v8.0.0 Release Notes for Websense V-Series Appliances

Topic 60190 | Release Notes | Websense V-Series Appliances | 2-February-2015

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

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

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

See, also:

- TRITON Manager Release Notes

Contents

For information on which product versions are supported on various appliance platforms, see the appliance compatibility matrix.

New in V-Series Appliances

Topic 60191 | Release Notes | Websense V-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

Previous 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.

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

v8.0.0 not supported on some older V-Series models

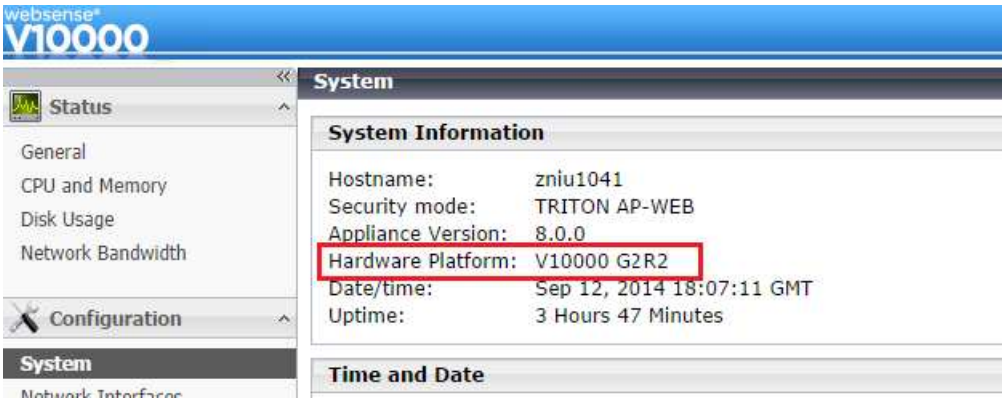
Older V10000 G2 and V5000 G2 appliances, known as revision 1 (or R1) appliances are not supported with version 8.0.0 and higher. Websense stopped shipping these models:

V10000 G2 R1	Third quarter, 2011
V5000 G2 R1	First quarter, 2012

If you plan to upgrade to version 8.0.x, you should verify the full model number of the appliances you plan to upgrade. See the knowledge base article titled V-Series appliances supported with version 8.0.

Full appliance model information

Beginning in version 8.0.0, the full appliance model number, including the *Generation* (e.g., G2) and *Revision* extension (e.g., R2), is displayed in the Appliance manager **System > System Information** section, and by selecting **Help > About Websense V-Series**. Is is also displayed in the output of the CLI 'show platform' command.



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.

SSLv3 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.

New in V-Series version 7.8.2

Topic 45132 / Updated: 10-February-2014

Applies To:	Websense V-Series Appliances Version 7.8.2 Models include: V10000 G2, V10000 G3, V5000 G2

Maximum segment size - DRAFT

You can now designate the value for the maximum segment size (MSS) when you add a new IPv4 route. To define the MSS parameters:

1. In the Appliance manager, go to Configuration > Routing > IPv4 tab.
2. Click the Add/Import button.
3. On the Add/Import IPv4 Routes page, enter the MSS value in the Maximum segment size field, or keep the default value. THIS IS DRAFT COPY. Feature not available for 7.8.1, but may be available after 7.8.1.

Installation and upgrade

Topic 60192 | Release Notes | Websense V-Series Appliances | 2-February-2015

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

V10000 G2 Quick Start poster

V10000 G3 Quick Start poster

V5000 Quick Start poster

V-Series Getting Started guide

Upgrading to version 8.0.0

You can upgrade directly to version 8.0.0 from 7.8.1, 7.8.2, 7.8.3, or 7.8.4, through the V-Series console by loading and applying the version 8.0.0 patch.

Complete upgrade instructions are located in the V-Series Appliance Upgrade Guide.

Important

If you have multiple appliances, and:

- They are running version 7.8.3 or 7.8.4
- You plan to download the upgrade patch and then upload it to a local host for download to the other appliances

You may run into a Java version error. For a complete description and work around, please see the knowledge base article V-Series patch upload Java version error.

Upgrade summary

To install the 8.0.0 patch, go to the **Administration** > **Patches / Hotfixes** > **Patches** tab, and click **Check for Patches**. Once the 8.0.0 patch has been downloaded, click **Install**.

After it is downloaded to one appliance, the patch file can be saved to a local machine. From the local machine, you can upload it to any 7.8.x appliance by going to the

Administration > **Patches / Hotfixes** > **Patches** tab and clicking **Upload Patch Manually**.

> **Important**
> The order of upgrade of the components in the deployment is extremely important. Please follow the detailed instructions described in the V-Series Appliance Upgrade Guide.

> **Important**
> After upgrading a filtering only appliance with an off-appliance policy source, the Web module of the TRITON Manager lists two Filtering Service instances with the same IP address in **Settings > Network Agent > Global**.
>
> To avoid this problem, before upgrading a filtering only appliance to v8.0.0:
>
> 1. Switch filtering only mode to full policy source mode.
> 2. Run the upgrade process.
> 3. Switch the mode back to filtering only.

For high-level upgrade flow diagrams, see:

- Web Security Gateway and Email Security Gateway on V-Series: Upgrade to 8.0.x
- Web Security and Web Security Gateway on V-Series: Upgrade to 8.0.x
- Email Security Gateway on V-Series: Upgrade to 8.0.x

Security mode provisioning

V-Series appliances support the following security modes. Note that the names of the modes change from v7.8.x to v.8.0.0. See *TRITON APX*, page 2.

Your subscription key should match the security modes you select during **firstboot**.

7.8.x Security Modes	New 8.0.0 Security Modes	V5000	V10000
Standalone mode			
Web Security	Web Filter & Security	X	
Web Security Gateway	TRITON AP-WEB	X	X

7.8.x Security Modes	New 8.0.0 Security Modes	V5000	V10000
Web Security Gateway Anywhere	TRITON AP-WEB with: ® Web Hybrid Module ® Web DLP Module ® Web Sandbox Module	X	X
Email Security Gateway	TRITON AP-EMAIL	X	X
Email Security Gateway Anywhere	TRITON AP-EMAIL with: ® Email Hybrid Module	X	X
Dual Mode			
Web Security and Email Security Gateway	Web Filter & Security and TRITON AP-EMAIL	X	X
Web Security Gateway or Gateway Anywhere and Email Security Gateway or Gateway Anywhere	TRITON AP-WEB and TRITON AP-EMAIL		X

Once configured, the appliance can be changed to another security mode only after restoring the appliance to the factory image. The security mode **cannot** be changed by running **firstboot** again.

Web browsers with the V-Series manager

V-Series appliances are configured and maintained with a Web-based user interface called the V-Series manager.

When you access the V-Series manager for the first time, you will get a certificate warning because the V-Series manager offers a self-signed certificate. To eliminate the warnings, install the certificate into your browser's CA store. For instructions, see your browser documentation.

The V-Series manager should be used with one of these supported browsers:

- Microsoft Internet Explorer 8
- Microsoft Internet Explorer 9
- Microsoft Internet Explorer 10 standard mode
- Microsoft Internet Explorer 11 standard mode

> **Note**
>
> **Do not use Compatibility View with any version of Internet Explorer.**

- Mozilla Firefox version 4.4 through 32

- Chrome 13 through 38

If you have another browser or version, the management interface may behave in unexpected ways or report an error.

Downloading the TRITON Unified Security Center Installer

The TRITON Manager and several other components are installed off of the appliance, on separate servers.

To download the TRITON version 8.0.0 Setup program:

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

   You are taken to the My Products and Subscriptions page.
2. Click the **Downloads** tab.
3. Under Download Product Installers, select your **Product and Version** (8.0.0).

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

Operating tips

Topic 60193 | Release Notes | Websense V-Series Appliances | 2-February-2015

Ethernet interface setup

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.

Avoiding port conflicts

See the ports list (Excel file) 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 V-Series.

Upgrade tip

After upgrade installation is complete:

- Log onto the V-Series manager, go to the **Configuration > System** page to confirm and adjust, if necessary, the **Time and Date** settings, paying particular attention to the time zone setting. [54636]
- If the upgraded appliance is a Policy Server, log onto TRITON console, go to the Web module **Settings > General > Policy Servers** page and add the appliance. Next go to the TRITON console **Appliances** tab and register the appliance. [54814]

Logging tip

If you want to examine log files for Network Agent in V-Series manager, be sure to turn on Network Agent logging in the Web module of TRITON Manager first. Go to **Settings > Network Agent > Global**. Hover over **Global** and select the Network Agent IP address that you're interested in. At the bottom of the page, open **Advanced Network Agent Settings**, go to the **Debug Settings** area, and set **Mode**, **Output**, and **Port**.

Deployment tips

- When Policy Broker is run on a V-Series appliance (configured as the **Full policy source**), all Policy Servers that point to that Policy Broker (configured as **User directory and filtering**) must be installed on V-Series appliances as well. 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.

  However, you can run Policy Server on multiple appliances (**User directory and filtering** mode) and point these appliances to a Policy Broker running either on or off an appliance.
- **Teamed NICs** share the load under one common identity, with multiple adapters load-balancing under a single IP address. This is also known as link aggregation or trunking.

  If you have implemented NIC teaming, but don't see load balancing working as expected, the problem may be resolved by configuring your switch to disable **flowcontrol send**. To do this, use the command **set port flowcontrol send off** for both the port-channel and channel member ports.
- When TRITON AP-WEB is deployed and 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 Content Gateway manager, unjoin the stale domain and join the domain with the new hostname. [53864]

Backup and restore tips

- When configuring schedule backups to a remote storage location (FTP server or Samba share), make sure that the account used for backup file creation has **read** and **write** permissions. If you plan to use the option to automatically delete backup files older than some period of time, you must use an account that has **delete** permissions for the backup file directory and its subdirectories.
- In a multiple appliance deployment, after restoring the configuration of a **Policy source** appliance, restart any **Filtering only** or **User directory and filtering** appliances in your network to ensure that user requests are filtered correctly.

Resolved and known issues

Topic 60194 | Release Notes | Websense V-Series Appliances | 2-February-2015

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

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