v7.7.3 Release Notes for Email Security Gateway

Topic 55407 | Release Notes | Email Security Gateway | Version 7.7.3 | Updated: 24-January-2013

Applies To:	Websense Email Security Gateway v7.7.3 Websense Email Security Gateway Anywhere v7.7.3

Websense® Email Security Gateway version 7.7.3 is a feature and correction release. It includes several improvements and fixes, many requested by our customers. Part of the TRITON™ Enterprise suite, 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.

- Existing Email Security Gateway customers can obtain the 7.7.3 patch on the Websense Web site and then patch up to this version. Please read these Release Notes for important preparation steps, especially if you are currently running version 7.6.x.
- Version 7.7.3 is the first version of Email Security Gateway for which the Recovery Image is provided in USB format (rather than a DVD image). This means that you can download the Recovery Image from the Websense Web site and then copy it to a USB thumb drive, for use if you desire to image an appliance to the 7.7.3 factory settings.

Use these Release Notes to find information about new features in Email Security Gateway and Personal Email Manager. Version 7.7.3 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 v7.7.3

Topic 55408 | Release Notes | Email Security Gateway | Version 7.7.3 | Updated: 24-January-2013

Applies To:	Websense Email Security Gateway v7.7.3 Websense Email Security Gateway Anywhere v7.7.3

In addition to four new alerts in the alerting system, new Email Security Gateway features are available in the following product areas:

URL Sandbox

URL sandboxing has been added in this release. Sandboxing provides real-time analysis of uncategorized URLs that are embedded in Email Security inbound mail.

When a user clicks an uncategorized URL in an email message, a landing page prompts the user to initiate URL analysis. If the analysis determines that the link is malicious, the site is blocked. If the link is not malicious, the user receives notification that he or she may proceed to the site.

You can create a list of domains to which URL sandbox settings do not apply, along with recipient-specific settings based on domain or email addresses.

The URL sandbox feature can be configured during hybrid service registration, and also any time after registration.

The **Settings > Inbound/Outbound > URL Sandbox** menu item facilitates URL sandbox configuration (after hybrid service registration).

- Clicking this menu item displays the hybrid service registration Delivery Route page, where URL sandboxing can be configured.
- You can add or modify URL sandbox settings from this location.

Detailed logging for connections

You can now collect and view detailed information about specific connections. To do this, you enable an Email Security function to save these details in the mail processing log, accessed via the V-Series appliance.

When the new function is activated, the log collects detailed data regardless of whether the connection control itself is enabled. This function is available for the following connection control options:

- Real-time blacklist (RBL)
- Reverse DNS lookup
- Reputation service
- SMTP greeting delay

Mark the **Save connection details in the mail processing log** check box to save detailed connection information in the appliance mail processing log.

Commercial bulk email filter

A new commercial bulk email filter can analyze a message to determine whether it was sent from a third-party bulk email management company or directly from a business.

Unlike spam email, commercial bulk email is often solicited by its recipients, sometimes inadvertently. For example, a user might neglect to clear a check box to “Share my personal information with selected partners” on a typical “opt out” privacy rights form.

When you select the commercial bulk email filter type,you can choose the sensitivity level for the filter:

- **Detect email messages sent from known commercial bulk email sources.** Use this option if you want the filter to detect email only from indirect (third-party) sources of bulk email (default).
- **Detect email messages that contain commercial content in addition to messages from known commercial bulk email sources.** Use this option if you want the filter to detect both direct and indirect sources of bulk email.

If you want message size to determine whether commercial bulk email analysis is bypassed, mark the **Bypass commercial bulk email detection if message size exceeds** check box and enter a message size in KB (default is 1024).

A commercial bulk default filter action can be used along with this filter:

> **Commercial Bulk.** Deliver the filtered message and add “COMMERCIAL:” to the message subject

A default policy rule is also available for use.

Commercial bulk will appear as a message analysis result in the Message Log and message queues.

Email header modification

This version offers new filter action message delivery options, for use when the filter action is “Deliver the filtered message.”

- **Delete message header Received tag.** Mark this check box if you want Email Security to strip all message header Received tags.
- **Modify message header Reply-To tag.** Email Security can change a Reply-To header tag based on Find and Replace field entries.

  Enter a domain, user name, or email address you want to search for in the Find field. Then enter a domain, user name, or email address with which you want to replace the found entry.

  You may replace a domain only with another domain, a user name only with another user name, and an email address only with an email address. You may also find or replace a blank email address entry by entering “<>” in the appropriate field. An asterisk (*) in the Find field lets you replace any domain, user name, or email address with the Replace field entry.
- **Delete X-header.** You can now enter up to 16 X-headers for deletion at one time. Specify X-headers for deletion by entering at least one header (without its header value) in the **Delete X-header** entry field. Each entry must begin with “X-” and contain alphanumeric characters using ASCII character codes 0 - 127. Use a semicolon to separate multiple X-header names.
- **Modify message header Subject tag.** Two new options have been added for modifying the original Subject tag. You can now specify Subject tag changes in 1 of 2 ways:
  - Modify the original message Subject tag by entering subject text that you want to find and replace in the Find and Replace fields, respectively.
  - Add text to the beginning or the end of an original Subject tag by entering the appropriate string in the Prepend or Append fields, respectively.
- **Add or edit X-header.** You can now add or edit up to 16 X-header name and value pairs at one time. Add X-headers to any message that triggers the filter associated with a specified action. Enter at least one X-header name and value pair in the **X-header name and value** entry field. The X-header name entry

must begin with “X-”, and both the name and value entries must contain alphanumeric characters using ASCII character codes 0 - 127. Use a colon to separate the X-header name and value (for example, x-header**:**value). Use a semicolon to separate multiple pairs containing an X-header name and its value.

Data Security disclaimer messages

Email Security Gateway allows administrators to add a disclaimer to messages processed and delivered by the system. Prior to version 7.7.3, if the email was quarantined by the Data Security Incident Manager and then later released, the disclaimer message was not added. The disclaimer message is now added to messages released from the Data Security quarantine as well.

Personal Email Manager custom URL access

You can now customize the URL for Personal Email Manager access, to suit your needs.

On the page **Settings > Personal Email > Notification Message > Notification Message Links**, use the Custom URL field to enter a URL path for Personal Email Manager user access that is different from the one automatically generated using the IP address and port.

This Custom URL is also used for notification message hyperlinks.

The path can have a maximum length of 250 alphanumeric characters, hyphens, and underscores; a hyphen cannot be the first character. The custom URL supports one subdirectory (for example, www.mycompany.com/pemserver) and should use the port designated in the Port field.

Personal Email Manager end user Deliver action

The **Deliver** option for PEM end users has been enhanced. The PEM administrator can now control how the **Deliver** option behaves.

Deliver (default selection), allows the user to release a blocked message. The email may be delivered directly to the user’s inbox, or it may be submitted for continued processing by subsequent filters if appropriate.

The behavior is determined in the **Settings > Personal Email > End-user Portal** page, in the Quarantined Message Delivery Options section.

The PEM administrator selects one of the following options:

- **Deliver quarantined message**, to allow end users to release blocked email for direct delivery to their inboxes
- **Resume quarantined message processing**, to force the analysis of blocked email to resume through all subsequent filters. If this option is used, a message may not be delivered to an end user if it triggers a subsequent filter.

Online Help addendum

The information in this section came to light after the embedded Help system was embedded into the product. These two items augment the information in the embedded Help system (they apply to both English and Simplified Chinese).

TRITON - Email Security Help:

- The maximum number of addresses allowed in the default Trusted IP Address group (**Settings > Inbound/Outbound > IP Groups**) is **128**. (Help topic is titled *Managing domain and IP address groups*)
- In the First-time Configuration Wizard Domain-based Route page, you can enter the SMTP server IP address or hostname. (Help topic is titled *Using the First-time Configuration Wizard*)

The following additional 2 fields are displayed when you view an email message in a message queue: (Help topic is titled *Viewing a message in a queue*)

Policy - Name of the policy applied to the message

Message type - Message type, indicating message analysis results (Clean, Virus, Spam, Data Usage, Exception, Commercial Bulk, or Custom Content)

Personal Email Manager User Help

In the Quarantined Messages List, the message type field can also include 2 entries for commercial bulk email: (Help topic is titled *Managing quarantined messages*)

- Commercial bulk
- Exception Commercial Bulk

Installation and upgrade

Topic 55409 | Release Notes | Email Security Gateway | Version 7.7.3 | Updated: 18-January-2013

Applies To:	Websense Email Security Gateway v7.7.3 Websense Email Security Gateway Anywhere v7.7.3

Please see the Requirements section immediately below for important operating system and browser information.

Access the Deployment and Installation Center for instructions on installing, upgrading, and deploying Websense Email Security Gateway v7.7.3. 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 and future models). 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.x is not compatible with an appliance running Email Security Gateway v7.6.x.

No support for Windows Server 2003

The TRITON - Email Security module and Log Server are not supported on Windows Server 2003 starting with v7.7.0. If your TRITON components are currently running on Windows 2003 and you are upgrading to version 7.7.3, you should migrate these components to Windows Server 2008 or 2008 R2 before beginning the upgrade process.

Web browser support

Email Security Gateway v7.7.3 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 secure your database connection with SSL encryption. Select this option in one 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 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

Customers who are upgrading from Email Security Gateway v7.6.x need to be aware that some Email Security Gateway inbound ports for Personal Email Manager were changed at v7.7.0. Inbound and outbound ports for connections to the Data Security module were also changed at v7.7.0. 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 during product installation.

The following table contains Email Security port changes for v7.7.0:

Description	Direction	v7.6.x Port	v7.7.x 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 55410 | Release Notes | Email Security Gateway | Version 7.7.3 | Updated: 18-January-2013

Applies To:	Websense Email Security Gateway v7.7.3 Websense Email Security Gateway Anywhere v7.7.3

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 does not appear 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 cannot 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

Note the following for 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 55412 | Release Notes | Email Security Gateway | Version 7.7.3 | Updated: 18-January-2013

Applies To:	Websense Email Security Gateway v7.7.3 Websense Email Security Gateway Anywhere v7.7.3

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