Getting Started

Websense® V-Series Appliance
(V10000 G2, V5000 G2, V10000)

v7.6.x

Published 2011 Revision E
Printed in the United States of America and Ireland

Trademarks

WinPcap

Contents

1 Introducing Websense V-Series Appliances

The Websense V-Series appliance is a high-performance security gateway appliance with a hardened operating system, optimized for analyzing Web and email traffic and content.

The appliance offers:

- A command-line interface for initial appliance settings, available through a USB keyboard and monitor or a serial port connection, providing basic appliance control commands
- Appliance Manager, a Web-based configuration interface that provides management features:
  - System dashboard, with up-to-the-minute status of the software modules and system resources on the appliance
  - Appliance configuration and network settings
  - System administration tools for patch management, troubleshooting, and backup and restore
- Full customization of proxy caching, Web filtering, and email filtering, available through Web-based configuration interfaces
- Event logging for appliance configuration and patching. Log entries can be viewed in Appliance Manager, and log files can be downloaded for later viewing.
- Integrated proxy caching and Web filtering after minimal initial configuration (Web security mode-enabled appliance)
- Configurable links to hybrid Web filtering and off-appliance Data Security features (Web security mode-enabled appliance)
- Robust antivirus and antispam scanning and filtering of email (email security mode-enabled appliance)
- Personal Email Manager facility allowing end users to manage quarantined messages and individual permit/block lists (email security mode-enabled appliance)

Security Modes

Websense V-Series appliances can run in the following security modes. Some modes are not supported by all appliance models.

Security Mode	Provides	Appliance Models
Web and Email Security	Both Web Security Gateway and Email Security Gateway features	V10000 G2 only
Web Security only	Web Security Gateway features	• V10000 • V10000 G2 • V5000 G2
Email Security only	Email Security Gateway features	• V10000 G2 • V5000 G2

The security mode of an appliance is chosen during initial *firstboot* configuration. See *Perform initial command-line configuration*, page 16 for more information about *firstboot*.

Choosing a security mode in *firstboot* does not automatically enable the associated features. The features become fully enabled only upon entry of a valid subscription key in the TRITON Unified Security Center. See *TRITON Unified Security Center*, page 10 for more information.

Once firstboot has been completed, if you want to change the security mode of an appliance you must restore it to its factory image. Then, during firstboot after re-imaging, you can select a different security mode. See *Restoring to Factory Image*, page 38.

It is always a best practice to perform a full backup of the appliance and of each module of the TRITON Unified Security Center prior to restoring to factory image. However, the backups can only be restored in particular situations if you are changing the security mode of an appliance.

If changing from *Web Security only* to *Email Security only* (and vice versa), backed up settings are not compatible with the new security mode and so cannot be restored.

If you are changing from *Web Security only* to *Web and Email Security* mode, you can perform a backup prior to restoring to factory image. Once the security mode has been changed, restore the backup so the appliance reflects the Web Security settings you had in place before.

Software provided on the appliance

Web Security

On an appliance running in *Web Security only* or *Web and Email Security* mode, the following core Web security components are pre-loaded for your convenience:

- Policy Database
- Policy Broker
- Policy Server
- Filtering Service
- User Service
- Usage Monitor
- Control Service
- Directory Agent
- TRITON Unified Security Center (*Web Security only* mode only), includes
  - Central Access
  - Unified Security Center
  - Settings Database
  - Investigative Reports Scheduler
  - Manager Web Server
  - Reporting Web Server
  - Reports Information Service

- Websense Content Gateway
- Network Agent (optional)

On a *Web Security only* appliance, TRITON Unified Security Center is installed on the appliance by default, but it is optional. It is important to note that TRITON Unified Security Center can run on the appliance only if the appliance runs in *full policy source* mode. Also, in production environments, it is a best practice to run TRITON Unified Security Center off-appliance on a separate Windows machine. See the Websense Appliance Manager Help for more information.

If your organization generates a high volume of reports, or a lower volume of very large reports, hosting TRITON - Web Security on the appliance can affect the performance of other appliance modules.

Important

If running on an appliance, TRITON Unified Security Center can have only its Web Security module enabled. If you want to use more than the Web Security module of the TRITON Unified Security Center—for example, TRITON - Web Security and TRITON - Data Security both—then TRITON Unified Security Center must be installed off-appliance on a Windows Server 2008 R2 machine.

Email Security

On an appliance running in *Email Security only* or *Web and Email Security* mode, the appliance contains the majority of email security features, including the following services:

- Configuration Service
- Authentication Service
- Quarantine Service
- Log Service
- Update Service
- Filtering Service
- Mail Transfer Agent

Only management (via the TRITON Unified Security Center), and logging (via Email Security Log Server) are performed by off-appliance components.

Software that runs off-appliance

The Websense components mentioned in this section must be installed off-appliance. Additionally, Microsoft SQL Server must be installed off-appliance.

Use the Websense Installer to install any of the components mentioned here. See the Websense Technical Library (www.websense.com/library) for more information about components and installation instructions.

Web Security

The following Websense Web Security components never run on the appliance. Some are Windows-only components.

- Web Security Log Server
- Real-Time Monitor
- Sync Service (for sites using hybrid Web security)
- Linking Service (for sites using any integrated Data Security features)
- Transparent identification agents (to apply user, group, or domain [OU] policies without prompting users for credentials)
  - DC Agent
  - Logon Agent
  - eDirectory Agent
  - RADIUS Agent

Note

If your subscription includes Websense Web Security Gateway Anywhere, TRITON Unified Security Center must run off-appliance, on a Windows Server 2008 R2 machine. This is due to the fact that both TRITON - Web Security and TRITON - Data Security are required. TRITON Unified Security Center, when on-appliance, can run TRITON - Web Security only.

Data Security

The following Websense Data Security components run off-appliance.

- TRITON - Data Security
- Protector
- SMTP agent
- Microsoft ISA/TMG agent
- Endpoint agent
- Printer agent
- The crawler
- Integration agent

Email Security

The following Websense Email Security Gateway components never run on the appliance. They are Windows-only components.

- TRITON - Email Security (i.e., the Email Security module of the TRITON Unified Security Center; see *TRITON Unified Security Center*, page 10)
- TRITON - Data Security (i.e., the Data Security module of the TRITON Unified Security Center; see *TRITON Unified Security Center*, page 10). The Data Security module is required for email DLP (data loss prevention) features.
- Email Security Log Server

TRITON Unified Security Center

The TRITON Unified Security Center is the Web-browser-based, graphical management application for your entire deployment. It consists of three modules: TRITON - Web Security, TRITON - Data Security, and TRITON - Email Security. Each module is used to configure and manage their respective product features.

Depending on your subscription, not all of these modules may be enabled.

To enable more than one module of the TRITON Unified Security Center—for example, both Web Security and Data Security—TRITON Unified Security Center must be installed on a Windows Server 2008 R2 machine. When TRITON Unified Security Center is installed on a separate machine, it must be able to reach the appliance's C interface (and E1 interface, if the appliance is in *Email Security only* or *Web and Email Security* modes).

For more information about the TRITON Unified Security Center and its modules, see the Websense Technical Library (www.websense.com/library).

TRITON Infrastructure

TRITON Infrastructure is comprised of common user interface, logging, and reporting components required by the TRITON modules.

TRITON Infrastructure also (optionally) includes SQL Server 2008 R2 Express that may be used for Websense logging data. It is important to note that, as a best practice, SQL Server 2008 R2 Express should be used only in non-production or evaluation environments. "Full" SQL Server should be used in production environments.

TRITON Infrastructure services include:

- Websense TRITON Unified Security Center
- Websense TRITON Central Access
- Websense TRITON Settings Database
- Websense TRITON Reporting Database (if using SQL Server 2008 R2 Express)

TRITON - Web Security

TRITON - Web Security is used to perform general configuration tasks, set up filtering policies, assign policies to users and groups, run reports, and other management tasks.

TRITON - Web Security services include:

- Websense TRITON - Web Security (formerly ApacheTomcatWebsense)
- Websense Web Reporting Tools (formerly Apache2Websense)
- Investigative Reports Scheduler
- Reports Information Service
- Websense RTM Client (if Real-Time Monitor is used)
- Websense RTM Database (if Real-Time Monitor is used)
- Websense RTM Server (if Real-Time Monitor is used)

On a *Web Security only* mode appliance, TRITON Unified Security Center with Web Security module only (i.e., TRITON - Web Security) is pre-installed as a convenience for evaluations and small installations. On a *Web and Email Security* mode appliance, this component is not installed on the appliance.

Note

The above service names are for an off-appliance installation of TRITON - Web Security. When on-appliance, Websense TRITON - Web Security is named *Manager Web Server*, and Websense Web Reporting Tools is named *Reporting Web Server.*

TRITON - Data Security

TRITON - Data Security consolidates all aspects of Websense Data Security setup and configuration, incident management, system status reports, and role-based administration.

TRITON - Data Security services include:

- Websense Data Security Management Server
- Websense TRITON - Data Security
- Websense Data Policy Engine
- Websense Data Fingerprint Database
- Websense Data Discovery and Fingerprint Crawler
- Websense PreciseID and Data Endpoint Server

TRITON - Email Security

TRITON - Email Security is used to configure and manage general system properties, administrator roles, user directories, email filtering, email policies, and Personal Email Manager end-user facility options. It is also used to generate and view email activity reports.

TRITON - Email Security consists of one service:

- Websense TRITON - Email Security

Database management software

Websense Web Security and Email Security require Microsoft SQL Server to host their reporting database, called the Log Database. Both the Web Security Log Database and the Email Security Database can be hosted by the same database engine instance. Information stored in the Log Database is used to create Web Security and Email Security reports.

Prior to installing Web Security Log Server or Email Security Log Server, SQL Server 2005 or 2008 must be installed and running on a machine in your network. See the Websense Technical Library (www.websense.com/library) for important detailed information about supported versions of SQL Server. Note that SQL Server must be obtained separately; it is not included with your Websense subscription. Refer to Microsoft documentation for installation and configuration instructions.

If you do not have SQL Server, you can use the Websense Installer to install SQL Server 2008 R2 Express. SQL Server 2008 R2 Express can be installed either on the same machine as TRITON Unified Security Center or on a separate machine. See the Websense Technical Library (www.websense.com/library) for installation instructions.

Note

It is a best practice to use “full” SQL Server in production environments. SQL Server 2008 R2 Express is most appropriate for non-production or evaluation environments.

2 Setting Up Websense V-Series Appliances

Setting up a Websense V-Series appliance involves the following tasks.

1. *Set up the appliance hardware*, page 13
2. *Perform initial command-line configuration*, page 16
3. *Configure the appliance*, page 18
4. *Install off-appliance or optional components*, page 37

Additional initial configuration steps may be necessary for your particular deployment. See deployment and installation information in the Websense Technical Library (www.websense.com/library) for more information.

Set up the appliance hardware

The Quick Start poster, which comes in the shipping box, shows you all items included in each Websense appliance shipping box. The 2-page Quick Start explains how to set up the hardware and shows how to connect cables to the appliance and to your network.

Read the section below that applies to your Websense appliance model.

V10000

Network interface C and the proxy interface (typically P1) must be able to access a DNS server. Both interfaces typically have continuous access to the Internet. Essential databases are downloaded from Websense servers through these interfaces.

- Ensure that interfaces C and P1 are able to access the download servers at **download.websense.com**. (As an alternative, some sites configure the P1 proxy interface to download the Websense Master Database as well as other security updates. In that situation, interface C does not require Internet access.)
- Make sure the above address is permitted by all firewalls, proxy servers, routers, or host files controlling the URLs that the C and P1 interfaces can access.

V10000 G2

The appliance's network interfaces must be able to access DNS and the Internet as described below. This information varies slightly depending on the security mode of the appliance.

Web Security only mode

Network interface C and the proxy interface (typically P1) must be able to access a DNS server. Both interfaces typically have continuous access to the Internet. Essential databases are downloaded from Websense servers through these interfaces.

- Ensure that interfaces C and P1 are able to access the download servers at **download.websense.com**. (As an alternative, some sites configure the P1 proxy interface to download the Websense Master Database as well as other security updates. In that situation, interface C does not require Internet access.)
- Make sure the above address is permitted by all firewalls, proxy servers, routers, or host files controlling the URLs that the C and P1 interfaces can access.

Email Security only mode

Network interfaces C, E1, and E2 (if used) must be able to access a DNS server. These interfaces typically have continuous access to the Internet once the appliance is operational. Essential databases are downloaded from Websense servers through these interfaces.

- Ensure that C, and E1 or E2 (if used), are able to access the download servers at **download.websense.com**.
- Make sure the above address is permitted by all firewalls, proxy servers, routers, or host files controlling the URLs that the C, E1, and E2 interfaces can access.

Web and Email Security mode

Network interfaces C, P1, E1, and E2 (if used) must be able to access a DNS server. These interfaces typically have continuous access to the Internet. Essential databases are downloaded from Websense servers through these interfaces.

- Ensure that interfaces C, P1, E1, and E2 (if used) are able to access the download servers at **download.websense.com**. (As an alternative, some sites configure the P1 proxy interface to download the Websense Master Database as well as other security updates. In that situation, interface C does not require Internet access.)
- Make sure the above address is permitted by all firewalls, proxy servers, routers, or host files controlling the URLs that the C, P1, E1, and E2 (if used) interfaces can access.

V5000 G2

The appliance's network interfaces must be able to access DNS and the Internet as described below. This information varies slightly depending on the security mode of the appliance.

Web Security only mode

Network interface C and the proxy interface (typically P1) must be able to access a DNS server. Both interfaces typically have continuous access to the Internet. Essential databases are downloaded from Websense servers through these interfaces.

- Ensure that interfaces C and P1 are able to access the download servers at **download.websense.com**. (As an alternative, some sites configure the P1 proxy interface to download the Websense Master Database as well as other security updates. In that situation, interface C does not require Internet access.)
- Make sure the above address is permitted by all firewalls, proxy servers, routers, or host files controlling the URLs that the C and P1 interfaces can access.

Email Security only mode

Interface C, P1, and P2 (if used) must be able to access a DNS server. These interfaces typically have continuous access to the Internet once the appliance is operational. Essential databases are downloaded from Websense servers through these interfaces.

- Ensure that C, and P1 or P2 (if used), are able to access the download servers at **download.websense.com**.
- Make sure the above address is permitted by all firewalls, proxy servers, routers, or host files controlling the URLs that the C, P1, and P2 interfaces can access.

All Models

After hardware setup, connect directly to the appliance through the serial port or the monitor and keyboard ports. For serial port activation, use:

- 9600 bits per second
- 8 data bits
- no parity

The activation script, called firstboot, runs when you start the appliance.

See *Perform initial command-line configuration* below.

Perform initial command-line configuration

The first time you start a Websense appliance, a brief script (firstboot) prompts you to supply settings for the network interface labeled C and a few other general items. You can run the script again if you want to examine your settings or change settings. You can also change settings through the Appliance Manager (user interface) after firstboot has been executed.

Gather the following information before running the script. Some of this information may have been written down on the Quick Start during hardware setup.

Hostname	
IP address for network interface C	
Subnet mask for network interface C	
Default gateway for network interface C (IP address) *Optional* NOTE: If you do not provide access to the Internet for interface C, configure: • P1 or P2 to download Master URL database updates from Websense (Web Security mode) • E1 or P1* to download antispam and antivirus database updates from Websense (Email Security mode) Configuring these interfaces to access the Internet for database downloads is done through the Appliance Manager and through the TRITON Unified Security Center. See the Appliance Manager Help for information about configuring the interfaces. See the TRTION - Web Security and - Email Security Help for information about configuring database downloads. * On a V5000 G2, use P1, there is no E1 interface.	
Primary DNS server for network interface C (IP address)	
Secondary DNS server for network interface C (IP address) *Optional*	

Tertiary DNS server for network interface C (IP address) *Optional*	
Unified password (8 to 15 characters, at least 1 letter and 1 number) This password is for the following, depending on the security mode of the appliance: *Web Security only* • Appliance Manager • TRITON - Web Security • Content Gateway Manager *Email Security only* • Appliance Manager *Web and Email Security* • Appliance Manager • Content Gateway Manager	

When you have gathered the necessary information, run the initial command-line configuration script (firstboot) as follows.

1. Access the appliance through a USB keyboard and monitor, or a serial port connection.

   Note

   To configure the appliance, connect through the serial port or the keyboard/video ports and complete the firstboot script. For serial port activation, use:

   - 9600 bits per second
   - 8 data bits
   - no parity

2. Accept the subscription agreement when prompted.
3. When asked if you want to begin, enter **yes** to launch the firstboot activation script.

   NOTE: To rerun the script manually, enter the following command:

   ```
   firstboot
   ```

4. At the first prompt, select a security mode:
   - **Web and Email Security**: provides both Web Security Gateway and Email Security Gateway features. Only the Websense V10000 G2 can run in this mode.
   - **Web Security only**: provides Web Security Gateway features. The Websense V10000, V10000 G2, and V5000 G2 can run in this mode.

- **Email Security only**: provides Email Security Gateway features. The Websense V10000 G2 and V5000 G2 can run in this mode.

On a V10000, you are not asked to choose a security mode. The V10000 can run only in *Web Security only* mode.

5. Follow the on-screen instructions to provide the information collected above.

After the activation script has been completed successfully, use the **Logon Portal** to access the Appliance Manager. To reach the **Logon Portal**, open a supported browser, and enter this URL in the address bar:

```
http://<IP address>
```

Replace <IP address> with the address assigned to network interface C during initial configuration of the appliance.

> **Note**
> On an *Email Security only* mode appliance, there is no Logon Portal. The above URL takes you directly to the Appliance Manager.

For information about supported browsers, see the Websense Technical Library (www.websense.com/library).

Configure the appliance

The Appliance Manager is the Web-based configuration interface for the appliance. Through it you can view system status, configure network and communication settings, and perform general appliance administration tasks.

After completing the initial configuration required by the firstboot script, use the Appliance Manager to configure important settings for network interfaces P1, P2, N, E1, and E2 (P2, N, and E2 are optional). Note that on a V5000 G2, there are no E1 and E2 interfaces.

Gather information as described in the following sections before running the Appliance Manager. Some of this information may have been written on the Quick Start during hardware setup. Complete only the section that applies to your appliance model and security mode:

- *V10000 G2 (Web and Email Security mode)*, page 19
- *V10000 G2, V10000, V5000 G2 (Web Security only mode)*, page 24
- *V10000 G2 (Email Security only mode)*, page 31
- *V5000 G2 (Email Security only mode)*, page 35

V10000 G2 (*Web and Email Security* mode)

After completing the initial configuration required by the firstboot script, use the Appliance Manager to configure important settings for network interfaces P1, P2, N, E1, and E2 (P2, N, and E2 are optional).

While the E1/E2 and P1/P2 interfaces can be bonded to each other if the V10000 G2 runs in either *Web Security only* or *Email Security only* modes, they cannot be bonded when the appliance is in *Web and Email Security* mode.

If you use the P2 interface, the P1 interface is bound to eth0, and the P2 interface is bound to eth1. Keep this in mind when you configure Websense Content Gateway. For example, suppose you are using a transparent proxy deployment, and the P1 interface is connected to a WCCP router. In this case, you must configure Websense Content Gateway to use eth0 for WCCP communications (in Content Gateway Manager, see **Configure** > **Networking** > **WCCP**, **General** tab).

Primary NTP server *Optional* Be sure that interface C can access the NTP server. If interface C does not have Internet access, you can install an NTP server locally on a subnet that can be accessed by interface C.	Domain:
Secondary NTP server *Optional*	Domain:
Tertiary NTP server *Optional*	Domain:
IP address for network interface P1	IP address:
Subnet mask for network interface P1	Subnet mask:
Default gateway for network interface P1and P2 (if used) If you use both P1 and P2, the default gateway is automatically assigned to P2 (which is bound to eth1). To ensure that outbound packets can reach the Internet, do not locate the IP addresses of P1 and P2 in the same subnet.	IP address:
Primary DNS server for network interface P1 and P2 (if used)	IP address:
Secondary DNS server for network interface P1 and P2 (if used) *Optional*	IP address:
Tertiary DNS server for network interface P1 and P2 (if used) *Optional*	IP address:
IP address for network interface P2 *Required only if P2 is enabled*	IP address:

Subnet mask for network interface P2 *Required only if P2 is enabled*	Subnet mask:
Choose interface for transporting blocking information for non-HTTP and non-HTTPS traffic	Choose (C or N):
If interface N transports blocking information, N must be connected to a bidirectional span port	Verify interface N setup.
IP address for network interface N	IP address:
Subnet mask for network interface N	Subnet mask:
Default gateway for network interface N *Required only if network interface N carries blocking information*	IP address:
Primary DNS server for network interface N	IP address:
Secondary DNS server for network interface N *Optional*	IP address:
Tertiary DNS server for network interface N *Optional*	IP address:
IP address for network interface E1	IP address:
Subnet mask for network interface E1	Subnet mask:
Default gateway for network interface E1and E2 (if used). If you use both E1 and E2, the default gateway and DNS configuration are shared by both.	IP address:
Primary DNS server for network interface E1 and E2 (if used)	IP address:
Secondary DNS server for network interface E1 and E2 (if used) *Optional*	IP address:
Tertiary DNS server for network interface E1 and E2 (if used) *Optional*	IP address:

After collecting the information needed, access the Appliance Manager through a supported browser.

Follow these steps to enable default proxy caching, and Web and email filtering. See the Appliance Manager Help for detailed instructions on any field or area, or for information about other available settings.

1. Open a supported browser, and enter the following URL in the address bar:

   ```
   https://<IP address>:9447/appmng
   ```

   Replace <IP address> with the address assigned to network interface C during initial configuration of the appliance (see *Perform initial command-line configuration*, page 16).

   For information about supported browsers, see the Websense Technical Library (www.websense.com/library).
2. Log on with the user name **admin** and the password set during initial appliance configuration.
3. In the left navigation pane, click **Configuration** > **System**.
4. Under **Time and Date**:
   a. Set the time zone.
   b. Set the time and date:
      - **Automatically synchronize with an NTP server**: select this option to use a Network Time Protocol server. Specify up to three NTP servers. Use of an NTP server is recommended, to ensure that database downloads and time-based policies are handled precisely.
      - **Manually set time and date**: select this option to enter a system time and date yourself.
   c. Click **Save** in the Time and Date area.
5. In the left navigation pane, click **Configuration** > **Network Interfaces**.
6. Under **Websense Content Gateway Interfaces**, configure the P1 and P2 (optional) interfaces.

   The P interfaces are used to accept users' Internet requests (inbound traffic) and communicate with Web servers (outbound traffic).

   To configure the P interfaces:

   a. Select **P1 only** or **P1 and P2**.

      If you choose P1 only, enter configuration information (IP address, subnet mask, default gateway, DNS IP addresses) under **P1**.

      If you choose P1 and P2, enter configuration information under both **P1** and **P2**. Note that default gateway and DNS configuration (under **Shared Setting**) are shared between both P1 and P2.

   b. Click **Save** in the **Websense Content Gateway Interfaces** area when you are done.

Important

When you use the P2 interface, the P1 interface is bound to eth0, and the P2 interface is bound to eth1. Keep this in mind when you configure Websense Content Gateway.

For example, suppose you are using transparent proxy, and the P1 interface is connected to the WCCP router. In this case, you must configure Websense Content Gateway to use eth0 for WCCP communications (in Content Manager, see **Configure** > **Networking** > **WCCP**, **General** tab).

When only P1 is used, it handles both inbound and outbound traffic for the proxy module (i.e., Content Gateway).

Alternatively, you could use both P1 and P2 such that P1 handles inbound traffic and P2 handles outbound traffic. To enable this configuration, be sure to set appropriate routing rules for P1 and P2 on the **Configuration** > **Routing** page. For example, you might set outbound traffic to go through P2.

Additionally, you can use P1 as a communication channel for multiple Content Gateway servers in a cluster. In this scenario, P1 should not be used for outbound traffic. For additional information on clusters, see the Content Gateway Manager Help.

7. Under **Network Agent Interface (N)**, configure the N interface.

   The N interface is used by the Network Agent module. It must be connected to a span (or mirror) port on a switch allowing it to monitor the Internet requests going through the switch. (Note: be sure to configure the switch so the span port is monitoring all the ports carrying the traffic of interest; see your switch manufacturer's documentation for configuration instructions). For non-HTTP/HTTPS protocols, the N interface can also be used to send block information to enforce policy.

   Note

   The appliance does not send block messages to users who are blocked from non-HTTP and non-HTTPS protocols.

   To configure the N interface:

   a. Under **Send blocking information for non-HTTP/HTTPS traffic via**, select whether non-HTTP/HTTPS blocking information is sent via the C or N interface.

   b. Enter IP address, subnet mask, default gateway (only if you select interface N for sending blocking information), and DNS IP addresses for the N interface.

   c. Click **Save** in the **Network Agent Interface (N)** area.

8. Under **Websense Email Security Gateway Interfaces (E1 and E2)**, configure the E1 and E2 (optional) interfaces.

   The E interfaces are used to accept users' requests (inbound traffic) and communicate with the Internet (outbound traffic).

   To configure the E interfaces:

   a. Select whether **E1 only** or both **E1 and E2** are used.

      If you choose E1 only, enter configuration information (IP address, subnet mask, default gateway, DNS IP addresses) under **E1**.

      If you choose E1 and E2, enter configuration information under both **E1** and **E2**. Note that default gateway and DNS configuration (under **Shared Setting**) are shared between both E1 and E2.

   b. Click **Save** in the **Websense Email Security Gateway Interfaces (E1 and E2)** area when you are done.

   When only E1 is used, it handles both inbound and outbound traffic.

   Alternatively, you could use both E1 and E2 such that E1 handles inbound traffic and E2 handles outbound traffic.

   See the Appliance Manager Help for more information about configuring E1 and E2.

9. Configure routes if necessary:

   a. In the left navigation pane, click **Configuration** > **Routing**.

   b. Under Static Routes, use the **Add/Import** button to specify customized, static routes.

   c. Under Module Routes, use the **Add** button to specify non-management Web Security or Email Security traffic through the C interface.

   d. For either static or module routes, use the **Delete** button to remove existing routes, if necessary.

   > **Note**
   > An existing route cannot be edited. If you want to edit a route, delete it and then use the **Add/Import** (static) or **Add** (module) button to specify the route with the changes you want.

   See the Appliance Manager Help for more information about static and module routes.

10. Select the policy mode of this appliance:

    a. In the left navigation pane, click **Configuration** > **Web Security Components**.

b. Specify the role of this appliance with respect to Websense Web Security policy information.

- Choose **Full policy source** if Websense Policy Broker and Policy Database for your deployment will run on the appliance being configured. (Only one appliance in the network runs these two components, as well as the other filtering components.) Policy Server must also be run on the *full policy source* appliance; Policy Server can run in multiple locations.

> **Note**
> If Policy Broker runs on an appliance, only on-appliance instances of Policy Server can communicate with Policy Broker. In this case, Policy Server cannot be installed off-appliance. If Policy Broker is installed off-appliance, however, both on-appliance and off-appliance instances of Policy Server can communicate with it.

- Choose **User directory and filtering** if the appliance currently being configured is *not* the location of the policy information, but will run Policy Server and User Service. Then, enter the **IP address** of the server that is used as the full policy source—a machine running Policy Broker. (If the full policy source is another appliance, enter the IP address of its C network interface.)
- Choose **Filtering only** if the appliance being configured will not run any policy components. (There are some disadvantages to this reduced role, as explained in the Appliance Manager help system.) Then, enter the **IP address** of the server that is used as the policy source—a machine running Policy Server. The policy source can also be another appliance in *full policy source* or *user directory and filtering* mode. In this case, enter the IP address of the appliance's C network interface.

11. Click **Save**.
12. Click **Log Off**, at the top right, when you are ready to log off Appliance Manager.

V10000 G2, V10000, V5000 G2 (*Web Security only* mode)

After completing the initial configuration required by the firstboot script, use the Appliance Manager to configure important settings for network interfaces N and P1 (and optionally P2), which are used for communications by Network Agent and Websense Content Gateway. Appliance models V10000 and V10000 G2 also offer expansion interfaces (E1 and E2) that can be bonded with P1 and P2, respectively, either for load balancing or active/standby.

If you use the P2 interface, the P1 interface is bound to eth0, and the P2 interface is bound to eth1. Keep this in mind when you configure Websense Content Gateway. For example, suppose you are using a transparent proxy deployment, and the P1 interface is connected to a WCCP router. In this case, you must configure Websense Content Gateway to use eth0 for WCCP communications (in Content Gateway Manager, see **Configure** > **Networking** > **WCCP**, **General** tab).

Gather the following information before running the Appliance Manager. Some of this information may have been written on the Quick Start during hardware setup.

Primary NTP server *Optional* Be sure that interface C can access the NTP server. If interface C does not have Internet access, you can install an NTP server locally on a subnet that can be accessed by interface C.	Domain:
Secondary NTP server *Optional*	Domain:
Tertiary NTP server *Optional*	Domain:
IP address for network interface P1	IP address:
Subnet mask for network interface P1	Subnet mask:
Default gateway for network interface P1 and P2 (if used) If both P1 and P2 are used, the default gateway is automatically assigned to whichever interface is in the same subnet with it. If both P1 and P2 are in the same subnet, the default gateway is automatically assigned to P2 (which is bound to eth1).	IP address:
Primary DNS server for network interface P1 and P2 (if used)	IP address:
Secondary DNS server for network interface P1 and P2 (if used) *Optional*	IP address:
Tertiary DNS server for network interface P1 and P2 (if used) *Optional*	IP address:
IP address for network interface P2 *Required only if P2 is enabled*	IP address:
Subnet mask for network interface P2 *Required only if P2 is enabled*	Subnet mask:
Choose interface for transporting blocking information for non-HTTP and non-HTTPS traffic. (interface C or interface N)	Choose one: C or N
If interface N transports blocking information, N must be connected to a bidirectional span port.	Verify interface N setup.
IP address for network interface N	IP address:
Subnet mask for network interface N	Subnet mask:

Default gateway for network interface N *Required only if network interface N carries blocking information*	IP address:
Primary DNS server for network interface N	IP address:
Secondary DNS server for network interface N *Optional*	IP address:
Tertiary DNS server for network interface N *Optional*	IP address:
Bond expansion interface E1 to P1? Yes or No *Optional*	If Yes, choose one: Active/standby or Load balancing
Bond expansion interface E2 to P2? Yes or No *Optional*	If Yes, choose one: Active/standby or Load balancing
Full policy source IP address	This appliance provides (choose one): • Full policy source • User directory and filtering (you must specify the IP address of a machine running Policy Broker, which can be a *full policy source* appliance) • Filtering only (you must specify IP address of a machine running Policy Server, which can be a *full policy source* or *user directory and filtering* appliance).
TRITON Unified Security Center location (user interface for managing Web Security Gateway) TRITON Unified Security Center can run on this appliance or on a separate Windows server. By default it is enabled to run on the appliance. During the setup procedure below you will decide where it should run. Note: Organizations with high traffic volume or large reporting needs are encouraged to install and run TRITON Unified Security Center on a separate Windows server, to optimize performance.See *Creating a TRITON management server*, page 38.	Choose: runs on this appliance or runs on separate server

After collecting the information needed, access the Appliance Manager through a supported browser.

Follow these steps to enable default proxy caching and filtering. See the Appliance Manager Help for detailed instructions on any field or area, or for information about other available settings.

1. Open a supported browser, and enter the following URL in the address bar:

   ```
   https://<IP address>:9447/appmng
   ```

   Replace <IP address> with the address assigned to network interface C during initial configuration of the appliance.

   (See *Perform initial command-line configuration*.)
2. Log on with the user name **admin** and the password set during initial appliance configuration.
3. In the left navigation pane, click **Configuration** > **System**.
4. Under **Time and Date**:
   a. Set the time zone.
   b. Set the time and date:
      - **Automatically synchronize with an NTP server**: select this option to use a Network Time Protocol server. Specify up to three NTP servers. Use of an NTP server is recommended, to ensure that database downloads and time-based policies are handled precisely.
      - **Manually set time and date**: select this option to enter a system time and date yourself.
   c. Click **Save** in the Time and Date area.
5. In the left navigation pane, click **Configuration** > **Network Interfaces**.
6. Under **Websense Content Gateway Interfaces**, configure the P1 and P2 (optional) interfaces.

   The P interfaces are used to accept users' Internet requests (inbound traffic) and communicate with Web servers (outbound traffic).

   To configure the P interfaces:

   a. Select **P1 only** or **P1 and P2**.

      If you choose P1 only, enter configuration information (IP address, subnet mask, default gateway, DNS IP addresses) under **P1**.

      If you choose P1 and P2, enter configuration information under both **P1** and **P2**. Note that default gateway and DNS configuration (under **Shared Setting**) are shared between both P1 and P2.

   b. Click **Save** in the **Websense Content Gateway Interfaces** area when you are done.

Important

When you use the P2 interface, the P1 interface is bound to eth0, and the P2 interface is bound to eth1. Keep this in mind when you configure Websense Content Gateway.

For example, suppose you are using transparent proxy, and the P1 interface is connected to the WCCP router. In this case, you must configure Websense Content Gateway to use eth0 for WCCP communications (in Content Gateway Manager: **Configure** > **Networking** > **WCCP**, **General** tab).

When only P1 is used, it handles both inbound and outbound traffic for the proxy module (i.e., Content Gateway).

Alternatively, you could use both P1 and P2 such that P1 handles inbound traffic and P2 handles outbound traffic. To enable this configuration, be sure to set appropriate routing rules for P1 and P2 on the **Configuration** > **Routing** page. For example, you might set outbound traffic to go through P2.

Additionally, you can use P1 as a communication channel for multiple Content Gateway servers in a cluster. In this scenario, P1 should not be used for outbound traffic. For additional information on clusters, see the Content Gateway Manager Help.

7. Under **Network Agent Interface (N)**, configure the N interface.

   The N interface is used by the Network Agent module. It must be connected to a span (or mirror) port on a switch allowing it to monitor Internet requests going through the switch. (Note: be sure to configure the switch so the span port is monitoring all the ports carrying the traffic of interest; see your switch manufacturer's documentation for configuration instructions). For non-HTTP/HTTPS protocols, the N interface can also be used to send block information to enforce policy.

   Note

   The appliance does not send block messages to users who are blocked from non-HTTP and non-HTTPS protocols.

   To configure the N interface:

   a. Under **Send blocking information for non-HTTP/HTTPS traffic via**, select whether non-HTTP/HTTPS blocking information is sent via the C or N interface.

   b. Enter IP address, subnet mask, default gateway (only if you select interface N for sending blocking information), and DNS IP addresses for the N interface.

   c. Click **Save** in the **Network Agent Interface (N)** area.

8. Under **Expansion Interfaces (E1 and E2)**, choose whether to bond to P1 and P2 interfaces. (This applies to the V10000 and V10000 G2 only; E1 and E2 interfaces are not present on the V5000 G2.)

   Interfaces E1 and E2 can be cabled to your network and then bonded through software configuration to P1 and P2 (the Websense Content Gateway interfaces). If you choose to bond the interfaces, E1 must be bonded to P1 and E2 to P2. No other pairing is possible.

   You can choose to bond or not bond each Websense Content Gateway interface (P1 and P2) independently. You do not have to bond at all. You do not have to bond both. Also, you can choose different bonding modes for P1 and P2 (e.g., P1/E1 could be **Active/Standby** while P2/E2 could be **Load balancing**).

   Make sure all interfaces are cabled properly before configuring bonding.

   To bond E1 to P1:

   a. Under **E1**, select the check box for **Bond to P1 interface**.

   b. Under E1/P1 bonding mode, select:

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

   c. Click **Save** in the **Expansion Interfaces (E1 and E2)** area.

   To bond E2 to P2:

   Follow the instruction above for bonding E1 to P1, substituting E2 in place of E1 and P2 in place of P1. Make sure P2 is enabled. Otherwise the **E2** options will be inactive. (See Step 6 for instructions on activating P2.)

9. Configure routes if necessary:

   a. In the left navigation pane, click **Configuration > Routing**.

   b. Under Static Routes, use the **Add/Import** button to specify customized, static routes.

   c. Under Module Routes, use the **Add** button to specify non-management Web Security or Email Security traffic through the C interface.

   d. For either static or module routes, use the **Delete** button to remove existing routes, if necessary.

   

   Note

   An existing route cannot be edited. If you want to edit a route, delete it and then use the **Add/Import** (static) or **Add** (module) button to specify the route with the changes you want.

   See the Appliance Manager Help for more information about static and module routes.

10. Select the policy mode of this appliance:
    a. In the left navigation pane, click **Configuration > Web Security Components**.
    b. Specify the role of this appliance with respect to Websense Web Security policy information.
        - Choose **Full policy source** if Websense Policy Broker and Policy Database for your deployment will run on the appliance being configured. (Only one appliance in the network runs these two components, as well as the other filtering components.) Policy Server must also be run on the *full policy source* appliance; Policy Server can run in multiple locations.

        Note

        If Policy Broker runs on an appliance, only on-appliance instances of Policy Server can communicate with Policy Broker. In this case, Policy Server cannot be installed off-appliance. If Policy Broker is installed off-appliance, however, both on-appliance and off-appliance instances of Policy Server can communicate with it.

        - Choose **User directory and filtering** if the appliance currently being configured is *not* the location of the policy information, but will run Policy Server and User Service. Then, enter the **IP address** of the machine running Policy Broker (i.e., the policy source). The policy source can be another appliance that is running in *full policy source* mode. In this case, enter the IP address of that appliance's C network interface.
        - Choose **Filtering only** if the appliance being configured will not run any policy components. (There are some disadvantages to this reduced role, as explained in the Appliance Manager help system.) Then, enter the **IP address** of the machine serving as policy source, which in this case is a machine running Policy Server. The policy source can also be another appliance running in either *full policy source* or *user directory and filtering* mode. In this case, enter the IP address of that appliance's C network interface.
    c. Click **Save**.

11. Enable/disable TRITON Unified Security Center on this appliance
    a. If you have not done so already, in the left navigation pane, click **Configuration** > **Web Security Components**.
    b. Under **TRITON - Web Security**, select:
       - **Off**: the TRITON Unified Security Center runs on a separate machine from the appliance.
       - **On**: the TRITON Unified Security Center runs on this appliance.

       TRITON - Web Security is the Web Security module of the TRITON Unified Security Center. For a Websense Web Security Gateway deployment, you can choose to run the TRITON Unified Security Center on or off the appliance.

       For other deployments requiring more than the Web Security module of the TRITON Unified Security Center (i.e., Data Security or Email Security modules), the TRITON Unified Security Center must be installed on a separate machine from the appliance. In this case, be sure to disable it here.

       Note

       Organizations with high traffic volume or large reporting needs are encouraged to install and run the TRITON Unified Security Center on a separate machine, to optimize performance.

12. Click **Log Off**, at the top right, when you are ready to log off Appliance Manager

V10000 G2 (*Email Security only* mode)

After completing the initial configuration required by the firstboot script, use the Appliance Manager to configure important settings for network interfaces E1, E2, P1, and P2 (E2, P1, and P2 are optional). Interfaces P1 and P2 can be bonded to E1 and E2, respectively, either for load balancing or active/standby.

Gather the following information before running the Appliance Manager. Some of this information may have been written on the Quick Start during hardware setup.

Primary NTP server *Optional* Be sure that interface C can access the NTP server. If interface C does not have Internet access, you can install an NTP server locally on a subnet that can be accessed by interface C.	Domain:
Secondary NTP server, (domain) *Optional*	Domain:
Tertiary NTP server, (domain) *Optional*	Domain:
IP address for network interface E1	IP address:

Subnet mask for network interface E1	Subnet mask:
Default gateway for network interface E1 and E2 (if used) If you use both E1 and E2, the default gateway and DNS configuration are shared by both.	IP address:
Primary DNS server for network interface E1 and E2 (if used)	IP address:
Secondary DNS server for network interface E1 and E2 (if used) *Optional*	IP address:
Tertiary DNS server for network interface E1 and E2 (if used) *Optional*	IP address:
IP address for network interface E2 *Required only if E2 is enabled*	IP address:
Subnet mask for network interface E2 *Required only if E2 is enabled*	IP address:
Bond expansion interface P1 to E1? Yes or No *Optional*	If Yes, choose one: Active/standby or Load balancing
Bond expansion interface P2 to E2? Yes or No *Optional*	If Yes, choose one: Active/standby or Load balancing

After collecting the information needed, access the Appliance Manager through a supported browser.

Follow these steps to configure basic system and network interface settings. See the Appliance Manager Help for detailed instructions on any field or area, or for information about other available settings.

1. Open a supported browser, and enter the following URL in the address bar:

   ```
   https://<IP address>:9447/appmng
   ```

   Replace <IP address> with the address assigned to network interface C during initial configuration of the appliance (see *Perform initial command-line configuration*, page 16).

   For information about supported browsers, see the Websense Technical Library (www.websense.com/library).

2. Log on with the user name **admin** and the password set during initial appliance configuration.
3. In the left navigation pane, click **Configuration > System**.

4. Under **Time and Date**:
   a. Set the time zone.
   b. Set the time and date:
      - **Automatically synchronize with an NTP server**: select this option to use a Network Time Protocol server. Specify up to three NTP servers. Use of an NTP server is recommended, to ensure that database downloads and time-based policies are handled precisely.
      - **Manually set time and date**: select this option to enter a system time and date yourself.
   c. Click **Save** in the Time and Date area.
5. In the left navigation pane, click **Configuration > Network Interfaces**.
6. Under **Websense Email Security Gateway Interfaces (E1 and E2)**, configure the E1 and E2 (optional) interfaces.

   The E interfaces are used to accept users' requests (inbound traffic) and communicate with the Internet (outbound traffic).

   To configure the E interfaces:

   a. Select whether **E1 only** or both **E1 and E2** are used.

      If you choose E1 only, enter configuration information (IP address, subnet mask, default gateway, DNS IP addresses) under **E1**.

      If you choose E1 and E2, enter configuration information under both **E1** and **E2**. Note that default gateway and DNS configuration (under **Shared Setting**) are shared between both E1 and E2.

   b. Click **Save** in the **Websense Email Security Gateway Interfaces (E1 and E2)** area when you are done.

   When only E1 is used, it handles both inbound and outbound traffic.

   Alternatively, you could use both E1 and E2 such that E1 handles inbound traffic and E2 handles outbound traffic.

   See the Appliance Manager Help for more information about configuring E1 and E2.
7. Under **Expansion Interfaces (P1 and P2)**, choose whether to bond P1 and P2 to E1 and E2.

   Interfaces P1 and P2 can be cabled to your network and then bonded through software configuration to E1 and E2. If you choose to bond the interfaces, P1 must be bonded to E1 and P2 to E2. No other pairing is possible.

   You can choose to bond or not bond E1 and E2 independently. You do not have to bond both. Also, you can choose different bonding modes for E1 and E2 (e.g., E1/P1 could be **Active/Standby** while E2/P2 could be **Load balancing**).

   Make sure all interfaces are cabled properly before configuring bonding.

   To bond P1 to E1:

   a. Under **P1**, select the check box for **Bond to E1 interface**.

b. Under P1/E1 bonding mode, select:

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

c. Click **Save** in the **Expansion Interfaces (P1 and P2)** area.

To bond P2 to E2:

Follow the instructions above for bonding E1 to P1, substituting E2 in place of E1 and P2 in place of P1. Make sure E2 is enabled. Otherwise the **P2** options will be inactive. (See Step 6 for instructions on activating E2.)

8. Configure routes if necessary:
   a. In the left navigation pane, click **Configuration > Routing**.
   b. Under Static Routes, use the **Add/Import** button to specify customized, static routes.
   c. Under Module Routes, use the **Add** button to specify non-management Web Security or Email Security traffic through the C interface.
   d. For either static or module routes, use the **Delete** button to remove existing routes, if necessary.

> **Note**
> An existing route cannot be edited. If you want to edit a route, delete it and then use the **Add/Import** (static) or **Add** (module) button to specify the route with the changes you want.

See the Appliance Manager Help for more information about static and module routes.

9. Click **Log Off**, at the top right, when you are ready to log off Appliance Manager.

V5000 G2 (*Email Security only* mode)

After completing the initial configuration required by the firstboot script, use the Appliance Manager to configure important settings for network interfaces P1 and (optionally) P2.

Gather the following information before running the Appliance Manager. Some of this information may have been written on the Quick Start during hardware setup.

Primary NTP server *Optional* Be sure that interface C can access the NTP server. If interface C does not have Internet access, you can install an NTP server locally on a subnet that can be accessed by interface C.	Domain:
Secondary NTP server *Optional*	Domain:
Tertiary NTP server *Optional*	Domain:
IP address for network interface P1	IP address:
Subnet mask for network interface P1	Subnet mask:
Default gateway for network interface P1 and P2 (if used) If you use both P1 and P2, the default gateway is automatically assigned to P2 (which is bound to eth1).	IP address:
Primary DNS server for network interface P1 and P2 (if used)	IP address:
Secondary DNS server for network interface P1 and P2 (if used) *Optional*	IP address:
Tertiary DNS server for network interface P1 and P2 (if used) *Optional*	IP address:
IP address for network interface P2 *Required only if P2 is enabled*	IP address:
Subnet mask for network interface P2 *Required only if P2 is enabled*	Subnet mask:

After collecting the information needed, access the Appliance Manager through a supported browser.

Follow these steps to configure basic system and network interface settings. See the Appliance Manager Help for detailed instructions on any field or area, or for information about other available settings.

1. Open a supported browser, and enter the following URL in the address bar:

   `https://<IP address>:9447/appmng`

   Replace <IP address> with the address assigned to network interface C during initial configuration of the appliance (see *Perform initial command-line configuration*)
2. Log on with the user name **admin** and the password set during initial appliance configuration.
3. In the left navigation pane, click **Configuration** > **System**.
4. Under **Time and Date**:
   a. Set the time zone.
   b. Set the time and date:
      - **Automatically synchronize with an NTP server**: select this option to use a Network Time Protocol server. Specify up to three NTP servers. Use of an NTP server is recommended, to ensure that database downloads and time-based policies are handled precisely.
      - **Manually set time and date**: select this option to enter a system time and date yourself.
   c. Click **Save** in the Time and Date area.
5. In the left navigation pane, click **Configuration** > **Network Interfaces**.
6. Under **Websense Email Security Gateway Interfaces (P1 and P2)**, configure the P1 and P2 (optional) interfaces.

   The P interfaces are used to accept users' requests (inbound traffic) and communicate with the Internet (outbound traffic).

   To configure the P interfaces:

   a. Select whether **P1 only** or both **P1 and P2** are used.

      If you choose P1 only, enter configuration information (IP address, subnet mask, default gateway, DNS IP addresses) under **P1**.

      If you choose P1 and P2, enter configuration information under both **P1** and **P2**. Note that default gateway and DNS configuration (under **Shared Setting**) are shared between both P1 and P2.

   b. Click **Save** in the **Websense Email Security Gateway Interfaces (P1 and P2)** area when you are done.

   When only P1 is used, it handles both inbound and outbound traffic.

   Alternatively, you could use both P1 and P2 such that P1 handles inbound traffic and P2 handles outbound traffic.

   See the Appliance Manager Help for more information about configuring Email Security interfaces.
7. Configure routes if necessary:
   a. In the left navigation pane, click **Configuration** > **Routing**.
   b. Under Static Routes, use the **Add/Import** button to specify customized, static routes.

c. Under Module Routes, use the **Add** button to specify non-management Web Security or Email Security traffic through the C interface.

d. For either static or module routes, use the **Delete** button to remove existing routes, if necessary.

> **Note**
> An existing route cannot be edited. If you want to edit a route, delete it and then use the **Add/Import** (static) or **Add** (module) button to specify the route with the changes you want.

See the Appliance Manager Help for more information about static and module routes.

8. Click **Log Off**, at the top right, when you are ready to log off Appliance Manager.

Install off-appliance or optional components

After the appliance has been configured, install the off-appliance components you want. See *Software that runs off-appliance*, page 8 for more information about these components. Run the Websense Installer (in custom installation mode) on the machine to which you want to install components. See the Websense Technical Library (www.websense.com/library) for instructions.

> **Note**
> If Policy Broker runs on an appliance, only on-appliance instances of Policy Server can communicate with Policy Broker. In this case, Policy Server cannot be installed off-appliance. If Policy Broker is installed off-appliance, however, both on-appliance and off-appliance instances of Policy Server can communicate with it.

Additional instances of Web security filtering components may be installed on machines in your network to provide additional functions or distribute processing load. For example, you can install additional Websense Network Agent instances on machines in your network.

Creating a TRITON management server

Important

The appliance must be set up before creating a TRITON management server. If you have not done so already, complete the following procedures before creating a TRITON management server:

- *Set up the appliance hardware*, page 13
- *Perform initial command-line configuration*, page 16
- *Configure the appliance*, page 18

The machine on which TRITON Unified Security Center is installed is referred to as the *TRITON management server.* See the Websense Technical Library (www.websense.com/library) for instructions on creating a TRITON management server.

Restoring to Factory Image

The V10000 G2 and V5000 G2 come with a recovery DVD that can be used to restore the appliance to its factory image. You can use this DVD (after saving a Full configuration backup) to re-image the appliance and then recover your custom appliance and module settings.

The recovery process for a V10000 involves additional steps because a version 7.6 recovery DVD is not supplied with it. You must use the original, prior-version recovery DVD that came with your appliance. After restoring it to this image, apply the necessary upgrade patch or patches to upgrade the appliance to version 7.6.

Important

Use the original recovery DVD that came with your appliance. If you have misplaced it, you can download a DVD image from MyWebsense (www.mywebsense.com.) It is important you use an image that is associated with the manufacture date of your appliance. The MyWebsense downloads page will indicate the appliance manufacture date appropriate for each image.

Note that all Websense components running off the appliance must be stopped before you resetting to factory image.

1. Stop all Websense components that are running off the appliance. For example, stop Web Security or Email Security Log Servers, Sync Service, Linking Service, transparent ID agents, and TRITON Unified Security Center.

2. If possible, back up any information you want preserved.
   a. Using a Web browser, log onto the Appliance Manager (https://<*C interface IP address*>:9447/appmng).
   b. Go to **Administration > Backup Utility**, and create a Full Configuration backup. See online Help for assistance. Save this backup file to another machine.
3. Go to the machine rack and insert the recovery disk into the appliance DVD drive.

   Important
   If you are recovering a V10000 (not G2), use the **prior-version** recovery DVD originally supplied with it. You will reset it to this prior-version factory image and then apply upgrade patches to bring the appliance up to version 7.6. Do not use a version 7.6 recovery DVD (it is not compatible with a V10000).

4. Reboot the appliance. (An alternative is to turn off the power, and then turn it on again.)
5. Watch the terminal screen closely after the reboot starts. When a list of function keys appears at the upper right during reboot, press **F11.** Then select one of the following:
   - **Boot from SATA Optical** drive (V10000 G2)
   - **Boot from Embedded SATA 1 TEAC DVD-ROM DV-28SW** drive (V5000 G2)
   - **Boot From IDE CD_ROM device** (V10000)
6. When asked whether you want to continue, enter **yes**.

   Restoring the image can take 20 minutes or more. When the DVD is ejected, be sure to remove it from the drive.
7. Press any key to view the subscription agreement.
8. Enter **yes** to accept the subscription agreement, and then enter **yes** to begin firstboot.

   This begins the firstboot script.
9. Follow the on-screen instructions at the terminal and provide the necessary information.

   See *Perform initial command-line configuration* for details about what information is requested.
10. (V10000 only) Apply the upgrade patch or patches to bring the appliance version to 7.6:

    Important
    These steps are for the V10000 only, not the V10000 G2.

    a. If you no longer have them available, obtain the necessary upgrade patch or patches to bring your appliance up to version 7.6.

       See www.websense.com/support for information about obtaining patches.

b. Using a Web browser, log onto the Appliance Manager (https://<*C interface IP address*>:9447/appmng).

c. In the Appliance Manager, go to **Administration** > **Patch Management**.

d. Click **Upload Patch Manually**, browse to and select the version 7.6 upgrade patch, and then click **Upload**.

e. Once uploaded, click the **Install** button for the version 7.6 upgrade patch.

f. Follow the prompts to install the patch.

> **Note**
> If your appliance version was originally prior to 7.5.x, you will need to use multiple patches. First, apply the required patches to bring your appliance to version 7.5.x. Then, apply the version 7.6 upgrade patch to bring it up to version 7.6. Repeat the above upload and install steps for each patch.

11. Restore the backed up configuration via the Appliance Manager.
    a. Using a Web browser, log onto the Appliance Manager (https://<*C interface IP address*>:9447/appmng).
    b. Go to **Administration > Backup Utility**.
    c. Choose **Restore**.
12. Select **Full Appliance Configuration** restore mode and click **Run Restore Wizard**.
13. In the Restore Wizard:
    a. File Location: Select **Another location (browse for file)**. Then click **Next**.
    b. Select File: **Browse** to the backup file (*.bak file) to select it. Then click **Next**.
    c. Confirm: Verify backup file details and then click **Restore Now**.

    The appliance will be rebooted automatically after the restore is complete. Appliance and software module settings are restored.
14. Ensure that the appliance time and date are synchronized with other servers.
15. Restart the components that run off the appliance.
16. (*Web Security only*- and *Web and Email Security*-mode appliances only) On occasion, a manual download of the Websense Web Security Master Database should be initiated after a recovery. Do this in the TRITON Unified Security Center (Web Security module) if you receive a warning message about the Master Database.