v8.1 Release Notes for On-Premises TRITON AP-EMAIL

Topic 70166 | Release Notes | TRITON AP-EMAIL | Version 8.1 | Updated: 12-Oct-2015

Applies To:	TRITON AP-EMAIL v8.1

Websense® TRITON® AP-EMAIL version 8.1 is a feature and correction release that includes email protection improvements and fixes, some requested by our customers. See *Important updates* for a list of vulnerability fixes included in this version.

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 (**WebsenseEmail81Setup_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 8.1 TRITON AP-EMAIL. Version 8.1 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

Logjam vulnerability

A man-in-the-middle (MITM) attack could result in a TLS connection downgrade to a vulnerable encryption level. Click here for more information.

Third-party library upgrades

Samba and bind libraries were upgraded to enhance network security.

Various upgrades for Windows and Linux functions

Several Windows and Linux code updates were implemented to improve system security, including vulnerabilities caused by buffer overflows and command injections.

Virtual appliance credentials

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.

Contents

New in version 8.1

Applies To:	TRITON AP-EMAIL v8.1

DomainKeys (DKIM) Identified Mail integration

The DKIM functionality provides an email authentication method to ensure that a received message has not been modified while in transit from an organization's protected domains. DKIM integration has both email signing and email verification components.

Previous versions of TRITON AP-EMAIL (and Websense Email Security Gateway/Anywhere) included the verification component, which uses the message header digital signature to associate a domain name with the email.

Version 8.1 adds the signing component: the ability to generate or import a private signing key. The private key can be associated with a signing rule that applies to specified user domains. The rules function also allows an administrator to generate a DNS text record that contains a public key.

The private key resides in the mail transfer agent, providing a digital signature that is added to the header of each message sent from a protected domain. A public key is generated and published in the DNS as a text record that is used by a recipient mail system in the verification process.

For detailed configuration information, see DomainKeys Identified Mail (DKIM) integration in the TRITON AP-EMAIL *Administrator Help*.

Domain-based Message Authentication, Reporting, and Conformance (DMARC) validation integration

DMARC uses the results of the Sender Policy Framework (SPF) and DKIM validation processes, along with the sender domain's DMARC policy to determine message disposition. Published in the sender's DNS record, a DMARC policy includes the sender's affirmation that its email is protected by SPF and DKIM validation, and provides a recipient organization with instructions for handling mail that does not pass either of those checks on the recipient's end.

When you enable DMARC validation, a reporting mechanism provides the sender with information about the number of messages received from that sender domain and the results of the recipient's validation checks. Reports are sent to the email address specified in the sender domain's DNS text record via the RUA (reporting URL of aggregate reports) tag.

For detailed configuration information, see Domain-based Message Authentication, Reporting, and Conformance (DMARC) validation integration in the TRITON AP-EMAIL *Administrator Help*.

Complex password enforcement

This version of TRITON AP-EMAIL implements a strong password policy across all end-user functions. When an administrator enables the new password policy, end users are asked to change their passwords to comply.

An end-user password must meet the following requirements:

- Between 8 and 15 characters
- At least 1 uppercase letter
- At least 1 lowercase letter
- At least 1 number
- At least 1 special character; supported characters include:
  ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~

This policy applies to Personal Email Manager and Websense Secure Messaging end users.

Personal Email Manager notification message redesign

A Personal Email Manager notification message contains a summary of a user's blocked messages. Users can manage these blocked messages using either the notification message or the Personal Email Manager end-user portal.

In this version, the notification message has been redesigned to more closely align with a unified TRITON look and feel in terms of appearance and the actions that are available for the user to take.

Installation and upgrade

Applies To:	TRITON AP-EMAIL v8.1

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

Important

To ensure that you install all required components of your email protection solution, we recommend that you select **TRITON AP-EMAIL** on the Installation Type page of the TRITON Unified Installer, rather than performing a Custom installation of the product.

When you select TRITON AP-EMAIL on this page, then TRITON AP-DATA is automatically selected as well. Data loss prevention functions are installed along with email protection functions.

A Custom installation does not automatically install TRITON AP-DATA with TRITON AP-EMAIL.

If you are upgrading from a previous email protection version, see Upgrading Email Protection Solutions.

Warning

On the Select Components screen in the TRITON upgrade installer, ensure that the **TRITON AP-EMAIL** option is selected. This option is required if you are running your email protection system on a V- or X-Series appliance or an on-premises (ESXi server) virtual appliance.

The **TRITON AP-DATA Email Gateway** option applies to a cloud-hosted virtual appliance running with TRITON AP-DATA. See the topic titled "Email Gateway for Microsoft Office 365" in the TRITON AP-DATA Installation Guide for details about this product feature.

Requirements

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

- Websense V-Series appliance (V10000 or V5000)

  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.

- 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 email security blades.

- Virtual appliance (ESXi VMware version 4.0 or later)

  Download the image file (**WebsenseEmail81Setup_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.

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 8.1 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 40
- Google Chrome 13 through 44

Upgrade paths

If you are running Email Security Gateway version 7.8.x or TRITON AP-EMAIL version 8.0.x, you can upgrade directly to TRITON AP-EMAIL version 8.1. 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.x > 7.7.0 > 7.8.0 (with V-Series appliance version 7.8.1) > 8.x
- 7.7.x > 7.8.0 (with V-Series appliance version 7.8.1) > 8.x
- 7.8.x > 8.x

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.

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 8.1. 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 8.1. 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 70169 | Release Notes | TRITON AP-EMAIL | Version 8.1 | Updated: 12-Oct-2015

Applies To:	TRITON AP-EMAIL v8.1

A list of resolved and known issues for this version of Websense TRITON AP-EMAIL is available in the ~~Forcepoint knowledgebase. If~~ you are not already logged on to MyWebsense, this link takes you to the log in screen.