Websense Appliance Manager Help

Websense V5000 G2 Appliance
for Web Security

v7.5.4

10240 Sorrento Valley Rd., San Diego, CA 92121, USA

Published 2011 Revision A
Printed in the United States and Ireland

Trademarks

1 V5000 G2 Appliance for Web Security

The Websense V5000 G2 appliance for Web Security works in conjunction with integration products such as Microsoft ISA Server, Citrix Presentation Server, and Cisco PIX to provide Internet filtering, user identification, alerting, reporting, and troubleshooting capabilities.

The V5000 G2 provides the engine and configuration tools to develop, monitor, and enforce Internet access policies, managing over 90 URL categories, Web reputation, 120 network and application protocols, and instant messaging attachment.

Appliance Manager

Appliance Manager is the name of the V5000 G2 management console. This is a graphical interface for configuring the appliance itself, checking the status of the software modules, updating passwords, troubleshooting, creating backups, 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 routes for the appliance's network interfaces.

Security best practices

- Lock the appliance inside an IT closet and enable a BIOS password. Physical access to the appliance can be a security risk for your network.
- Ensure that administrator credentials are restricted to a select few persons. This helps preclude unauthorized access to the system.
- Enable troubleshooting ports and permit remote access only when requested to do so by Websense Technical Support. Return these settings to the disabled state immediately after the Websense specialist logs off.

Management consoles for Websense software modules

Configuring the software modules on the appliance (such as setting up users and defining and applying Internet filtering policies) is not performed through the Appliance Manager.

Instead, these settings are handled through each software module's management console. The table below shows the name of each management console and shows how to access it through a browser.

A combined Logon Portal that can access the Appliance Manager and the consoles for all software modules is available at `http://<IP-address-of-interface-C>`.

Software module	Description	Management console name	How to launch the management console
Websense Web Security	Filtering Internet requests from client machines. Filtering policies and their assignments to clients.	TRITON - Web Security	Point a browser to: **`https://<IP-address-of-TRITON - Web Security server>:9443/mng/`**
Network Agent	Works with Filtering Service to enable protocol management, bandwidth-based filtering, and reporting on bytes transferred. • In a stand-alone deployment, enables HTTP and non-HTTP filtering • In an integrated deployment, enables filtering for protocols not managed by your integration product and provides enhanced logging information	TRITON - Web Security	Point a browser to: **`https://<IP-address-of-TRITON - Web Security server>:9443/mng/`**

Using the TRITON console in version 7.5.4

The interface used to manage Websense Web Security is called the TRITON™ console.

NOTE: The TRITON console supports Internet Explorer 7 and 8 and Firefox 3.0.1 - and 3.5.x. [The Compatibility View of IE 8 is not supported.] If you use a different browser version, unexpected behavior may result.

The TRITON Web-based console enables you to perform basic setup, system maintenance, policy creation, reporting, and incident management for both modules from the same location.

A combined Logon Portal that can access the Appliance Manager and the TRITON console is available at `http://<IP-address-of-interface-C>`.

Reporting on the V5000 G2 appliance

Software on the appliance generates detailed reporting records (log records) of Web usage and Web security actions.

Management reports from these logs are provided through software modules:

- TRITON - Web Security
- Websense Log Server

TRITON - Web Security is:

- Pre-installed on the appliance
- Accessed through a browser

Important

To enhance performance at sites with large log files, most sites download a Websense Web Security installer archive from www.websense.com and then install the **TRITON - Web Security** console on a separate Windows server for production use. This is recommended.

Websense **Log Server** is:

- Not on the appliance. It must be downloaded as part of a larger download archive for Websense Web Security components. www.websense.com
- Installed separately on a Windows server
  - that has access to Microsoft SQL Server
  - and is networked to the appliance

The following reports produced in the **TRITON - Web Security** module help you evaluate the effectiveness of your security policies.

Web security reports

- The **Today** page appears first when you open **TRITON - Web Security** in a browser. It shows the operating status of Websense software, and can display charts of filtering activities in the network since midnight.

- The **History** page shows charts of filtering activities in the network for up to 30 days.
- **Presentation reports** and **Investigative reports** are extensive reporting tools that give you options for generating, customizing, and scheduling Internet usage reports.

Presentation reports

Presentation reports offer a list of report definitions. Some are tabular, some combine a bar chart and a table. To generate a presentation report, open TRITON - Web Security in a supported browser and choose Presentation Reports from the navigation bar at the left.

In addition to generating predefined charts, you can copy the charts and apply a customized report filter that identifies specific clients, categories, protocols, or actions to include. Mark the report definitions that you use frequently as Favorites, to make them easier to find.

You can schedule any presentation report to run once, at a particular time, or on a repeating cycle.

Investigative reports

Investigative reports let you browse through reporting log data interactively. The main page shows a summary-level bar chart of activity. Click the different elements on the page to update the chart or get a different view of the data.

Databases used with the V5000 G2 appliance

Websense software filters Internet activity based on your active policy and information stored in databases.

Master Database

The **Master Database** is downloaded daily from a Websense server.

- The Websense Master Database houses the category and protocol definitions that provide the basis for filtering Internet content.
- A limited version of the filtering database is pre-installed on the appliance, so that filtering can begin immediately. Download the full Master Database (using the TRITON - Web Security console to start the download) as soon as possible, to enable comprehensive Internet filtering capabilities. See the *Websense V5000 G2 Appliance for Web Security Getting Started Guide* after you complete initial setup of the appliance.
- After the first Master Database download, Websense software downloads database changes on a schedule that you establish in TRITON - Web Security.

Because the Master Database is updated frequently, default database downloads are scheduled to occur daily.

- If the Master Database on the appliance is more than 14 days old, Websense software does not filter Internet requests.

Real-time database updates

In addition to scheduled downloads, Websense software performs emergency updates to the Master Database as needed. A real-time update might be used, for example, to recategorize a site that was temporarily miscategorized. These updates ensure that sites and protocols are filtered appropriately.

Websense software checks for real-time database updates every hour.

Real-Time Security Updates™

In addition to receiving the standard real-time database updates, users of Websense Web Security can enable Real-Time Security Updates in TRITON - Web Security to receive security-related updates to the Master Database as soon as they are published by Websense, Inc.

Real-Time Security Updates provide an added layer of protection against Internet-based security threats. Installing these updates as soon as they are published reduces vulnerability to new phishing scams (identity fraud), rogue applications, and malicious code infecting mainstream Web sites or applications.

Websense Filtering Service checks for security updates every 5 minutes. Because updates are sent only when security threats occur, actual changes are occasional, and tend not to disrupt normal network activity.

Logging on to the Appliance Manager

Log on to Appliance Manager by pointing a browser to either of these URLs:

```
(Logon Portal)  http://<IP-address-of-interface-C>
(Console only)  https://<IP-address-of-interface-C>:9447/appmng/
```

The user name is: **admin**.

The password was set on the appliance when the script **firstboot** was run.

To change the console password, see *Account management*.

Navigation pane

At the left side of the Appliance Manager is the navigation pane. Use this pane to select the console screen you want to view.

Status

- *Modules*
- *CPU and memory status*
- *Disk usage*
- *Network bandwidth*

Configuration

- *General configuration*
- *Network interfaces*
- *Web Security components*

Administration

- *Patch management*
- *Backup utility*
- *Logs*
- *Toolbox*
- *Account management*

Modules

The **Status** > **Modules** page appears first after you log on to the the appliance. It presents the current status of each software module on the appliance.

Use this screen to stop or start software services, restart an entire software module, restart or shut down the appliance itself, and gauge resource usage per module.

Important

For security purposes, an Appliance Manager session ends after 30 minutes of inactivity. You can choose to monitor the status pages even after the 30-minute timeout is reached.

To do this, mark the box labeled **Monitor status without timing out** on this page.

Information on all Status pages then continues to update normally until you close the browser or navigate away from the Status pages. Be sure to **Save** all changes; these are lost if not saved before 30 minutes of inactivity.

Modules on the the appliance may include:

- The **Appliance Controller** software operates behind the scenes. It manages appliance configuration, downloads and applies patches, accesses the backup utility, requests module restarts, initiates shutdowns, and handles other appliance management tasks.
- **Websense Web Security** is the software that handles Web filtering. Several services (daemons) comprise this software.
- **Network Agent**, in a stand-alone deployment, monitors Internet traffic and filters HTTP and non-HTTP protocols, such as instant messaging.

The table below describes the action of each button on the **Status > Modules** screen.

Button	Description
Restart Appliance	Causes this appliance to be rebooted. All modules are stopped. Modules are then restarted.
Shutdown Appliance	Causes this appliance and all software modules to be shut down gracefully.
Restart Module (Websense Web Security)	Causes the Websense Web Security module on this appliance (all services in use) to be stopped and then restarted.
Launch (TRITON - Web Security)	Launches the TRITON Web security management console.
Stop Services (Websense Web Security)	Causes all Websense Web Security services running on this appliance to be stopped. [If this appliance is not designated to be the policy source for your network, some services may not be in use.]
Restart Module (Network Agent)	Causes the Network Agent service on this appliance to be stopped and then restarted.
Stop Services (Network Agent)	Causes the Network Agent service on this appliance to be stopped.

CPU and memory status

The **Status > CPU and Memory** page provides information about CPU and memory usage for each software module running on this appliance, for the previous 60 seconds.

- **CPU Usage** displays:
  - An aggregate of all CPU usage during the previous 60 seconds, based on occupied resources and total available resources for the module
  - The percentage of each available CPU used by the module during the previous 60 seconds
- **Memory Usage** displays:

- The percentage of available memory used by the module during the previous 60 seconds
- The actual memory used by the module during the previous 60 seconds, in megabytes
- The total memory available to this module during the previous seconds, in megabytes

Disk usage

The **Status > Disk Usage** page provides a summary of system disk usage on this appliance, during the previous 60 seconds.

- **System Disk** is used to store the appliance management system, all Websense services, and files used by the services.

Network bandwidth

The **Status > Network Bandwidth** screen provides information about throughput on the appliance network interfaces listed here:

- **Appliance Controller Interface** (C)
- **Network Agent Interface** (N)

For each interface, the following information is displayed for the previous 60 seconds:

- Current megabits per second, inbound and outbound, on the interface
- Total megabits of data received and sent
- Total number of packets received and sent
- Packets dropped, inbound and outbound
- Total errors, inbound and outbound
- Rate in megabits per second, inbound and outbound

2 Configuration

The Appliance Manager accepts general appliance settings and enables you to define each network interface.

Use the Configuration screens in the Appliance Manager to set the time and date; define the network interfaces for the appliance; and identify which computer is hosting the filtering policies for the network.

Configuration options

- *General configuration*
- *Network interfaces*
- *Web Security components*

General configuration

Use the **Configuration** > **General** page to:

- View basic appliance information
- View a list of the software modules installed on the appliance and their version numbers
- Set the system *Time and Date*
- Set the *Hostname*

In each panel:

- **Save** applies and saves new values in the panel.
- **Cancel** discards all changes entered since the last **Save** and restores entry fields in the pane to their current settings.

Time and Date

This pane is used to set and update the system time and date.

Important

If any Websense services are running, stop all Websense services before changing the time. Then, reset the time, making certain that the time is consistent across all servers running Websense services. Then, restart Websense services. If you do not stop the services first, client updates and policy changes entered after the time reset are not saved.

Time zone: (displays the current setting)

From the drop-down list, select the time zone to be used on this system.

GMT (*Greenwich Mean Time*) is also known as UTC (*Universal Time, Coordinated*). Other time zones are calculated by adding or subtracting from GMT. GMT is sometimes chosen to provide a common time stamp for geographically distributed systems.

Click **Save** to apply and save the change.

Time and date: (displays their current values)

Set the time and date manually, or synchronize the system clock with an Internet Network Time Protocol (NTP) server (the default).

If you synchronize the system clock:

Important

NTP protocol packets and their response packets must be allowed on any firewall or NAT device between the appliance and the NTP server. Ensure that you have outbound connectivity to the NTP server(s). Add a firewall rule that allows outbound traffic to UDP port 123 on the NTP server. If the firewall does not have stateful logic for UDP, also add a rule that allows inbound traffic for port 5678 on the appliance.

Time is set and displayed in 24-hour notation.

Automatic synchronization	To synchronize with an Internet Network Time Protocol (NTP) server, select the **Automatically sychronize** option and enter the address of a primary NTP server. The secondary and tertiary fields are optional. If interface C on this appliance is not connected to the Internet, then you must provide a way for interface C to reach an NTP server. One solution is to install an NTP server on the local network where interface C can reach it. www.ntp.org
Manual settings	Select **Manually set time and date** and change the values in the Time and Date fields. Use the format indicated adjacent to the entry field.

Click **Save** to apply and save the changes.

Hostname

Hostname is the system name of the appliance.

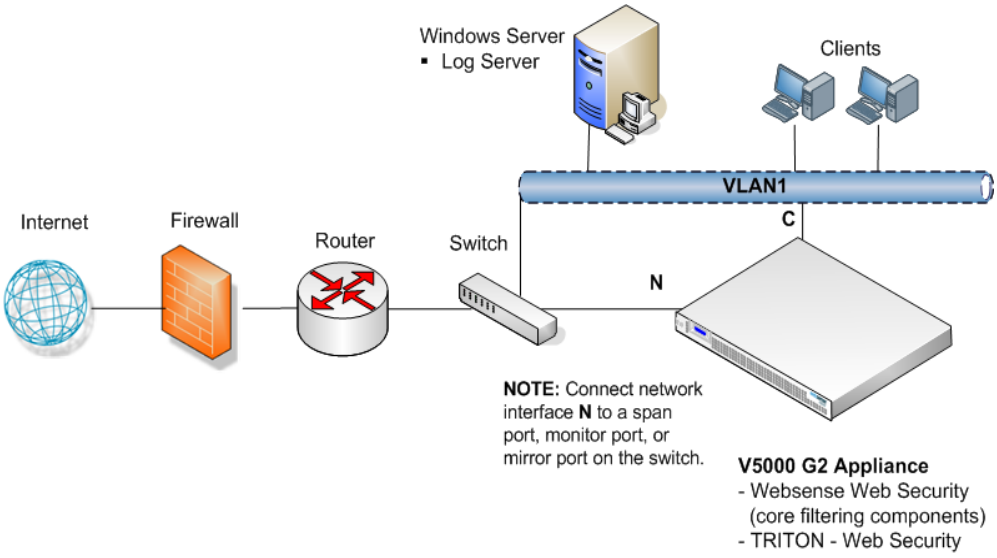
- Hostname can be 1 to 32 characters.
- The first character must be a letter.
- Other characters can be letters, numbers, dashes, or periods.

Click **Save** to apply and save the change.

Network interfaces

Use the **Configuration** > **Network Interfaces** screen to specify the IP address, subnet mask, and DNS addresses for each network interface on the appliance.

- *Appliance Controller Interface (C)*
- *Network Agent Interface (N)*



In each panel:

- **Save** applies and saves new values in the panel.
- **Cancel** discards all changes entered since the last **Save** and restores entry fields in the pane to their current settings.

Appliance Controller Interface (C)

The Appliance Controller interface (C) handles communication with all Websense management interfaces; provides inter-appliance communication; (optionally) transports HTTP and non-HTTP protocol enforcement; and handles Websense Master Database downloads via the Internet. Initial configuration of the C interface is completed when the appliance is first powered on; a script called **firstboot** prompts you for the values needed to configure interface C.

When you use a third-party integration product, such as Microsoft ISA Server, communication between that third-party product and Websense Filtering Service goes through interface C.

Guidelines for configuring network interface C

IP address (C interface)	Required. This interface requires continual access to the Internet. If you change the IP address for the C interface, the update process may require about 10 minutes. The IP is changed, and then you are redirected to a Web logon page. Enter your user name and password. Notice on the **Status > Modules** page that the services are starting up. Allow for all services to start.
Subnet mask (C)	Required.
Default Gateway (C)	Optional. IP address of the router that allows traffic to be routed outside of the subnet.
Primary DNS (C)	Required. IP address of the domain name server.
Secondary DNS (C)	Optional. Serves as a backup in case the primary DNS is unavailable.
Tertiary DNS (C)	Optional. Serves as a backup in case the primary and secondary DNSs are unavailable.

Network Agent Interface (N)

In Stand-alone mode, the Network Agent software component filters HTTP and non-HTTP protocols. It provides bandwidth optimization data and enhanced logging detail.

> **Note**
> If your site integrates Websense modules with a third-party integration product (such as Microsoft ISA Server), then Network Agent filters only non-HTTP protocols.

Network Agent continually monitors overall network usage, including bytes transferred over the network. The agent sends usage summaries to other Websense software at predefined intervals.

Network Agent is typically configured to see both inbound and outbound traffic in your network. The agent distinguishes between:

- Requests sent from internal machines to internal machines (hits to an intranet server, for example)
- Requests sent from internal machines to external machines such as Web servers (user Internet requests, for example)

You choose whether blocking information for HTTP and non-HTTP protocols is routed through interface C or interface N.

Guidelines for configuring network interface N on the appliance

Select the Interface C button only if you want to use interface C to send blocking information for HTTP and non-HTTP traffic.	
Select the Interface N button if network interface N is connected to a bidirectional span port, and you want to use N to transport blocking information for HTTP and non-HTTP protocols.	If interface N is connected to a bidirectional span port, then you can use it to transport blocking information for HTTP and non- HTTP protocols. To set this up, you must select the Interface N button near the top of this pane. Interface N is then used to transport blocking information for protocols other than HTTP and HTTPS. Complete all required fields, as described below. If the box is not checked, then network interface C (not interface N) is used to transport blocking information for HTTP and non-HTTP protocols. Settings for the Network Interface blocking NIC in TRITON - Web Security do not override the settings you enter in this pane. The settings in Appliance Manager take precedence.
IP address of interface N	Required. Network Agent should be able to see the outbound and inbound traffic in your network. Network Agent ignores ports 80 and 443.
Subnet mask	Required.
Default gateway	Required if Interface N is checked. Otherwise, entry field is disabled.
Primary DNS	Required. IP address of the domain name server.
Secondary DNS	Optional. Serves as a backup in case the primary DNS is unavailable.
Tertiary DNS	Optional. Serves as a backup in case the primary and secondary DNSs are unavailable.

Network Agent can instead be installed on a different server in the network. See the *Web Security Installation Guide* for requirements.

Web Security components

Use the **Configuration** > **Web Security Components** screen to specify where the appliance gets Internet filtering policy information, and to define the location of your TRITON - Web Security manager.

Policy source

Whether you have one location or many, designate a single appliance (or other server) to host a centralized Websense Policy Database. The other Websense appliances point to this server and receive regular updates from it. This appliance (or other server) 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.

The selections you make on this **Configuration** screen reflect your plan for appliance deployment.

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

Single location

In a single location where multiple appliances filter behind a common load balancer, all Websense appliances in the network typically share policy information and policy components installed on one appliance that you designate as the full *policy source*. (A server that is not a Websense appliance may be used as the *policy source* instead of an appliance.)

Other appliances in the network can be designated to run either *filtering only* or to run both *user directory and filtering*. These options are described in detail below.

Multiple locations

With multiple geographical locations, you have the choice of treating each site independently, designating a full *policy source* machine at every location, and designating local policy management and reporting privileges.

Alternatively, you can establish a centralized *policy source* at one location, and have all of the other locations communicate with that centralized source to receive policy updates.

Web Security deployment choices for Web security modules

An appliance that is not serving as the *policy source* can be designated to run either:

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

These options are described in detail below, along with the benefits of each. (See *Choosing a role for an appliance*.)

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

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

Other appliances must point to the *policy source* machine by IP address to receive changes to your policies. To make that association, 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 secondary appliance, a lightweight version of the *policy source* machine. It runs:
  - Policy Server
  - User Service
  - Usage Monitor
  - Filtering Service
  - Control Service

  - Network Agent 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
  - Network Agent module

See the Websense *Deployment Guide* for recommendations about the optional components.

User directory with the appliances

If your organization relies on user identification or authentication, each appliance that is running Websense User Service must be configured to talk to a user directory. Multiple appliances can talk to the same user directory or to different user directories.

Choosing a role for an 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 close 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 on a remote network, with a WAN connection, it can be difficult to obtain user name/IP address maps for the local users.

TRITON - Web Security panel

Use this panel to enter information that the Logon Portal needs to connect to the TRITON console, the management console for Web Security software.

For the *policy source* appliance, 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.

Production sites with heavy traffic or large reports are advised to download the Websense Web Security installer archive from www.MyWebsense.com and install the TRITON - Web Security console on a separate Windows server.

When 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**. If you are upgrading, 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 TRITON - Web Security console.

> **Note**
> If you switch from an off-appliance TRITON - Web Security manager to an on-appliance version, or vice versa, you should reconfirm configuration settings in your new instance of TRITON - Web Security.

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

Click **Save** to save and apply your changes.

Redundancy

Internet usage filtering requires interaction between several Websense software components:

- User requests for Internet access are monitored by Network Agent.
- The requests are sent to Websense Filtering Service for processing.
- Filtering Service communicates with Policy Server and Policy Broker to apply the appropriate policy in response to the request.

In some networks, additional machines may be used to deploy additional instances of Network Agent or other components. For example, in a large, segmented network, you may need a separate Network Agent for each segment. Or, you might deploy the Remote Filtering Server on a separate computer, to enable filtering of laptops and other computers that are outside the organization's network.

Be sure to configure each separate Network Agent to communicate with Filtering Service on the **Settings > Network Agent > Local Settings** page in TRITON - Web Security. See the Websense Web Security Help for additional information.

Check the Websense *Deployment Guide* and associated *Deployment Guide Supplements* for component distribution options. Contact your Websense Sales Engineer, or your authorized Websense reseller, for assistance in planning a more complex deployment.

When you are ready to install individual components, refer to the Websense *Installation Guide* for instructions.

3 Administration

Websense, Inc., maintains a customer portal at www.mywebsense.com where you can download product updates, get patches, access customer forums, read product news, and access other technical support resources for your Websense software and Web Security appliance.

Best Practice: create your MyWebsense account when you first set up the appliance, so that (a) you can immediately apply any new patches made available since your appliance was assembled, and (b) you can get access whenever you need support or updates.

Administration options

Administration screens on the Web Security appliance enable you to change passwords, access system logs, prepare and restore backups of your Policy Database, and install software patches.

- *Patch management*
- *Backup utility*
- *Logs*
- *Toolbox*
- *Account management*

Patch management

Use the **Administration** > **Patch Management** screen to upload and install software patches and review patch history.

Best practices for appliance patches

- A new appliance at your site should immediately be patched to the latest version.
- Keep all Web Security appliances on your network at the same version.
- Install software patches as soon as they become available.

Patch process for appliance

The Web Security appliance supports manual upload and installation of patch files. First, you must download the new patch with your MyWebsense account.

- Create a MyWebsense account at www.mywebsense.com.
- Check your MyWebsense account regularly for updates and news about Websense releases and patches.
- Download appliance patches to a folder on your network as soon as they become available.
- Use the **Administration** > **Patch Management** screen to upload and install each patch on the appliance, during a low-activity period on your network.
- Install patches in consecutive sequence.
- The appliance version number is the number of the latest patch installed.
- Be sure that all Websense modules running off the appliance (such as Log Server) are upgraded to the appropriate level, each time you patch the appliance.
- The *V-Series Certified Matrix* shows a table of the Websense software module versions that are compatible with each appliance version.
- Multiple appliances may be installed in your network. However, 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.

Available patch update options

Upload patch	Click **Browse** to navigate to the folder containing a downloaded patch. Then click **Upload** to upload the patch to this appliance. **Caution**: Do not navigate away during the upload process. This can cause the patch upload to fail. After a successful upload, the patch is listed in the patch window on the console, and the **Status** column indicates that the patch is Ready to install.

Install	Click the **Install** button in the **Action** column to the right of the patch. The **Status** column shows the progress of the installation in a progress bar. You are notified if a restart is required after installation. After you restart, the patch is removed from the patch queue and logged in **Patch History**. The version number of the appliance (shown in the patch pane) is updated. If a previous patch is not installed on the appliance but is required, you receive a message in the **Status** column indicating which earlier patch is required, and the **Install** button is disabled. Install the previous patch first.
Delete	Click the **Delete** button in the **Action** column to the right of a patch you want to delete. If a patch installation fails, any installed files from that patch are immediately uninstalled. You receive a message indicating that the patch installation failed. You can try installing it again. If that fails, delete the patch, then re-upload it, and then start the installation again.

Patch History

The Patch History pane in Appliance Manager displays all patches installed on this appliance. For each patch, you see:

- Version number
- Date and time of patch installation
- Confirmation of successful installation
- Link to patch log file, showing patch details

Backup utility

To access steps for restoring a backup, see *Restoring a backup file*.

There are 2 types of backups available on your network:

- Appliance backup: The full configuration backup saves all settings for the appliance and for all software modules. You can perform a full backup on any appliance. Websense recommends running it on every appliance in your network. (Note that the full backup file may be smaller than the module backup, because it is compressed.)
- Module backup: This saves all configuration information, including client and policy data, stored in the Policy Database. Only the policy source appliance can perform this task.

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.

Data saved by the Backup Utility can be used to import Websense configuration and policy information in the event of a power failure, equipment malfunction, or equipment replacement.

The backup function must be triggered by you; it is not automatic.

Up to 5 appliance backup files and 5 module backup files can be stored on the appliance. If you request a sixth backup file, the oldest one is automatically deleted when the new one is created.

Backup files are stored on the appliance in an internal directory. This directory cannot be moved or renamed.

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. This 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.

Backing up the full appliance configuration (full backup)

This backs up all settings for the appliance and for all Websense software modules on the appliance. Although 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.

Note

If you have system components that are installed off the appliance— such as reporting or Log Server machines— Websense recommends you perform backup on all components and appliances at approximately the same time. Then when you restore the system, restore from a time-compatible set of backups on all machines.

Appliance backup files include:

- All configuration files for the appliance on which the backup is run, including configuration files for the Appliance Manager
- All configuration settings for Websense Web Security, captured by the Websense Backup Utility, **wsbackup**. This includes:
  - Global configuration information
  - Local configuration information, such as Filtering Service and Log Server settings, stored by each Policy Server
  - Websense component initialization and configuration files: .**ini** files, .**cfg** files, and **config.xml**
  - The Policy Database and settings in **policy.xml** if run on the *policy source* appliance

Performing a full backup:

1. From the chosen appliance, select **Administration** > **Backup Utility**.
2. Select the Backup tab.
3. Select **Full Appliance Configuration**.
4. Click **Perform Backup**.
5. The backup file for this operation is added to the table on the bottom portion of the page. The table lists:
   - The date and time of the backup.
   - The name of 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.
   - The host name of the backup source, so you can see which appliance generated the backup file.
   - 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.
6. To download the file to another location on your network, left-click the file name, select **Save**, and browse to the new file location.
7. To delete the backup file, click on the checkbox to the left of the file to select it, and click **Delete**.

Backing up modules (policy backup)

This saves all configuration information, including client and policy data, stored in the Policy Database. Only the *policy source* appliance can perform this task.

1. From your *policy source* appliance, select **Administration > Backup Utility**.
2. Select the Backup tab.
3. Select **Websense Web Security**.
4. Click **Perform Backup**.
5. When the backup process is completed, the backup file description is added to the Websense Web Security Configuration Backup pane, at the bottom of the page. The table lists:
   - Date and time of the backup.
   - File name of the backup file. Click the file name to view the contents.
6. To download the file to another location on your network, left-click the file name, select **Save**, and browse to the new file location.
7. To delete the backup file, click on the checkbox to the left of the file to select it, and click **Delete**.

Restoring a backup file

When you initiate the restore process, all current settings for the appliance and modules are erased. The backup files stored on the appliance are not affected. The appliance then restarts.

Before starting a Restore process, stop all Websense components that are running off the appliance. For example, stop Log Server, transparent ID agents, and **TRITON - Web Security**.

To revert to an earlier appliance configuration, select **Restore** on the **Administration > Backup Utility** screen.

Restoring a full appliance configuration

When you restore a full configuration, you are, in effect, re-creating the original machine that was backed up. The following requirements must be met:

- The current appliance version, displayed on the **Restore** tab, must match the backup file version. Thus, a version 7.5.4 backup can be restored only to a version 7.5.4 appliance.
- The hardware model of the current appliance must be the same as the model that was backed up. (For example, a backup from a V5000 G2 appliance for Web Security must be used to restore a V5000 G2 appliance for Web Security.)
- The original appliance that was backed up cannot also be running elsewhere in the network. Restoring a full configuration re-creates the original appliance and makes use of unique ID numbers from that appliance.

To restore a full configuration:

1. Stop all Websense components that are running off the appliance. For example, stop Log Server, transparent ID agents, and **TRITON - Web Security**.
2. From any appliance in the network, select **Administration > Backup Utility**.
3. Click the Restore tab.
4. For the Restore mode pane, select **Full Appliance Configuration**.
5. Select a radio button to indicate where the full backup file is stored, on the appliance or elsewhere.
   - **Restore from a backup stored elsewhere.** Browse to and select the backup file you want. Click **Restore Policies** to initiate the upload of the selected backup and verify version compatibility. When the upload is complete, a popup window appears with details of the selected backup file.

     Note

     If you want to restore from a backup stored elsewhere and there are already 5 backup files stored on this appliance, you must delete 1 backup file from the appliance before you can upload the required backup from its location.

   - **Restore from a backup stored on the appliance.** Select a backup from the list. Files that are incompatible with the current version of the appliance display their version number in gray text.
6. When you have selected a valid backup file, click **Restore Full Configuration**. The appliance restarts and is restored to its original configuration.
7. Start the Websense components that are running off the appliance.

Restoring a policy configuration

Restore the policy configuration to an appliance that you plan to use as a *policy source* machine.

1. Before starting a Restore process, stop all Websense components that are running off the appliance. For example, stop Log Server, transparent ID agents, and **TRITON - Web Security**.
2. From your policy source appliance, select **Administration > Backup Utility**.
3. Click the Restore tab.
4. From the Restore mode list, select **Websense Web Security**.
5. Select a radio button to indicate where the Policy Database backup file is stored, on the appliance or elsewhere.

- **Restore from a backup stored elsewhere.** Browse to and select the backup file you want. Click **Restore Policies** to initiate the upload of the selected backup and verify version compatibility. When the upload is complete, a popup window appears with details of the selected backup file.

> **Note**
> If you want to restore from a backup stored elsewhere and there are already 5 backup files stored on this appliance, you must delete 1 backup file from the appliance before you can upload the required backup from its location.

- **Restore from a backup stored on the appliance.** Select a backup from the list. Files that are incompatible with the current version of the appliance display their version number in gray text.

6. When you have selected a valid backup file, click **Restore Policies**. The Policy Database is restored to its previous condition.
7. Start the Websense components that run off the appliance.

Logs

Websense Technical Support may request log files to assist you with troubleshooting. This screen provides access to these log files for viewing and download.

> **Note**
> Network Agent generates a log file only if you have enabled logging in the **TRITON - Web Security** console. 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.

Select the module for which you want to view logs:

- Appliance Controller
- Websense Web Security
- Network Agent

Then select the date range.

- Use the drop-down list to choose the date range.
- Log files are available in weekly increments for up to 5 weeks.

Then select the view option. Select either:

- View last __ lines

  Indicate how many lines of the log you want to see in a pop-up window:

  - last 50 lines
  - last 100 lines
  - last 500 lines
- Download entire log file

Click **Submit** to begin the process of gathering the requested log file.

If you are downloading the entire log file, use the **File Download** dialog box to navigate to the folder where you want to save it.

Toolbox

Use the **Administration** > **Toolbox** screen to set up customized block pages, access basic Linux appliance commands, and assist with troubleshooting.

Web Security Block Pages

The appliance is pre-installed with a set of default Web Security block pages. (A block page is displayed to end users each time a Web request is blocked.)

There are two main types of block pages: standard and security. You can see the appearance and behavior of these block pages by going to testdatabase.websense.com and trying to access sites in categories blocked by your organization's policies.

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

Customizing block pages

You can make a copy of the files used to construct standard and security bock pages and customize them to add your own styles, text, and graphics.

Note

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

To a copy the block page files and start customizing block pages:

1. Select **Custom block page**.

   The first time you choose **Custom block pages**, the default block page files are copied to an editable directory on the appliance and then listed on the Appliance Manager screen.

2. Select the files you want to change, and then click **Download File(s)**.
   - When you select a single file, its details are displayed, including its default use, last modification date, and size.
   - If you select more than one file to download, the files are packaged into a single ZIP file.

3. Make modifications locally.

   Important

   Do **not** change the default file names.

   - To replace the Websense logo with another image, see *Changing the block page logo*.
   - If the information that you want to display in the block message is longer than the space provided, see *Changing the size of the message frame*.
   - If you want to start again from the original, default set of block page files, see *Starting over*.
   - Additional information about customizing block pages can be found in the *Block Pages* topic of the TRITON - Web Security Help.

4. Click **Upload File(s)** to place the modified files and any supporting graphics files on the appliance.
   - The edited files can refer to custom graphics files (like logos). If you use custom graphics, be sure to upload these additional graphics files to the editable directory.
   - If you have more than 5 files to upload, select the first 5 files to be uploaded, and then click **Add More Files**. You can upload a maximum of 10 files at a time.

5. Click **Apply Changes**. This restarts Filtering Service.
6. To test the customized block pages, go to testdatabase.websense.com and try to access various Web sites that you know your policies do not permit users to access.
7. Return to Step 2 if adjustments are needed.

Changing the block page logo

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

1. Download the **master.html** file to a temporary directory.
2. Locate an image file for your organization's logo, and copy it 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 the image name for your organization's logo:

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

   - Replace the value of the **title** parameter to reflect name of your organization.
   - Change the path to indicate that your image file is located in the **Custom** folder (not in the Images folder).
   - Replace **wslogo_block_page.png** with the name of the image file containing your organization's logo.

     The result will look something like this:

     <img title="ABC_Corporation" src="/en/Custom/myimage.png" ...>
     NOTE: The parameter and folder names are case-sensitive.
4. Save and close the file.
5. Upload both the image file (containing your logo) and the edited copy of **master.html** to your appliance, and then click **Apply Changes**.

Changing the size of the message frame

Depending on what information you want to provide in the block message, the default width of the block message and height of the top frame may not be appropriate. To change these size parameters:

1. Download the **master.html** file.
2. Open the file in a text editor, such as Notepad or vi (not an HTML editor).
3. To change the width of the message frame, edit the following line:

   ```
   <div style="border: 1px solid #285EA6;width: 600px...">
   ```

   Change the value of the **width** parameter as required.
4. To cause the top frame of the message to scroll, in order to show additional information, edit the following line:

   ```
   <iframe src="$*WS_BLOCKMESSAGE_PAGE*$*WS_SESSIONID*$" ...
      scrolling="no" style="width:100%; height: 6em;">
   ```

   Change the value of the **scrolling** parameter to **auto** to display a scroll bar when message text exceeds the height of the frame.

   You can also change the value of the **height** parameter to change the frame height.
5. Save and close the file.
6. Upload the file to the appliance, and click **Apply Changes**.

Starting over

If you need to start over with a default block page file at any time, click the **default files** link under the Upload and Download buttons. This allows you to download a copy of the default block page files to your local machine.

Edit the files you want to change, and then upload the edited files to the appliance.

Command-line utility

Use the CLI utility to run basic Linux appliance commands for network troubleshooting and debugging. Results are displayed on screen. You can download the output file for the most recent command displayed.

Click **Launch Utility** to open the command-line 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 Web Security
- Network Agent

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

Command	Description	Parameters
ethtool	Displays the current ethernet card settings of the specified network interface (NIC) device. This includes: • Supported ports • Supported link modes • Auto-negotiation support • Advertised link modes • Advertised auto-negotiation • Speed • Duplex • Port • PHYAD • Transceiver • Auto-negotiation setting • Wake-on support • Wake-on status • Link detection Use **ethtool** to verify local network connectivity. For example, if the ping command fails, use this to determine if you are using the right IP address.	No input is required.
ethtool -k	Displays offload parameters, including checksum, for the selected network interface (NIC) device. This can be used to investigate a variety of problems. For example, if your NIC settings are right, but you are having duplex issues, you know you need to change your duplex settings. **-k** Change the checksumming parameters of the specified ethernet device.	No input is required.
ifconfig	Use to troubleshoot network interface issues. Helps you identify IP issues and check subnets and network interfaces. Displays status information about the specified NIC, including but not limited to: • IP and broadcast address • Subnet mask • Number of packets received and transmitted • Number of bytes received and transmitted	[Interface]: Enter the NIC for which you want settings. Click the information icon for valid NIC values. Enter ‘all’ to display all interface status. Example: eth0 or eth1

Command	Description	Parameters
nc -uvz	Attempts to read and write data across a network using user datagram protocol (UDP) to the specified server. Use it for functional tests of components and verification of connectivity. Use it to check data going across a UDP network. If you are having problems loading a Web page, or are getting a block, this command can help determine the problem. **-u** Run netcat in UDP mode **-v** Run netcat in verbose mode.	[Destination]: Enter the IP address of the server with which you want to communicate. [Port]: Enter the port number of that server.
nc -vz	The netcat (nc) utility. Attempts to read and write data across a network using transmission control protocol (TCP) to the specified server. Use it for functional tests of components and verification of connectivity. **-v** Run netcat in verbose mode.	[Destination]: Enter the IP address of the server with which you want to communicate. [Port]: Enter the port number of that server.
netstat -neatup	Displays a list of open sockets on the selected module, appended with the process column. **-n** Displays active TCP connections. However, addresses and port numbers are expressed numerically, and no attempt is made to determine names. **-e** Displays ethernet statistics, such as the number of bytes and packets sent and received. **-a** Displays all active TCP connections and the TCP and UDP ports on which the computer is listening. **-t** Indicates which open ports are using TCP. **-u** Indicates which open ports are using UDP. **-p** Limits display of statistics or state of all sockets to those applicable to protocol.	No input is required.

Command	Description	Parameters
netstat -ng	Displays multicast group membership information about the selected module. **-n** Displays active TCP connections. However, addresses and port numbers are expressed numerically, and no attempt is made to determine names. **-g** Shows the multicast group memberships for all interfaces.	No input is required.
netstat - nItup	Use one of the netstat commands if you are having network connection and routing issues. **netstat -nItup** displays the following: • The amount of traffic in your network. • All active TCP connections and the TCP and UDP ports on which the computer is listening. Addresses and port numbers are expressed numerically, and no attempt is made to determine names. • Ethernet statistics, such as the number of bytes and packets sent and received. **-n** Displays active TCP connections and the ports they use when they connect. (This is useful if, for example, Filtering Service is not filtering. You can look at the connection the module is using here. If it is not the IP and port of the Filtering Service machine, you have found the source of the problem.) **-I** Shows the state of a particular interface, such as eth0 or eth1. **-t** Indicates which open ports are using TCP. **-u** Indicates which open ports are using UDP. **-p** Limits display of statistics or state of all sockets to those applicable to protocol.	No input is required.

Command	Description	Parameters
netstat -s	Displays summary statistics for each protocol on the selected module. By default, statistics are shown for the IP, ICMP, TCP, UDP, and TCPEXT protocols. This includes such things as: • IP - the number of packets received, forwarded, and discarded for each protocol. • ICPM - the number of messages received, failed, sent. • TCP - the number of active and passive connection openings and failed connection attempts. • UDP - the number of packets received and set. • TCPEXT - statistics about SYN cookies, ACKs, packets received and queued, retransmits, and DSACKs. This is just a sampling. Many more statistics are shown.	No input is required.
nslookup	Use this for DNS resolution problems. For example, if a particular Web site is not loading, perform an nslookup on it to view its IP address. **nslookup** lets you query DNS servers to find DNS details, including IP addresses of a particular computer, MX records for a domain, and the DNS servers of a domain.	[Host]: Enter the hostname (for example myintranet.com) or IP address of the host for which you want DNS information. [DNS server]: Enter the hostname or IP address of the DNS server for the appliance.
ping	Checks that a hostname or IP address exists, can accept requests from the selected module, and that DNS is resolving. Use this to test connectivity to another host— for example, the Data Security Management Server or TRITON - Web Security machine—and determine response time.	[Destination]: Enter the hostname (for example myintranet.com) or IP address of the host you want to test.
ping -I	Checks that a network interface can communicate with a hostname or IP address and that DNS is resolving. Use this to test connectivity to another host— for example, the Data Security Management Server or TRITON - Web Security machine—from one of the appliance NICs.	[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 IP address of the host you want to test.
route -n	Display the current contents of the selected module's kernel IP routing table in numeric format. This is useful in complex network environments to show if the environment is set up properly.	No input is required.

Command	Description	Parameters

tcpdump	Use for any Web traffic issues to get packet captures—for example, if a site will not load or if you are having authentication problems.
	tcpdump intercepts and displays packets being transmitted or received by the specified network interface. Use the Expression field to select which packets are displayed.
	The output from **tcpdump** can help you determine whether all routing is occurring properly, to and from the interface. The output is verbose; it displays the data of each package in both hex and ASCII; and it includes a link-level header on each line,
	Note: If you do not stop the tcpdump command manually, 10,000 packets are captured, the maximum allowed.
		[Interface]: Enter the name of the NIC you are debugging. Click the information icon for valid NIC values.
		Example: eth0
		[Expression]: Enter a boolean expression that filters the packets to those of interest. Click the information icon for examples.
		Example 1: To capture all TCP traffic to the site google.com, enter this expression:
		`tcp and dst host google.com`
		Example 2: To capture all TCP traffic from a specific end-user machine, enter this expression:
		`tcp and src host user.websense.com`
		Note: You can enter a hostname if it is resolvable by a DNS server, but the output uses IP addresses either way.

tcpdump -w	Use this to dump traffic (raw packets) from the specified NIC to a file. To download the file, click the link, **Download output file for last command**, after running the command. This link is under the console output window. Websense Technical Support may request this file on occasion.	[Interface]: Enter the name of the appliance NIC you are debugging. Click the information icon for valid NIC values. [Expression]: Enter a boolean expression that filters the packets to those of interest. Click the information icon for examples. Enter ‘all’ to dcapture all packets. **Note:** You can enter a host name if it is resolvable by a DNS server, but the output uses IP addresses either way.
top -bn1	Displays all operating system tasks that are currently running on the selected module. Use this to help troubleshoot CPU and memory issues. **-b** Run in batch mode. **-n** Update the display for a number of iterations, then exit. **-1** Do not display idle processes.	No input is required.

Command	Description	Parameters
traceroute	Use this to determine the route taken by packets across a network to a particular host. If some machines are not getting filtered or blocked, or if traffic is not even getting to the appliance, this shows the devices (or hops) that are between the machines that may be blocking access to the host. Use **tcpdump** to get a packet capture from each device. If you are having latency issues, **traceroute** can also help identify the causes. (Note that **traceroute** is of limited utility if an IP is being spoofed.)	[Destination]: Enter the hostname or IP address of the host destination you are investigating
triton-websecurity-services (Websense Web Security module)	Use this to manage TRITON - Web Security operation on this appliance:	status, start, stop, restart.
wget	Use to initiate a non-interactive download of files from the Web, so you can diagnose connectivity issues. This command supports HTTP, HTTPS, and FTP protocols.	[URL]: Enter the URL of the Web site from which you want to download files.

Technical Support tools

When you collaborate with Websense Technical Support or a Websense partner to examine possible causes for network issues, these built-in tools can assist with troubleshooting:

- *Troubleshooting ports*
- *Appliance Configuration summary*
- *Remote access*

Troubleshooting ports

Websense Web Security provides the option to open troubleshooting ports temporarily, so that various troubleshooting tests can be run. Use this tool only when directed to do so by Websense Technical Support.

Check **Enable troubleshooting ports**, and then click **Save** to cause the special ports to be enabled.

Important

Be sure to **clear** the check box and click **Save** to disable the ports when Technical Support is done using them. Do not leave these ports open and unattended.

Appliance Configuration summary

The configuration summary tool gathers data from the appliance and generates an archive file that can be sent to Websense Technical Support for analysis and debugging. The process takes about 5 minutes.

When Websense Technical Support requests this file:

- Click **Generate File**.
- When the file is ready, a message appears at the top of the screen: Configuration summary has been successfully collected. Click the link in the message to download the archive file to your desktop.
- You can then open the file or save it.
- Your technician will provide an FTP site for secure file transfer to Websense Technical Support.

Remote access

Enable remote access only at the request of Websense Technical Support.

- When you check **Enable Remote Access** and then click **Save**, a passcode is generated and displayed on screen.
- Provide the passcode to your Websense Technical Support technician. This enables SSH, so that the technician can log on to your appliance.
- Each time you allow remote access to the appliance and a Websense technician logs on, a record is added to the **Remote access login history** at the bottom of the **Toolbox** screen.
- When the technician is done, be sure to click **Disable remote access** and click **Save** to disable the access.

Account management

Use the **Administration** > **Account Management** page to change the password for Appliance Manager or to reset the password for **TRITON - Web Security**.

- *Change password for Appliance Manager*
- *TRITON - Web Security password reset*

Change password for Appliance Manager

1. Enter the current password.
2. Enter the new password.
3. Confirm the new password.

Save applies and saves new values in the pane.

Cancel discards all changes entered since the last **Save** and restores entry fields in the pane to the last saved values.

TRITON - Web Security password reset

1. Log on to your MyWebsense account.
2. On the page **My Products and Subscriptions**, locate the V5000 G2 Appliance for Web Security and open the drop-down window for that product.
3. Select **reset password**.
4. Copy and paste the subscription key shown on the appliance screen into the text box on the MyWebsense screen.
5. Check the box: **I have a V-Series console**
6. Click **Reset**.
7. Copy the security string displayed on MyWebsense.
8. Return to Appliance Manager and paste the encrypted security string into the text box (Enter security string).
9. Click **Submit** to reset your **TRITON - Web Security** password.
10. The new password appears at the bottom of the frame. Write it down.
11. Use this password to log on to **TRITON - Web Security** and change your password.
12. As soon as you navigate away from the **Account Management** screen in Appliance Manager, your reset password is no longer displayed.