v7.7 Release Notes for Websense V-Series Appliances

Topic 60060 / Updated: 2-July-2012

Applies To:	Websense® V-Series Appliances Version 7.7 Models include: V10000G2, V10000, V5000G2

Use these Release Notes to find information about what's new and improved in V-Series Appliance version 7.7.

V-Series appliances can host the TRITON Web and Email security components of TRITON Enterprise.

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 Unified Security Center
Websense Web Security	Uses policies to filter Internet requests from clients.	TRITON – Web Security
Network Agent	An Internet traffic sniffer that enforces filtering for protocols other than HTTP and HTTPS.	TRITON – Web Security
Websense Content Gateway	A Web proxy that includes real-time content analysis.	Content Gateway Manager
Websense Email Security Gateway	Filters inbound and outbound email messages.	TRITON – Email Security

Software module	Description	Console name
Websense Data Security	Provides robust data loss prevention management.	TRITON – Data Security
Websense Mobile Security	A cloud-based service for Apple iOS mobile devices that provides remote device management and protection against Web threats.	TRITON – Mobile Security

New in V-Series Appliance v7.7

Topic 60061 / Updated: 2-July-2012

Applies To:	Websense V-Series Appliances Version 7.7 Models include: V10000G2, V10000, V5000G2

Single sign-on and two-factor authentication

Using the TRITON Unified Security Center, V-Series appliances can be accessed via single sign-on (no-prompt) and two-factor authentication.

Single sign-on

In TRITON Unified Security Center, you can configure administrator accounts for single sign-on (no-prompt) access to the V-Series Appliance Manager. In this configuration, when the administrator is logged onto TRITON console, she or he can go to the **Appliances** tab, locate the registered appliance he or she wants to access, and click the **Single Sign-On** button to get transparent access to the corresponding Appliance Manager. See the TRITON console Help system for configuration details. In this configuration, administrators can still access the Appliance Manager directly via its IP address. The administrator is prompted for credentials.

Two-factor authentication

TRITON console can also be configured as the access point for certificate-based, two-factor authentication.

Two-factor authentication:

- Is configured for and applies to TRITON Unified Security Center logon only.
- Requires administrators to perform certificate authentication to log on.
- Can be made to apply to Appliance Manager and Content Gateway Manager by forcing administrators to log on to TRITON console before accessing other consoles.
- Requires single sign-on to be configured for administrators allowed access to Appliance Manager and Content Gateway Manager.
- Requires that the password logon capability be disabled using an appliance command line interface command. This prevents administrators not configured for single sign-on from accessing the Appliance Manager and Content Gateway Manager. See V-Series Appliance Manager Help.

For more information about configuring two-factor authentication, see “Configuring certificate authentication” in TRITON console Help.

Hotfix management facility

Modeled on the Appliance Manager patch management facility, the hotfix management facility is an all-inclusive resource for downloading, installing, uninstalling, and maintaining a history of hotfix use on the appliance.

When necessary, Websense, Inc. releases a targeted hotfix to address a specific issue in an appliance module. In most cases, you receive notification of hotfixes in a

Websense Technical Alert email, or a Technical Support Agent recommends a specific hotfix to address a problem that you have reported.

In the Appliance Manager, go to the **Administration > Patches / Hotfixes > Hotfixes** page to manage hotfixes.

- The Hotfix facility will not install a hotfix that is not valid for the module versions on your appliance.
- A hotfix may have dependencies on or conflicts with other hotfixes, in which case the hotfix facility will not install the hotfix until its dependents are installed or the conflicts are resolved. Specific hotfix dependencies and conflicts are described within the hotfix facility.
- As a best practice, unless otherwise instructed by a Websense Technical Support Agent, do not install a hotfix for an issue that you have not experienced.

See "Hotfix management" in Appliance Manager Help.

Ability to permanently disable Network Agent

It is possible to permanently disable Network Agent on appliances provisioned with Web Security Gateway (Anywhere). This is beneficial for deployments that do not use Network Agent because permanently disabling it redistributes system resources—CPU and memory—to other modules provisioned on the appliance.

However, when Network Agent is permanently disabled, the only way to restore Network Agent to the system is to re-imaged the appliance.

Note

Network Agent cannot be disabled on Websense Web Security (no Gateway) appliances.

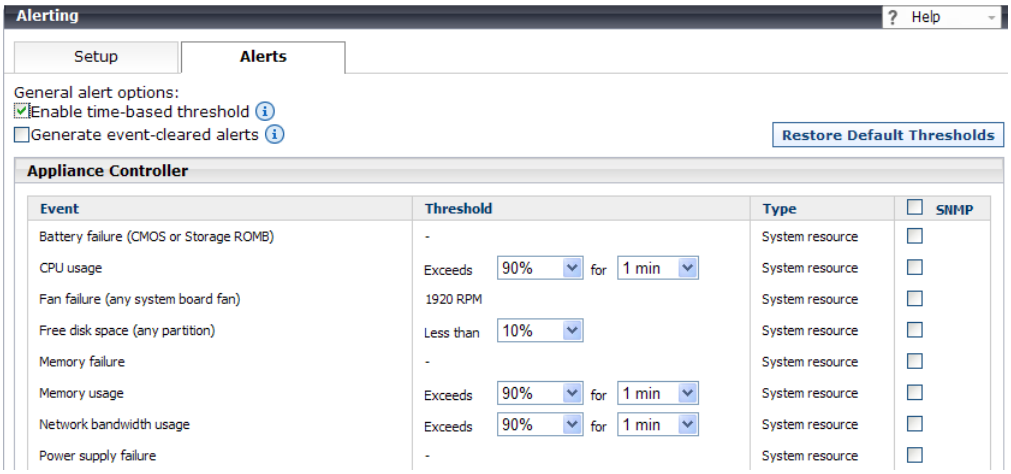
Note

When Network Agent is permanently disabled, its status continues to be reported in the TRITON console on **Dashboard > Health Alert Summary**. Its status is reported as: "Network Agent at <appliance IP address> is not running." On the **Settings > Network Agent > Global** page, the Network Agent IP address still displays and can be clicked.

SNMP alerting enhancements

Time-based alert thresholds

Most event alerts that offer a configurable threshold, now also offer a configurable time-based threshold, specified in minutes. When the time-based threshold is set and both thresholds are exceeded, an alert is sent. To enabled time-based thresholds, select the **Enable time-based thresholds** check box. The time-based threshold is enabled on every event for which it is configurable.



Event-cleared alerts

In addition to event threshold alerts, you can configure alerts to be sent when conditions return below the threshold. These are called **event-cleared alerts**. To enable event-cleared alerts, select the **Generate event-cleared alerts** check box.

The following events do not generate event-cleared alerts:

- Hostname change
- IP address change
- Scheduled backup failure
- SNMP authentication failure

SIEM integration

Log records for traffic managed by Content Gateway and sent to Websense Web Security Filtering Service can also be routed to your Security Information and Event Management (SIEM) solution.

See the section titled, “Integration with third-party SIEM solutions” in the Websense Web Security v7.7 Release Notes.

On V-Series appliances, on the **Full policy source** and each **User directory and filtering** machine, use the **Administration > Toolbox > Command Line Utility** to enable the **multiplexer** service.

Credentials required to access the CLI through the KVM

After **firstboot** is run, physical access to the appliance Command Line Interface (CLI) from the serial console (KVM) is protected by the 'admin' credentials. To get this protection, administrators must end each CLI session with the "quit" command, otherwise the session remains open.

Email Security Gateway virtual interfaces

For users of Email Security Gateway who need to support multiple domains or large volumes of outbound traffic, there is now support for multiple virtual interfaces. Multiple virtual IP addresses can be configured on E1 and E2 (or P1/P2 on a V5000G2).

- Virtual IP addresses are used for outbound traffic only
- Virtual IP addresses are bound to the specified physical interface
- Virtual IP addresses must be in the same subnet as the specified physical interface
- A maximum of 10 virtual IP addresses can be specified for each physical interface (P1/P2 V10000G2, E1/E2 V5000G2)

Support for IPv6

Version 7.7 of TRITON Enterprise, including 7.7 V-Series appliances, provides incremental support for IPv6.

IPv6 support is included for Websense Web Security, Web Security Gateway, and Web Security Gateway Anywhere.

IPv6 is not supported with Websense Email Security Gateway.

Important

To use IPv6 with Web Security Gateway (Anywhere), Content Gateway must be deployed as an **explicit proxy**.

IPv6 is **not** supported in transparent proxy deployments.

For Websense Web Security, IPv6 support includes:

- Dual IP stack implementation on interfaces C and N

- IPv6 traffic to the Internet or clients on interfaces C and N. For Network Agent (non-HTTP/S traffic), reset packet sent on C or N
- IPv6 static routes
- SNMP traps and counters for IPv6 data
- Network diagnostic tools in the Command Line Utility and Command Line Interface

For Websense Web Security Gateway and Gateway Anywhere, support includes all of the above, plus:

- Dual IP stack implementation on interfaces P1 and P2
- Traffic to the Internet or clients on interfaces P1 and P2, and their bonded interface (E1/E2), if configured

Limits and restrictions:

- IPv6-only internal networks are not supported
- IPv4 must be used to communicate among V-Series appliances and with TRITON components

See Content Gateway Help for proxy support, limits, and restrictions.

IPv6 configuration summary

IPv6 support is disabled by default.

IPv6 is enabled in the Appliance Manager at the top of the **Configuration > Network Interfaces > IPv6** page. When it is enabled, IPv6 support is enabled for all affected capabilities on the appliance.

In any field that accepts an IPv6 address, the address can be entered in any format that conforms with the standard. For example:

- Leading zeros within a 16-bit value may be omitted
- One group of consecutive zeros may be replaced with a double colon

Disabling IPv6 support requires a full restart of the appliance.

When IPv6 is disabled, IPv6 values remain in the configuration files, but are not editable.

Recovering the admin password

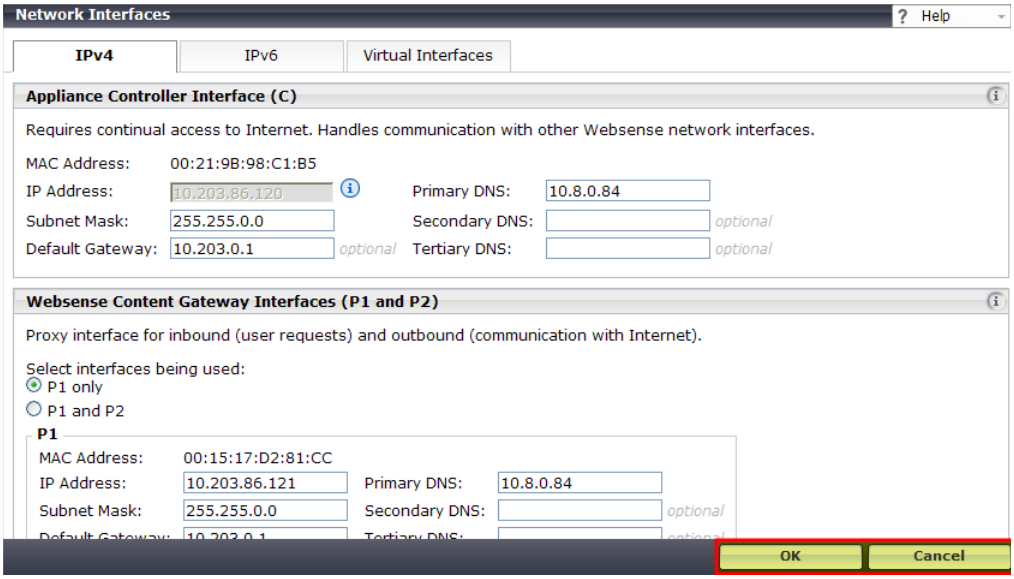
The password recovery (reset) method for the Appliance Manager “admin” account has been expanded to use a pre-configured email account to which a temporary password is sent when the “Forgot my password” link is clicked on the login page.

If the email account and SMTP service information are not configured, the recovery method falls back to providing a passcode for use when contacting Technical Support.

See “Appliance Manager password reset” in Appliance Manager Help.

Page-level OK and Cancel operations

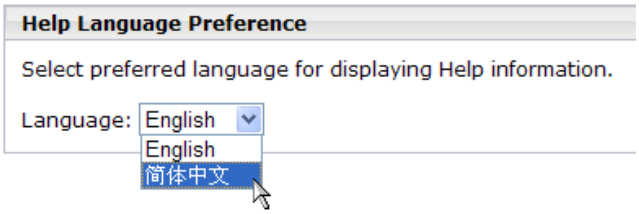
To be consistent with the work flow of other TRITON managers, many Appliance Manager configuration pages have moved from a unit-level “Save” activity model to a page-level “OK/ Cancel” model.



Other enhancements

Chinese language Appliance Manager Help

Appliance Manager Help is available in Chinese. To select Chinese language Help, log onto the Appliance Manager and go to **Administration > Account management**. In the **Help Language Preference** section, select Chinese from the **Language** drop down list and click **OK**.



Additions to the Command Line Utility

These commands have been added to the Command Line Utility:

Command	Description	Parameters
copy-MasterCA	Applies to the Websense Web Security module only. When TRITON console is located on the appliance and a new master certificate is created following changes to the certificate authentication root certificate, use this command to copy the new Master CA to the Websense Web Security module.	None
directory-agent-service	Applies to the Websense Web Security module only. This command disables and enables the directory agent service.	[Action]: Enter **enable** to enable the directory agent service. Enter **disable** to disable the directory agent service.
esg-license-reset	Applies to the Email Security Gateway module only. This command clears all Email Security Gateway subscription information. After the command is run, the user must re-enter the subscription key to use Email Security Gateway. Note: If the network is unreachable, the command takes 30 minutes to timeout.	None.
multiplexer	Applies to the Websense Web Security module only. Enables and disables the Multiplexer service that supports SIEM integrations. See TRITON – Web Security Help.	[Action]: Enter **enable** to enable the Multiplexer service. Enter **disable** to disable the Multiplexer service.
ping6	Checks that a hostname or IPv6 address exists, can accept requests from the selected module, and that DNS is resolving. Use this to test connectivity to another host and to measure response time. **Note:** ping6 is not supported in the Websense Web Security module.	[Destination]: Enter the hostname (for example myintranet.com) or IPv6 address of the host you want to test.

Command	Description	Parameters
ping6 -I	Checks that a network interface can communicate with a hostname or IPv6 address and that DNS is resolving. Use this to test connectivity to another host, from one of the appliance NICs. **Note:** ping6 -I is not supported in the Websense Web Security module.	[Interface]: Enter the name of the NIC you want to test. Click the information icon for valid NIC values. **Example**: eth0 [Destination]: Enter the hostname or IPv6 address of the host you want to test.
route -A inet6 -n	Display the contents of the selected module's kernel IP routing table IPv6 entries in numeric format. This is useful in complex network environments—for example, those with proxy chaining—to see if the environment is set up properly.	None.
state-server	Applies to Websense Web Security module when the appliance is configured as a Full policy source or User directory and filtering system. In multiple Filtering Service deployments, Websense State Server is required for proper application of time-based filtering actions (Quota, Confirm, Password Override, and Account Override). See **Policy Server, Filtering Service, and State Server** in TRITON - Web Security Help.	[Action]: Enter **enable** to enable the state server service. Enter **disable** to disable the state server service.
traceroute6	Use this to determine the route taken by packets across a network to a particular host. **Note:** **traceroute6** is not supported in the Websense Web Security module.	[Destination]: Enter the hostname or IP address of the host destination you are investigating
user-group-ip-precedence	Applies to the Web Security module only. Use this command to change the precedence of identification attributes applied to: filtering policy, Delegated Administrator (DA) role identification, protocol policy, and quota time available.	[Action]: Enter **enable** to modify the precedence order to: User > Group > Domain > Computer > Network Enter **disable** (default) to set the precedence order to: User > Computer > Network > Group > Domain Enter **status** to display the current setting.

Additions to the Command Line Interface

Command	Description
admin email	Specify the email address to which password recovery email is sent.
password-logon disable	Disable password logon via IP address and credentials.
password-logon enable	Enable password logon via IP address and credentials.
show password-logon	Show the status of password logon.
show smtp server	Show the SMTP server settings through which password recovery email is routed.
smtp server	Specify the SMTP server through which password recovery email is routed.

Installation and upgrade

Topic 60062 / Updated: 2-July-2012

Applies To:	Websense V-Series Appliances Version 7.7 Models include: V10000G2, V10000, V5000G2

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

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

Comprehensive **upgrade** instructions start here in the Deployment and Installation Center.

Security mode provisioning

Version 7.7 V-Series appliances support the following security modes.

Your subscription keys should be for the security modes you select during **firstboot**.

Security Mode	V5000	V10000 G2
Standalone mode		
Web Security	**X**	
Web Security Gateway	**X**	**X**

Security Mode	V5000	V10000 G2
Web Security Gateway Anywhere	X	X
Email Security Gateway	X	X
Email Security Gateway Anywhere	X	X
Dual Mode		
Web Security and Email Security Gateway	X	X
Web Security Gateway or Gateway Anywhere and Email Security Gateway or Gateway Anywhere		X

First generation V10000 appliances (not G2) support Web Security Gateway (Anywhere) by patch upgrade, only.

Once configured, the appliance cannot be changed to another security mode without first restoring the factory image. The security mode **cannot** be changed by running **firstboot** again.

Web browsers with the Appliance Manager

V-Series appliances are configured and maintained with a Web-based user interface called the Appliance Manager. The Appliance Manager should be used with one of these supported browsers:

- Microsoft Internet Explorer 8 and 9
- Mozilla Firefox versions 5 and later
- Google Chrome 13 and later

Note

If you are using Internet Explorer, make sure that Enhanced Security Configuration is turned off.

When you access the Appliance Manager for the first time, you will get a certificate warning because the Appliance 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.

Downloading the TRITON Unified Security Center Installer

The TRITON Unified Security Center and several support components are installed off of the appliance, on separate servers.

To download the TRITON version 7.7 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 your **Product and Version** (7.7).

   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 60063 / Updated: 9-May-2013

Applies To:	Websense V-Series Appliances Version 7.7 Models include: V10000G2, V10000, V5000G2

Interface setup tip

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 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 patch installation is complete:

- Log onto the Appliance Manager, go to the **Configuration > System** page and confirm and adjust, if necessary, the **Time and Date** settings, paying particular attention to the time zone setting.
- If the upgraded appliance is a Policy Server, log onto TRITON console, go to the TRITON – Web Security **Settings > General > Policy Servers** page and add the appliance. Next go to the TRITON console **Appliances** tab and register the appliance.

Logging tip

If you want to examine log files for Network Agent in Appliance Manager, be sure to turn on Network Agent logging in the TRITON - Web Security console first. To do this, log on to **TRITON - Web Security** and navigate to the **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 Web Security Gateway (Anywhere) 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.
- Websense Web Security Log Server now supports **SQL Server SSL encryption**. However, if you are running TRITON – Web Security (manager) on the appliance (recommended only for evaluations and very small deployments), the connection from the console to the database **cannot be encrypted**. This means that if the

Microsoft SQL Server “Force Protocol Encryption” option is set to Yes, no data will appear in the Web Security Dashboard or other reporting tools.

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 600064 / Updated: 2-July-2012

Applies To:	Websense® V-Series Appliances v7.7 Models: V5000 G2, V10000 G2, V10000

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.