v8.0.1 Release Notes for On-Premises TRITON AP-EMAIL

Topic 70145 | Release Notes | TRITON AP-EMAIL | Version 8.0.1 | Updated: 01-Jun-2015

Applies To:	TRITON AP-EMAIL v8.0.1

Websense® TRITON® AP-EMAIL version 8.0.1 is a correction release that includes email protection updates and fixes, some requested by our customers. This release also includes important fixes for recent system vulnerabilities. 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 for details.

You can also deploy TRITON AP-EMAIL on a virtual appliance. Download the image file (**WebsenseEmail801Setup_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 Getting Started Guide
- X-Series Appliance Command Line Interface Guide

Use these Release Notes to find information about version 8.0.1 TRITON AP-EMAIL. Version 8.0.1 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, see Upgrading Email Protection Solutions.

Important updates

The initial username and password for the TRITON AP-EMAIL virtual appliance have been changed as of version 8.0.1, as part of a security update that removed ssh root access to the appliance. Use the following username and password for initial logon:

```
email_va
email_va#123
```

See the virtual appliance Quick Start Guide for more deployment information.

TRITON AP-EMAIL now includes the TRITON AP-DATA mobile agent, a Linux-based appliance that lets you secure the type of email content that is synchronized to users' mobile devices when they connect to the network. This includes content in email messages, calendar events, and tasks. For more information, see the topic titled Installing AP-DATA Agents and Servers in the TRITON AP-DATA Help.

The following critical vulnerabilities are also resolved in TRITON AP-EMAIL version 8.0.1:

OpenSSL vulnerability (FREAK)

This vulnerability was identified in CVE-2015-0204.

An OpenSSL client may accept the use of an RSA temporary key in a non-export RSA key exchange cipher suite. A server could present a weak temporary key and downgrade the security of the session.

Java vulnerability (SKIP-TLS)

This vulnerability was identified in CVE-2014-6593.

This Java vulnerability allows the use of a man-in-the-middle (MITM) attack to spoof the identity of any server. In the worst case, an attack could completely disable TLS encryption. At the least, encryption could be made susceptible to cracking. A likely scenario for exploitation of this vulnerability may be a WiFi hotspot or local network attack.

Java cross-site scripting vulnerability

A cross-site scripting vulnerability allows a user to enter and save JavaScript in the email system user database. Entering that script as a Personal Email Manager password gives an attacker access to a web session while posing as a valid user.

Operating system (OS) command injection

A command injection vulnerability allows a user to introduce system-level commands into code to change program execution. A flaw in a Java application could permit an attacker to execute server commands in TRITON AP-EMAIL.

Contents

Installation and upgrade

Topic 70146 | Release Notes | TRITON AP-EMAIL | Version 8.0.1 | Updated: 01-Jun-2015

Applies To:	TRITON AP-EMAIL v8.0.1

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, 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 (**WebsenseEmail801Setup_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 and later 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 8.0.1 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 35
- Google Chrome 13 through 40

Upgrade paths

If you are running Email Security Gateway version 7.8.x or TRITON AP-EMAIL version 8.0, you can upgrade directly to TRITON AP-EMAIL version 8.0.1. 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) > 8.0.1
- 7.6.2 > 7.7.0 > 7.8.0 (with V-Series appliance version 7.8.1) > 8.0.1
- 7.6.7 > 7.7.0 > 7.8.0 (with V-Series appliance version 7.8.1) > 8.0.1

Any version 7.6.x Email Security Gateway 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) > 8.0.1
- 7.7.3 > 7.8.0 (with V-Series appliance version 7.8.1) > 8.0.1

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 8.0.1. See Upgrading Email Protection Solutions for complete instructions.

You must upgrade a version 7.8.4 Email Security Gateway X-Series chassis security blade to TRITON AP-EMAIL version 8.0.0 before you can upgrade to version 8.0.1. 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 70147 | Release Notes | TRITON AP-EMAIL | Version 8.0.1 | Updated: 01-Jun-2015

Applies To:	TRITON AP-EMAIL v8.0.1

A list of resolved and known issues for this version of 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.