v7.6 Release Notes for V-Series Appliances

Topic 60030 / Updated: 28-April-2011

Applies To:	Websense® V-Series Appliances v7.6.0 Models: V5000 G2, V10000 G2, V10000

These Release Notes describe new features, best practices, corrections, and known issues in version 7.6 for V-Series appliances.

For detailed information about each TRITON™ component, see their Release Notes:

- TRITON Unified Security Center
- Websense Web Security
- Websense Data Security
- Websense Email Security Gateway
- Websense Content Gateway

For V-Series appliance upgrade information, see Upgrading V-Series Appliances to v7.6.

Contents

Introducing Websense® V-Series v7.6

Topic 60031 / Updated: 28-April-2011

Applies To:	Websense V-Series Appliances v7.6.0 Models: V5000 G2, V10000 G2

Email Security Gateway

Single and multiple security mode provisioning

TRITON™ Unified Security Center

Backup and restore

Patch handling

Route handling

SNMP support

Command Line Interface (CLI)

Command Line Utility (CLU)

NIC teaming

System watchdog daemon

Statistics on disk usage and activity

> **Important**
>
> For more information about any new or existing V-Series feature, see Appliance Manager online Help.

Email Security Gateway

In version 7.6, Websense introduces Email Security Gateway. Email Security Gateway brings the full power of Websense Essential Information Protection™ to email security on the V-Series appliance, including support for hybrid email security and data loss prevention (DLP). For more information, see the Websense Email Security Gateway Release Notes.

Single and multiple security mode provisioning

With the addition of Email Security Gateway, V-Series appliances are able to support these combinations of security modes.

V-Series model	Security mode
V5000 G2	Web Security **or** Email Security Gateway
V10000 G2	Web Security **or** Email Security Gateway **or** Web Security and Email Security Gateway
V10000	Web Security only (by patch upgrade only)

The security mode is selected when the **firstboot** script is run. 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.

TRITON™ Unified Security Center

The TRITON Unified Security Center now provides a section for registering and accessing V-Series appliances in your network. If you have installed one or more appliances as part of a TRITON installation, use the **Appliances** > **Manage Appliances** page to add, remove, monitor, and access your appliances. When the link is used to access an appliance, the administrator is prompted for the appropriate credentials.

The following information is displayed for each appliance added to this page:

- IP address for the management interface (C) on the appliance
- Appliance hostname
- Security mode (Web Security, Email Security, or Web and Email Security)
- Policy source (Full, User directory and filtering, or Filtering only). This information is only for appliances that have Web Security enabled.
- Software version (for example 7.6.0)
- Hardware platform (for example V5000 or V10000)
- The unique description that is entered on the System page in the Appliance Manager.

For more information, see TRITON Unified Security Center online Help.

Backup and restore

The V-Series backup and restore facility has been enhanced and made easier to use. The new facility provides:

- A friendlier user interface
- Simplified work flow
- Remote storage support for backup files, including Samba and FTP server support
- Selective backup of modules
  - Full appliance configuration
  - Web Security configuration
  - Email Security configuration
- The ability to schedule backups
  - Daily, weekly, or monthly at a specific time
  - Can be stored locally or on a remote Samba share or FTP server
- An easy-to-use restore wizard

Patch handling

The patch handling facility has been enhanced and made easier to use. The new facility provides:

- A friendlier user interface
- Simplified work flow
- Automatic checking and notification of new patches
- The ability to manually check for new patches
- Direct download of patches to the appliance
- The ability to pause, resume, or cancel a patch download
- The ability to upload patches from an off-appliance location
- Improved status information while a patch is being applied
- The ability to specify an upstream proxy through which to communicate with the Websense download server.
- Improved patch download and application log

Route handling

Support for static routes has been expanded, and support for routes through the management interface (C), called module routes, has been added.

- Static routes can be defined for any active appliance interface.

- Static routes can be imported from and exported to a text file.
- Module Routes can be defined through the management interface (C) for traffic to and from a module to a specific network.
- The route table size limit is 5000 entries for each.

SNMP support

Support has been added for SNMP polling and alerting. V-Series appliances use Net-SNMP to support SNMP.

V-Series SNMP support includes:

- SNMP v1, v2c, and v3
- NMS polling of SNMP counters
  - Enabled in the **Setup** tab of the **Configuration** > **Alerting** page under **Monitoring Server**.
- Sending of SNMP traps
  - Includes a proprietary MIB file that can be downloaded from the **Setup** tab of the **Configuration** > **Alerting** page under **Traps Server**.
  - Can send traps for the Appliance Controller, Content Gateway, Web Security, Network Agent, and Email Security Gateway modules.
  - The administrator controls which traps are sent.

Command Line Interface (CLI)

The V-Series CLI is enhanced in 3 ways:

- The CLI can be accessed using SSH if it's enabled on the Toolbox page.
- When the CLI is accessed through SSH, Appliance Manager administrator credentials are required.
- The set of debugging and configuration commands that is provided in the Command Line Utility (CLU) is also available in the CLI as arguments to the command "debug-util". In the CLI, enter "help debug-util".

Command Line Utility (CLU)

The Appliance Manager Toolbox Command Line Utility offers several new commands:

- **arp --** Displays the kernel ARP table for the selected module.
- **cache-user-names --** Turns on, off, or queries the status of cached user names resolved from IP addresses by Content Gateway.

- **directory-agent-service** -- Disables and enables the directory agent service.
- **esg-license-reset** -- Clears all Email Security Gateway subscription information.
- **policy-broker-token** -- Retrieves the Policy Broker token for this appliance. This may be needed to configure support for Remote Filtering.
- **show-triton-admin-email --** Displays the email address to which alerts, password resets, and other TRITON administrator messages are sent.
- **show-triton-smtp-settings** -- Displays the SMTP server information and sender email settings used when notifications are sent from TRITON.
- **sysctl-tcp-timestamps** -- Displays and changes the setting for TCP timestamps.
- **sysctl-tcp-window-scaling** -- Displays and changes the setting for TCP window scaling.
- **triton-admin-email** -- Sets the email address to which alerts, password reset notifications, and other administrator communication is sent. (Pertains only to the Websense Web Security module, and only when TRITON - Web Security is running on the appliance.)
- **triton-smtp-settings** -- Sets the SMTP server and sender settings. (Pertains only to the Websense Web Security module, and only when TRITON - Web Security is running on the appliance.)
- **triton-websecurity-services --** Starts, stops, restarts, and queries the status of TRITON - Web Security services.
- **wget-proxy** -- Tests connectivity between the specified URL and the proxy (file download not supported). Supports HTTP, HTTPS, and FTP protocols.

See Appliance Manager online Help for more information.

NIC teaming

On the V10000 G2, in Websense Web Security only, or Websense Email Security Gateway only modes, network interfaces can be bonded (teamed) for either Active/ Standby or Load balancing. Configuration is performed on the **Configuration** > **Network Interfaces** page.

System watchdog daemon

A new system watchdog daemon monitors critical system processes and performs a reset or restart should a failure or fault occur. Checkpoints include:

- Appliance kernel -- is the kernel active.
- Domain agent -- is the Domain Agent running. This is an essential process that is responsible for communicating between the user interface and appliance back end processes.
- Journal Commit I/O -- detect a “journal commit I/O” error.

- File table -- detect a file table overflow condition.

Statistics on disk usage and activity

Statistics on disk usage and activity are shown for each module. Disk usage reporting now includes:

- Input/Output activity per second (IOPS), per disk, per module
- The amount of total, used, and free disk space per disk, per module

Operation tips

Topic 60032 / Updated: 28-April-2011

Applies To:	Websense® V-Series Appliances v7.6.0 Models: V5000 G2, V10000 G2, V10000

Setup tip

If the P2 interface is used, it must be in the same subnet as P1. In this configuration, 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 proxy 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.

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 page. Then scroll down to **Additional Settings** to enable logging of protocol traffic and specify a logging interval.

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.

Subscription key tips

In a deployment with multiple Policy Server appliances, use the Websense Web Security Gateway Anywhere subscription key for the policy source appliance (the Policy Server that connects to Sync Service), and use a Web Security Gateway subscription key for all other appliances. Otherwise, you receive superfluous hybrid filtering alerts.

Importing routes

Routes can be imported via a plain text file. How invalid entries are handled depends on the type of invalid data.

If a route specifies an invalid port (one that does not exist on the appliance), an error displays and **no** routes are added.

If a route specifies an invalid IP address, that route is not added, while properly formed entries are added.

Backup and restore tips

- When configuring a remote storage location (FTP server or Samba share) for backup files, make sure that the account used for backup file creation has **read**, **write**, and, if you have enabled the automatic deletion option, **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 600033 / Updated: 28-April-2011

Applies To:	Websense® V-Series Appliances v7.6.0 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 above takes you to a login prompt. Log in to view the list.