v8.0 Release Notes for On-Premises TRITON AP-EMAIL

Applies To:	TRITON AP-EMAIL v8.0

Websense® TRITON® AP-EMAIL version 8.0 (the on-premises email protection solution formerly known as Email Security Gateway) is the first product version that uses a new, simplified product naming and grouping of the familiar Websense TRITON product line. For more information about on-premises email protection solution renaming, see *New in version 8.0*.

Version 8.0 is also a correction release that includes email protection improvements and fixes, some requested by our customers. This release also includes important fixes for the Bash vulnerabilities (Shellshock) and SSL vulnerability (POODLE). See *Important updates* for details.

Part of the TRITON APX security solutions, TRITON AP-EMAIL is a Websense on-premises, 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**
> Some older V10000 and V5000 appliances are not supported with version 8.0.0 and higher. See V-Series appliances supported with version 8.0.

You can also deploy TRITON AP-EMAIL on a virtual appliance. Download the image file (**WebsenseEmail800Setup_VA.ova**) from the MyWebsense downloads page. See the virtual appliance Quick Start Guide for deployment information.

In addition, TRITON AP-EMAIL can be deployed on a Websense X-Series modular chassis blade server, part of a high-performance network security system. This support has the benefit of making on-premises email protection available on a platform that is scalable for large enterprise organizations. 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](#)

Use these Release Notes to find information about version 8.0 TRITON AP-EMAIL. Version 8.0 Release Notes are also available for the following Websense products:

- [TRITON Manager](#)
- [Websense Web Protection Solutions (including Content Gateway)](#)
- [Websense Data Protection Solutions](#)
- [V-Series Appliance](#)
- [X-Series Appliance](#)

See the [Administrator Help](#) for details about on-premises TRITON AP-EMAIL operations.

If you are installing this on-premises email protection solution for the first time, see [Installing Websense Appliance-Based Solutions](#).

If you are upgrading from a previous email protection system version (known as Email Security Gateway), see [Upgrading Email Protection Solutions](#).

Important updates

The following software updates are included in TRITON AP-EMAIL version 8.0:

Bash vulnerabilities (Shellshock)

The critical Bash vulnerabilities were first identified in CVE-2014-6271. Subsequent investigation of the Bash code revealed other, related vulnerabilities.

The vulnerabilities present in Bash (Bourne Again Shell) up to version 4.3 can be exploited by malicious persons, including over HTTP.

Many programs like SSH, telnet, and CGI scripts allow Bash to run in the background, allowing the vulnerability to be exploited remotely over the network.

TRITON AP-EMAIL includes a new version of the Bash program that has been corrected to eliminate these vulnerabilities.

SSL vulnerability (POODLE)

The critical SSLv3 vulnerability was identified in CVE-2014-3566.

SSL (Secure Sockets Layer) is the standard security technology for establishing an encrypted link between a web server and a browser. TLS (Transport Layer Security) has since superseded SSL. However, support for the older SSL version 3.0 still exists in many applications and can therefore lead to software (such as browsers) being forced into using a vulnerable SSLv3 connection.

The vulnerability can be exploited by inducing a client's browser into making multiple browser requests over HTTPS with SSLv3, and inferring details about the encrypted contents that allow an attacker to compromise the security of SSLv3.

Two components of TRITON AP-EMAIL were affected by this vulnerability: the Personal Email Manager end-user portal and the appliance mail transfer agent.

- SSLv3 is now disabled in the Personal Email Manager portal.
- SSLv3 is not disabled in the appliance mail transfer agent. However, this version of TRITON AP-EMAIL does include an updated OpenSSL library to reduce the possibility of attack from this vulnerability.

  You may manually disable SSLv3 on the appliance with the assistance of Websense Technical Support, but you should use this option with caution. Disabling SSLv3 means the mail transfer agent will block all connection requests from servers that use SSLv3.

Contents

- *New in version 8.0*
- *Installation and upgrade*
- *Resolved and known issues*

New in version 8.0

Topic 70121 | Release Notes | TRITON AP-EMAIL | Version 8.0 | Updated: 02-Feb-2015

Applies To:	TRITON AP-EMAIL v8.0

- *Websense TRITON product renaming*
- *Help updates*

Websense TRITON product renaming

To address the wide-scale adoption of cloud and mobile technologies, along with a rapid growth in distributed workforces, Websense, Inc., is excited to launch a new, industry-leading security suite — Websense TRITON APX 8.0. This new modular platform provides advanced threat and data theft protection for organizations that wish to embrace new technologies and working practices. TRITON APX provides protection across the entire kill-chain, reveals actionable intelligence, and enables real-time feedback to educate and motivate end users to avoid risky behavior. This product release is the culmination of 18 months of business transformation and innovation. As a result, Websense customers are now able to maximize the unparalleled protection and ROI of Websense TRITON APX solutions well into the future.

Websense TRITON AP-EMAIL version 8.0 adopts the new, simplified product naming and grouping of the familiar Websense TRITON product line. "AP" is added to the core Websense product names to emphasize the Advanced Protection provided by the latest Websense solutions.

Previous product functionality remains intact. The user interface has the same familiar look and feel. The core on-premises email protection solution continues to provide the strong protections you have come to rely on.

Expanded capabilities for email protection are now offered as optional modules that can easily be subscribed as add-ons. The following modules are available for the TRITON AP-EMAIL on-premises solution:

● Email Hybrid Module, for email hybrid service functionality

● Email Sandbox Module, for URL sandbox, file sandbox, and phishing education capabilities

● Email Encryption Module, for email hybrid service Advanced Email Encryption functionality

● Image Analysis Module, a data protection solution function that provides explicit image detection

Help updates

The following updates do not appear in the product embedded Administrator Help for TRITON AP-EMAIL, because the changes were made after embedded Help files had been delivered:

● Recipient validation user authentication includes the following new options (**Settings > Users > User Authentication > Add** (or **Edit**) **User Authentication**):

■ If a user directory cannot be reached to perform recipient validation (e.g., server is down or not connected), you can allow the system to continue the recipient search in the next user directory listed in the User Directories section Recipients box. Mark the check box under the **Recipient validation** Authentication option to enable this functionality.

■ You can change the order of the user directories in the Recipients list by selecting 1 or more directories in the list and using the **Move Up** and **Move Down** buttons.

● The pop-up alert function, which displays alerts on the **Main > Status > Alerts** page, is not available on Windows 2008 and Windows 2012 platforms.

● Personal Email Manager notification message template (**Settings > Personal Email > Notification Message**) includes a new field for sender username.

Installation and upgrade

Topic 70122 | Release Notes | TRITON AP-EMAIL | Version 8.0 | Updated: 02-Feb-2015

Applies To:	TRITON AP-EMAIL v8.0

If you are installing the on-premises email protection system for the first time, see Installing Websense Appliance-Based Solutions.

If you are upgrading from a previous email protection version (known as Email Security Gateway), see Upgrading Email Protection Solutions.

Requirements

On-premises TRITON AP-EMAIL is supported on the following platforms:

- Websense V-Series appliance (V10000 or V5000)
- 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 (WebsenseEmail800Setup_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 Manager and Email 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 Log Database. See

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

> ❗ **Important**
>
> Although a version 8.0 Email management console can allow an earlier version appliance (e.g., version 7.8.4) to be added on the Email Appliances page, the management settings for that appliance are read-only and cannot be modified.
>
> For optimal system efficiency and performance, we strongly recommend that manager console and appliance versions match.

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

Web browser support

TRITON AP-EMAIL on-premises version 8.0 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 through 32
- Google Chrome 13 through 38

Upgrade paths

If you are running Email Security Gateway version 7.8.x, you can upgrade directly to TRITON AP-EMAIL version 8.0. You must perform intermediate upgrades if you are running any other previous version of Email Security Gateway.

See Upgrading Email Protection Solutions for:

- Links to all intermediate upgrade instructions
- Important information about backing up your system before you upgrade

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) > 8.0
- 7.6.2 > 7.7.0 > 7.8.0 (with V-Series appliance version 7.8.1) > 8.0
- 7.6.7 > 7.7.0 > 7.8.0 (with V-Series appliance version 7.8.1) > 8.0

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 an upgrade to version 7.7.0. Migration to Windows Server 2012 may be performed after an upgrade to version 7.8.0.

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) > 8.0
● 7.7.3 > 7.8.0 (with V-Series appliance version 7.8.1) > 8.0

> **Important**
>
> See Upgrading Email Protection Solutions for detailed upgrade preparation and process instructions.
>
> Ensure that you perform all recommended activities before and after your upgrade, including the repair to your Data module registration.

You may upgrade an Email Security Gateway virtual appliance directly from version 7.8.x to TRITON AP-EMAIL version 8.0. See Upgrading Email Protection Solutions for complete instructions.

You may upgrade a version 7.8.4 Email Security Gateway X-Series chassis security blade directly to TRITON AP-EMAIL version 8.0. To upgrade an X-Series security blade, see the following materials:

● X-Series Appliance Release Notes
● X-Series Appliance Command Line Interface Guide

Resolved and known issues

Topic 70123 | Release Notes | TRITON AP-EMAIL | Version 8.0 | Updated: 02-Feb-2015

Applies To:	TRITON AP-EMAIL v8.0

A list of resolved and known issues for Websense TRITON AP-EMAIL 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.