v7.5.0 Release Notes for V-Series Appliances

Topic 55120 / Updated: 16-February-2011

Applies To:	Websense V10000 v7.5 Websense V10000 G2 v7.5 Websense Web Security Gateway v7.5 Websense Web Security Gateway Anywhere v7.5

Use the Release Notes to find information about what's new and improved in V-Series Appliances at Version 7.5.0.

Important

Disable the Websense Content Gateway SNMP option prior to applying this patch. To do this: Log on to Content Gateway Manager and go to **Configure > MyProxy > Basic > General**. In the Features section, locate the SNMP option and, if necessary, disable it, then restart Content Gateway.

See the *V-Series Certified Products Matrix* at www.websense.com/support for a table of the Websense software module versions that are compatible with each appliance version.

Overview of V-Series v7.5.0

Topic 55121 / Updated: 23-August-2010

Applies To:	Websense V10000 v7.5 Websense V10000 G2 v7.5 Websense Web Security Gateway v7.5 Websense Web Security Gateway Anywhere v7.5

The Websense V-Series appliance is a high-performance platform for Websense Web Security Gateway Anywhere, combining Websense Web Security filtering, real-time content scanning, and Content Gateway proxy cache on a single, high-powered machine.

The appliance provides advanced analytics—including rules, signatures, heuristics, and application behaviors—to detect and block proxy avoidance, hacking sites, adult content, botnets, keyloggers, phishing attacks, spyware, and many other types of unsafe content.

The V-Series also closes a common security gap: decrypting and scanning SSL traffic before it enters the network.

The V-Series appliance works with a separate Windows 2003 or Windows 2008 server in the network that hosts one or more components. At a minimum, Log Server must be installed off the appliance (processes filtering log records into a separate Microsoft SQL Server database for management reporting).

The **TRITON Console**, introduced in this release, provides a single access point into the configuration interfaces for Websense Web Security and Websense Data Security. TRITON can be launched from any supported browser. Most sites install and run the software management interfaces themselves on Windows servers.

How long does a V-Series upgrade take?

New features in V-Series 7.5.0

Tips before a V-Series upgrade

V-Series Upgrade instructions

Known and resolved issues

How long does a V-Series upgrade take?

Topic 55122 / Updated: 23-August-2010

Applies To:	Websense V10000 v7.5 Websense V10000 G2 v7.5 Websense Web Security Gateway v7.5 Websense Web Security Gateway Anywhere v7.5

Off appliance components:	Websense software running off of the appliance, such as the **TRITON Web Security** console, Data Security Management Server, and Log Server, **must be moved to** version 7.5.x **after** you upgrade the appliance.
Estimated time to completion:	Installation of this upgrade takes approximately 90 to 100 minutes (one V-Series appliance and one Windows server).
Estimated duration of service disruption:	Service may be disrupted for 50 to 60 minutes while the upgrade is being applied to the appliance and the appliance restarts. Note that service is not disrupted while the off-box components are upgraded.
Restart requirements:	At completion of the appliance upgrade, you must restart the appliance. You will then be able to use the new features. At completion of the Windows components upgrade, you must restart each Windows server.
Upgrade installation verification:	To confirm that the upgrade was successful, open the V-Series console and look for version 7.5.0 to display in **Configuration > General**.

New features in V-Series 7.5.0

Topic 55123 / Updated: 23-August-2010

Applies To:	Websense V10000 v7.5 Websense V10000 G2 v7.5 Websense Web Security Gateway v7.5 Websense Web Security Gateway Anywhere v7.5

Software modules now at version 7.5.0

The version number of the appliance software is now synchronized with the Websense modules running on it. Version 7.5.0 of the Websense V-Series appliance updates all Websense software modules on the appliance to version 7.5.0. New v7.5.0 components are available both on and off the appliance, and can be enabled by subscription key.

- Appliance Controller v7.5.0

- Websense Web Security v7.5.0
- Websense Content Gateway v7.5.0
- Network Agent v7.5.0

Important

All networked V-Series appliances, and all Websense software modules running off the appliance and communicating with the V-Series, must be at the same base version. Ensure that the **policy source** (primary) appliance and all other appliances are at version 7.5. Consult the Websense *Deployment Guide* for information about modules that run off the appliance. Any Websense modules running off the appliance must also be at v7.5.x:

- **TRITON - Web Security** v7.5.0
- **TRITON - Data Security** v7.5.1
- **Data Security Suite** v7.5.1
- **Log Server** v7.5.0
- **Remote Filtering Server** v7.5.0
- **DC Agent** v7.5.0
- **eDirectory Agent** v7.5.0
- **Logon Agent** v7.5.0
- **RADIUS Agent** v7.5.0
- **Sync Service** v7.5.0
- **Linking Service** v7.5.0
- and any other Websense modules

Which features and fixes are in version 7.5.0 software?

New features and corrections included in v7.5.0 software modules are described in separate Release Notes in the Websense Technical Library:

Release Notes for Websense Web Security v7.5

Release Notes for Websense Content Gateway v7.5

Updates for the V-Series appliance

Appliance Manager

Appliance Manager is the new name for the familiar appliance management console. This is a graphical interface for configuring the appliance itself, checking the status of

the software modules, updating passwords, troubleshooting, and applying patches to the appliance.

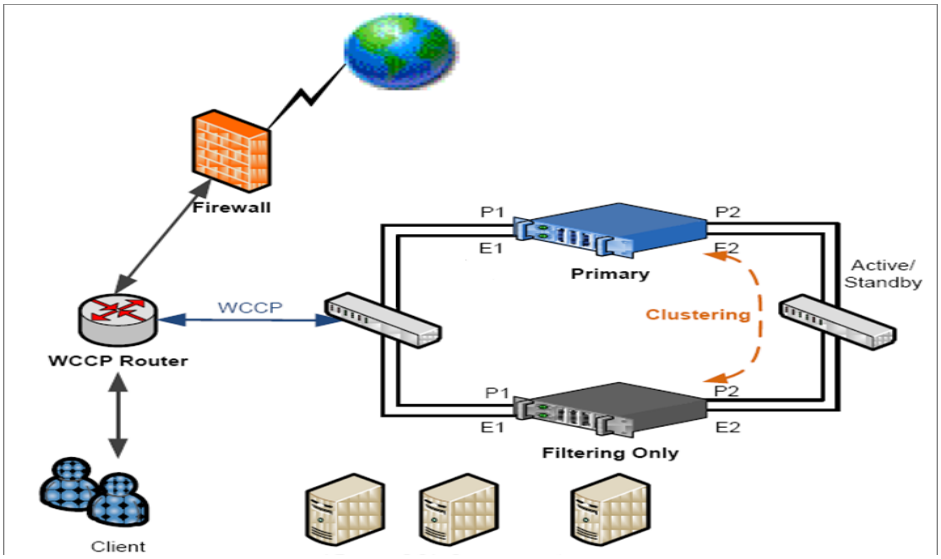
Appliance Manager provides status information about each module running on the appliance and enables you to establish assignments and network routes for the appliance's network interfaces.

Appliance Manager now offers setup options for expansion interfaces; provides access to selected command-line utilities such as ping and netstat; enables you to edit the block pages that display when users are prevented from accessing a Web page; and expands several other key features.

Expansion interfaces (NIC teaming)

V-Series appliances (except the V5000 G2) now support two optional, expansion interfaces called E1 and E2.

Each of these interfaces can be cabled to your network and then bonded through software settings to a Websense Content Gateway interface, with E1 optionally bonded to P1, and E2 optionally bonded to P2.



Interface bonding provides two alternatives:

- Active/Standby mode: P1 (or P2) is active, and E1 (or E2) is in standby mode. Only if the primary interface fails would its bonded interface (E1 or E2) become active.
- Load balancing: If your switch or router supports load balancing, then traffic to and from the primary interface is balanced between the primary interface and its bonded interface (E1 or E2).

You can choose to bond or not bond each Websense Content Gateway interface (P1 and P2) independently.

Full configuration backup and restore

You now have the option to back up and restore the full configuration of the appliance.

Thus, with v7.5.0, there are 2 types of backups available:

- **Appliance backup:** This backs up all settings for the appliance and for all Websense software modules on the appliance. You can perform the backup from any appliance on your network; the data included in the backup file varies according to the appliance on which you run it. Websense recommends you run a full backup on each appliance in your network regularly.
- **Module backup:** This saves all configuration information, including client and policy data, stored in the Policy Database. Only the *policy source* (primary appliance) can perform this task.

Up to 5 backup files of each type can be stored on the appliance.

After you select the type of backup you want, the Backup Utility checks all Websense components on the machine, collects the data eligible for backup, and creates an archive file. The file name includes a date stamp.

Full appliance backup files are displayed in the **Appliance Manager** with the following information:

- The hostname of the backup source, so you can see which appliance generated the backup file.
- The patch version of the appliance that generated the backup. When you restore from a backup, the backup file must be the same version as the appliance you are restoring.
- A comment on the policy information in each backup file:
  - **Full policy source** is the standard comment if the backup was generated on the policy source appliance.
  - **User directory and filtering** is the standard comment if the backup was generated on an appliance configured to run those components.
  - **Filtering only** is the standard comment if the backup was generated on a filtering only appliance.

You can download backup files from the appliance to another location on your network. This enables you to:

- Store appliance and Websense policy backup files in a safe and secure location. These files should be part of your organization's regular backup procedures.
- Move a module backup file to another appliance if needed.

You can also delete old backup files.

Backup process for appliance

1. Initiate an immediate backup by selecting **Backup** on the **Administration > Backup Utility** screen.

2. Select **Back up full configuration**.
3. Click **Perform Backup**.

Backup process for policies

1. On your *policy source* appliance, initiate an immediate backup by selecting **Backup** on the **Administration > Backup Utility** screen.
2. Select **Back up module configuration**.
3. Highlight the software module under **Select Module**.
4. Choose **Websense Web Security** to back up the Policy Database.
5. Click **Back Up Policies**.

Note that backup operations for Websense Content Gateway are managed through the Content Gateway Manager (proxy user interface).

Toolbox

You can now use the **Administration > Toolbox** screen to set up customized block pages and access a command line to assist with troubleshooting.

- *Customizing Web Security block pages*
- *Command line utility*

Customizing Web Security block pages

The appliance is pre-installed with a set of default Web Security block pages. (A block page displays to an end user each time the user's Web request is blocked.)

You can observe how the block pages appear for your policy configuration by going to http://testdatabase.websense.com and trying to access various Web sites that you know your policies do not permit users to access.

The default Websense block page files are always available. Simply choose the **Default block page** option on the **Administration > Toolbox** screen in **Appliance Manager** to use the defaults provided by Websense.

You can also make a copy of all default block page files, customize any of the copied files, and add your own graphics.

Note

The original default files remain stored on the appliance, unchanged, and you can revert to them at any time.

To customize a copy of the default block pages, follow the steps below:

1. Select **Custom block page.**
2. Download any files you want to change.
3. Make modifications locally, keeping the file names as they were.

4. Upload modified files.
5. Upload additional graphics files (if any).
6. Click **Apply Changes**.
7. Filtering Service is restarted automatically at this time.
8. Test the customized block pages by opening a browser on a client machine that is filtered by Websense Web Security on this appliance. Navigate to: http://testdatabase.websense.com and try to access various Web sites that you know your policies do not permit the client to access.
9. Return to Step 2 if adjustments are needed.

Your edited files can make use of custom logo files and other custom graphics files. If you use custom graphics, be sure to upload these additional graphics files to the editable directory, and make any edits necessary for other block files to point to them.

Note that the Help system for **TRITON - Web Security** contains detailed instructions for modifying any portion of the default block pages. These steps are located under the heading: *Working with block pages*.

For example, to change the logo that displays on the block page:

The file **master.html** includes the HTML code used to display to a Websense logo on the block page. To display your organization's logo instead:

1. Download the file **master.html**.
2. Copy an image file containing your organization's logo to the same location.
3. Open **master.html** in a text editor, such as Notepad or vi (not an HTML editor), and edit the following line to replace the Websense logo with your organization's logo:

   ```
   <img title="Websense" src="/en/Custom/wslogo_block_page.png"
   ...>
   ```

   - Replace **wslogo_block_page.png** with the name of the image file containing your organization's logo.
   - Replace the value of the **title** parameter to reflect name of your organization.
4. Save and close the file.

Filtering Service is restarted automatically when you finish uploading your customized files to the appliance and click **Apply Changes**.

Command line utility

The new command line utility enables you to run basic Linux commands for network troubleshooting and debugging from the Appliance Manager. Results are displayed on screen. You can download the output file for the most recent command displayed.

Click **Launch Utility** on the **Toolbox** page to open the command utility.

The utility includes a tab for each module you have installed. Select the tab for the module that you want to troubleshoot:

- Appliance Controller

- Websense Content Gateway
- Network Agent
- Websense Web Security

Choices include all settings for variables in the file `records.config` in Websense Content Gateway, and:

- ping
- traceroute
- nslookup
- netstat
- tcpdump
- nc
- wget
- ethtool
- ifconfig
- and more

Select the command you want to run from the drop-down list, enter appropriate parameters as described in the Help, then use the **Run** and **Stop** buttons as appropriate.

Websense Manager is now TRITON - Web Security and can run on the appliance

The **TRITON** console, introduced in this release, provides a single access point into the configuration interfaces for Websense Web Security and Websense Data Security. **TRITON** can be launched from any supported browser.

Websense Manager has been renamed to **TRITON - Web Security**. This manager component is now pre-installed on the appliance for use in evaluations and small organizations. You can choose to run it on the *policy source* appliance or (instead) install it off-box. Production sites with heavy traffic or large reports are advised to download the Websense Web Security installer archive from www.websense.com and install the **TRITON - Web Security** console on a separate Windows server.

Use the **Configuration > Web Security Components** screen in **Appliance Manager** to specify the location of your **TRITON - Web Security** manager.

On the *policy source* appliance only, you can choose whether to use **TRITON - Web Security** on the appliance, or elsewhere on your network. The default for evaluations is to use **TRITON - Web Security** on the *policy source* appliance. See *New policy source configuration option* for more details about the *policy source*.

After you upgrade from an earlier version of the appliance, your previous Web Security management IP settings are already populated on this screen (your off-appliance Web security manager location is known and is preserved). If you do not

have a manager location already established off the appliance, then the system uses **TRITON - Web Security** on the *policy source* appliance by default.

- To administer Websense Web Security on your *policy source* appliance, select **TRITON - Web Security on this appliance**. After you upgrade from an earlier version, you can use this option to override a previous manager location on your network.
- To specify that **TRITON - Web Security** is installed elsewhere, select **TRITON - Web Security located on another appliance or server on your network**, and enter the IP address for the appliance or server where the manager is installed in your network. The default port is displayed. This option disables the on-appliance Web Security manager.

> **Note**
> If you switch from an off-appliance **TRITON - Web Security** manager to an on-appliance version, or vice versa, you need to re-configure some settings in your new instance of **TRITON - Web Security**. Be sure to check all settings.

If you are configuring an appliance that is not a *policy source* machine, **TRITON - Web Security** settings are not needed. The **TRITON** console does not run on *non-policy source* appliances.

If you run the **TRITON - Web Security** manager on a Websense appliance, be sure that **Log Server** points to the **Policy Server** on that same appliance (point **Log Server** to the IP address of appliance interface C).

> **Important**
> Websense **Log Server** and **TRITON - Web Security** (manager component) must exchange connection information about the Log Database via **Policy Server**, so they must both point to the same **Policy Server**.

Expanded Logon Portal

The Logon Portal now provides access to all manager consoles used with Websense Web Security Gateway Anywhere, including:

- **TRITON - Web Security**
- **TRITON - Data Security**
- Content Gateway Manager
- Appliance Manager

New policy source configuration option

Whether you have one location or many, you designate a single appliance (or other server) to host a centralized Websense Policy Database. The other Websense appliances in your network point to this server and receive regular updates from it. This appliance is called the *policy source*. All available Websense Web Security services run on the *policy source* appliance.

- With a centralized Policy Database on the *policy source* machine, you manage one set of filtering policies for all appliances and all domains in the network.
- You can add services quickly as your network expands, and make necessary policy revisions only once, for the entire network.

If the appliance being configured is not the policy source machine, then it must point to the policy source.

In previous versions, the V-Series appliance could serve as either (a) the policy source machine or (b) a filtering machine, taking action on URL requests based on user information and policy data obtained from the *policy source* appliance located elsewhere on your network.

Version 7.5.0 introduces a third option.

Deployment choices in v7.5.0 for Websense Web Security modules

Any Websense V-Series appliance that is not serving as the *policy source* can now run either:

- *filtering only*
- *user directory and filtering*

These options are described in detail below, along with the benefits of each.

An appliance that is designated as the full *policy source* machine runs these components:

- All Websense Web Security core components, including:
  - Policy Database
  - Policy Broker
  - Policy Server
  - Filtering Service
  - User Service
  - Usage Monitor
  - Control Service
  - Directory Agent
  - **TRITON - Web Security** (optional)
    - Investigative Reports Scheduler
    - Manager Web Server
    - Reporting Web Server

    - Reports Information Service
- Websense Content Gateway module
- Network Agent module (optional)

Other appliances must point to the *policy source* machine by IP address to receive changes to your policies. To make that association in the **Appliance Manager**, use the **Configuration > Web Security Components** screen, under **Policy Source**.

1. First, choose the role that this appliance plays in your network. (Either it is a *policy source*, or it points to one.)
2. Second, provide the IP address where this appliance should look for its *policy source*.

Any appliance that is not the *policy source* can be designated to run either:

- *User directory and filtering* (these appliances must point to the *policy source* IP address). You might think of the *user directory and filtering* appliance as a lightweight version of the *policy source* machine. It runs:
    - Policy Server
    - User Service
    - Usage Monitor
    - Filtering Service
    - Control Service
    - Directory Agent
    - (optional) Network Agent module
    - Websense Content Gateway module
- *Filtering only* (these appliances must point to the *policy source* IP address). A *filtering only* appliance does not run Policy Server. It runs only:
    - Filtering Service
    - Control Service
    - (optional) Network Agent module
    - Websense Content Gateway module

See the Websense *Deployment Guide* for recommendations about the optional components and components that run off the appliance.

Choosing a role for each appliance

After you select your *policy source* machine, how do you determine which role is more effective for the other appliances in your network: *filtering only*, or *user directory and filtering*? The following information can be helpful:

User directory and filtering

- Having User Service together with Policy Server on remote appliances means that you are able to obtain local network user names.

- Latency between User Service and Policy Server is eliminated, because both run on the same appliance.
- Whenever you make a policy change, that change is immediately updated on the *policy source* appliance. The change is pushed out to the appliances that run Policy Server (*user directory and filtering*) within 30 seconds.
- Appliances that run Policy Server (you might think of these as lightweight versions of the *policy source* machine) can continue filtering for as long as 14 days if their connection with the *policy source* machine is interrupted. Thus, even if a network connection is poor or is lost, filtering continues as expected.

Filtering only

Appliances that run *filtering only* typically work best when they are local to the *policy source* and on the same network.

- These appliances require a continual connection to the centralized *policy source,* not only to stay current, but also to continue filtering. If the connection to the *policy source* machine becomes unavailable for any reason, filtering on a *filtering only* appliance can continue for up to 3 hours.
- If the *policy source* machine is instead on a remote network, with a WAN connection, it can be difficult to obtain user name/IP address maps for the local users.

If you run the **TRITON - Web Security** manager on a Websense appliance, be sure that **Log Server** points to the **Policy Server** on that same appliance (point **Log Server** to the IP address of appliance interface C).

Important

Websense **Log Server** and **TRITON - Web Security** (manager component) must exchange connection information about the Log Database via **Policy Server**, so they must both point to the same **Policy Server**.

Overview of V-Series v7.5.0

How long does a V-Series upgrade take?

New features in V-Series 7.5.0

Tips before a V-Series upgrade

V-Series Upgrade instructions

Known and resolved issues

Tips before a V-Series upgrade

Topic 55124 / Updated: 30-August-2010

Applies To:	V-Series Appliances

To prepare to upgrade a deployment that includes one or more Websense V-Series appliances, follow these guidelines:

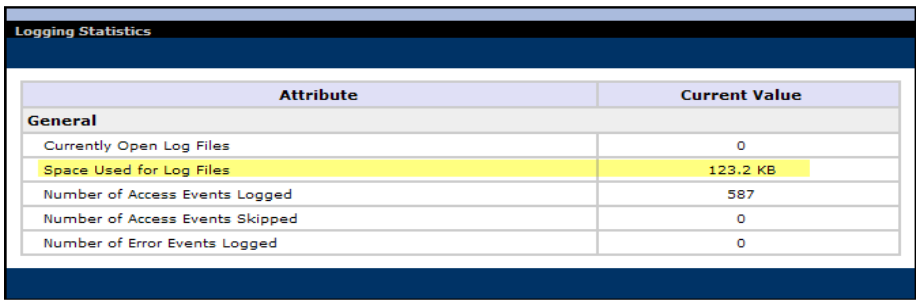
- If you have **multiple appliances** or are using a non-appliance **policy source** (Policy Broker, Policy Database, and Policy Server) installation, upgrade the policy source machine before upgrading user directory and filtering or filtering only appliances.

  To see whether an appliance is a policy source, go to the Configuration > Web Security Components page.

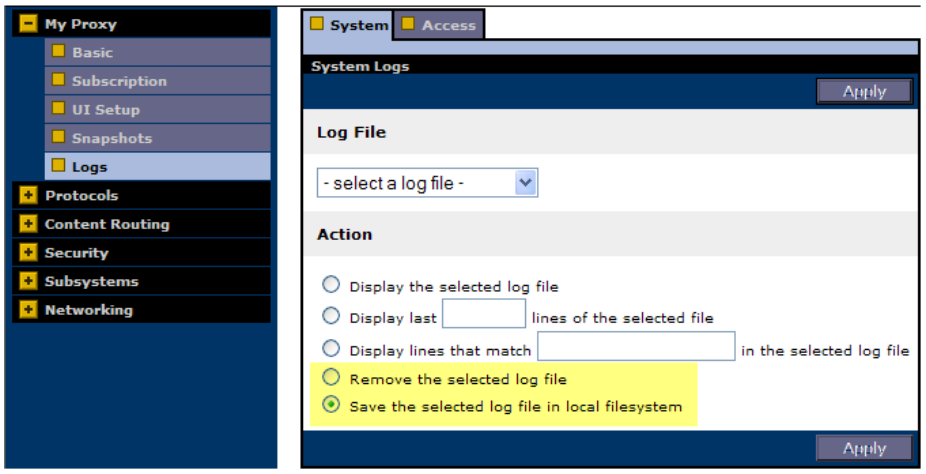
- Make sure that all appliances that share a policy source or that are in the same cluster are at the **same version**.
- If you have enabled **full clustering**, be sure to **disable** clustering before upgrading. After completing the upgrade process for all appliances and off-box components, enable clustering again.
- If you are upgrading a cluster, please see this essential supplement: V-Series Appliance Upgrade when Content Gateway is in Cluster Mode.
- Make sure that the SNMP option in Content Gateway Manager (Configure > MyProxy > Basic > General) is **disabled**. (The **Off** radio button should be selected.)

  SNMP monitoring is configured elsewhere for V-Series appliances. Websense Technical Support can assist with the configuration process.

- To ensure that there is sufficient free disk space in the Websense Content Gateway module, open Content Gateway Manager and go to the Monitor > Subsystems > Logging page. Verify that the space used for log files is **less than 2.5 GB**.



If the log files use more than 2.5 GB of space, go to the Configure > MyProxy > Logs page and delete the log files from the appliance. System logs can be deleted on the System tab; proxy logs can be deleted on the Access tab.

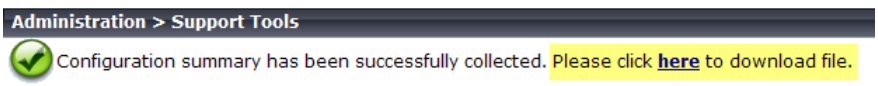


If you want to download a backup copy of the logs before deleting them, first make sure that your appliance version is 1.2.3 (Websense Content Gateway version 7.1.6). Backup of very large log files fails with earlier versions.

- **Back up** each appliance and any off-box components before starting the upgrade process. On each appliance:

  1. In Appliance Manager, go to the **Administration > Backup Utility** page and back up all modules on the appliance.
  2. Go to the **Administration > Support Tools** page and click **Generate File** (under V10000 Configuration Summary).

     Wait until the process completes and a success message is displayed at the top of the screen, then click the link in the success message to download a copy of the file.



3. Take a screenshot of the **Configuration > Network Interfaces** page and save it in a safe location.
4. Take a screenshot of the **Configuration > Routing** page and save it is a safe location.

- **Reboot** each appliance before applying patches or starting the upgrade to ensure that the appliance is in the cleanest state possible for a smooth upgrade.

> **Important**
> Take the appliances that you are upgrading out of production before starting the upgrade process.

Additional information is available to Websense Technical Support representatives and partners assisting customers with the upgrade process. (Requires an appropriate MyWebsense account.)

Setup tip

If you set up the P1 and P2 interfaces in the same subnet, note that the default gateway for the proxy is automatically assigned to P2 (which is bound to eth1). Ensure that outbound packets can reach the Internet.

Avoiding port conflicts

See the Solution Center article titled *V-Series: Which ports are used by the proxy*, 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 article first, to avoid conflict with ports already in use by the V-Series.

Logging tip

If you wish 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 the **TRITON - Web Security** console and navigate to **Settings > Network Agent > Global**. Then scroll down to **Additional Settings** to enable logging of protocol traffic and specify a logging interval.

Deployment tip

When Policy Broker is run on a V-Series appliance, you cannot install and run Policy Servers on off-box machines and point them to the Policy Broker that runs on the appliance. This configuration is not currently supported.

However, if you run Policy Broker on the V-Series or off the V-Series, you can run multiple Policy Servers on appliances (in secondary mode, pointing to the Policy Broker).

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 secondary appliances. Otherwise, you receive superfluous hybrid filtering alerts.

Overview of V-Series v7.5.0

How long does a V-Series upgrade take?

New features in V-Series 7.5.0

Tips before a V-Series upgrade

V-Series Upgrade instructions

Known and resolved issues

V-Series Upgrade instructions

Topic 55125 / Updated: 23-August-2010

Applies To:	Websense V10000 v7.5 Websense V10000 G2 v7.5 Websense Web Security Gateway v7.5 Websense Web Security Gateway Anywhere v7.5

Before applying the upgrade:

Be certain to follow the preparatory steps listed here: *Tips before a V-Series upgrade*

Upgrade details

You must have a **MyWebsense** account to obtain the Websense appliance upgrade software.

NOTE: Version 7.5.0 is a feature upgrade, as described above. However, the upgrade process is the same as for a patch.

Upgrade file name:	**Websense-V-Series-Upgrade-7.5.0.rpm** **Websense75Setup.exe**
Upgrade location:	Go to MyWebsense.com and select the Websense V10000 on your My Products and Subscriptions page. Open the drop-down list and choose the v7.5 patch.
Upgrade dependencies:	**Upgrade 7.5.0 requires that the appliance is at least at version 1.2.0 *before* you upload 7.5.0. If you have not already patched to v1.2.0, do that first.**
Off appliance components:	Websense software running off of the appliance, such as **TRITON - Web Security** and **Log Server**, **must be upgraded** to version 7.5.x. **after** you upgrade the appliance. Navigate to the Downloads page and select Websense Web Security. Download the file Websense75Setup.exe. Data Security Suite components require a new installation for version 7.5.x
Estimated time to completion:	Installation of this upgrade takes approximately 90 to 100 minutes (one V-Series appliance and one Windows server), which includes: • 10 minutes to download the upgrade file • 10 minutes to back up the V-Series files • 40 to 50 minutes to run the upgrade • 10 minutes to restart the V-Series and verify that the upgrade was successful • 5 minutes to download the Websense Web Security v7.5 installer • 10 minutes to run the installer to upgrade the off-box components • 5 minutes to restart the Windows server and verify that the upgrade was successful
Estimated duration of service disruption:	Service may be disrupted for 50 to 60 minutes while the upgrade is being applied to the V-Series and the appliance restarts. Note that service is not disrupted while the off-box components are upgraded.
Restart requirements:	At completion of the V-Series upgrade, you must restart the appliance. At completion of the Windows components upgrade, you must restart the Windows server.
Upgrade installation verification:	To confirm that the upgrade was successful, open the V-Series console and inspect the system information in **Configuration > General**. To confirm that the Windows components were successfully upgraded, log on to **TRITON - Web Security**.

Installation steps

CAUTION: Upgrade all Websense V-Series appliances to v7.5.0 **before** upgrading the Websense software on the Windows servers to v7.5.x. If your deployment uses several appliances, upgrade the primary appliance first (this is the appliance that hosts the policy source), then the secondaries, and finally the off-box components. See *Upgrading multiple V-Series appliances*, below.

The appliance upgrade has 3 required steps:

1. If the appliances in your network have not already been updated with patch 1.2.x, download and apply patch 1.2.x to all appliances.
2. For appliances currently at v1.2.x: Download and apply upgrade v7.5.0 to all appliances, upgrading the primary appliance first. Your policy database and console configuration settings are preserved.
3. Download and apply Websense Web Security upgrade v7.5.0 to the off-box components, typically **TRITON - Web Security** and **Log Server** (some sites use additional components).

Applying the upgrade

V-Series services are disrupted (not available) while the patch is applied until the V-Series completes its restart, approximately 50 to 60 minutes. It is best to perform the upgrade at a time when service demand is at a minimum.

After all backups have been completed and the upgrade file has been downloaded from MyWebsense.com:

1. Take all precautions to ensure that power to the V-Series is not interrupted during the upgrade. Power failure can result in operating system and software component corruption.
2. Log on to the V-Series console by pointing a browser to:

   `https://<IP-address-for-interface-C>:9447/appmng/`

   The user name is: **admin**.

   The password was set on your appliance when **firstboot** was run.
3. Navigate to **Administration > Patch Management**.
4. Click **Browse**, and select the v7.5.0 upgrade file.
5. Click **Upload**. After a few seconds, the upgrade is listed in the **Uploaded patches** list.
6. Click **Install** to apply the upgrade. It takes 40 to 50 minutes for the upgrade process to complete, and then you are prompted to restart the appliance. During this time proxy services are unavailable to users.
7. When the installation is complete, restart the appliance right away; click **Restart Now** when prompted. Do not cycle the power.
8. When the appliance has restarted, log on to the console and verify on the **Configuration > General** page that the V-Series version is 7.5.0.

9. Upgrade all Websense modules running off the appliance (such as **TRITON - Web Security** and **Log Server**). See *Windows server upgrades*, below.

If multiple V-Series appliances are installed in your network, they must all be running the same version of Websense software modules. Websense, Inc., does not support running different versions of the software on different appliances on one network. Filtering results are not expected to be consistent in that scenario.

Windows server upgrades

Upgrade your Windows server only after all V-Series appliances have been upgraded. An upgrade for Websense software running off of the appliance involves these steps:

1. Point your browser to MyWebsense.com and log on. Then navigate to the **Downloads** page.
2. Download the Windows installer for Websense Web Security version 7.5.0 (**Websense75Setup.exe**).
3. Run the installer on your Windows server(s) to upgrade **TRITON - Web Security**, **Log Server**, and any other Websense components running on the server(s). See the Websense Web Security version 7.5 Installation Guide for step-by-step instructions.

Upgrading multiple V-Series appliances

When multiple V-Series appliances are deployed on the same network, it is very important that they be upgraded in the prescribed order. For each appliance, follow the basic upgrade procedure described above (*Applying the upgrade*).

When multiple appliances are deployed in a cluster, see this essential supplement: V-Series Appliance Upgrade when Content Gateway is in Cluster Mode.

Best practice for upgrade sequence if policy source is on V-Series

Multiple V-Series appliances (1 primary, 1 or more secondaries). Policy Broker and Policy Server run on the primary:

1. Apply the v7.5.0 upgrade to the primary (*policy source*) V-Series and immediately restart when the upgrade completes.
2. Sequentially apply the v7.5.0 upgrade to all secondary appliances. Restart each appliance when the upgrade completes.
3. Use the Websense Web Security v7.5 installer to upgrade all off-box components. See the Websense Web Security version 7.5 Installation Guide for step-by-step instructions.

Best practice for upgrade sequence if policy source is not on V-Series

If you have multiple V-Series appliances with the policy source (Policy Broker and Policy Server) located on a Windows server:

1. Use the Websense Web Security v7.5 installer (**Websense75setup.exe**) to upgrade the Policy Broker and Policy Server components (only) on the Windows server. See the Websense Web Security version 7.5.0 Installation Guide for step-by-step instructions.
2. Apply the v7.5.0 upgrade to each appliance and immediately restart as each upgrade completes.
3. Use the Websense Web Security v7.5 installer to upgrade remaining off-box components. See the Websense Web Security version 7.5 Installation Guide for step-by-step instructions.

Best practice for upgrade sequence if Filtering Service and Network Agent (or only Network Agent) run off the appliance

If you run Filtering Service and Network Agent off the appliance, and both point to the policy source (primary) appliance

1. Apply the v7.5.0 upgrade to the primary V-Series and immediately restart when the upgrade completes.
2. Use the Websense Web Security v7.5 installer to upgrade all off-box components. See the Websense Web Security version 7.5 Installation Guide for step-by-step instructions.

If you run Network Agent off the appliance, and it points to the policy source (primary) appliance

1. Apply the v7.5.0 upgrade to the primary V-Series and immediately restart when the upgrade completes.
2. Use the Websense Web Security v7.5 installer to upgrade all off-box components. See the Websense Web Security version 7.5 Installation Guide for step-by-step instructions.

If you run Network Agent off the appliance, and it points to a secondary appliance

1. Before you upgrade, record all settings you have established for Network Agent, so that you can reset them.
   a. Run Websense Manager and navigate to **Settings > Network Agent > Global > IP Address of off-box Network Agent > NIC Configuration** and save a screen shot for this page.
   b. Navigate to **Settings > Network Agent > Global > IP Address of off-box Network Agent > NIC Configuration > Monitor List** and save a screen shot for this page.
2. Uninstall the off-box Network Agent.
3. Apply the v7.5.0 upgrade to the primary V-Series and immediately restart the appliance when the upgrade completes.
4. Apply the v7.5.0 upgrade to the secondary V-Series and immediately restart the appliance when the upgrade completes.

5. Use the Websense Web Security v7.5 installer to upgrade off-box components. See the Websense Web Security version 7.5 Installation Guide for step-by-step instructions.
6. Install Network Agent v7.5 on the off-box server, then use the screen shots you saved in step1 to reconfigure the off-box Network Agent settings.

If you have previously specified the IP address for the server where Websense Manager is running (either with the Status > Modules page or on the Logon Portal page)

In this situation, the **TRITON** console located on the appliance will be disabled by default after the upgrade. The IP address for the **TRITON - Web Security** console will be the IP address previously established for Websense Manager. Some settings will need to be reconfigured.

If you are upgrading an appliance that had no IP address specified for Websense Manager

After upgrade, the **TRITON - Web Security** console on the appliance will be *enabled* by default. You can disable it in the Appliance Manager on the page **Configuration > Web Security Components**.

Avoid installing multiple copies of the **TRITON - Web Security** console. If you install and use the **TRITON** console on a Windows server, then be sure to disable the copy on the appliance. In the Appliance Manager, navigate to the page **Configuration > Web Security Components**. If you use the **TRITON** console on the appliance, then uninstall any copy you may have running on a Windows server. Each time you change the location of the **TRITON** console, be sure to reconfirm settings. Some settings will need to be reconfigured.

Best practice for upgrade sequence if a custom policy source is configured

Policy Broker is not on a V-Series appliance. The appliance you are upgrading is pointing to the central Policy Broker (which is on Windows)

1. Before you upgrade, record all settings you have established for any instances of Network Agent running off the appliance, so that you can reset them after the upgrade.
   a. For each off-box Network Agent, run Websense Manager and navigate to **Settings > Network Agent > Global > IP Address of off-box Network Agent > NIC Configuration** and save a screen shot for this page.
   b. Navigate to **Settings > Network Agent > Global > IP Address of off-box Network Agent > NIC Configuration > Monitor List** and save a screen shot for this page.
2. Uninstall all off-box Network Agent instances.

3. Use the Websense Web Security v7.5 installer (Websense75setup.exe) to upgrade the Policy Broker and Policy Server components on the off-box machine. See the Websense Web Security version 7.5 Installation Guide for step-by-step instructions.
4. Apply the v7.5.0 upgrade to each appliance that points to the central Policy Broker, and immediately restart each appliance as the upgrade completes.
5. Install Network Agent v7.5 on the off-box server(s), then use the screen shots you saved in step1 to reconfigure the off-box Network Agent settings.
6. Use the Websense Web Security v7.5 installer to upgrade all other off-box components.

Important note if Policy Source appliance is down or unavailable

Best practice is to upgrade the primary appliance first, then the secondary appliances, and finally the off-box Websense components. These steps are shown above.

However, if your site must upgrade a secondary appliance before the primary appliance, or if your primary appliance is unavailable, is being replaced, or is being re-imaged, then set the secondary appliance (temporarily) to be the policy source. To do this:

1. On that secondary appliance, in the V-Series console, move to the page **Configuration > Web Security Components**.
2. For **Policy information resides on**, select **This V-Series appliance**. Save the setting.
3. Upgrade the secondary appliance to version 7.5.0 (following all steps above) and restart it.

After the primary appliance has been upgraded, replaced, or re-imaged, change the upgraded secondary machine to point to the primary again, for its policy information. To do this:

1. Upgrade the primary appliance (following all steps above) and restart it.
2. On the previously upgraded secondary appliance, in the V-Series console, move to the page **Configuration > Web Security Components**.
3. For **Policy information resides on**, select **Another V-Series appliance or server on your network** and enter the IP address of the policy source machine (primary). Save the setting.

Use the Websense Web Security v7.5 installer to upgrade all off-box components, after all V-Series appliances have been upgraded.

Overview of V-Series v7.5.0

How long does a V-Series upgrade take?

New features in V-Series 7.5.0

Tips before a V-Series upgrade

V-Series Upgrade instructions

Known and resolved issues

Known and resolved issues

Topic 55126 / Updated: 23-August-2010

Applies To:	Websense V10000 v7.5 Websense V10000 G2 v7.5 Websense Web Security Gateway v7.5 Websense Web Security Gateway Anywhere v7.5

A list of known and resolved 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.

Additional information for Websense employees and partners is available here.

Overview of V-Series v7.5.0

How long does a V-Series upgrade take?

New features in V-Series 7.5.0

Tips before a V-Series upgrade

V-Series Upgrade instructions