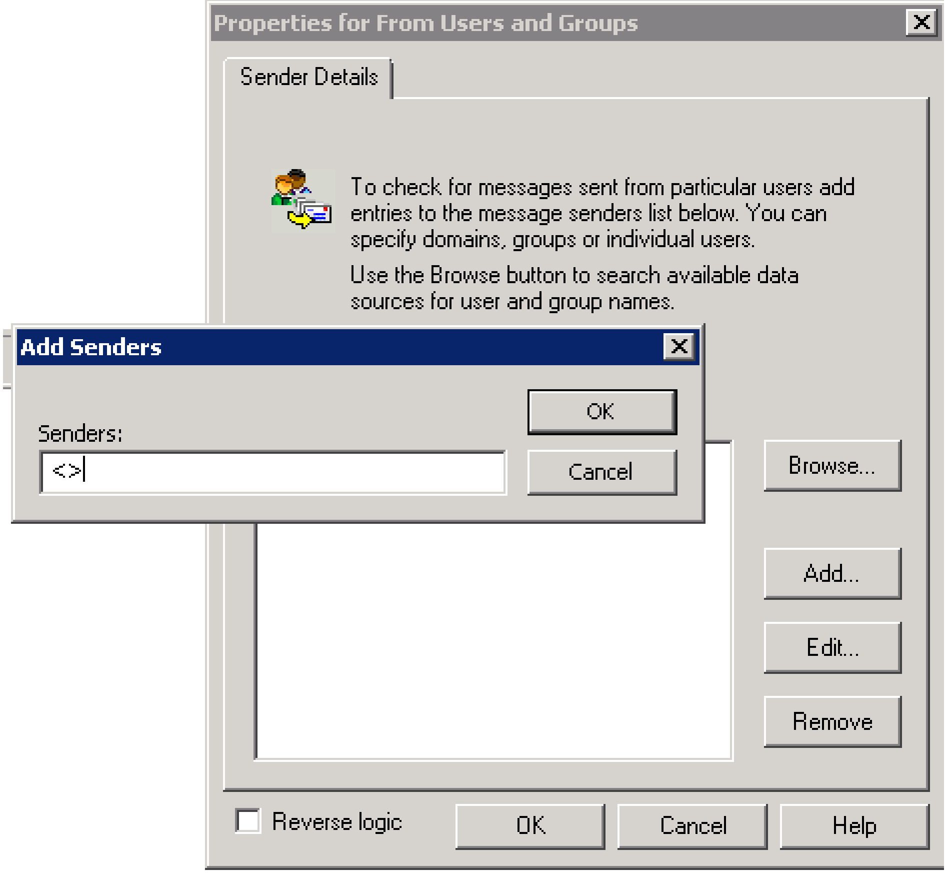
Websense Email Security environment

To create a rule in Websense Email Security that blocks messages without a sender's address, follow these steps:

1. In the Websense Email Security Rules Administrator module, create a new rule:
   a. Select **Rule** > **New Rule**.
   b. Enter the properties for the new rule.
2. Specify a sender.
   a. On the **Who** tab, drag and drop **From Users and Groups** to the Rules pallet.
   b. Click **Add** in the Properties page.

c. In the **Senders** field, type < > and then click **OK**.

Note
The empty < > indicates an empty sender's address.



Properties for From Users and Groups

Sender Details

To check for messages sent from particular users add entries to the message senders list below. You can specify domains, groups or individual users.

Use the Browse button to search available data sources for user and group names.

Add Senders

Senders: <>

3. Click **OK**.
4. On the **Actions** tab, drag and drop the **Isolate Message** object to the Rules pallet.

Email Security Gateway environment

You do not need to manually configure Email Security Gateway to block email messages without a sender's address. By design, Email Security Gateway automatically blocks email messages that do not contain any envelope sender information.

Block some keywords

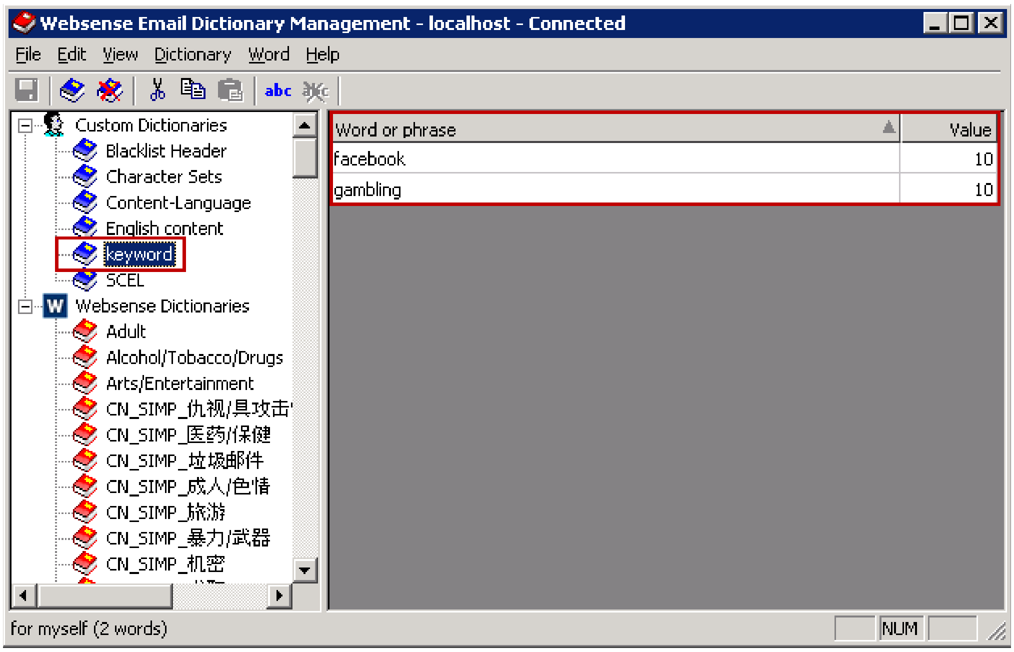
You can create a policy to quarantine email messages that contain specific keywords that appear either in the subject or body of the message.

- *Websense Email Security environment*, page 32
- *Email Security Gateway environment*, page 34

Websense Email Security environment

To create a rule in Websense Email Security that blocks certain keywords, follow these steps:

1. Create a Custom Dictionary.
   a. Open the **Websense Email Security > Dictionary Management** module.
   b. Right click on **Custom Dictionary** and then click **Add**.
   c. Enter the properties for the new dictionary and then click **OK**.
2. Add keywords to the dictionary.
   a. Highlight the new dictionary under **Custom Dictionaries**.
   b. Select **Word > Add**.
   c. Specify keywords and assign a phrase value, and then click **OK**.


Websense Email Dictionary Management - localhost - Connected
File
Edit
View
Dictionary
Word
Help
abc

- Custom Dictionaries
  - Blacklist Header
  - Character Sets
  - Content-Language
  - English content
  - keyword
  - SCEL
- Websense Dictionaries
  - Adult
  - Alcohol/Tobacco/Drugs
  - Arts/Entertainment
  - CN_SIMP_仇视/具攻击'
  - CN_SIMP_医药/保健
  - CN_SIMP_垃圾邮件
  - CN_SIMP_成人/色情
  - CN_SIMP_旅游
  - CN_SIMP_暴力/武器
  - CN_SIMP_机密

Word or phrase	Value
facebook	10
gambling	10

for myself (2 words)

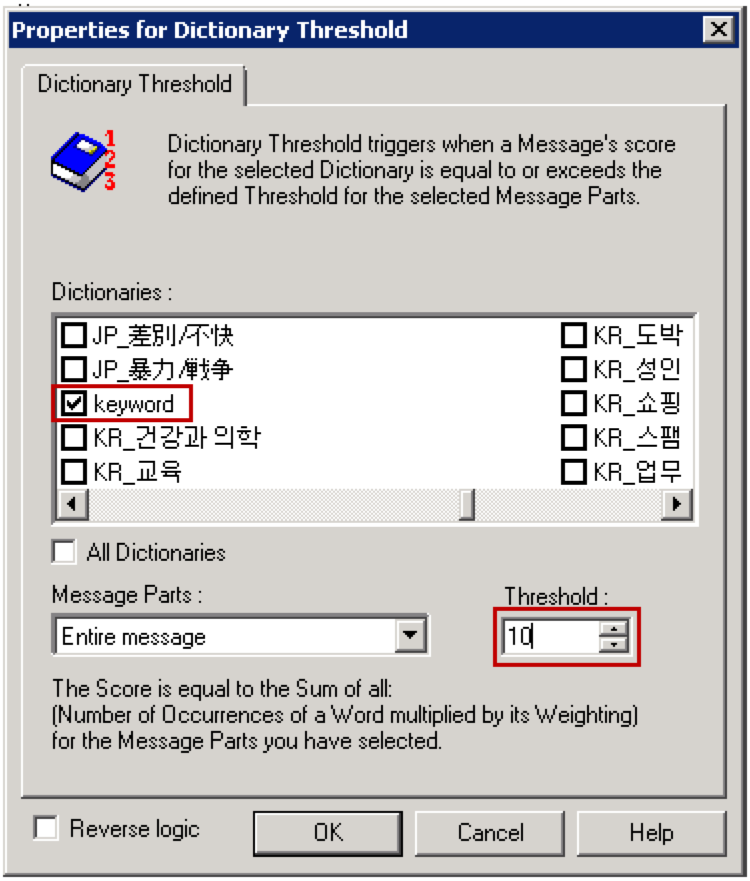
3. Save the changes using **File > Save changes**.
4. Configure the **Rules Administrator**.
5. In the Websense Email Security Rules Administrator module, create a new rule:

a. Select **Rule** > **New Rule**.

b. Enter the properties for the new rule.

6. On the **What** tab, drag and drop the **Dictionary Threshold** object to the Rules pallet.

7. Use the scroll bar to find and select the custom dictionary you have just created.



Properties for Dictionary Threshold

Dictionary Threshold

Dictionary Threshold triggers when a Message's score for the selected Dictionary is equal to or exceeds the defined Threshold for the selected Message Parts.

Dictionaries :

☐ JP_差別/不快
☐ JP_暴力/戦争
☑ keyword
☐ KR_건강과 의학
☐ KR_교육
☐ KR_도박
☐ KR_성인
☐ KR_쇼핑
☐ KR_스팸
☐ KR_업무

☐ All Dictionaries

Message Parts : Entire message

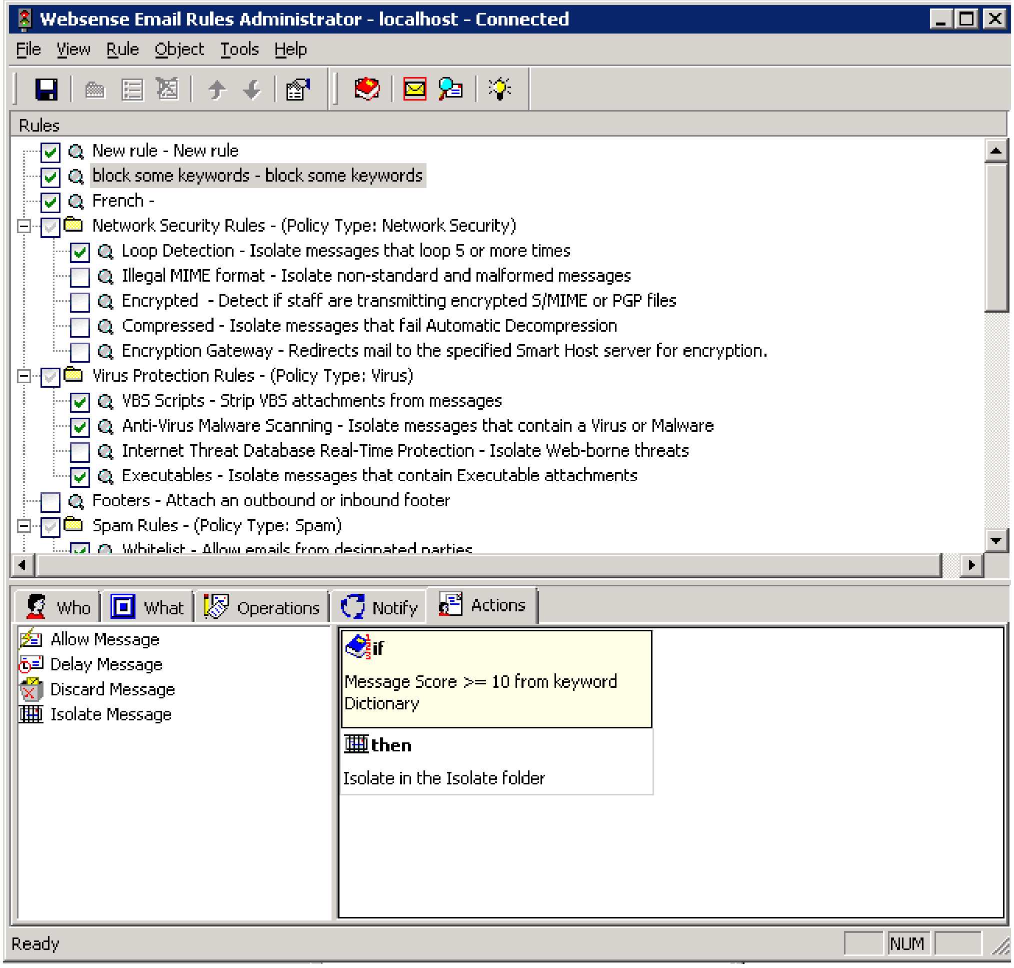
Threshold : 10

The Score is equal to the Sum of all:
(Number of Occurrences of a Word multiplied by its Weighting)
for the Message Parts you have selected.

☐ Reverse logic

8. Assign a **Threshold** value and then click **OK**.

9. On the **Actions** tab, drag and drop the **Isolate Message** object to the Rules pallet and then click **OK**.


Websense Email Rules Administrator - localhost - Connected
File View Rule Object Tools Help
Rules
Who
What
Operations
Notify
Actions
Ready
NUM

Rules

- ☑ New rule - New rule
- ☑ block some keywords - block some keywords
- ☑ French -
- ☑ Network Security Rules - (Policy Type: Network Security)
  - ☑ Loop Detection - Isolate messages that loop 5 or more times
  - □ Illegal MIME format - Isolate non-standard and malformed messages
  - □ Encrypted - Detect if staff are transmitting encrypted S/MIME or PGP files
  - □ Compressed - Isolate messages that fail Automatic Decompression
  - □ Encryption Gateway - Redirects mail to the specified Smart Host server for encryption.
- ☑ Virus Protection Rules - (Policy Type: Virus)
  - ☑ VBS Scripts - Strip VBS attachments from messages
  - ☑ Anti-Virus Malware Scanning - Isolate messages that contain a Virus or Malware
  - □ Internet Threat Database Real-Time Protection - Isolate Web-borne threats
  - ☑ Executables - Isolate messages that contain Executable attachments
- □ Footers - Attach an outbound or inbound footer
- ☑ Spam Rules - (Policy Type: Spam)
  - ☑ Whitelist - Allow emails from designated parties

Allow Message
Delay Message
Discard Message
Isolate Message

if

Message Score >= 10 from keyword Dictionary

then

Isolate in the Isolate folder

Email Security Gateway environment

To create a policy to block keywords for Email Security Gateway, you must configure it in the Websense Data Security module.

1. In the Data Security module, select **Main > Policy Management > DLP Policies > Email DLP Policy**.
2. Select either the **Outbound** or **Inbound** tab, and then select the **Patterns & phrases** attribute.
3. Add a keyword.
   a. Select the **Enable attribute** check box and then click **Add** to define a keyword.
   b. Select the **Key phrase** option and then type a precise word or phrase you would like to block.

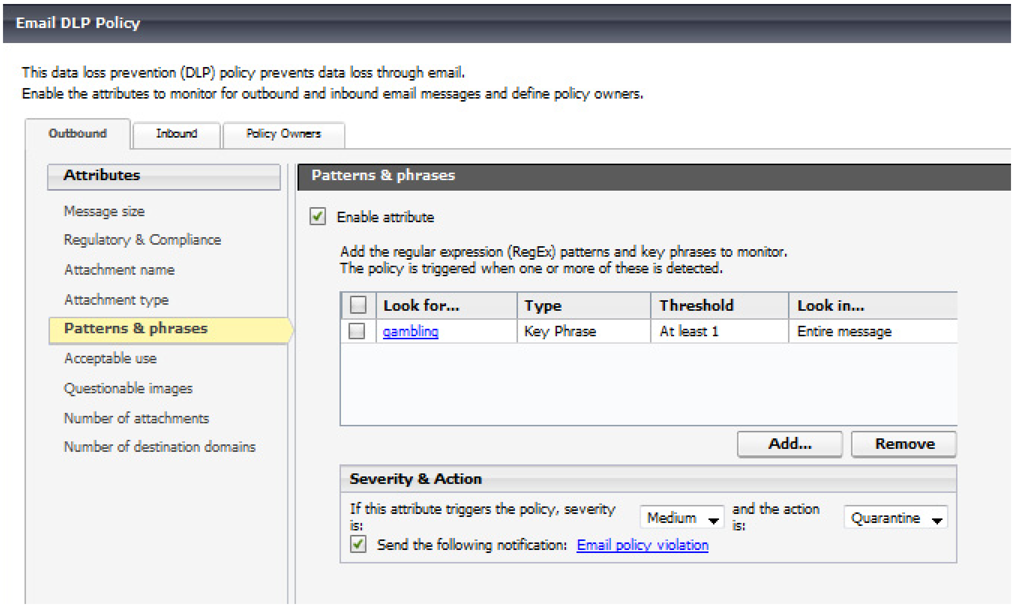
c. Select how many phrase matches must be made for the policy to trigger. The default number of matches is 1.

d. Specify whether you want to search all email fields or only specific fields.

e. Click **OK**.

4. Specify the **Severity** (High, Medium, or Low) and set the **Action** to **Quarantine**.

5. Click **OK**.



Email DLP Policy

This data loss prevention (DLP) policy prevents data loss through email.
Enable the attributes to monitor for outbound and inbound email messages and define policy owners.

Patterns & phrases

☑ Enable attribute

Add the regular expression (RegEx) patterns and key phrases to monitor.
The policy is triggered when one or more of these is detected.

□	Look for...	Type	Threshold	Look in...
□	gambling	Key Phrase	At least 1	Entire message

Severity & Action

If this attribute triggers the policy, severity is: Medium and the action is: Quarantine

☑ Send the following notification: Email policy violation

Add custom rules to a policy

You can add custom rules to new or existing policies in Email Security Gateway so that you can granularly control email messages.

- *Websense Email Security environment*, page 35
- *Email Security Gateway environment*, page 36

Websense Email Security environment

Since the concept of policies does not exist in In Websense Email Security, you can create a group rule, and then create an exception to the group rule in order to control messages on a granular level.To do so, follow these steps:

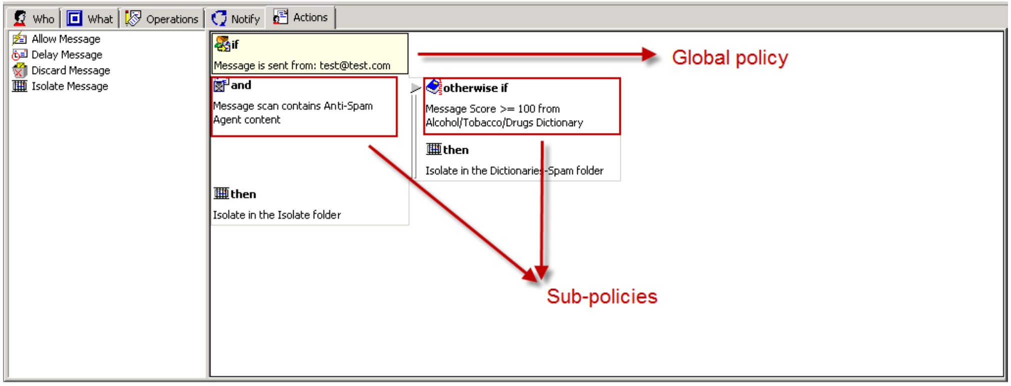
1. In the Websense Email Rules Administrator module, create a new rule:

   a. Select **Rule** > **New Rule**.

   b. Enter the properties for the new rule.

2. Create a condition for a group rule. For example, define a sender’s address.

3. Create a condition for a sub-rule. For example, specify an antispam condition.
4. Assign an action to the rules.
5. Create another sub-rule by dragging and dropping an object to the column next to the first sub-rule in the Rules pallet.
6. Assign an action to the second sub-rule.



if
Message is sent from: test@test.com

and
Message scan contains Anti-Spam Agent content

then
Isolate in the Isolate folder

otherwise if
Message Score >= 100 from Alcohol/Tobacco/Drugs Dictionary

then
Isolate in the Dictionaries-Spam folder

Global policy

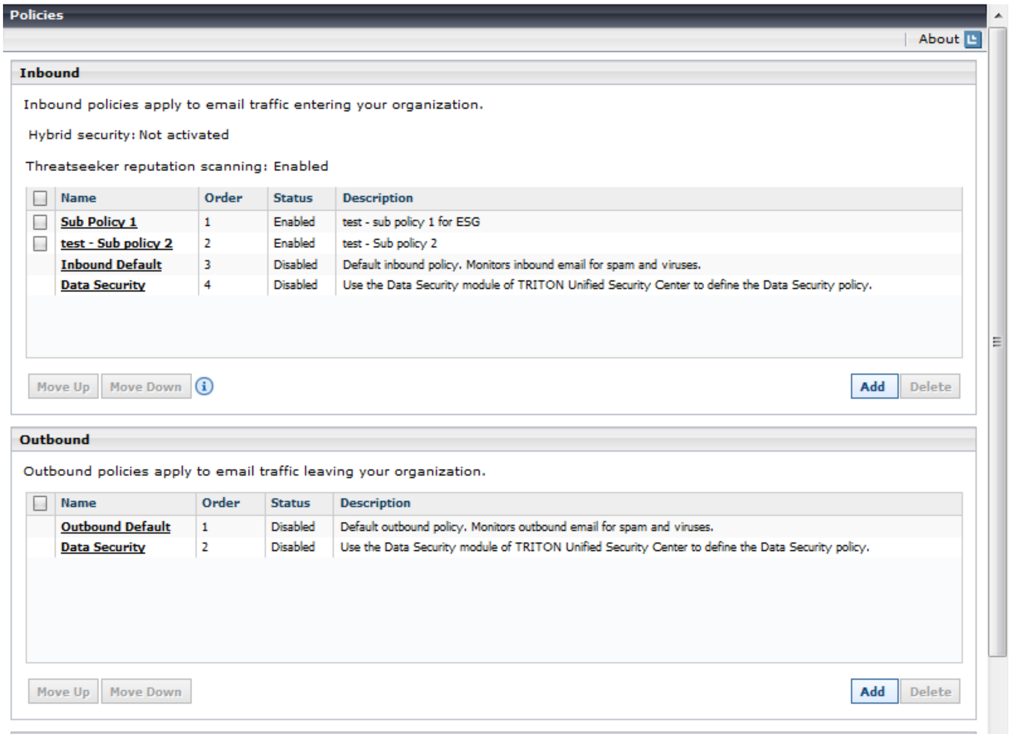
Sub-policies

Email Security Gateway environment

To add a custom rule to a policy in Email Security Gateway, follow these steps:

1. In the Email Security module, select **Main > Policy Management > Policies** and then click **Add**.
2. Define the policy conditions:
   a. Specify a name and description for the policy.
   b. Set the status and assign the policy order.
3. Optionally, you can add new or edit existing rules to the policy. In the Rules section, click on a rule.
   a. To edit existing conditions, click **Edit**.
   b. To add new a new filter, select **Add filter** from the Filter name drop-down list.
   c. To add a new action, select **Add action** from the Action name drop-down list.
   d. Click **OK**.

4. Click **OK**.



Inbound

Inbound policies apply to email traffic entering your organization.

Hybrid security: Not activated

Threatseeker reputation scanning: Enabled

□	Name	Order	Status	Description
□	Sub Policy 1	1	Enabled	test - sub policy 1 for ESG
□	test - Sub policy 2	2	Enabled	test - Sub policy 2
	Inbound Default	3	Disabled	Default inbound policy. Monitors inbound email for spam and viruses.
	Data Security	4	Disabled	Use the Data Security module of TRITON Unified Security Center to define the Data Security policy.

Outbound

Outbound policies apply to email traffic leaving your organization.

□	Name	Order	Status	Description
	Outbound Default	1	Disabled	Default outbound policy. Monitors outbound email for spam and viruses.
	Data Security	2	Disabled	Use the Data Security module of TRITON Unified Security Center to define the Data Security policy.

Block custom rules within a policy

You can block rules within a policy by disabling the policy. For example, you want to define a policy to block all email messages with the subject containing specific keywords (for example, "confidential"), that are only sent from a specific user group such as sender A, B, C etc.

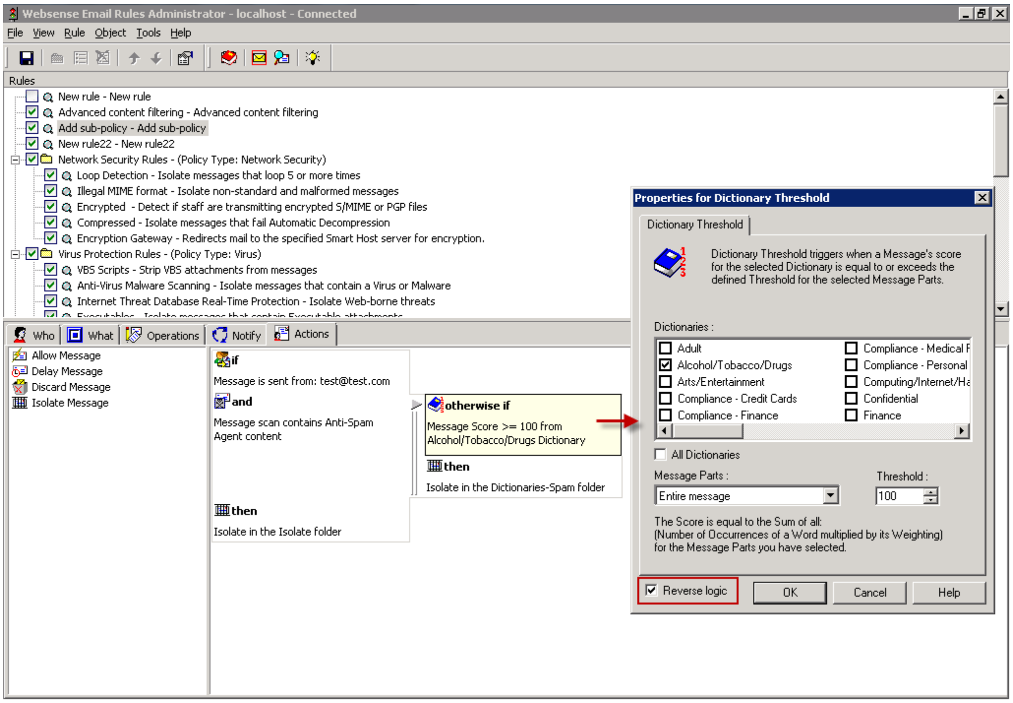
- *Websense Email Security environment*, page 37
- *Email Security Gateway environment*, page 38

Websense Email Security environment

To block sub-rules within a group rule in Websense Email Security, follow these steps:

1. From the Rules panel, select a group rule that includes a sub-rule.
2. In the Rules pallet, double click a sub-rule condition. The **Properties for Dictionary Threshold** dialog appears.
3. Select the **Reverse logic** check box.

4. Click **OK**.



Websense Email Rules Administrator - localhost - Connected

Rules

- □ New rule - New rule
- ☑ Advanced content filtering - Advanced content filtering
- ☑ Add sub-policy - Add sub-policy
- ☑ New rule22 - New rule22
- ☑ Network Security Rules - (Policy Type: Network Security)
  - ☑ Loop Detection - Isolate messages that loop 5 or more times
  - ☑ Illegal MIME format - Isolate non-standard and malformed messages
  - ☑ Encrypted - Detect if staff are transmitting encrypted S/MIME or PGP files
  - ☑ Compressed - Isolate messages that fail Automatic Decompression
  - ☑ Encryption Gateway - Redirects mail to the specified Smart Host server for encryption.
- ☑ Virus Protection Rules - (Policy Type: Virus)
  - ☑ VBS Scripts - Strip VBS attachments from messages
  - ☑ Anti-Virus Malware Scanning - Isolate messages that contain a Virus or Malware
  - ☑ Internet Threat Database Real-Time Protection - Isolate Web-borne threats

if

Message is sent from: test@test.com

and

Message scan contains Anti-Spam Agent content

then

Isolate in the Isolate folder

otherwise if

Message Score >= 100 from Alcohol/Tobacco/Drugs Dictionary

then

Isolate in the Dictionaries-Spam folder

Properties for Dictionary Threshold

Dictionary Threshold

Dictionary Threshold triggers when a Message's score for the selected Dictionary is equal to or exceeds the defined Threshold for the selected Message Parts.

Dictionaries :

- □ Adult
- ☑ Alcohol/Tobacco/Drugs
- □ Arts/Entertainment
- □ Compliance - Credit Cards
- □ Compliance - Finance
- □ Compliance - Medical F
- □ Compliance - Personal
- □ Computing/Internet/Ha
- □ Confidential
- □ Finance

□ All Dictionaries

Message Parts : Entire message

Threshold : 100

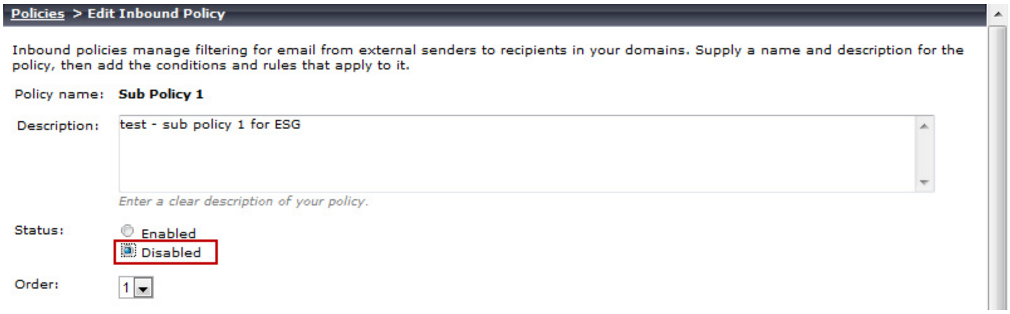
The Score is equal to the Sum of all:
(Number of Occurrences of a Word multiplied by its Weighting)
for the Message Parts you have selected.

☑ Reverse logic

Email Security Gateway environment

To disable a sub-policy in Email Security Gateway, follow these steps:

1. In the Email Security module, select **Main > Policy Management > Policies**.
2. Select a sub-policy from the **Inbound** or **Outbound** list.
3. Select **Disabled** for the status.
4. Click **OK**.



Policies > Edit Inbound Policy

Inbound policies manage filtering for email from external senders to recipients in your domains. Supply a name and description for the policy, then add the conditions and rules that apply to it.

Policy name: **Sub Policy 1**

Description: test - sub policy 1 for ESG

Enter a clear description of your policy.

Status:
○ Enabled
● Disabled

Order: 1

Spoofed message policy

Spoofed mail is a form of spam and occurs when the sender manipulates the sender address information. The message header or sender information is modified to appear as though the message originated from a different source. You can create a policy to detect incoming spoofed email messages. To do so, define a rule that scans the envelope address and header address to detect legitimately sent email messages.

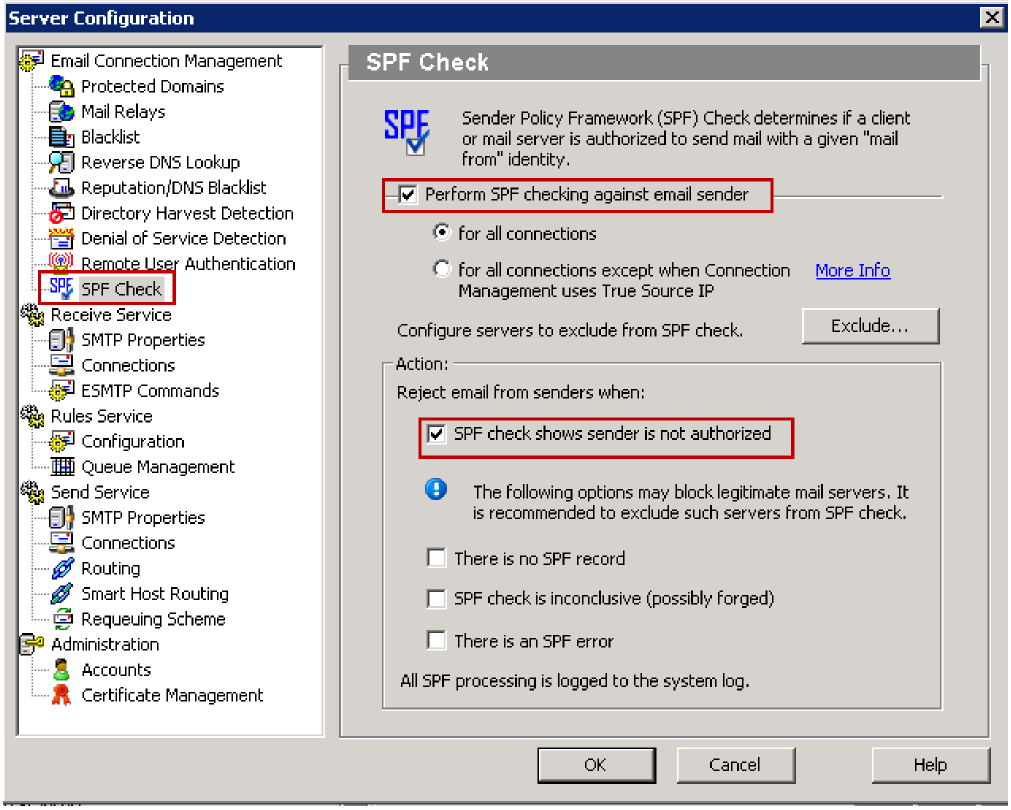
- *Websense Email Security environment*, page 39
- *Email Security Gateway environment*, page 40

Websense Email Security environment

To create a policy in Websense Email Security that denies messages with spoofed "from" addresses, then use the SPF check feature.

1. Open the Websense Server Configuration.
   a. Open Websense Email Monitor **Start** > **Programs** > **Websense Email Security** > **Monitor**.
   b. Select **File** > **Server configuration**.
2. Under Email Connection Management, select **SPF Check**.
3. Select the **Perform SPF checking against email sender** check box.
4. Select the **SPF check shows sender is not authorized** check box.

5. Click **OK**.



SPF Check

Sender Policy Framework (SPF) Check determines if a client or mail server is authorized to send mail with a given "mail from" identity.

☑ Perform SPF checking against email sender

● for all connections

○ for all connections except when Connection Management uses True Source IP

Configure servers to exclude from SPF check.

Action:

Reject email from senders when:

☑ SPF check shows sender is not authorized

The following options may block legitimate mail servers. It is recommended to exclude such servers from SPF check.

□ There is no SPF record

□ SPF check is inconclusive (possibly forged)

□ There is an SPF error

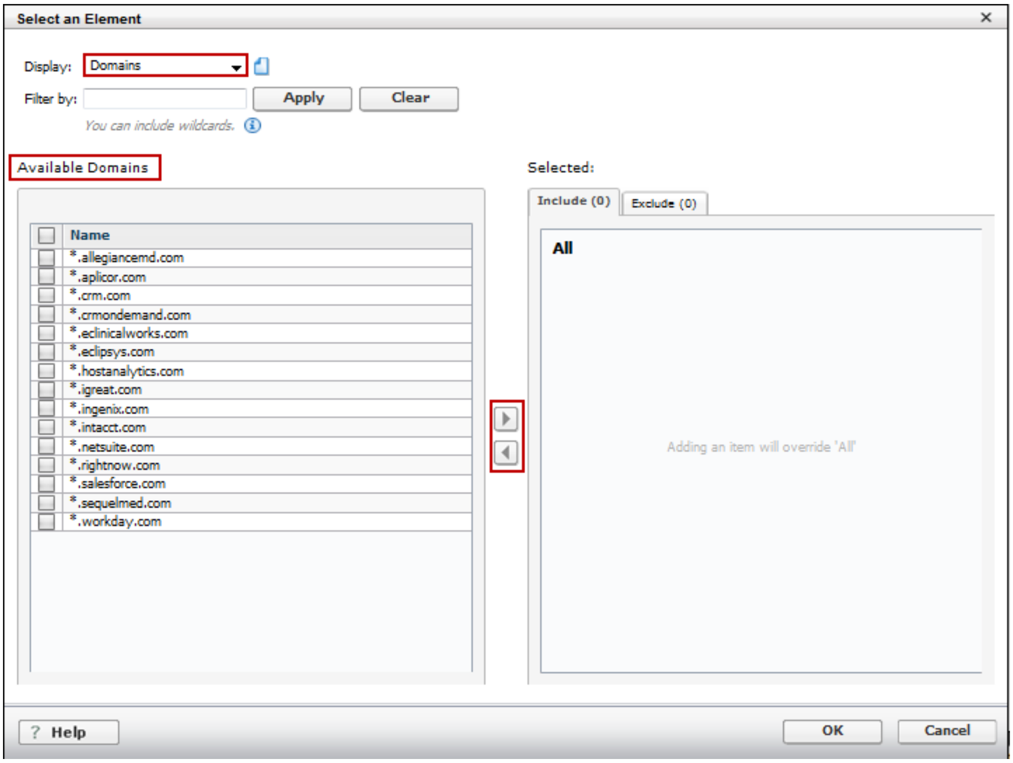
All SPF processing is logged to the system log.

Email Security Gateway environment

To create a policy in Email Security Gateway that blocks spoofed email messages, follow these steps:

1. In the Data Security module, select **Main > Policy Management > DLP Policies**.
2. Click **Create custom policy** to create a policy using the Custom Policy Wizard.
3. Continue using the wizard to create a new policy until you reach the **Source** tab.
4. Click **Edit** and then select **Domains** from the Display drop-down menu.
5. Add domains to be blocked by selecting the domain from the list and clicking the > arrow. Click **OK**.

6. Click **Next** to continue using the Custom Policy Wizard to complete creating the policy.



Select an Element

Display: Domains

Filter by:

You can include wildcards.

Available Domains

□	Name
□	*.allegiancemd.com
□	*.aplicor.com
□	*.crm.com
□	*.crmondemand.com
□	*.eclinicalworks.com
□	*.eclipsys.com
□	*.hostanalytics.com
□	*.igreat.com
□	*.ingenix.com
□	*.intacct.com
□	*.netsuite.com
□	*.rightnow.com
□	*.salesforce.com
□	*.sequelmed.com
□	*.workday.com

Selected:

Include (0) Exclude (0)

All

Adding an item will override 'All'

Configure message and attachment size

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

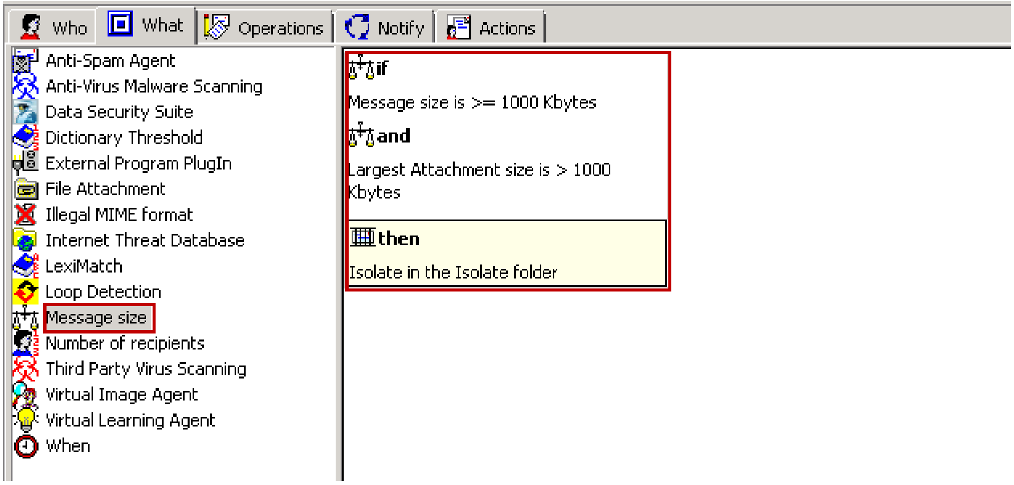
- *Websense Email Security environment*, page 41
- *Email Security Gateway environment*, page 42

Websense Email Security environment

To create a policy in Websense Email Security that restricts email messages of a certain message data size, follow these steps:

1. Create a new **Content Guardian** filter.
   a. Select **Policy Manager** > **Global Policy** > **Filters**, and then click **Add**.
   b. Select the **Content Guardian** option, and then click **Next**.
2. Define the **Filter property** conditions - Specify a name, status, and permission for the filter.

3. In the **Filter criteria** section, select **any of the items match** for **the condition for the following rules is** option.
4. Define the message size criteria:
   a. Select **Message size - is greater than** and then specify a size and unit.
5. Define the attachment size criteria:
   a. Click **Add** to define another filter criteria.
   b. Select **Attachment size - is greater than** and then specify a size and unit.
6. In the **Action if filter triggered** section, select the **Drop message** option.



if
Message size is >= 1000 Kbytes
and
Largest Attachment size is > 1000 Kbytes
then
Isolate in the Isolate folder

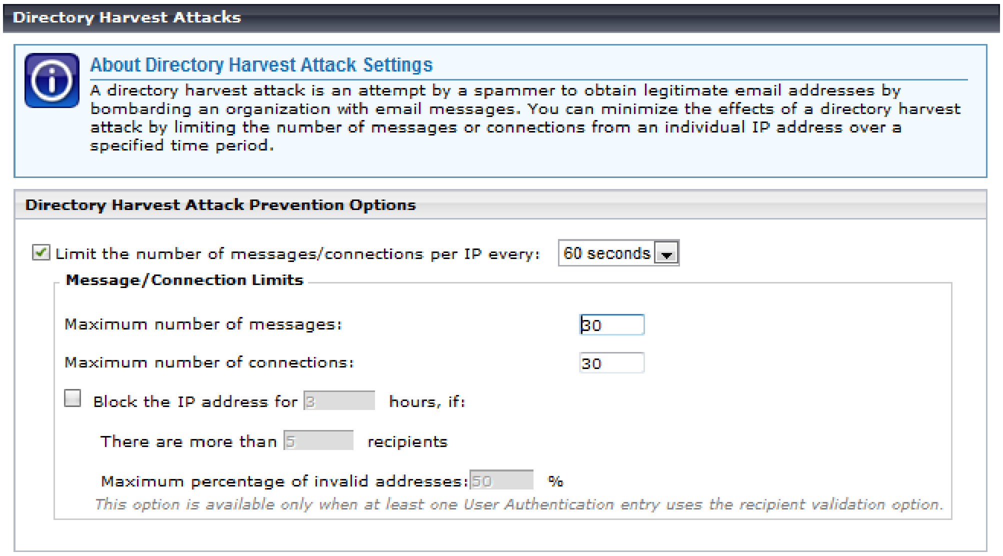
Email Security Gateway environment

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

To restrict the message and attachment size per connection using the TRITON - Email Security Gateway module, follow these steps:

1. Select **Settings > Receive/Send > Directory Attacks**.
2. Select the **Limit the number of messages/connections per IP every** option, and then specify a time limit using the drop-down menu.
3. Specify a message limit in the **Maximum number of messages** field.
4. Specify a Connection limit in the **Maximum number of connections** field.
5. Click **OK**.

For more information about setting size and volume limitations in Email Security Gateway, refer to the Email Security Help sections Managing domain and IP address groups and Managing Messages.



Directory Harvest Attacks

About Directory Harvest Attack Settings

A directory harvest attack is an attempt by a spammer to obtain legitimate email addresses by bombarding an organization with email messages. You can minimize the effects of a directory harvest attack by limiting the number of messages or connections from an individual IP address over a specified time period.

Directory Harvest Attack Prevention Options

☑ Limit the number of messages/connections per IP every: 60 seconds

Message/Connection Limits

Maximum number of messages: 30

Maximum number of connections: 30

□ Block the IP address for 3 hours, if:

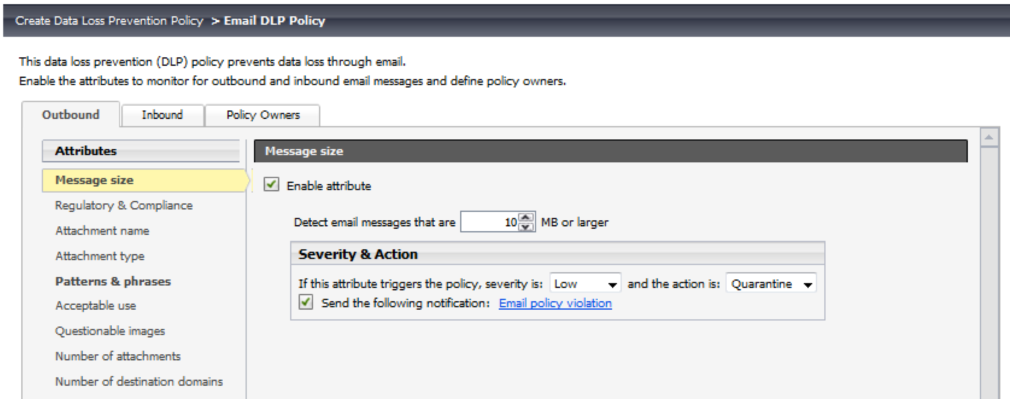
There are more than 5 recipients

Maximum percentage of invalid addresses: 50 %

This option is available only when at least one User Authentication entry uses the recipient validation option.

To restrict the message and attachment size per connection using the TRITON - Data Security module, follow these steps:

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



Create Data Loss Prevention Policy > Email DLP Policy

This data loss prevention (DLP) policy prevents data loss through email.
Enable the attributes to monitor for outbound and inbound email messages and define policy owners.

Message size

☑ Enable attribute

Detect email messages that are 10 MB or larger

Severity & Action

If this attribute triggers the policy, severity is: Low and the action is: Quarantine

☑ Send the following notification: Email policy violation

Configure advanced content filtering

The advanced content filter provides more comprehensive checking of message header, message body, and message attachments. It also supports the dynamic evaluation of keyword frequency to enhance flexibility.

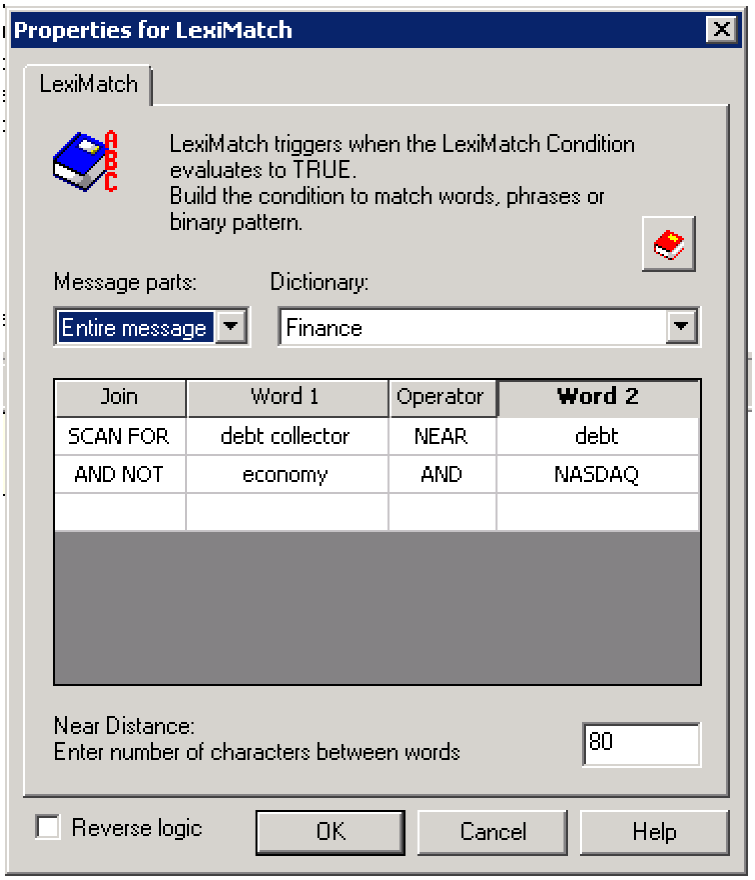
- *Websense Email Security environment*, page 44
- *Email Security Gateway environment*, page 45

Websense Email Security environment

To configure advanced content filtering in Websense Email Security, follow these steps:

1. In the Websense Email Rules Administrator module, create a new rule:
   a. Select **Rule** > **New Rule**.
   b. Enter the properties for the new rule.
2. On the **What** tab, drag and drop **Leximatch** to the Rules pallet.
3. From the **Dictionary** drop-down menu in the Properties dialog box, select a filter dictionary.
4. Create word patterns by specifying word combinations, and then select an **Operator** to define the relationship between the 2 words.

5. Click **OK**.



LexiMatch triggers when the LexiMatch Condition evaluates to TRUE.
Build the condition to match words, phrases or binary pattern.

Message parts: Entire message

Dictionary: Finance

Join	Word 1	Operator	Word 2
SCAN FOR	debt collector	NEAR	debt
AND NOT	economy	AND	NASDAQ

Near Distance:
Enter number of characters between words: 80

□ Reverse logic

Email Security Gateway environment

Advanced content filtering is configured in the TRITON - Data Security module. You can configure advanced content filtering settings for each of the following content classifiers:

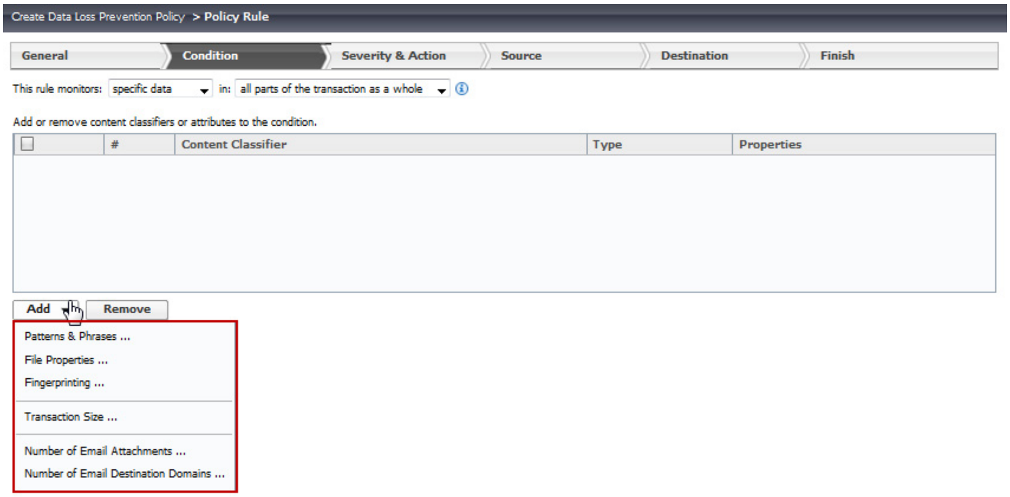
- Patterns and phrases
- File Properties
- Fingerprint
- Transaction Size
- Number of Email Attachments
- Number of Email Destinations

To configure advanced content filtering for Email Security Gateway, follow these steps:

1. In the Data Security module, select **Main** > **Policy Management** > **DLP Policies**.

2. Click **Create custom policy** to create a new policy using the Custom Policy Wizard.
3. Use the wizard to guide you through the steps until you reach the **Condition** tab. Select **Add** and select a content classifier from the list to configure advanced settings for its content filtering.

   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.
4. Click **Next** to continue using the Custom Policy Wizard to create a policy.



Create Data Loss Prevention Policy > Policy Rule

This rule monitors: specific data in: all parts of the transaction as a whole

Add or remove content classifiers or attributes to the condition.

☐	#	Content Classifier	Type	Properties

Configure message attachment filter

Websense email security products can block incoming and outgoing messages that contain attachments.

- *Websense Email Security environment*, page 46
- *Email Security Gateway environment*, page 47

Websense Email Security environment

To create a policy in Websense Email Security that blocks messages which contain attachments, follow these steps:

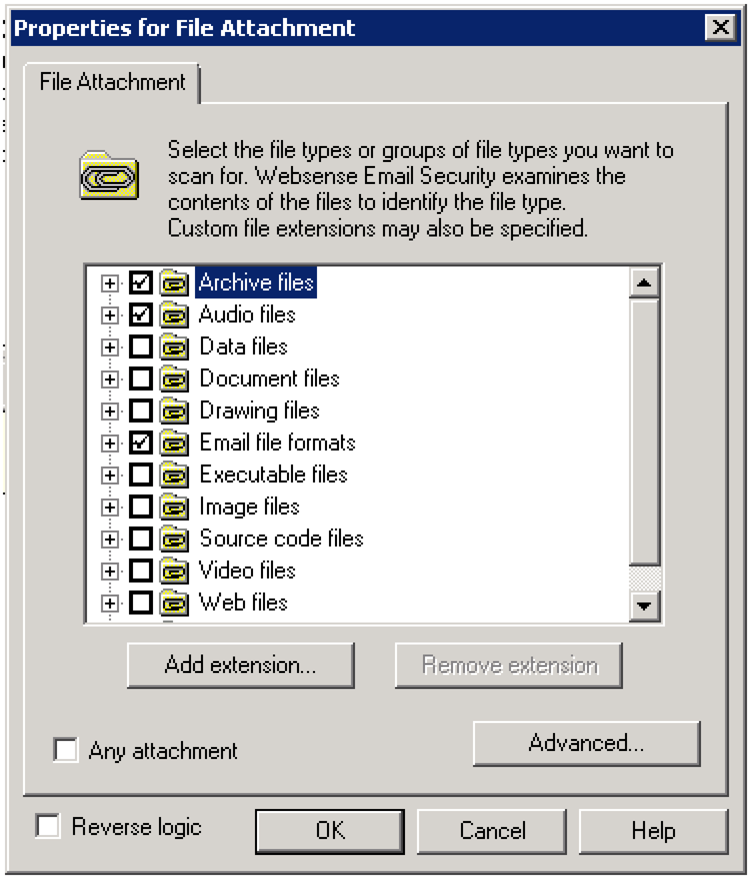
1. In the Websense Email Rules Administrator module, create a new rule:
   a. Select **Rule > New Rule**.
   b. Enter the properties for the new rule.
2. On the **What** tab, drag and drop the **File Attachment** object to the Rules pallet. The **Properties for File Attachment** dialog box displays.
3. You can select:

a. Groups of file types, such as image files.

b. Individual file types, such as .jpg, .mp3, and others.

c. The **Any attachment** check box.

4. Click **OK**.



Select the file types or groups of file types you want to scan for. Websense Email Security examines the contents of the files to identify the file type. Custom file extensions may also be specified.

- ☑ Archive files
- ☑ Audio files
- □ Data files
- □ Document files
- □ Drawing files
- ☑ Email file formats
- □ Executable files
- □ Image files
- □ Source code files
- □ Video files
- □ Web files

□ Any attachment

□ Reverse logic

Email Security Gateway environment

To configure the message attachment filter for Email Security Gateway, follow these steps:

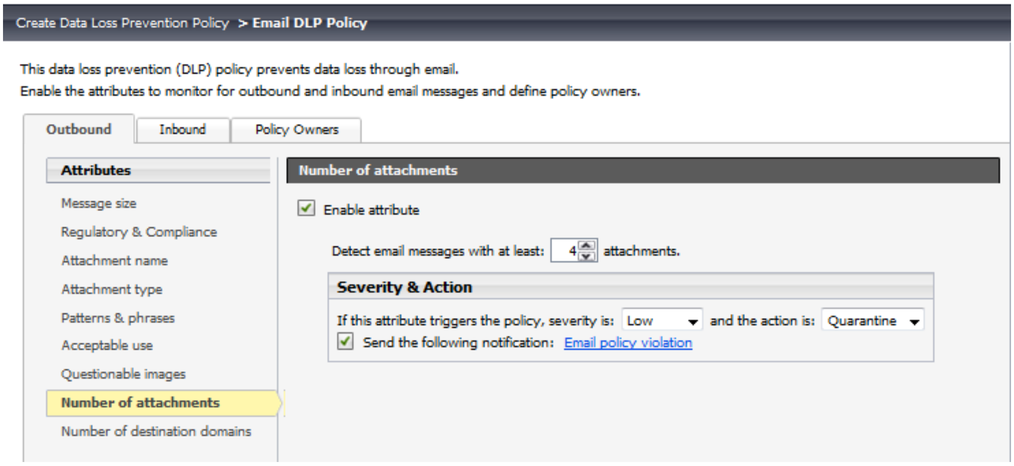
1. In the Data Security module, select **Main > Policy Management > DLP Policies > Email DLP Policy**.
2. Click either the **Inbound** or **Outbound** tab, and then select the **Number of attachments** attribute.
3. Specify the attributes for number of attachments.

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**.



Create Data Loss Prevention Policy > Email DLP Policy

This data loss prevention (DLP) policy prevents data loss through email.
Enable the attributes to monitor for outbound and inbound email messages and define policy owners.

Number of attachments

☑ Enable attribute

Detect email messages with at least: 4 attachments.

Severity & Action

If this attribute triggers the policy, severity is: Low and the action is: Quarantine

☑ Send the following notification: Email policy violation

Configure dictionary threshold filter

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.

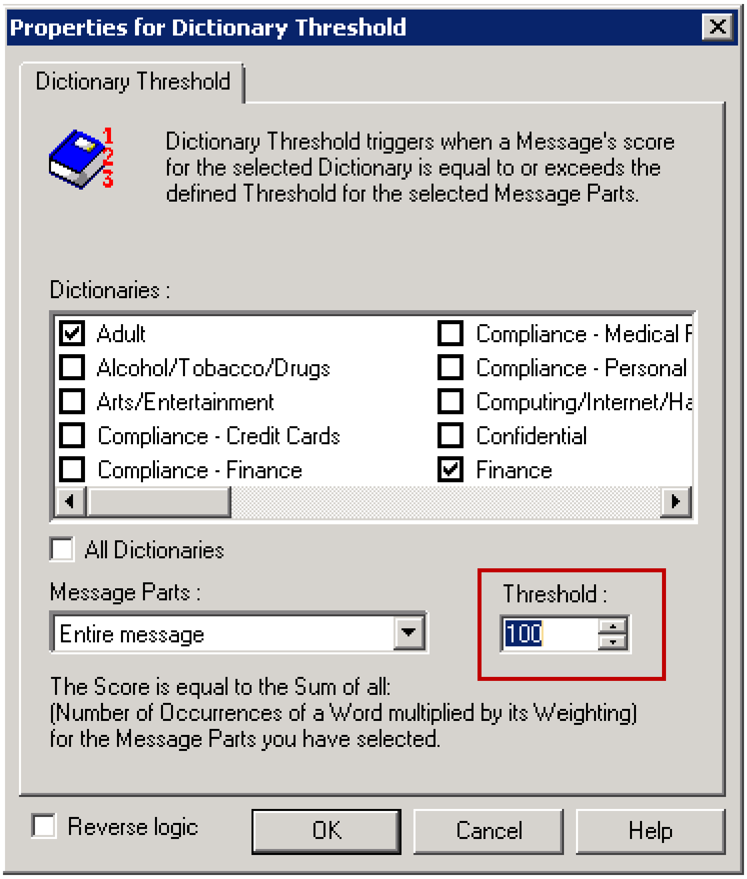
- *Websense Email Security environment*, page 48
- *Email Security Gateway environment*, page 49

Websense Email Security environment

To configure the dictionary threshold filter in Websense Email Security, follow these steps:

1. Select an existing dictionary rule from the Rules panel.
2. From the Rules pallet, double click the **If** action to open the **Properties for Dictionary Threshold** dialog.

3. Adjust the **Threshold** to the desired value and then click **OK**.



Dictionary Threshold triggers when a Message's score for the selected Dictionary is equal to or exceeds the defined Threshold for the selected Message Parts.

Dictionaries :

☑ Adult
□ Alcohol/Tobacco/Drugs
□ Arts/Entertainment
□ Compliance - Credit Cards
□ Compliance - Finance
□ Compliance - Medical F
□ Compliance - Personal
□ Computing/Internet/Ha
□ Confidential
☑ Finance

□ All Dictionaries

Message Parts : Entire message

Threshold : 100

The Score is equal to the Sum of all:
(Number of Occurrences of a Word multiplied by its Weighting)
for the Message Parts you have selected.

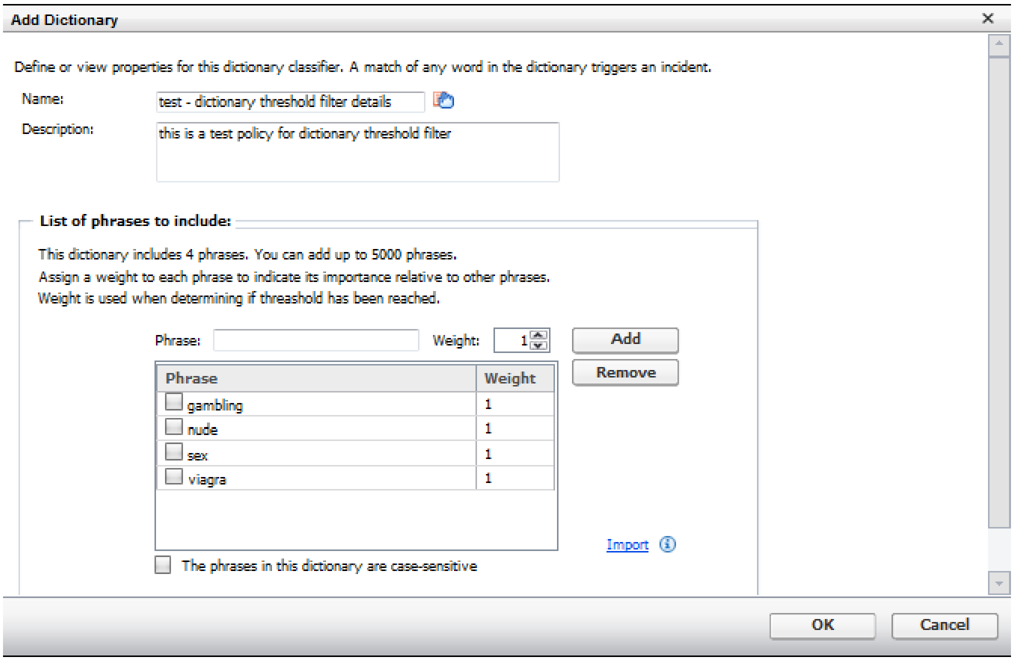
□ Reverse logic

Email Security Gateway environment

To configure the dictionary threshold for Email Security Gateway, follow these steps:

1. Create a new custom rule. In the Data Security module:
   a. Select **Main > Policy Management > DLP Policies**.
   b. Click **Create custom policy** to create a new rule.
2. On the **General** tab, type details for the policy such as policy name, description, and then click **Next**.
3. Add a custom dictionary classifier.
   a. On the **Condition** tab, select **Add > Patterns & Phrases**.

b. On the **General** tab, select **New > Dictionary**.



Add Dictionary

Define or view properties for this dictionary classifier. A match of any word in the dictionary triggers an incident.

Name: test - dictionary threshold filter details

Description: this is a test policy for dictionary threshold filter

List of phrases to include:

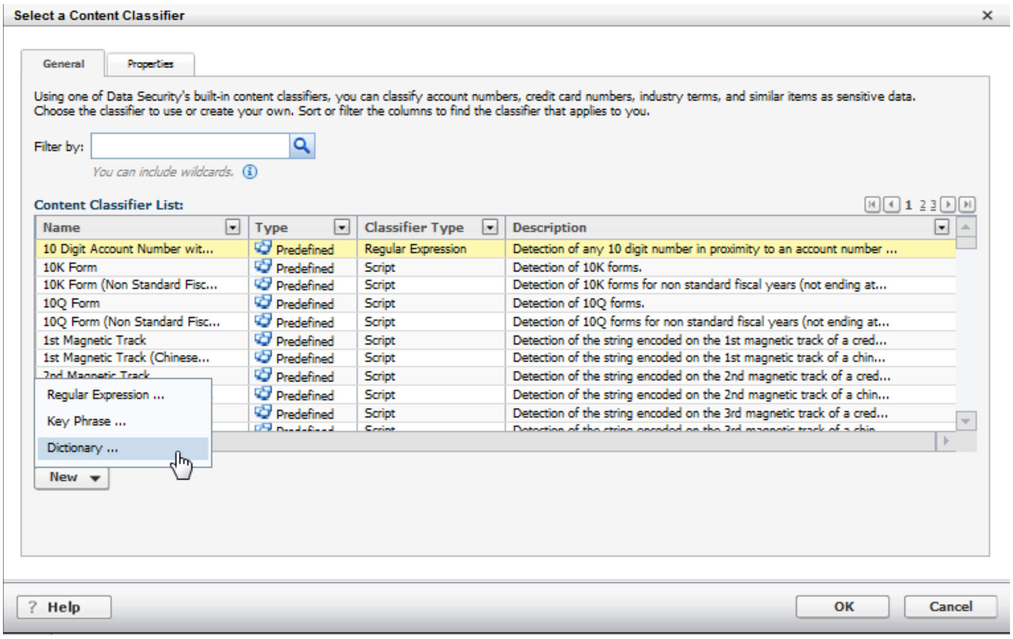
This dictionary includes 4 phrases. You can add up to 5000 phrases.
Assign a weight to each phrase to indicate its importance relative to other phrases.
Weight is used when determining if threashold has been reached.

Phrase: Weight: 1

Phrase	Weight
□ gambling	1
□ nude	1
□ sex	1
□ viagra	1

□ The phrases in this dictionary are case-sensitive

c. In the **Add Dictionary** dialog, define the properties for the dictionary classifier and then click **OK**. For more information about creating dictionary classifiers, refer to the Data Security Online Help section Adding a dictionary classifier.



Select a Content Classifier

Using one of Data Security's built-in content classifiers, you can classify account numbers, credit card numbers, industry terms, and similar items as sensitive data. Choose the classifier to use or create your own. Sort or filter the columns to find the classifier that applies to you.

Filter by:

You can include wildcards.

Content Classifier List:

Name	Type	Classifier Type	Description
10 Digit Account Number wit...	Predefined	Regular Expression	Detection of any 10 digit number in proximity to an account number ...
10K Form	Predefined	Script	Detection of 10K forms.
10K Form (Non Standard Fisc...	Predefined	Script	Detection of 10K forms for non standard fiscal years (not ending at...
10Q Form	Predefined	Script	Detection of 10Q forms.
10Q Form (Non Standard Fisc...	Predefined	Script	Detection of 10Q forms for non standard fiscal years (not ending at...
1st Magnetic Track	Predefined	Script	Detection of the string encoded on the 1st magnetic track of a cred...
1st Magnetic Track (Chinese...	Predefined	Script	Detection of the string encoded on the 1st magnetic track of a chin...
2nd Magnetic Track	Predefined	Script	Detection of the string encoded on the 2nd magnetic track of a cred...
	Predefined	Script	Detection of the string encoded on the 2nd magnetic track of a chin...
	Predefined	Script	Detection of the string encoded on the 3rd magnetic track of a cred...
	Predefined	Script	Detection of the string encoded on the 3rd magnetic track of a chin...

4. Click **Next**.

5. Specify the **Severity** (High, Medium, Low) and set the **Action** to **Quarantine**. You can also define **Advanced** conditions for the rule where you can define the severity at a more granular level.
6. Specify a **Source** filter range and then click **Next**.
7. Specify a **Destination** filter range and then click **Next**.

✓ **Note**

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

8. Click **Finish**.

APPENDIX A

Configuration Settings

There is no automated process to migrate your Websense Email Security settings to Websense Email Security Gateway. This data needs to be manually entered and reconfigured.

Determining the correct settings and location of these settings can take a lot of time. This appendix lists the location of configuration settings found in Websense Email Security, and maps them to the corresponding locations in Email Security Gateway.

Mapped settings in Websense Email Security

Email Security Gateway includes email filtering features that are similar to those in Websense Email Security and other features that are not available in Websense Email Security. Some Websense Email Security features do not exist in Email Security Gateway.

The following table lists Websense Email Security configuration settings and the user interface location of the corresponding settings in Email Security Gateway.

To access Websense Email Security configuration settings, open the Websense Email Monitor module (**Start > Programs > Websense Email Security > Monitor**), and then select **File > Server Configuration**.

Websense Email Security	Email Security Gateway
Email Connection Management	
Protected Domains	Settings > General > Domain Groups
Mail Relays	Settings > Receive/Send > Relay Control
Blacklist	Main > Policy Management > Always Block/ Permit
Reverse DNS lookup	Settings > Receive/Send > Connection Control
Reputation/DNS blacklist	Settings > Receive/Send > Connection Control
Directory Harvest Detection	Settings > Receive/Send > Directory Attacks

Websense Email Security	Email Security Gateway
Denial of Service Detection	Settings > Receive/Send > Connection Control
Remote User Authentication	N/A
SPF check	Settings > Receive/Send > Relay Control
Receive Service	N/A
SMTP Properties	Settings > General > Configuration
Connections	Settings > Receive/Send > Message Control
ESMTP Commands	N/A
Rules Service	Main > Policy Management > Policies, Filters, and Actions **Note**: You can also configure email DLP policies in the Data Security module.
Configuration	N/A
Queue Management	Main > Message Management > Blocked Messages
Send Service	N/A
SMTP Properties	To set the SMTP greeting text: Settings > General > Configuration To set the SMTP greeting delay interval: Settings > Receive/Send > Connection Control
Connections	Settings > Receive/Send > Delivery
Routing	Settings > Receive/Send > Mail Routing
Smart Host Routing	N/A
Requeuing Scheme	Settings > General > Configuration Retrying message delivery options: Settings > Receive/Send > Delivery
Administration	Settings > General > Administrator Accounts **Note**: Administrator accounts are created in TRITON Unified Security Center settings. A Super Administrator can manage those created accounts in the Administrator Accounts page.
Accounts	Settings > General > Administrator Accounts Settings > General > Configuration
Certificate Management	Settings > General > TLS Certificate