v8.0.0 Release Notes for Websense X-Series Appliances

60196 | Release Notes | X-Series Appliances | 2-February-2015

Use these Release Notes to learn about what's new and improved for Websense® X-Series™ appliances in version 8.0.0.

Contents

See these companion Release Notes for information about the TRITON®security solutions that run on X-Series appliances:

- v8.0.0 Release Notes for Websense Web Protection Solutions
- v8.0.0 Release Notes for TRITON AP-EMAIL

And:

- TRITON Manager Release Notes

See, also, these supporting documents:

- Quick Start poster
- Getting Started guide
- X10G Switch Configuration guide
- Using the X-Series Command Line Interface (CLI)

New in X-Series v8.0.0

60197 | Release Notes | X-Series Appliances | 2-February-2015

TRITON APX

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 eighteen 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.

The version 8.0 release adopts new, simplified product naming and grouping of the familiar Websense TRITON product line.

Former Name	New Name
Websense Web Filter	Websense Web Filter & Security
Websense Web Security	Websense Web Filter & Security
Websense TRITON Web Security Gateway	Websense TRITON AP-WEB
Websense TRITON Web Security Gateway Anywhere	Websense TRITON AP-WEB with: • Web Hybrid Module • Web DLP Module • Web Sandbox Module
Websense TRITON Email Security Gateway	Websense TRITON AP-EMAIL
Websense TRITON Email Security Gateway Anywhere	Websense TRITON AP-EMAIL with: • Email Hybrid Module

Existing product functionality is unchanged. The user interface has the same familiar look and feel and the core product continues to provide the strong protections you've come to rely on.

Websense appliance product names – X-Series and V-Series – are unchanged.

In addition to new names, our web and email protection solutions offer new features and includes product corrections. Refer to their Release Notes for additional product information.

- v8.0.0 Release Notes for TRITON AP-WEB
- v8.0.0 Release Notes for TRITON AP-EMAIL

Following is a list of the TRITON security modules and their console name:

Software module	Description	Console name
TRITON Unified Security Center	Manages configuration and settings common to all modules. Provides centralized access to consoles.	TRITON Manager
TRITON AP-WEB or Web Filter & Security	Applies analytics to detect and block malicious content (TRITON AP-WEB). Uses policies to filter Internet requests from clients to meet *acceptable use policies* (TRITON AP-WEB, Web Filter & Security).	Web module of the TRITON Manager
Network Agent	An Internet traffic sniffer that enforces filtering for protocols other than HTTP and HTTPS.	Web module of the TRITON Manager
Content Gateway	A Web proxy that supports real-time content analysis.	Content Gateway manager
TRITON AP-EMAIL	Filters inbound and outbound email messages.	Email module of the TRITON Manager
TRITON AP-DATA	Provides robust data loss prevention management.	Data module of the TRITON Manager

Changes to CLI commands due to rebranding

CLI commands sometimes use abbreviations for module names. Some of these abbreviations have changed as part of rebranding.

Former name	New name
appliance (for Appliance)	appliance (no change)
esg (for Email Security Gateway)	email (for TRITON AP-EMAIL) Example: restart email
wcg (for Content Gateway	proxy (for Content Gateway) Example: start proxy
wse (for Web Security)	web (for TRITON AP-WEB, or Web Filter & Security) Example: show web

Enhanced patch handling

On systems running v8.0.0, the “load patch” command supports *one-step* download and installation with *express* upgrade packages. Express packages are specially prepared to support the one-step procedure. When used, combined download and install progress status is shown.

In addition, express patches may be prepared in a bundle that supports one-step upgrade for all modules on the appliance. This packaging ensures that modules are upgraded in the order needed to meet all dependencies (e.g., if the Appliance module must be upgraded before Content Gateway, it is). As a result, the express package supports version upgrades in the fewest number of steps.

Note that appliances must be upgraded to v8.0.0 or higher to take advantage of the express packaging and one-step upgrade features.

Here is how the “load patch” command might be used.

- Enter the “load patch” command with no parameters to see a list of patch files and express upgrade packages available on Websense servers.
- Select an express upgrade package to download it to the appliance and automatically initiate the upgrade process.
- Or, select a standard patch file from the list to download it to the appliance, and then use the “install patch” command to start the upgrade.

Should a patch fail to install successfully, the system automatically rolls back.

See Using the X-Series Command Line Interface (CLI).

ShellShock vulnerability

Critical Bash (Bourne Again Shell) vulnerabilities described in CVE-2014-6271 are patched in all modules of version 8.0.0. (The vulnerabilities are also patched in past releases; see Shellshock Bash Vulnerability Hotfix Table - CVE-2014-6271)

This is a critical fix. Vulnerabilities present in Bash, up to version 4.3, can be exploited by malicious persons, including over HTTP. Many programs, such as SSH, telnet, and CGI scripts, allow Bash to run in the background, allowing the vulnerability to be exploited remotely over the network.

SSL vulnerability (POODLE)

Critical SSLv3 vulnerabilities described in CVE-2014-3566 are patched in all modules of version 8.0.0. For more information about Poodle and Websense products, see SSLv3 POODLE Vulnerability CVE-2014-3566.

Installation and upgrade

60198 | Release Notes | X-Series Appliances | 2-February-2015

New X-Series appliances are delivered pre-loaded with the software needed for provisioning via the **firstboot** script.

The Quick Start poster, Getting Started guide, and Switch Configuration guide are your comprehensive resources for installing the physical unit, running **firstboot**, and completing initial configuration.

Upgrading

A comprehensive, step-by-step article is available to guide you through upgrading from v7.8.x. See these X-Series upgrade instructions.

Downloading the TRITON Unified Installer or the Web Linux installer

The TRITON console, reporting components, and other support components are installed off of the appliance, on separate servers.

To download the TRITON Unified Installer or the Web Linux installer:

1. Go to mywebsense.com and log in to your account.

   You are taken to the My Products and Subscriptions page.
2. Click the **Downloads** tab.
3. Under Download Product Installers, select the **Product** and **Version** that you want to install or upgrade to (**8.0.0**).

   The available installers are listed in the form.
4. Click the plus sign ("+") next to an installer entry for more information about the installer.

Click the **download** link to download the installer.

Operating tips

60199 | Release Notes | X-Series Appliances | 2-February-2015

Interface setup tips

Using the P2 interface

If the P2 interface is used and it is in the same subnet as P1, the default gateway is automatically assigned to P2, which is bound to eth1. You should perform a test to ensure that outbound packets can reach the Internet.

Changing the P1 interface IP address

Sometimes it is necessary to change the blade server P1 interface IP address. What is affected and what must be done depends on the configuration of your blade servers and the details of your deployment. The number of activities that must be performed

and the service disruption can be significant. **If possible, retain the current P1 interface IP address.**

If you must change the address, see X-Series: Changing the P1 Interface IP Address for complete details.

Avoiding port conflicts

See the ports list for a table of the Websense software module versions that are compatible with each appliance version.

Check the ports article to avoid port conflicts if you plan to make a change from a default port.

For example, if you want to use an HTTP proxy server port that is different from the default port (8080), be sure to check the ports list first, to avoid conflict with ports already in use by the X-Series.

Web security deployment tips

Policy source tips

- When Policy Broker is run on an X-Series appliance (configured as the *full policy source*), all Policy Server instances that point to that Policy Broker must be installed on X-Series appliances (configured as *user directory and filtering appliances*). You cannot install and run Policy Servers on off-box machines and point them to a Policy Broker that runs on an appliance. This configuration is not supported.
- You can run Policy Server on multiple appliances (configured in user directory and filtering mode) and point these appliances to a Policy Broker running either on or off an appliance.
- Policy Broker replication is not supported when Policy Broker resides on an appliance. If you plan to enable Policy Broker replication, be sure that your policy source is not an appliance.

Subscription key tip

- In a deployment with the TRITON AP-WEB Hybrid Module and multiple Policy Server appliances, use the TRITON AP-WEB with Hybrid Module subscription key for the policy source appliance (the Policy Server that connects to Sync Service), and use a TRITON AP-WEB subscription key for all other appliances. Otherwise, you receive superfluous alerts from the hybrid service.

Integrated Windows Authentication (IWA) tip

- When Content Gateway Integrated Windows Authentication (IWA) is configured, if the appliance hostname is changed, IWA will immediately stop working. To repair the IWA configuration, log onto the Content Gateway manager, unjoin the stale domain and join the domain with the new hostname.

Backup and restore tips

- When configuring scheduled backups to a remote storage location (FTP or Samba share), make sure that the account used for backup file creation has read and write permissions.
- In a multiple Web security blade deployment, after restoring the configuration of a policy source security blade, restart any filtering only or user directory and filtering security blades in your network to ensure that user requests are managed correctly.

Resolved and known issues

60200 | Release Notes | X-Series Appliances | 2-February-2015

A list of known issues in this release is available to customers with a current MyWebsense account.

If you are not currently logged in to MyWebsense, the above link takes you to a login prompt. Log in to view the list.