v7.7 Release Notes for Websense Email Security Gateway

Topic 70023 | Release Notes | Email Security Gateway | Version 7.7 | Updated: 10-July-2012

Applies To:	Websense Email Security Gateway v7.7 Websense Email Security Gateway Anywhere v7.7

Websense® Email Security Gateway version 7.7 is a robust feature release that includes several improvements and fixes, many requested by customers. Part of the TRITON™ Unified Security Center, Email Security Gateway is a Websense V-Series™ appliance-based system that prevents malicious email threats from entering an organization's network and protects sensitive data from unauthorized email transmission.

Use these Release Notes to find information about new version 7.7 Email Security Gateway and Personal Email Manager features and system support. Version 7.7 Release Notes are also available for the following Websense products:

- TRITON Unified Security Center
- Web Security Gateway
- Data Security
- V-Series Appliance
- Content Gateway

This version of Email Security Gateway features embedded TRITON - Email Security Help in 2 languages: English and Simplified Chinese. You select the language you want in the **TRITON Settings > My Account** page in the TRITON Unified Security Center. See the TRITON Unified Security Center Help for details.

Contents

New in Email Security Gateway v7.7

Topic 70024 | Release Notes | Email Security Gateway | Version 7.7 | Updated: 10-July-2012

Applies To:	Websense Email Security Gateway v7.7 Websense Email Security Gateway Anywhere v7.7

New Email Security Gateway features are available in the following product areas:

Email Security Gateway system management

Email Security Gateway v7.7 has the following new system management features:

Security information and event management (SIEM) integration

Third-party SIEM tools allow the logging and analysis of internal alerts generated by network devices and software. Integration with SIEM technology lets Email Security Gateway transfer message activity events to a SIEM server for analysis and reporting.

Access SIEM integration settings on the **Settings > General > SIEM Integration** page. See TRITON - Email Security Help for details about entering SIEM integration server information and selecting data transport protocols.

You can configure the display and distribution of system alerts associated with SIEM server status in the **Settings > Alerts > Alert Event**s page.

Appliance C interface traffic management

Email Security supports the use of the C appliance interface for system management traffic. Registering Email Security with the TRITON - Data Security module can now be accomplished via the V-Series appliance C interface. Previous versions required that either E1 or E2 be used. You can also specify the C interface for appliance cluster communications.

Policy management

Enhancements to Email Security Gateway policy management functionality are included in this version. The following email policy, filter, and policy action features and options are now available:

- *Custom content filter*
- *URL scanning filter*
- *Filter bypass condition settings*
- *New virus filter options*
- *New message disclaimer filter feature*
- *New filter action options*

Custom content filter

Use a new custom content filter to allow Email Security to analyze messages based on message attribute conditions you specify. You can choose to trigger your filter on the match of a single condition or the match of a complete set of defined conditions.

Add or modify a custom content filter on the **Main > Policy Management > Filters > Add** (or **Edit**) **Filter** page. Select the Custom Content filter type, and then click **Add** in the Filter Conditions box. Choose from a selection of filtering criteria, including message attributes and operators, from the drop-down lists in the Add Condition dialog box. Message attributes may include sender or recipient address or message size. Operators may include “equals,” “does not equal,” or “contains.” See TRITON - Email Security Help for a complete list of custom content filtering criteria.

You can use the **Add** (or **Edit**) **Rule** page to add a rule for a custom content filter. You must have already defined a custom content filter before you attempt to add a custom content rule. Note that you may create a new rule only for a custom content filter. The Add Rule function is not available for other Email Security filters.

Two new filter action options are available in version 7.7 and recommended for use with custom content filters. See *New filter action options*, page 5, for information.

You can also determine the order in which custom content rules are applied. By default, a new custom content rule is created in the first position in the Rules list. Use the **Move Up** and **Move Down** buttons to adjust custom content rule order. The default Disclaimer rule, if enabled, is always applied last.

URL scanning filter

A new URL scanning filter analyzes email content for embedded URLs and classifies them according to a Websense database of known spam URLs. This functionality was included in the antispam filter in previous versions of Email Security Gateway.

This filter is available only when your system includes Websense Web Security and the URL database server is identified on the Email Security **Settings** > **General** > **URL Scanning** page.

When you select the URL scanning filter type in the **Main** > **Policy Management** > **Filters** > **Add** (or **Edit**) **Filter** page, mark the **URL scanning** check box to display a list of URL categories in the Filter Properties area. Select the URL categories that you want the filter to detect by marking the associated check boxes.

You can specify a text string with which to replace a URL that matches an entry in a selected database category. You can also specify that URL scanning not be performed for any message that exceeds a particular size.

A new filter action option of "Resume message scanning" is added to accommodate the URL scanning filter. See *New filter action options*, page 5, for information.

New Today and History dashboard charts summarize the instances of embedded URLs that Email Security detects. See *New dashboard charts*, page 8, for details.

Filter bypass condition settings

The ability to define message sender/recipient conditions that when matched allow a message to bypass filter analysis is added to this version of Email Security Gateway. This capability can help to improve system performance because unnecessary scanning can be avoided.

Bypass conditions are configured in the Rules section of a policy. In the **Main** > **Policy Management** > **Policies** > **Add** (or **Edit**) **Policy** page, click the rule for which you want to create sender/recipient bypass conditions, then click **Add** in the Filter Bypass Condition section. Enter your conditions in the Add Filter Bypass Conditions page.

Note

You cannot configure filter bypass settings for a custom content filter.

New virus filter options

The following antivirus filter options are new to Email Security Gateway, expanding virus filter capabilities to include the detection of malicious content in a PDF document and embedded iFrames in HTML pages:

- **Treat suspicious document as infected.** If a virus filter encounters a PDF document that contains active content, including exploits and malicious scripts, the message is handled as if it is infected.
- **Treat malicious embedded iFrame as infected.** If a virus filter detects an HTML page that contains a hidden malicious iFrame, the message is treated as infected.

You can enable these options in the **Main** > **Policy Management** > **Filters** page by clicking **Add** and selecting the virus filter type.

New message disclaimer filter feature

Allow message recipients to report a message as spam via a new message disclaimer filter feature (**Main > Policy Management > Filters**). Click **Add** and select the disclaimer filter type. You can then mark the **Enable Report Spam feature** check box on this page. The link in the disclaimer text sends the email recipient to the Personal Email Manager, where the message can be reported to Websense from the quarantine list as spam.

New filter action options

The following filter action options are new to Email Security Gateway policy rules. They are recommended for use with the new custom content and URL scanning filters.

- **Delay message delivery until.** When you want to delay delivery of a message, you can configure a custom content filter to detect a particular message attribute (e.g., message subject) and use this filter action to delay delivery.

  Specify a day and time for message delivery.
- **Use IP address.** When you want to route a large volume of outbound mail through multiple IP addresses, configure a custom content filter to detect specified message attributes (e.g., sender domain) and use this filter action to determine the IP address to which messages are sent.

  Specify a standalone appliance IP address from the drop-down list for message delivery. (Only appliances configured as standalone appear in the list.) The IP addresses in the list are configured in the V-Series appliance manager. (See Websense Appliance Manager Help for information.)
- **Resume message scanning.** This option allows message analysis to continue, moving to the next filter in sequence if the current filter is triggered. This action may be used if you want message analysis to continue after a URL match is detected in a message.

Message management

Enhancements to Email Security Gateway message processing include the following features and options:

Quarantine administrator options

Previous versions of Email Security Gateway included the capability for a Super Administrator to assign a quarantine administrator role to an Email Security administrator. The quarantine administrator could search for, access, and release blocked messages but could not modify any Email Security settings.

In this version, an Email Security Super Administrator can assign specific blocked message queues to each quarantine administrator. The administrator has access only to those assigned message queues.

A Super Administrator creates Email Security administrator accounts in the TRITON Unified Security Center Administrators page (**TRITON Settings > Administrators)**. Accounts created here appear in the Email Security **Settings > General > Administrator Accounts** page.

By default, a new Email Security module-specific administrator is an Auditor. Click **Edit Role** for the account you want to modify and change the role to Quarantine Administrator. See TRITON - Email Security Help for information regarding quarantine administrator queue assignments.

A quarantine administrator who is granted Data Security access is allowed to view the Message Log to determine if a message was blocked by the Data Security data loss prevention (DLP) function. The ability to view DLP incident details is configured in the TRITON - Data Security module. See TRITON - Data Security Help for information.

Address rewriting

An email envelope recipient address can be rewritten to redirect message delivery to a different address. Envelope sender and message header addresses can also be rewritten to mask address details from message recipients. You can configure address rewriting for inbound, outbound, and internal messages.

Configure address rewriting in the **Settings > Inbound/Outbound > Address Rewriting** page. See TRITON - Email Security Help for details regarding email or domain address rewriting capabilities.

Centralized blocked message queue search

In previous versions of Email Security Gateway, the **Main > Message Management > Blocked Messages** page displayed a list of message queues. Each message queue could be viewed and searched separately after you clicked the queue name.

In this version, the **Main > Message Management > Blocked Messages** page lists all blocked messages together in a single table, with a column entry that indicates the queue in which a message is stored.

Clicking **Search** at the top of the blocked messages list allows you to perform a search on all the messages displayed in that list across queues. Note that quarantine

administrators can view and search only the messages in their respective assigned blocked message queues.

A new **Main > Message Management > Message Queues** page displays the queue list previously accessed from the **Main > Message Management > Blocked Messages** page. See TRITON - Email Security Help for details about all message queue functions.

Scheduled message delay feature

Schedule a message delivery day and time via a new filter action (see *New filter action options*, page 5), and view all delayed messages in the Delayed Messages queue (**Main > Message Management > Delayed Messages**). An entry of **Scheduled delay** in the Reason for Delay column of the queue indicates a message whose delivery has been intentionally delayed. An entry of **Exception delay *n*** indicates a temporary message delivery delay due to connection issues (where *n* is the number of delivery retry attempts remaining for that message).

Message Log details

View Message Log message details in the **Main > Status > Logs > Message Log** page. When you click a message in the Message Log ID column to view recipient details, a new **View Log Details** button appears at the bottom of the page. Message details displayed after you click the button include the date and time of receipt, the type of log or the source of the message details (connection, message, policy, or delivery), and the message details. Information shown may include connection type, message direction (inbound, outbound, or internal), policy applied, and delivery status. See TRITON - Email Security Help for more information about message details.

New connection control option

Email Security Gateway can now control the use of the SMTP VRFY command via a new **Settings > Inbound/Outbound > Connection Control** option. Marking the **Enable SMTP VRFY command** option helps Email Security validate usernames. See TRITON - Email Security Help for information regarding this option.

New message control option

DomainKeys Identified Mail (DKIM) is a validation method that uses a message header digital signature to associate a domain name with an email message. Email Security Gateway now has a DKIM signature verification function that can retrieve signer information, including a public key, from the DNS. Email Security analyzes and verifies the signer information to determine message legitimacy.

Enable Email Security Gateway DKIM verification in the **Settings > Inbound/Outbound > Message Control** page.

You can configure a custom content policy filter to detect a DKIM signature in a message header. See *Custom content filter*, page 3, in these Release Notes for information.

Trusted IP address group capacity

In previous versions, the Email Security Trusted IP address group (**Settings > Inbound/Outbound > IP Groups**) was limited to 32 addresses. In version 7.7, this limit is now 1024 addresses.

Reporting

The following new reporting features are added to this version of Email Security Gateway:

- *New dashboard charts*
- *More custom report templates*
- *Custom report logo*

New dashboard charts

Email Security now includes the new charts described in the following table. The charts can be displayed on the Today or History dashboard pages, as indicated in the table descriptions. Click **Customize** on the dashboard page to add any of these charts to your display.

Chart Name	Description
Outbound Encrypted Message Summary	Displays the number of outbound messages that are encrypted, sorted by the encryption method used (mandatory TLS, hybrid service, or third-party application). The chart can appear on the Today and the History dashboard pages. This information is also available as a presentation report.
Inbound Message Throughput	Displays both the average and peak inbound message throughput rates for the Email Security Gateway appliance. This chart is available only for the Today dashboard page.
Outbound Message Throughput	Displays both the average and peak outbound message throughput rates for the Email Security Gateway appliance. Internal messages (those between protected domains) are included in this chart's calculation. The chart is available only for the Today dashboard page.
Inbound Message Embedded URL Summary	Displays the percentage of scanned inbound messages that contain at least 1 embedded URL. Results are sorted by message analysis results (clean, virus, spam, data usage, or exception). This chart is available for the Today and History dashboard pages.

Chart Name	Description
Outbound Message Embedded URL Summary	Displays the percentage of scanned outbound messages that contain at least 1 embedded URL. Results are sorted by message analysis results (clean, virus, spam, data usage, or exception). This chart is available for the Today and History dashboard pages.
Inbound Message Embedded URL Classification Summary	Displays the percentage of embedded URL categories found in scanned inbound messages. The unique categories represented in each message are counted rather then the actual number of URL occurrences in the message. This chart is available for the Today and History dashboard pages.
Outbound Message Embedded URL Classification Summary	Displays the percentage of embedded URL categories found in scanned outbound messages. The unique categories represented in each message are counted rather then the actual number of URL occurrences in the message. This chart is available for the Today and History dashboard pages.

More custom report templates

In this version of Email Security Gateway, more presentation reports in the Report Catalog can be customized to suit your needs. These new customizable templates allow you to generate reports based on domains.

Report templates that can be customized display a different icon in the Report Catalog from reports that cannot be customized. If the **Save As** button is enabled when you select a report name, then you can save and edit the report format and content to meet your specific reporting needs. The **Save As** button is not enabled if you select a report that cannot be customized.

Custom report logo

When you create a custom report and edit its report filter, you can choose a custom logo for that report. You must have already prepared and copied a logo file to the appropriate directory. See TRITON - Email Security Help for logo file format requirements and image file directory location.

Email hybrid service

This section describes changes to the Email Security Gateway Anywhere hybrid service component. The hybrid service provides an extra layer of email filtering, stopping spam, virus, phishing, and other malware attacks before they reach your network.

Hybrid Service Log

A new Hybrid Service Log contains records of the email messages that are blocked by the hybrid service before they reach the network. View the log at **Main** > **Status** > **Logs** by clicking the Hybrid Service tab.

Log viewing and scrolling options are the same as for the other Email Security logs. See TRITON - Email Security Help for Hybrid Service Log details.

Hybrid Service Log options are set on the **Settings** > **Hybrid Service** > **Hybrid Service Log** page. You can enable the Hybrid Service Log and determine the log's data transfer schedule on this page.

These options are available only if you have already entered a valid Email Security Gateway Anywhere subscription key and you have registered Email Security with the hybrid service.

Hybrid service configuration

Several changes are made to the hybrid service registration wizard to enhance the configuration experience for the user. In particular, the following changes are made:

- New, more descriptive names, instructions, and informational messages for the various hybrid service registration steps
- A Check Status button on the **CNAME Records** screen (previously named **DNS**), to verify that your CNAME records are correctly configured in your domain name system. A subsequent check for domain ownership is not performed once the hybrid service verifies the ownership of a particular domain.
- A Check Status button on the **MX Records** screen (previously named **MX**), to verify that your MX entries are correctly set in your domain name system

Personal Email Manager

The following enhancements to the Personal Email Manager end-user utility are added to this version of Email Security Gateway:

- *User account management options*
- *Personal Email Manager server alert notifications*

User account management options

You can enable the following functions for a Personal Email Manager end user by marking the **Enable user account management** check box on the **Settings** > **Personal Email** > **User Accounts** page:

- Delegate blocked email management to another individual.

- Allow an end user in a non-LDAP based user directory to manage multiple Personal Email Manager email accounts in the same session.

  Important

  For Personal Email Manager users in LDAP-based user directories, this function can be enabled on the Add (or Edit) User Directory page by marking the **Enable multiple user email account access in a single Personal Email Manager session** check box.

  All email accounts for this user are automatically available in the Personal Email Manager tool, in the **View user account** drop-down list.

  See TRITON - Email Security Help for details.

An end user can delegate blocked email management to another individual by clicking **User Account Access** in the left pane menu in the Personal Email Manager utility and entering the desired email addresses. See Personal Email Manager User Help for details.

Similarly, a user with multiple email accounts who is part of a non-LDAP user directory can manage all those accounts in a single Personal Email Manager interface. The user logs in to Personal Email Manager once as each account and specifies 1 email account to manage the other accounts. User email accounts are then available in the **View user account** drop-down list. See Personal Email Manager User Help for details.

Note

In previous versions of Email Security, the v7.7 User Accounts page was called the **Settings** > **Personal Email** > **Block/Permit Options** page.

Personal Email Manager server alert notifications

Personal Email Manager server status is now monitored. You can configure the display and delivery of Personal Email Manager server event notifications in the **Settings** > **Alerts** > **Alert Events** page.

Installation and upgrade

Topic 70025 | Release Notes | Email Security Gateway | Version 7.7 | Updated: 10-July-2012

Applies To:	Websense Email Security Gateway v7.7 Websense Email Security Gateway Anywhere v7.7

Access the Deployment and Installation Center for instructions on installing, upgrading, and deploying Websense Email Security Gateway v7.7. In particular, see the following topics:

- Installing Email Security Gateway on a V-Series appliance
- Installing the TRITON Unified Security Center
- Deploying Email Security Gateway
- Upgrading Email Security Gateway to v7.7

Requirements

Email Security Gateway is supported only on a Websense V-Series appliance (V10000 G2 or V5000 G2). The TRITON management server and Email Security Log Server are hosted on a separate Windows Server machine (this server must be running an English language instance of Windows Server). Microsoft SQL Server is used for the Email Security log database. Click here for a detailed list of TRITON - Email Security system requirements.

Note

The TRITON - Email Security module is not compatible with instances of Email Security at previous versions.

For example, the TRITON - Email Security management server v7.7 is not compatible with an appliance running Email Security Gateway v7.6.

End of support for Windows Server 2003

The TRITON - Email Security module and Log Server are no longer supported on Windows Server 2003 starting with v7.7. If your TRITON components are currently running on Windows 2003 and you are upgrading to version 7.7, you should migrate these components to Windows Server 2008 or 2008 R2 before beginning the upgrade process.

Web browser support

Email Security Gateway v7.7 supports the use of the following Web browsers:

- Microsoft Internet Explorer 8 and 9
- Mozilla Firefox versions 5 and later
- Google Chrome 13 and later

Note

If you use Internet Explorer, ensure that Enhanced Security Configuration is switched off.

If you use Internet Explorer 8, note that Compatibility View is not supported.

Installation tips

This section contains information about new features that may affect your product installation and deployment.

Database connection encryption

You can now secure your database connection with SSL encryption. Select this option in 1 of the following ways:

- During Email Security Gateway product installation
- In the **Settings** > **Reporting** > **Log Database** page. See TRITON - Email Security Help for information.
- In the Email Security Log Database Configuration utility. See Log Server Configuration Utility Help for information.

Please note the following issues associated with using the encryption feature:

- You must have imported a trusted certificate to the Log Server machine in order to use the encryption option. See your database documentation for information about importing a trusted certificate.
- The Bulk Copy Program (BCP) option for inserting records into the Log Database in batches cannot be used. Not using the batch method may affect Log Database performance.
- The connection from the Email Security module on the TRITON Console to the V-Series appliance cannot be encrypted. If you enable encryption for Log Database, you must disable the SQL Server force encryption feature. See your Microsoft SQL Server documentation for details.

Non-standard database port selection

You can now configure a non-standard port for Log Database during Email Security product installation. Non-standard ports may be used to provide added security for the database connection.

The Email Security installer displays the standard default port of 1433, but the entry field can be edited.

Default ports

Some Email Security Gateway inbound ports for Personal Email Manager are changed in v7.7. Inbound and outbound ports for connections to the Data Security module are also changed. Email Security v7.6.x port 9080 (inbound) for email data loss prevention resource allocation requests is no longer in use.

If you are upgrading from Email Security v7.6.x, you must open the following ports in your firewall:

- Inbound ports for communication with Email Security Gateway: 17700 - 17714
- Outbound ports for communication with Data Security: 17500 - 17514.

Note that the base port can be customized on product installation.

The following table contains Email Security port changes for v7.7:

Description	Direction	v7.6.x Port	v7.7 Port
Personal Email Manager load balancing	Inbound	6643	9449
Personal Email Manager user interface	Inbound	9449	6643
Email data loss prevention system health and log data	Inbound	8888	17700-17714*
Fingerprint status	Outbound	8888	17500-17514*
Fingerprint repository	Outbound	5821	17500-17514*
Message analysis	Outbound	18404	17500-17514*
*This is the default range. The starting location of the range is configurable.			

A complete list of Email Security Gateway default ports is available in the Deployment and Installation Center.

Updates for Simplified Chinese online Help system users

Topic 70028 | Release Notes | Email Security Gateway | Version 7.7 | Updated: 10-July-2012

Applies To:	Websense Email Security Gateway v7.7 Websense Email Security Gateway Anywhere v7.7

This section contains some online Help system updates for Simplified Chinese Help users. The English-language version of online Help includes these updates.

Headings shown in this section are the corresponding Help topic titles.

Using the First-time Configuration Wizard

The Data Security registration page no longer appears in the first-time Configuration Wizard. If necessary, you can register Email Security with Data Security on the **Settings > General > Data Security** page.

Also, you can no longer skip any page in the wizard. You must enter all required wizard settings on all screens in order to save the configuration.

Managing administrator accounts

The following changes are made to the administrator change process:

- In step 1 of the administrator change process, you should click **Edit Role** (rather than **Change Role**) in the accounts table Role column on the **Settings > General > Administrator Accounts** page.
- In step 4 of the same process, you should mark the **Allow access to DLP incident queue** check box (rather than **Access to Data Security incident queue** check box) to allow a quarantine administrator to view DLP incidents in the Email Security Message Log.

Appliances overview

The following issues must be considered when you change the host name or system communication IP address of an Email Security appliance in the V-Series Appliance Manager:

- You must update the **Settings > General > Email Appliances** page with the new IP address.
- You should also change the address for the Personal Email Manager notification message (**Settings > Personal Email > Notification Message**).
- For Email Security Gateway Anywhere deployments, the hybrid service must be re-registered.

Managing domain and IP address groups

The descriptions of the Protected Domain and Trusted IP Address groups in the Help are modified as follows:

Protected Domain group

The Protected Domain group should contain all the domains that an organization owns and needs Email Security Gateway to protect. Message direction in Email Security is determined on the basis of an organization's protected domains:

- 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.

An open relay results when both the sender and recipient addresses are not in a protected domain.

Unless you entered a protected domain name in the Domain-based Route page of the First-time Configuration Wizard, the default Protected Domain group is empty after you install Email Security. Domains may be added to or deleted from the Protected Domain group, but you cannot delete the Protected Domain group itself.

Important

Ensure that the Protected Domain group contains all the domains you want Email Security to protect.

An open relay is created when mail from an unprotected domain is sent to an unprotected domain within your organization. As a result, Email Security may reject all mail from any domain that is not protected. Mail from an external trusted IP address to an unprotected domain within your organization bypasses analysis and is delivered.

The hybrid service uses the Protected Domain group during hybrid service registration to verify that the domains specified in its delivery routes are all from this group. The Protected Domain group should not be used to configure Email Security Gateway delivery routes (in the **Settings > Inbound/Outbound > Mail Routing** page) if you need to define domain-based delivery routes via multiple SMTP servers.

Trusted IP Address group

Like the Protected Domain group, the Trusted IP Addresses default group is empty after you install Email Security. IP addresses may be added to or deleted from the Trusted IP Addresses group, but you cannot delete the Trusted IP Addresses group itself.

Trusted IP addresses may include your internal mail servers or a trusted partner mail server.

Mail from an address in the Trusted IP Addresses group can bypass some inbound email filtering. Use of the Trusted IP Addresses group can result in improved email processing time.

Specifically, mail from trusted IP addresses bypasses the following email filtering:

- Global Always Block and Always Permit lists (**Main > Policy Management > Always Block/Permit**)
- All message controls except message size limitations (**Settings > Inbound/Outbound > Message Control**)
- Recipient validation (**Settings > Users > User Authentication**)
- All connection controls (**Settings > Inbound/Outbound > Connection Control**)
- Directory harvest attack (**Settings > Inbound/Outbound > Directory Attacks**)
- Relay controls (**Settings > Inbound/Outbound > Relay Control**)

> **Note**
> Mail from trusted IP addresses does not bypass policy and rule application, and it is always subject to antispam and antivirus filtering.

You may delete a domain or IP address group from its respective list by selecting the check box to the right of the name and clicking **Delete**. The default groups (Trusted IP Addresses and Encryption Gateway) cannot be deleted.

Encryption Gateway IP address group

The default Encryption Gateway IP address group supports only the entry of individual IP addresses. Subnet address entries are considered invalid and are not accepted for this IP address group.

Subnet addresses may be entered for other default and custom IP address groups.

Creating and configuring a filter

The following filter option has been removed from the Websense antivirus filter:

Treat damaged files as infected.

Message control settings

In the **Settings > Inbound/Outbound > Message Control** page Message Volume Options, the upper value for the range of maximum number of recipients allowed is changed to 4096.

Resolved and known issues

Topic 70026 | Release Notes | Email Security Gateway | Version 7.7 | Updated: 10-July-2012

Applies To:	Websense Email Security Gateway v7.7 Websense Email Security Gateway Anywhere v7.7

A list of resolved and known issues for Websense Email Security Gateway is available in the Websense Technical Library. If you are not already logged on to MyWebsense, this link takes you to the log in screen.