v7.8.x Release Notes for Email Security Gateway

Topic 70036 | Release Notes | Email Security Gateway | Version 7.8.x | Updated: 22-Oct-2013

Applies To:	Websense Email Security Gateway v7.8.x Websense Email Security Gateway Anywhere v7.8.x

Websense® Email Security Gateway version 7.8 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.

Use these Release Notes to find information about new features in Email Security Gateway and the Personal Email Manager end-user component. Version 7.8 Release Notes are also available for the following Websense products:

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

See the *Email Security Manager Help* for details about Email Security Gateway operations.

If you are installing Email Security Gateway for the first time, see Installing Websense Appliance-Based Solutions.

If you are upgrading from a previous version of Email Security Gateway, see Upgrading Email Security Gateway Solutions.

Contents

- *New in Email Security Gateway v7.8.x*
- *Installation and upgrade*
- *Known issues*

New in Email Security Gateway v7.8.x

Topic 70037 | Release Notes | Email Security Gateway | Version 7.8.x | Updated: 22-Oct-2013

Applies To:	Websense Email Security Gateway v7.8.x Websense Email Security Gateway Anywhere v7.8.x

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

- *Virtual appliance deployment*
- *Policy management*
- *Message management*
- *Reporting*
- *Email Security Gateway system management*
- *Email hybrid service*
- *Personal Email Manager Audit Log*
- *Find Answers portal*

Virtual appliance deployment

Email Security Gateway may now be deployed on a virtual appliance using a VMware platform (ESXi v4.0 or later). The appliance image is available for download from MyWebsense in an open virtualization format (OVF) package. A TRITON manager installed on a separate Windows machine is required for Email Security Gateway administration functions.

The virtual appliance security mode is Email Security only. Dual mode functions are not supported.

You may create a cluster of virtual appliances, but you cannot cluster a virtual appliance with a V-Series appliance.

See the virtual appliance Quick Start Guide for complete information about deploying and configuring the virtual appliance.

Appliance hotfix download and SNMP alerting capabilities are not supported. The following appliance status functions are also not supported in this version of the virtual appliance:

- CPU and memory usage
- Disk usage
- Network bandwidth
- Service status

Some of this status information may be obtained via other, existing Linux commands. For example, you can use the **iostat** or **du** command to view disk usage capacity information. See the Quick Start Guide for other examples.

Important

You must restart the Email Security services any time you change the host name or IP address configuration for your virtual appliance.

- Use the configuration utility **Restart Network Service** command during the first-time virtual appliance configuration or any time you add a virtual appliance to an existing TRITON installation.
- You should run the **esg_restart.sh** command in the virtual appliance any time you change host name or IP address information for the appliance after the initial configuration.

Policy management

- *Websense ThreatScope analysis*
- *Additional filter action message delivery options*
- *Threat detection enhancements*

Websense ThreatScope analysis

ThreatScope is a cloud-hosted sandbox for deep content inspection of types of files that are common threat vectors. This functionality is available only if your Email Security Gateway subscription includes the ThreatScope add-on feature.

ThreatScope cloud-hosted analysis inspects email attachment file types that commonly contain security threats (including .exe, .pdf, .xls, .xlsx, .doc, .docx, .ppt, .pptx, and archive files). A severity level equal to or greater than 7 results in a ThreatScope alert.

Configure ThreatScope analysis on the **Main > Policy Management > Filters** page, using the default ThreatScope filter or creating a new filter based on the ThreatScope filter type.

ThreatScope can be enabled in 1 of the following operational modes:

- **Monitor** (default). Message is delivered to its recipient, and a copy is sent to ThreatScope for analysis. If analysis determines that the attachment is clean, no report is returned. If ThreatScope analysis determines the attachment is malicious, the message is copied to a specified queue. A notification email regarding the analysis result can be configured.

The corresponding filter action should be configured to ensure that the email message that triggered the filter is dropped and saved to a specified queue (**Main > Policy Management > Actions)**. Default queue is the virus queue.

- **Enforce.** Message is held in a queue until ThreatScope analysis is performed. If analysis determines that the attachment is clean, message processing is resumed. If ThreatScope analysis determines the attachment is malicious, the email is quarantined. A notification email regarding the analysis result can be configured.

  The corresponding filter action should be configured to ensure that the email message that triggered the filter is dropped and saved to a specified queue (**Main > Policy Management > Actions)**. Default queue is the virus queue.

- **Enforce and notify.** Message is held in a queue until ThreatScope analysis is performed, and an email notifying the recipient that ThreatScope analysis is underway can be configured. Mark the **Send enforcement notification** check box to configure this message, which contains the original message as an attachment. The message attachment is handled as follows:

  - Some file types are converted to plain text (.pdf, .doc/.docx, .xls/.xlsx, and .ppt/.pptx).
  - Files of other types are removed and only the filename appears in the message (.exe and archive files).

  The corresponding filter action should be configured to ensure that the email message that triggered the filter is dropped and saved to a specified queue (**Main > Policy Management > Actions)**. Default queue is the virus queue.

Select the attachment file types you want ThreatScope to analyze by marking the appropriate check boxes. You can also define conditions that, when met, allow a message to bypass ThreatScope analysis.

A default ThreatScope filter action is available for use with the ThreatScope filter, to form a ThreatScope policy rule. See *Email Security Manager Help* for information.

Note

If ThreatScope analysis does not return a result after 1 hour, the message is considered clean. If you want Email Security Gateway to consider such a message malicious, please contact Websense Technical Support.

Additional filter action message delivery options

New filter action options are added in this version of Email Security Gateway (**Main > Policy Management > Actions > Add** [or **Edit**] **Action**):

- Header modification conditions for the Resume Processing and Deliver Message actions are enhanced. After you mark the **Enable Header Modification** option, use the drop-down list to select the type of header modification you would like performed on a message, then provide the needed modification parameters.

- **Bcc to**, to send a blind copy of a message that triggers a filter to a specified email address. This option is available for the Resume Processing and Deliver Message actions.
- Message delivery based on a defined domain-based route. Mark the appropriate check box and select a domain-based route from the drop-down list. This option is available for the Resume Processing and Deliver Message actions.
- **Forward to**, to send a copy of a message that triggers a filter to a specified email address (for example, an administrator). This option is available only for the Drop Message action.
- Personal Email Manager portal options are now included with the **Save the original message to a queue** selection. You can specify whether the message:
  - Can be managed by a Personal Email Manager end user
  - Is not displayed in the Personal Email Manager end-user portal
  - Is referenced only by a log entry in Personal Email Manager

  These Personal Email Manager options are available for all message delivery actions.

Threat detection enhancements

Enhancements to the custom content filter allow you to detect and provide separate message handling for individual Websense message analysis tools. For example, if you configure a custom content filter to detect when digital fingerprinting analysis indicates that a message is spam, you can configure a corresponding filter action to save that message in a separate, user-defined queue.

You can set up filters for the following engines:

- Digital fingerprinting
- LexiRules
- Heuristics
- Hybrid service (if your subscription is for Email Security Gateway Anywhere)

Configure a custom content filter on the **Main > Policy Management > Filters > Add Filter** page, Custom Content filter type. Then configure an antispam filter action to handle any message that triggers the filter.

Message management

- *URL sandbox enhancement*
- *Traffic shaping*
- *True source IP detection*
- *Enforced TLS connections*
- *Routing delivery preference setting*

- *Relay control SPF check bypass option*

URL sandbox enhancement

In previous versions of Email Security Gateway Anywhere, URL sandbox features were configured as part of email hybrid service registration.

These configuration settings are now available in the **Settings > Inbound/Outbound > URL Sandbox** screen. You must complete hybrid service registration successfully before you can configure URL sandbox capabilities.

This functionality is available only if your Email Security Gateway Anywhere subscription includes the add-on URL sandbox feature.

Traffic shaping

Enhancements to message delivery settings provide more administrator control over message delivery. The **Settings > Inbound/Outbound > Traffic Shaping** screen lets you determine the rate of traffic delivery for a specified source or destination group based on domain group or user directory settings. For example, these settings allow you to send large volumes of email at a rate that prevents possible blacklisting of the domain.

In previous versions of Email Security Gateway, message delivery options were configured on the **Settings > Inbound/Outbound > Delivery** screen.

The following message delivery settings may be modified for traffic shaping:

- Maximum number of concurrent connections
- Maximum number of messages per connection within a designated time period
- Maximum number of recipients per message
- Use of the SMTP session cache, for which the maximum number of messages per session and the session duration are specified

> **Note**
> Undeliverable message options that previously appeared on the **Settings > Inbound/Outbound > Delivery** screen are now accessed on a new **Settings > Inbound/Outbound > Undeliverable Options** screen.

True source IP detection

True Source IP detection uses message header information and the number of network hops to Email Security Gateway to determine the IP address of the first sender outside the network perimeter. This feature enables connection control techniques (such as real-time blacklists and reputation checks) to be applied effectively to sender information, even when Email Security Gateway is downstream from a firewall or an internal mail relay.

Configure your Email Security direct relay and all network edge devices in the **Settings > Inbound/Outbound > True Source IP** page.

Enforced TLS connections

You can specify that connections to or from a specific IP or domain group use mandatory Transport Layer Security (TLS) and determine the security level used by that connection. Use the **Settings > Inbound/Outbound > Enforced TLS Connections** page to specify the IP addresses or domain groups for which Email Security Gateway forces TLS connections.

When you add a connection for which you want mandatory TLS used, you can also specify the security level for that connection. Security level options include the following:

- **Encrypt**, the minimum enforcement level, used in all security level options
- **Encrypt and check CN**, encryption and validation of a certificate's common name
- **Verify**, encryption and validation that the certificate is from a trusted CA
- **Verify and check CN**, encryption, along with validation of the certificate's common name and that the certificate is from a trusted CA

Only the Encrypt security level is available for inbound traffic. All 4 levels are supported for outbound traffic.

The following connection encryption strength options are available:

- **Medium**, which involves the use of cipher suites that use 128-bit encryption
- **High**, which includes most cipher suites with key lengths larger than 128 bits

Routing delivery preference setting

When you add an SMTP server address for a mail route on the **Settings > Inbound/Outbound > Mail Routing > Add** (or **Edit**) **Route** page, you can now indicate a delivery preference for that server address.

Previous versions of Email Security Gateway used a round robin method.

If a single route has multiple defined server addresses, Email Security attempts to deliver mail in order of server preference. When multiple routes have the same preference, round robin delivery is used.

Note

Upgrading to v7.8.x may cause changes in routing behavior. If multiple servers are configured for a single route, each server is assigned a preference of 5 after the upgrade.

Relay control SPF check bypass option

You can designate a domain group for which SPF checks are not performed as part of the relay control function on the **Settings > Inbound/Outbound > Relay Control** screen.

In the Bypass SPF Option box, mark the **Bypass SPF validation for senders in the following domain group** check box, and select a sender domain from the **Domain group** drop-down list.

Reporting

- *Real-time email traffic monitor*
- *New presentation reports and dashboard charts*

Real-time email traffic monitor

Available on the **Main > Status > Real-Time Monitor** page, a new email traffic monitor displays log information details in real time for email traffic on selected appliances. This information can be valuable for troubleshooting purposes.

You can specify any of the following types of log information for display:

- Message status
- Connection status
- Message delivery status
- Message analysis result

Use the search filter to find individual log entries, or use advanced search functions to filter the log entries by subject, IP address, or email address.

New presentation reports and dashboard charts

Several new dashboard charts and presentation reports are included in this version of Email Security Gateway. These charts and reports provide administrators with more information about the types and characteristics of the email processed in the network.

In some cases, drill-down data is available when a user clicks a data element in a Today or History page dashboard chart. For example, when you view the total number of ThreatScope-detected malicious attachments for the previous 24 hours, sorted by attachment file type, you can click a single file type bar to view the hourly detection levels for that file type.

Some new reports and charts display the following:

- Message volume by traffic direction
- Message volume by message type

- Message volume of TLS message transmission
- Commercial bulk, spam, or virus email by volume or percentage
- Malicious attachments detected by ThreatScope

See the complete list of reports in the Report Catalog (**Main > Status > Presentation Reports**). For a list of dashboard charts, click **Customize** on the Today or History pages.

Setting a date range for reports has been simplified in the Run Report and Report Scheduler wizards. See Email Security Gateway Manager Help for information.

Email Security Gateway system management

- *Delegated administration*
- *Custom SMTP port number*
- *Trusted CA certificate import*
- *Non-spam email transmission to Websense*

Delegated administration

This version of Email Security Gateway offers more options for delegation of administrator responsibilities among individuals with different administrator roles. View administrator management settings on the **Settings > Administrators > Delegated Administrators** screen.

The following new administrator roles may be defined on the **Settings > Administrators > Roles** page:

- **Security administrator**, who has permissions identical to a Super Administrator with the exception of managing other administrators
- **Policy administrator**, who can create and manage email policies for specified users or groups. Permissions include reporting and quarantine management for those specified users.
- **Group reporting administrator**, who can schedule, run, and edit reports only for users in specified groups

Existing administrators may be granted new, more granular permissions, for example, covering policy management, log access, or report management. The Auditor role is unchanged from previous releases.

When you create roles for Email Security Gateway delegated administrators, you specify the users or groups managed by the role along with the permissions associated

with the role. Then assign an administrator to that role. An administrator may be assigned to only 1 role at a time.

> **Note**
> Managed users and user groups settings are used only for the following permissions:
>
> - Policies
> - Reports
> - Queues and quarantined messages

Custom SMTP port number

You can change the SMTP port number, if needed, from the default value of 25. Find this setting on the **Settings > Inbound/Outbound > Connection Control** page in the SMTP Port Option section. Valid values are from 25 to 5000.

You should note that proper communication with the Email Security Gateway Anywhere hybrid service requires the use of port 25 for SMTP.

> **Note**
> Changing this port setting causes Email Security Gateway services to restart.

Trusted CA certificate import

You can manage trusted Certificate Authority (CA) certificates for outgoing connections. A table on the TLS Certificate page (**Settings > Inbound/Outbound > TLS Certificate**) displays information about each certificate, including common name, certificate issuer, and expiration date.

An import function lets you browse to the location of a trusted certificate and add it to the Trusted CA Certificate for Outgoing Connection table. A search function allows you to perform a keyword search of all your trusted CA certificates.

Non-spam email transmission to Websense

In previous versions of Email Security Gateway, email released by administrators and end users as “not spam” was forwarded to Websense for classification research in plain text format. This type of mail is now delivered using opportunistic TLS. In other words, TLS transmission for this type of mail is used if possible. If TLS is not available, plain text format is used.

Email hybrid service

- *Hybrid service commercial bulk email filtering*

- *Hybrid service spam threshold configuration*

Hybrid service commercial bulk email filtering

Previous versions of Email Security Gateway included commercial bulk email analysis among the on-premises detection tools. This version now includes commercial bulk email analysis in the hybrid service prefiltering capability. The results of prefiltering are added in the message header passed to Email Security, which uses the hybrid service score to determine how a message is processed.

This new feature can enhance Email Security Gateway processing performance.

Enable this feature on the **Main > Policy Management > Filters > Add** (or **Edit**) **Filter** page for a Commercial Bulk Email filter. This functionality is available only if your subscription is for Email Security Gateway Anywhere.

Hybrid service spam threshold configuration

You can specify a value for email hybrid service analysis that indicates the threshold at which a message should be considered spam. Enable hybrid service analysis on the **Main > Policy Management > Filters** page for the Websense Antispam filter type. Enter a spam threshold value between 0 and 20 (floating point) in the drop-down list.

Personal Email Manager Audit Log

The Personal Email Manager Audit Log records end-user email management activities performed from either the Personal Email Manager notification message or the Quarantined Messages List. Click the Personal Email Manager tab to access this new log on the **Main > Status > Logs** page.

Audit log data includes the following:

- The date and time an end user performed an action on a quarantined message
- The email address of the Personal Email Manager user who performed the message action
- The action performed on the message in Personal Email Manager (Deliver, Delete, or Reprocess; does not include the Add to Always Block list, Add to Always Permit list, or Download actions)
- A database-generated message identifier
- An indicator of whether the Personal Email Manager end-user action was completed successfully

Find Answers portal

This version of Email Security Gateway introduces a new element of the embedded Help system in the right navigation pane: the Find Answers portal.

Depending on the active screen, this portal may include the following components:

- A **Top Picks** section containing links to information related to the screen content
- A **Show Me How** section with links to on-screen step-by-step instructions for performing a task on or related to the current screen
- A **Search** field that you can use to find topics of interest in the Websense eSupport site

Installation and upgrade

Topic 70038 | Release Notes | Email Security Gateway | Version 7.8.x | Updated: 22-Oct-2013

Applies To:	Websense Email Security Gateway v7.8.x Websense Email Security Gateway Anywhere v7.8.x

If you are installing Email Security Gateway for the first time, see Installing Websense Appliance-Based Solutions.

If you are upgrading from a previous version of Email Security Gateway, see Upgrading Email Security Gateway Solutions.

Requirements

Email Security Gateway is supported only on a Websense V-Series appliance (V10000 G2, V10000 G3, or V5000 G2).

You can also deploy Email Security Gateway on a virtual appliance. Download the image file (WebsenseESGA780Setup_VA.ova) from the MyWebsense downloads page. See the virtual appliance Quick Start Guide for deployment information.

Appliance clusters may include a mix of V10000 G2 and V10000 G3 appliances. Please contact Websense Technical Support for help if you want to deploy this type of appliance cluster.

You cannot cluster a V-Series appliance with a virtual appliance.

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. This version introduces support for Microsoft Windows Server 2012

Standard Edition and Microsoft SQL Server 2012. See System requirements for this version for detailed information.

> **Note**
> The Email Security Gateway module is not compatible with instances of Email Security at previous versions.
>
> For example, the Email Security manager v7.7 is not compatible with an appliance running Email Security Gateway v7.6.

Web browser support

Email Security Gateway v7.8 supports the use of the following Web browsers:

- Microsoft Internet Explorer 8, 9, and 10 (desktop interface only)
- Mozilla Firefox versions 4.4 and later
- Google Chrome 13 and later

Database conversion with upgrade

The upgrade process includes a conversion task for existing database files. Any v7.7.x data in the current database partition will be converted after the upgrade operation is complete. Data in other partitions will be converted during a database maintenance job scheduled for midnight after the upgrade.

This job may take a few hours, depending on the number and size of the partitions.

The Message Log displays the following status information for v7.7.x messages until the conversion is complete:

Message Log Field	Content
Scanning Result	Waiting for message analysis
Message Status	Waiting for delivery
Sender IP	(field is blank)

Known issues

Topic 70040 | Release Notes | Email Security Gateway | Version 7.8.x | Updated: 22-Oct-2013

Applies To:	Websense Email Security Gateway v7.8.x Websense Email Security Gateway Anywhere v7.8.x

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.