v7.8.4 Release Notes for Email Security Gateway

Topic 70084 | Release Notes | Email Security Gateway | Version 7.8.4 | Updated: 26-Aug-2014

Applies To:	Websense Email Security Gateway v7.8.4 Websense Email Security Gateway Anywhere v7.8.4

Websense® Email Security Gateway version 7.8.4 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 appliance-based system that prevents malicious email threats from entering an organization's network, and protects sensitive data from unauthorized email transmission.

You can also deploy Email Security Gateway on a virtual appliance. Download the image file (WebsenseESGA784Setup_VA.ova) from the MyWebsense downloads page. See the virtual appliance Quick Start Guide for deployment information.

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.

Email Security Gateway version 7.8.3 and later 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. Version 7.8.4 Release Notes are also available for the following Websense products:

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

- X-Series Appliance

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 v7.8.4

Topic 70085 | Release Notes | Email Security Gateway | Version 7.8.4 | Updated: 26-Aug-2014

Applies To:	Websense Email Security Gateway v7.8.4 Websense Email Security Gateway Anywhere v7.8.4

Enhancements added to version 7.8.4 focus on new appliance platform support, simplified configuration of Data Security policy actions, and enhanced system health awareness. The following new Email Security Gateway features are available in version 7.8.4:

- *Websense X-Series modular chassis support*
- *Enhanced Data Security action plan configuration*
- *System health monitoring alert enhancements*

Embedded *Help updates* are also included in these Release Notes.

Websense X-Series modular chassis support

Email Security Gateway can now be deployed on a Websense X-Series modular chassis blade server, part of a high-performance network security system. This new support has the benefit of making Email Security Gateway available on a platform that is scalable for large enterprise organizations.

Websense X-Series appliances are configured and maintained through a command line interface (CLI). The CLI is a text-based user interface for configuring, troubleshooting, and monitoring the appliance.

See the following resources for information about X-Series appliance deployment:

- X-Series Appliance Release Notes
- X-Series Appliance Getting Started Guide
- X-Series Appliance Command Line Interface Guide

Enhanced Data Security action plan configuration

The version 7.8.3 release provided 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**). That implementation included some configuration limitations that applied when a Data Security action was created in a network with multiple standalone appliances or appliance clusters.

This version simplifies policy action configuration in those types of networks. The following action properties are affected:

- **Use IP address.** Available for a Data Security action being created in a multiple standalone appliance environment. The default setting is the appliance E1 interface.

  This setting may be customized for each standalone appliance.
- **Deliver email messages based on domain-based route.** Available for a Data Security action being created in a multiple appliance/multiple cluster environment. The default setting is the default route (**Settings > Inbound/Outbound > Mail Routing**).

  This setting may be customized for each appliance.
- **Save the original message to a queue.** Available for a Data Security action being created in a multiple appliance/multiple cluster environment. The default setting is **data-security**.

  This setting may be customized for each appliance.

Deliver message is now the default policy action option rather than **Resume processing**.

The **Strip attachment** option is now called **Drop attachment**. It is available only for Data Security policy actions.

See the topic titled *Creating and configuring a filter action* in Email Security Manager Help for more information.

System health monitoring alert enhancements

The previous version of Email Security Gateway included a new inbound undelivered email health alert, for which you could configure a frequency threshold that triggered the alert. In version 7.8.4, you can create a list of backup external recipient email addresses to which this notification can be sent.

This version of Email Security Gateway also includes 2 new system health alerts:

- **Work queue growth rate alert.** Notification provides an estimate of when the message work queue will reach its size limit, based on growth rate.

  The work queue includes inbound messages waiting for analysis, messages waiting for Email Security Gateway to deliver, and deferred messages waiting for subsequent delivery attempts.
- **Exception queue capacity alert.** Notification alerts an administrator when the exception queue capacity reaches a specified percentage.

  The exception queue includes any message that currently cannot be delivered because it has encountered an exception situation during message analysis.

Use the **Settings > Alerts > Alert Events** page to configure these alerts. Click the **Configure alert thresholds** link for each alert type to open a configuration dialog box. See the topic titled *Configuring system alerts* in Email Security Manager Help for details.

The email notification for each alert contains helpful troubleshooting information to help an administrator resolve these queue size issues.

Help updates

The following updates have been made to the Email Security Gateway Help system after product release files had been delivered:

- A message from an address listed in the Trusted IP Addresses group:
  - Bypasses Personal Email Manager Always Block List analysis
  - Does not bypass message control invalid recipient or internal sender verification settings
  - Does not bypass the connection control timeout value
- A message from an address listed in the Allow Access List Options (**Settings > Inbound/Outbound > Connection Control**) bypasses True Source IP detection.

Installation and upgrade

Topic 70086 | Release Notes | Email Security Gateway | Version 7.8.4 | Updated: 26-Aug-2014

Applies To:	Websense Email Security Gateway v7.8.4 Websense Email Security Gateway Anywhere v7.8.4

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 the following platforms:

- Websense V-Series appliance (V10000 G2, V10000 G3, or V5000 G2)
- Websense X-Series modular chassis security blade (X10G)

  See the X-Series appliance Getting Started Guide and Command Line Interface (CLI) Guide for information about setting up and configuring an X-Series modular chassis and security blades.
- Virtual appliance (ESXi VMware version 4.0 or later)

  Download the image file (WebsenseESGA784Setup_VA.ova) from the MyWebsense downloads page. See the virtual appliance Quick Start Guide for deployment information.

> **Note**
> You may encounter a set of warning messages during virtual appliance installation. These postfix warnings do not affect virtual appliance operation.

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 or an X-Series security blade 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**
> For version 7.8.3 and earlier, the Email Security Gateway module was not compatible with instances of Email Security at previous versions.
>
> At version 7.8.4, the Email Security manager can control an appliance at a previous 7.8.x version, but manager settings cannot be modified for that appliance.

If your Email Security Gateway SQL Server installation uses a named instance, port 1433 is opened on the firewall even if you specify a different port during Email Security Gateway installation. You must manually change this port setting after installation is complete.

Web browser support

Email Security Gateway v7.8.4 supports the use of the following Web browsers:

- Microsoft Internet Explorer (IE) 8, 9, 10, and 11 (desktop interface only) Compatibility view is not supported.
- 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), version 7.8.2, or 7.8.3, you can upgrade directly to version 7.8.4. 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) > 7.8.4
- 7.6.2 > 7.7.0 > 7.8.0 (with V-Series appliance version 7.8.1) > 7.8.4
- 7.6.7 > 7.7.0 > 7.8.0 (with V-Series appliance version 7.8.1) > 7.8.4

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) > 7.8.4
- 7.7.3 > 7.8.0 (with V-Series appliance version 7.8.1) > 7.8.4

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 preparation and process instructions.

You may upgrade an Email Security Gateway virtual appliance directly from version 7.8.0, 7.8.2, or 7.8.3 to version 7.8.4. See Upgrading Email Security Gateway Solutions for complete instructions.

Resolved and known issues

Topic 70087 | Release Notes | Email Security Gateway | Version 7.8.4 | Updated: 26-Aug-2014

Applies To:	Websense Email Security Gateway v7.8.4 Websense Email Security Gateway Anywhere v7.8.4

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.