v7.8.2 Release Notes for Email Security Gateway

Topic 70055 | Release Notes | Email Security Gateway | Version 7.8.2 | Updated: 25-Feb-2014

Applies To:	Websense Email Security Gateway v7.8.2 Websense Email Security Gateway Anywhere v7.8.2

Websense® Email Security Gateway version 7.8.2 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.

Use these Release Notes to find information about new features in Email Security Gateway and the Personal Email Manager end-user component. Version 7.8.2 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 (WebsenseESGA782Setup_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.

Contents

- *Known issues*

New in Email Security Gateway v7.8.2

Topic 70056 | Release Notes | Email Security Gateway | Version 7.8.2 | Updated: 25-Feb-2014

Applies To:	Websense Email Security Gateway v7.8.2 Websense Email Security Gateway Anywhere v7.8.2

Enhancements added to version 7.8.2 focus on protecting sensitive data and educating administrators and end users about email-borne threats to an organization's network. The following new Email Security Gateway features are available in version 7.8.2:

- *Secure message delivery*
- *Phishing detection and education*
- *New dashboard*

Other enhancements are also included in this release.

Secure message delivery

Secure message delivery is an on-premises encryption feature that provides a secure portal in which your organization's customers may view, send, and manage email that contains sensitive information. For example, you may wish to include personal financial information in a message to a client. The portal provides a secure location for the transmission of this data.

Users within your organization who send and receive secure messages handle these messages via their local email clients, not the secure portal.

As with other encryption options in Email Security Gateway, you must configure an email DLP policy in the Data Security manager. Configure secure message delivery in the **Settings > Inbound/Outbound > Encryption** page. Specify the appliance that hosts the secure portal, then select the message-handling options you want your customers to have in the portal, including:

- Reply all to secure messages
- Forward secure messages.
- Send new secure messages

You can also define the recipients to which your end users are allowed to send secure mail:

- Only email addresses within your organization
- At least 1 email address within your organization. Addresses external to your organization may be included.

Use the message template editor to design the notification that your customers receive when a secure message is available for viewing. You can use the default template or customize it to suit your needs.

Secure messages are stored in a searchable secure-encryption queue (**Main > Message Management > Message Queues**). The maximum queue size and number of days a message is retained in the portal are configured on the Edit Queue page.

See Secure Message Delivery in Email Security Manager Help for configuration details.

In addition to the user actions listed earlier, your customers may view and search messages in the secure message portal after they create an account. Users may also select 1 of 9 languages in which to view the portal interface. See Websense Secure Messaging User Help for the secure message portal end-user instructions.

Phishing detection and education

The phishing detection and education feature provides the capability to prevent phishing email from penetrating your network and an opportunity to instruct your organization's email users how to recognize and deflect phishing threats.

The phishing detection feature is part of Websense ThreatScope for Email Security Gateway Anywhere. Your subscription must include ThreatScope and the email hybrid service if you want to use this function.

An inbound email message can be analyzed in the cloud for specific characteristics of phishing email. Use the Phishing Rules tab on the **Settings > Inbound/Outbound > Phishing Detection** page to define the rules that determine which sender domains are analyzed and how a suspected phishing email is handled. Suspect email may be treated like spam (blocked and saved to a spam queue) or be replaced by a message that educates the recipient about phishing attack email. The Phishing Education Pages tab lets you create these pages.

See Phishing detection and education in Email Security Manager Help for configuration details.

New dashboard charts and presentation reports are available to display suspected phishing attack data.

New dashboard

A new dashboard format replaces the Today and History pages available in previous releases of Email Security Gateway (**Main > Status > Dashboard**). The new format provides administrators added flexibility to display more message data and system information on the dashboard than previously available in the Today and History pages.

The type of information and level of detail shown depends on your subscription level. Email Security Gateway Anywhere is required, for example, to display information about the email hybrid service and how it safeguards your system.

The new dashboard can display up to 7 dashboard tabs, each of which can accommodate up to 12 charts. Populate your dashboard tabs with any of the more than 40 customizable charts. Most dashboard charts can be customized to change their time period and their display format (for example, stacked column, stacked area, multi-series line). You can include multiple versions of the same chart on a tab (for example, showing different time periods).

You can edit, enlarge, copy, and print dashboard charts. Data drill-down capabilities are available in the edit, enlarge, and preview chart views. Use a drag-and-drop function to move charts from one location to another within a tab.

See The Email Security Gateway Dashboard in Email Security Manager Help for configuration details and a list of available dashboard charts.

Other enhancements

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

- Improved Message Log search performance
- New rules that contribute to the URL scanning heuristics tool score (available only with Websense Web Security URL server integrations)
- Changes to Personal Email Manager processing of messages sent to a distribution list:
  - A quarantined message is delivered to a recipient who is part of a distribution list only when that recipient releases it in Personal Email Manager. Previously, when 1 recipient released the message, it was delivered to the entire distribution list.
  - A quarantined message sent to a distribution list now appears in each recipient's Personal Email Manager quarantine list. Previously, the email appeared only in the Personal Email Manager notification message.

Installation and upgrade

Topic 70057 | Release Notes | Email Security Gateway | Version 7.8.2 | Updated: 25-Feb-2014

Applies To:	Websense Email Security Gateway v7.8.2 Websense Email Security Gateway Anywhere v7.8.2

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 (WebsenseESGA782Setup_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. 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 supports the use of the following Web browsers:

- Microsoft Internet Explorer 8, 9, 10, and 11
- 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), you can upgrade directly to version 7.8.2. 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) > 7.8.2
- 7.6.2 > 7.7.0 > 7.8.0 (with V-Series appliance version 7.8.1) > 7.8.2
- 7.6.7 > 7.7.0 > 7.8.0 (with V-Series appliance version 7.8.1) > 7.8.2

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) > 7.8.2
- 7.7.3 > 7.8.0 (with V-Series appliance version 7.8.1) > 7.8.2

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 to 7.8.2. See Email Security Gateway virtual appliance upgrade guide for complete instructions.

Known issues

Topic 70058 | Release Notes | Email Security Gateway | Version 7.8.2 | Updated: 25-Feb-2014

Applies To:	Websense Email Security Gateway v7.8.2 Websense Email Security Gateway Anywhere v7.8.2

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.