v7.8.3 Release Notes for Email Security Gateway

Topic 70079 | Release Notes | Email Security Gateway | Version 7.8.3 | Updated: 26-May-2014

Applies To:	Websense Email Security Gateway v7.8.3 Websense Email Security Gateway Anywhere v7.8.3

Websense® Email Security Gateway version 7.8.3 is a feature and correction release that includes improvements and fixes 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.

Important

In some previous versions of Email Security Gateway, a vulnerability in OpenSSL could allow a remote attacker to expose sensitive data, possibly including user authentication credentials and secret keys, due to incorrect memory handling in the TLS heartbeat extension.

Version 7.8.3 of Email Security Gateway does not contain this vulnerability (known as CVE-2014-0160 or Heartbleed).

Use these Release Notes to find information about new features in Email Security Gateway and the Personal Email Manager end-user component. Version 7.8.3 Release Notes are also available for the following Websense products:

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

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.

You can also deploy Email Security Gateway on a virtual appliance. Download the image file (WebsenseESGA783Setup_VA.ova) from the MyWebsense downloads page. See the virtual appliance Quick Start Guide for deployment information.

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

Email Security Manager Help for this release is also available in Simplified Chinese.

Contents

New in Email Security Gateway v7.8.3

Topic 70080 | Release Notes | Email Security Gateway | Version 7.8.3 | Updated: 26-May-2014

Applies To:	Websense Email Security Gateway v7.8.3 Websense Email Security Gateway Anywhere v7.8.3

Enhancements added to version 7.8.2 focus on tighter integration with Data Security DLP policies, enhanced spam detection, and increased system health awareness. The following new Email Security Gateway features are available in version 7.8.3:

- *Email Security Gateway filter action in DLP policy*
- *Spamhaus service integration*
- *Inbound undelivered email alert*

Other enhancements are also included in this release.

Email Security Gateway filter action in DLP policy

Currently, an email DLP policy for Email Security Gateway is configured in Data Security, where the policy's action plan is also specified. This release provides tighter integration between Email Security Gateway and Data Security by allowing a DLP policy action plan to include a filter action configured in Email Security Gateway (**Main > Policy Management > Actions**). DLP policy action plans can now receive the benefit of the following Email Security Gateway filter action capabilities:

- Email header modification
- Notification message delivery
- Personal Email Manager end-user portal options

- Delivery to a specified message queue
- Scheduled message delivery
- Virtual IP address use for large-volume message delivery
- Domain-based routing message delivery
- Blind copy delivery
- Message forwarding

For most network configurations (i.e., single standalone appliance or single appliance cluster), the property settings available for creating an action for an email DLP policy are the same as those for an Email Security Gateway policy action. However, if your network includes multiple standalone appliances or multiple clusters, the DLP policy action settings available when an action is first created are limited.

The following Email Security Gateway message action options are available for use in a filter action created for a Data Security action plan:

- **Resume processing.** Message action options for the resume processing option are the same as those described for the deliver message option, as long as you are creating an Email Security action or you are creating a Data Security action and your network is configured in a single appliance/appliance cluster. (See Email Security Manager Help for information.)

  However, if you are creating an action for use in Data Security, and your network consists of multiple standalone appliances or appliance clusters, the following action property settings are limited:

  - **Use IP address.** Only the IP address of the appliance E1 interface is supported.
  - **Deliver email messages based on domain-based route.** Only the default domain-based route is supported (**Settings > Inbound/Outbound > Mail Routing**).
  - **Save the original message to a queue.** Only Email Security Gateway default queues are supported. You may not specify a user-configured queue.
- **Drop message.** For a Data Security action created in a multiple appliance/multiple cluster environment, only Email Security Gateway default queues are available.
- **Strip attachment option.** Select this option if you want Email Security Gateway to remove an attachment from an email message as part of the policy action. This option is available only for Data Security policy actions.

Spamhaus service integration

A Real-Time Blacklist (RBL) is a third-party published list of IP addresses that are known sources of spam. When RBL checking is enabled, messages from a sender listed on an RBL are prevented from entering your system.

Email Security Gateway now supports the use of the Spamhaus Datafeed server for RBL lookups (**Settings > Inbound/Outbound > Connection Control**). With the

Spamhaus service enabled, a connection IP address is sent to the Spamhaus Datafeed server for analysis. If a connection IP address is on the Spamhaus blacklist, the connection is dropped.

Inbound undelivered email alert

This version of Email Security Gateway includes a new system health alert, **inbound undelivered email notifications**, which are sent when messages are not being delivered because your mail server is down. Undelivered messages are stored in a delayed inbound queue, where they can use an increasingly large amount of disk space.

After you enable this alert type, you can also specify a frequency threshold at which the alert should be sent. Click **Configure alert thresholds** to open the Undelivered Inbound Email Alert Configuration dialog box. Enter a value for the number of connection errors per minute that you want to trigger an alert (default is 1).

Use the **Settings > Alerts > Alert Events** page to configure this alert type.

Other enhancements

This release of Email Security Gateway also includes the following enhancements:

- Improved Personal Email Manager end-user Quarantined Messages List performance
- A new user validation/authentication method called Distribution List, in which individual members of an email distribution list are validated (**Settings > Users > User Authentication**). Ensure that you include group email addresses in your user directories if you want to use this option.
- The Connection Log now displays a connection status of Accepted, along with the reason for an accepted connection.
- A new **Check Status** button on the **Settings > General > Backup/Restore** page which, when clicked, ensures that the specified remote log database server is accessible
- A new **Check Status** button on the **Settings > Alerts > Enable Alerts** page which, when clicked, sends a test message to your SNMP server and verifies that the specified SNMP port is open

Installation and upgrade

Applies To:	Websense Email Security Gateway v7.8.3 Websense Email Security Gateway Anywhere v7.8.3

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 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 (WebsenseESGA783Setup_VA.ova) from the MyWebsense downloads page. See the virtual appliance Quick Start Guide for deployment information.

Note

If Data Security policies are not automatically deployed after a virtual appliance installation, you may need to register Email Security Gateway manually:

1. In the Email Security Gateway module, navigate to **Settings > General > Data Security** and click **Unregister**.
2. Click **Register** to re-register the Email Security Gateway appliance with Data Security.
3. In the Data Security module, click **Deploy** in the upper right area of the screen.

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. See System requirements for this version for detailed information about supported applications and versions.

Note

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

For example, the Email Security manager v7.8 is not compatible with an appliance running Email Security Gateway v7.7.

Web browser support

Email Security Gateway v7.8.3 supports the use of the following Web browsers:

- Microsoft Internet Explorer 8, 9, 10, and 11 (desktop interface only)
- Mozilla Firefox versions 4.4 and later
- Google Chrome 13 and later

Upgrade paths

If you are running Email Security Gateway version 7.8.0 (with V-Series appliance version 7.8.1) or version 7.8.2, you can upgrade directly to version 7.8.3. You must perform intermediate upgrades if you are running any other previous version of Email Security Gateway.

The following upgrade paths are available from version 7.6.x:

- 7.6.0 > 7.7.0 > 7.8.0 (with V-Series appliance version 7.8.1) > 7.8.3
- 7.6.2 > 7.7.0 > 7.8.0 (with V-Series appliance version 7.8.1) > 7.8.3
- 7.6.7 > 7.7.0 > 7.8.0 (with V-Series appliance version 7.8.1) > 7.8.3

Any version 7.6.x Email Security component that is currently installed on Windows Server 2003 must be migrated to Windows Server 2008 R2 before the upgrade to v7.7.0. Migration to Windows Server 2012 may be performed after an upgrade to v7.8.0.

The following upgrade paths are available from version 7.7.x:

- 7.7.0 > 7.8.0 (with V-Series appliance version 7.8.1) > 7.8.3
- 7.7.3 > 7.8.0 (with V-Series appliance version 7.8.1) > 7.8.3

Important

Ensure that you perform all recommended activities before and after your upgrade, including the repair to your Data Security registration.

See Upgrading Email Security Gateway Solutions for detailed upgrade instructions.

You may upgrade an Email Security Gateway virtual appliance directly from version 7.8.0 or 7.8.2 to version 7.8.3. See Upgrading Email Security Gateway Solutions for complete instructions.

Known issues

Topic 70082 | Release Notes | Email Security Gateway | Version 7.8.3 | Updated: 26-May-2014

Applies To:	Websense Email Security Gateway v7.8.3 Websense Email Security Gateway Anywhere v7.8.3

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.