websense

Getting Started

Websense® V-Series Appliance

v7.5.x

Published 2010 Revision D
Printed in the United States of America and Ireland

Every effort has been made to ensure the accuracy of this manual. However, Websense, Inc., makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. Websense, Inc., shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or the examples herein. The information in this documentation is subject to change without notice.

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 traffic and content.

The appliance offers:

- Command line interface for initial appliance settings, available through a USB keyboard and monitor or a serial port connection, that provides 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, including patch management; troubleshooting tools with basic command-line utilities; backup; and restore
- Logging of events related to appliance configuration and patching. Log entries can be viewed in Appliance Manager, and the entire log file can be downloaded for later viewing.
- Integrated proxy caching and Web filtering after minimal initial configuration
- Full customization of proxy caching and Web filtering, available through separate Web-based configuration interfaces.
- Configurable links to hybrid Web filtering and off-appliance Data Security features.

Software provided on the appliance

With an appliance-based Web Security Gateway or Web Security Gateway Anywhere solution, the following components are pre-loaded for your convenience:

- Websense Web Security core components, including:
  - Policy Database
  - Policy Broker
  - Policy Server
  - Filtering Service
  - User Service
  - Usage Monitor
  - Control Service
  - Directory Agent
  - TRITON - Web Security (optional; can be run on separate Windows server)
    - Investigative Reports Scheduler
    - Manager Web Server
    - Reporting Web Server
    - Reports Information Service
- Websense Content Gateway
- Network Agent (optional)

Larger enterprises might use 2 or more Websense appliances, with one designated as the *policy source* machine (the only machine to run Policy Broker and Policy Database, along with other components). All other appliances point to the *policy source* machine for policy updates. Alternatively, you can add a Windows or Linux server and designate it as the *policy source*.

In all cases, Network Agent and Websense Content Gateway run as separate modules on each appliance, if they are enabled.

Software that runs off the appliance

Regardless of how many appliances you have, the following Websense Web Security components must be installed separately. Most are Windows-only components.

- Log Server (required for reporting)
- Sync Service (for sites using hybrid Web security)
- Linking Service (for sites using any integrated Data Security features)
- (optional) Transparent identification agents (for filtering by user or group)
  - DC Agent
  - Logon Agent
  - eDirectory Agent
  - RADIUS Agent

Data Security Management Server

The Websense Data Security Management Server must be installed on a Windows server, for sites using any Data Security features. This includes:

- Policy Engine
- Crawler
- PreciseID Fingerprint Repository
- Forensics Repository

The off-appliance Web security and data security components can be installed on virtual machines that you have created on a single, physical Windows machine with a supported version of VMware, if desired.

Database management software

You are required to have a Windows database server running a supported version of Microsoft SQL Server. This is where the Log Database is built. Log Database provides the information for Websense Web Security reporting.

TRITON - Web Security

The **TRITON - Web Security** console is pre-installed on the appliance as a convenience for evaluations and small installations. This management console allows you to set up filtering policies, assign policies to users and groups, read alerts, and perform other management tasks.

The **TRITON** console also displays a variety of filtering reports and can be used to create and schedule custom reports. Organizations with high traffic volume or large reporting needs should install and run **TRITON - Web Security** on a ***separate Windows server***, to optimize performance.

TRITON - Web Security services include:

- Investigative Reports Scheduler
- Manager Web Server
- Reporting Web Server
- Reports Information Service

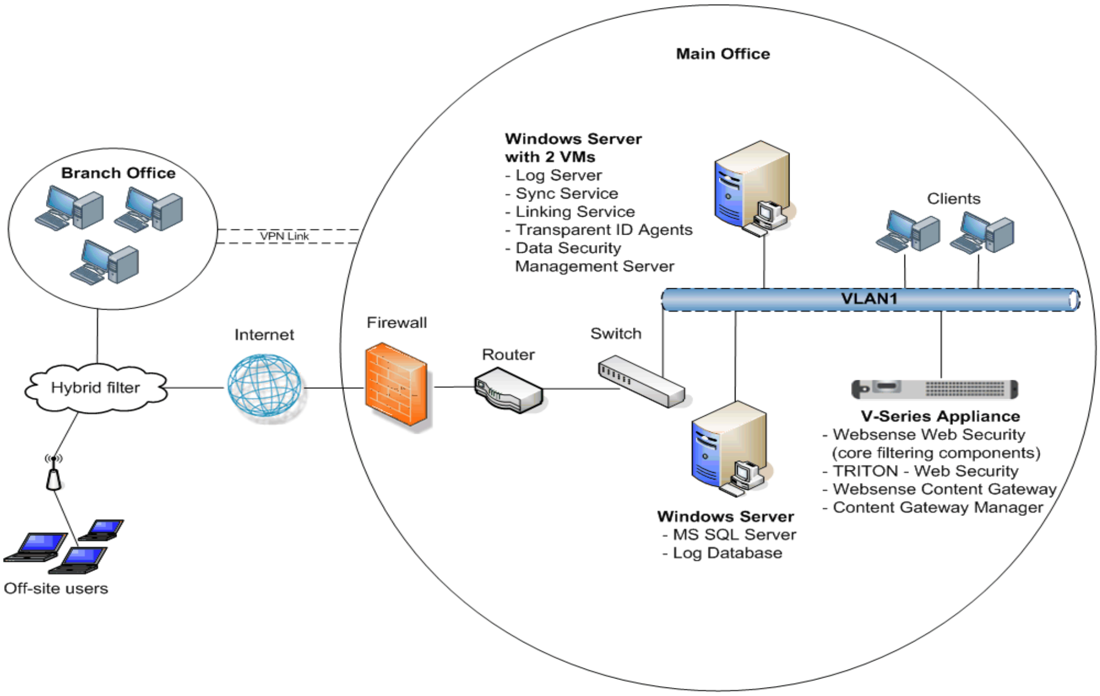
Sample deployment

This is what a Web Security Gateway Anywhere deployment might look like when deployed on a V-Series appliance for evaluation or in a small office.

Larger networks typically install and run the **TRITON - Web Security** management console on a Windows server. (The console is depicted here on the appliance, but this is not a recommended practice for production environments.

Large installations might have 2 or more appliances and 2 or more Windows machines.

Note that Log Database and the MS SQL Server are not located on the same server with other modules.



Windows Server requirements for Web security components

In addition to the Websense appliance, you must have one or more separate server machines that meet or exceed the requirements listed below for Websense Web Security components that run off the appliance.

Organizations with high traffic volume or large reporting needs are encouraged to install and run **TRITON - Web Security** on a separate Windows server, to optimize performance. Log Server (the component that receives Internet activity information and processes it into a Log Database), Sync Service, and Linking Service must be located off the appliance.

Important

Self-signed certificates are created to secure communications between Websense components. In order for these certificates to be valid, and for communication to succeed, all the machines running Websense components **must** have the same date.

Please set the appliance time and the time on the Windows server machine before installing Websense components.

If you need to reset the time and date, be sure to reset all machines.

Hardware

- Quad-Core Intel Xeon processor, 2.5 GHz or higher
- 4-16 GB RAM
- 100 GB free disk space utilizing a disk array
- High speed disk access

Operating System

- Windows Server 2008 (Standard, Enterprise, and Datacenter) installed in 32-bit native mode
- Windows Server 2003, R2 (Standard or Enterprise)
- Windows Server 2003, SP1 or SP2 (Standard or Enterprise)
- Windows Server 2003 (Standard or Enterprise)

Additional Software

- Internet Explorer 7 or 8 (Compatibility View is not supported), or Firefox 2 or 3
- Common Desktop Environment (CDE)
- Apache Tomcat 6.0.13 (installed automatically with Websense Manager)
- Adobe Flash Player 8 or later

Windows Server requirements for Data Security Management Server

In addition to the Websense appliance, you must have a separate Windows server machine that meets the requirements listed below if you run Websense Data Security Management Server.

Hardware requirements for Data Security Management Server

Data Security Management Server	Minimum Requirements	Recommended
CPU	2 Dual-core Intel Xeon processors (2.0 GHz) or AMD equivalent	2 Quad-core Intel Xeon processors (2.0 GHz) or AMD equivalent Note: The Management Server can **not** have more than 8 cores.
Memory	2 GB	4 GB
Free disk space	144 GB	292 GB
Hardware RAID	1 + 0	1 + 0
NICs	1	2

Database Engine

One of the following supported database engines is required to store log data for reporting. Although this software can run on the same Windows server machine that runs Log Server, better performance is achieved when it runs on a dedicated server.

One of these databases:

- Microsoft SQL Server 2005 SP2 or SP 3 (Workgroup, Standard, Enterprise, or 64-bit edition) (recommended)
- Microsoft SQL Server 2000 SP4
- MSDE 2000 SP4 - suitable for smaller networks (does not run on Microsoft Windows Server 2008)

The following recommendations apply to the machine running the database engine:

- You can improve I/O performance by installing the Log Database on a disk array running RAID level 1+0.
- The amount of required RAM depends on the total number of requests being stored and the number of requests per second being processed. To optimize RAM usage, use the Enterprise Edition of Microsoft SQL Server on a machine running Windows Server 2003 Enterprise Edition or Windows Server 2008 Enterprise Edition or Datacenter.

Directory Service

If your network includes one of the supported directory services listed below, you can apply Web filtering to individual users, groups, and domains (OUs). Additionally, you can install an optional transparent identification agent from Websense, to ensure that clients in a supported directory service are filtered without being prompted to log on when they open a browser. (If no directory service is installed, Websense Web Security uses IP addresses for Web filtering.)

For organizations where multiple administrators may access Content Gateway Manager or **TRITON - Web Security** (the Web-based configuration interfaces for Websense Content Gateway and Websense Web Security), administrators with accounts in most supported directory services can log on with their network credentials.

> ✓ **Note**
>
> If your network uses a Windows NTLM directory service, or Active Directory in mixed mode, you must create Websense accounts for any administrators who must log on to **TRITON - Web Security.** This configuration does not support logging on to **TRITON - Web Security** with network credentials.

- Microsoft Active Directory 2000, 2003, or 2008 (specific permissions need to be granted to Websense Logon Agent to run with 2008)
- Novell eDirectory 8.51 or later
  - NMAS authentication is supported.
  - Recommend Novell Client v4.83 or v4.9 (v4.81 and later are supported)
- Other LDAP-based directory services
- Most standard RADIUS servers

  The following RADIUS servers have been tested:
  - Livingston (Lucent) 2.x
  - Cistron RADIUS server
  - Merit AAA
  - Microsoft IAS

Other servers

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

Important

If you change the *policy source* (machine running Policy Broker and Policy Server) after deploying components on additional machines, you must reconfigure those components to communicate with the new *policy source.*

Go to the Websense Knowledge Base, and search for the article titled *Changing the Policy Server (or Policy Broker) IP address*.

For information about system requirements and appropriate placement of machines for additional or optional components, see the *Websense Deployment Guide*.

Network scenarios

One or more Websense V-Series appliances can be deployed in a network, depending on the traffic volume and security goals.

Appliances can serve different roles, and thus all deployments should be well planned in advance. Please contact your Websense Sales Engineer, or your authorized Websense reseller, for assistance in planning your deployment.

Basic deployment scenarios are shown below:

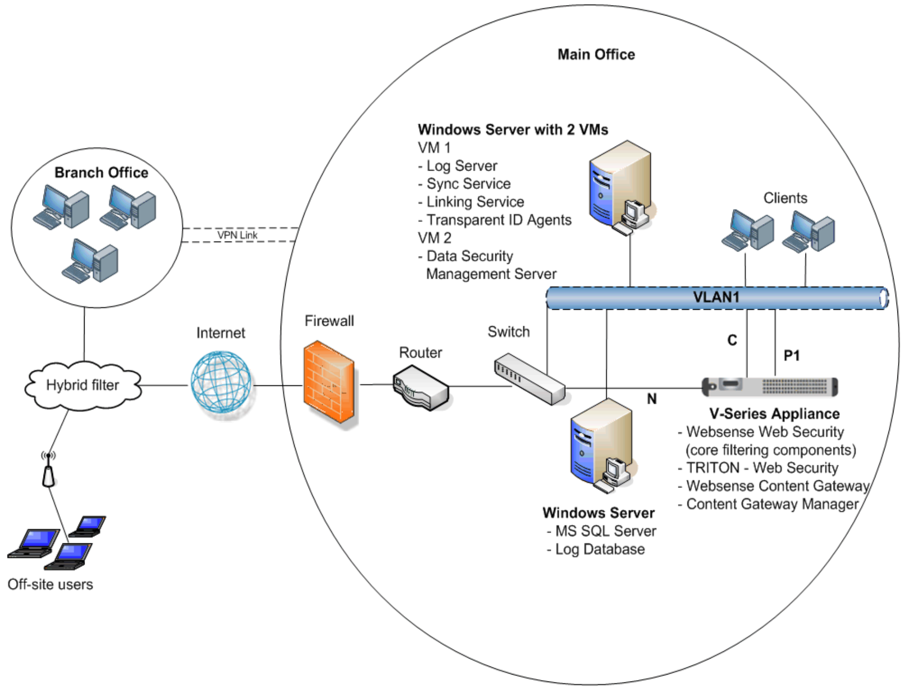
- *Single appliance deployment*
- *Multiple appliance deployment*

Single appliance deployment

When you deploy a single Websense appliance to host all major features, one additional Windows server is required to run Log Server, Sync Service (optional; used to access hybrid filtering), and Linking Service (optional; used to integrate with Data Security). Organizations with high traffic volume or large reporting needs should install and run **TRITON - Web Security** on a Windows server, to optimize performance.

In all environments, the cable for appliance network interface N must be connected to a span port, monitor port, or mirror port on a router or switch. This enables it to see traffic from all clients being filtered.

- Typically, network interfaces C and P1 are both able to access a DNS server. Both typically have access to the Internet. (You can choose instead to use P1 for all Internet access by configuring this in the **TRITON -Web Security** console on the **Settings** > **Database Download** page. Select **Use proxy server or firewall** and enter the IP address and port number.)
- If network interface C is used to send protocol blocking information, as it is by default, C must be able to communicate with client machines.
- Network interface P2 can be connected the same way as P1, if you need 2 interfaces. The P2 interface is optional. When P2 is used, ensure that P1 and P2 are in different subnets.



If you plan to implement explicit proxy, ensure that clients can reach the VLAN where interface P1 is connected.

Expansion interfaces are available on models V10000 and V10000 G2 only. These can be used to provide standby interfaces for P1 and P2, respectively, or for load balancing.

If you plan to implement transparent proxy for Websense Content Gateway, WCCP should be enabled on the switch.

See the Websense Content Gateway *Administrator's Guide* for additional information about deploying transparent or explicit proxy.

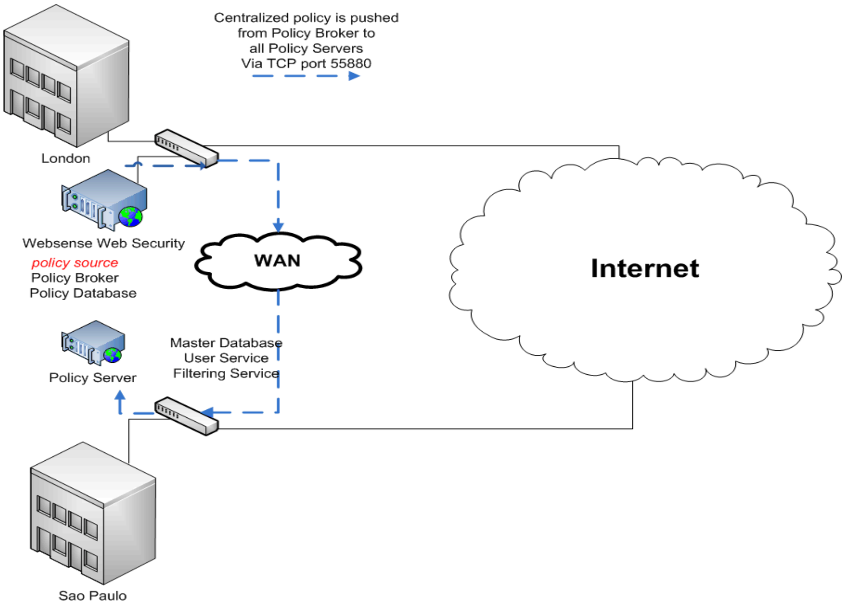
Multiple appliance deployment

Organizations that need to filter a large number of users or a large volume of Internet traffic may deploy multiple Websense appliances. One appliance is designated as the *policy source*, and all others point to the *policy source* for policy and configuration settings.

The policy source appliance is configured first. See *Configure the appliance*, page 19, for more information.

Important

If you change the policy source (machine running Policy Broker and Policy Server) after deploying components on additional machines, you must reconfigure those components to communicate with the new policy source.



Expansion interfaces

Appliance models V10000 and V10000 G2 offer two optional, expansion interfaces called E1 and E2. (These interfaces are not available on the model V5000 G2.)

Each of these interfaces can be cabled to your network and then bonded through software settings to a Websense Content Gateway interface, with E1 optionally bonded to P1, and E2 optionally bonded to P2. No other pairing is possible.

Interface bonding provides these alternatives:

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

You can choose to bond or not bond each Websense Content Gateway interface (P1 and P2) independently. You do not have to bond at all. You do not have to bond both.

If you do bond an interface (P1 or P2), you can choose only one mode for that bonding (either active/standby or load balancing). You can choose different bonding modes for P1 and P2.

Ensure that all interfaces are cabled properly before bonding.

2 Setting up Websense appliances

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

Steps 4 and 5, the installation and configuration of components that run off the appliance, are covered in the *Getting Started Guide* for **Websense Web Security Gateway Anywhere**.

1. *Set up the appliance hardware*
2. *Perform initial command-line configuration*
3. *Configure the appliance*
4. Install and configure components off the appliance.
5. Test and refine your policies.

When setup is complete, you can use the Logon Portal to log on to any of the related management consoles.

Set up the appliance hardware

The Quick Start poster, which comes in the shipping box with your appliance, 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 the cables to the appliance and to your network.

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 that this address is permitted by all firewalls, proxy servers, routers, or host files that control the URLs that the C and P1 interfaces can access.

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*.

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, then you must configure either P1 or P2 to receive Master URL Database downloads from Websense. This extra step must be done through the Appliance Manager (to configure P1 and P2) and through the TRITON - Web Security console (to configure the proxy for database downloads).
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 to be used for these consoles: Appliance Manager; TRITON - Web Security; and Content Gateway Manager. (8 to 15 characters, at least 1 letter and 1 number)	

When you have gathered the necessary information, run the initial command line configuration, 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. Follow the onscreen 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.

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 N and P1 (and optionally P2), which are used for communications by Network Agent and Websense Content Gateway. Appliance model V10000 and model V10000 G2 also offer expansion interfaces (E1 and E2) that can be bonded with P1 and P2, respectively, either for load balancing or 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**, WCCP version 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, (domain) *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.	
Secondary NTP server, (domain) *Optional*	
Tertiary NTP server, (domain) *Optional*	
IP address for network interface P1	
Subnet mask for network interface P1	
Default gateway for network interfaces P1 (and P2); (IP address) 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.	
Primary DNS server for network interfaces P1 (and P2); (IP address)	
Secondary DNS server for network interfaces P1 (and P2); (IP address) *Optional*	
Tertiary DNS server for network interfaces P1 (and P2); (IP address) *Optional*	
IP address for network interface P2 *Required only if P2 is enabled*	
Subnet mask for network interface P2 *Required only if P2 is enabled*	
Choose interface for transporting blocking information for non-HTTP and non-HTTPS traffic. (interface C or interface N)	
If interface N transports blocking information, N must be connected to a bidirectional span port.	Ensure that interface N has been set up appropriately, if N will transport blocking information.
IP address for network interface N	
Subnet mask for network interface N	
Default gateway for network interface N (IP address) *Required only if network interface N carries blocking information*	

Primary DNS server for network interface N (IP address)	
Secondary DNS server for network interface N, (IP address) *Optional*	
Tertiary DNS server for network interface N, (IP address) *Optional*	
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
Policy Source IP address	Choose one: This appliance is the policy source. This appliance runs User directory and filtering (specify policy source IP address). This appliance runs filtering only (specify policy source IP address).
TRITON - Web Security (user interface for Websense Web Security) IP address	TRITON - Web Security runs on this appliance. *or* TRITON - Web Security runs at the specified IP address. *Organizations with high traffic volume or large reporting needs are encouraged to install and* *run TRITON - Web Security on a separate Windows server, to optimize performance.*

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** > **General**.
   a. Set the time zone.
   b. Select Internet Network Time Protocol (NTP) servers for time synchronization, or specify the system time and date. (Use of an NTP server is recommended, to ensure that database downloads and time-based policies are handled precisely.)
   c. Click **Save** in the Time and Date area.
4. In the left navigation pane, click **Configuration** > **Network Interfaces**.
   a. Configure network interfaces P1 (and optionally P2) for Websense Content Gateway. Then, click **Save** in the Websense Content Gateway Interface area.

> **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**, WCCP version tab).

   These network interfaces can accept users' Internet requests (inbound traffic) and communicate with Web servers (outbound traffic).

   One common configuration is to use P1 for traffic into and out of the proxy module. Another common configuration uses P1 for inbound traffic and P2 for 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 P2 as a communication channel for multiple proxy servers in a cluster. In this scenario, P2 cannot be used for outbound traffic. For additional information on clusters, see the Websense Content Gateway *Administrator's Guide*.

   b. Decide whether network interface N (for Network Agent) will transport blocking information for non-HTTP/HTTPS traffic. Enter all required IP addresses and enter the subnet mask. Then, click **Save** in the Network Agent Interface area.

   Network interface N monitors all Internet requests, and can enforce policy for protocols other than HTTP and HTTPS.

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

   c. Configure *Expansion interfaces*, if desired. Then, click **Save** in the Expansion Interfaces area.

5. In the left navigation pane, click **Configuration** > **Routing**.
6. Use the **Add Route** button to specify customized, static routes.
7. Use the **Edit** and **Delete** buttons to modify existing routes, as needed.
8. In the left navigation pane, click **Configuration** > **Web Security Components**.

Components running off the appliance

When you are ready to install components off the V-Series appliance, refer to the *Getting Started Guide* for **Websense Web Security Gateway Anywhere**. All Websense guides are available at MyWebsense.com.

Most off-box components are Windows-only components.

- Log Server (required for reporting)
- Sync Service (for sites using hybrid Web security)
- Linking Service (for sites using any integrated Data Security features)
- (optional) Transparent identification agents (for filtering by user or group)
  - DC Agent
  - Logon Agent
  - eDirectory Agent
  - RADIUS Agent

Data Security Management Server

The Websense Data Security Management Server must be installed on a Windows server, for sites using any Data Security features. This includes:

- Policy Engine
- Crawler
- PreciseID Fingerprint Repository
- Forensics Repository

The off-appliance Web security and data security components can be installed on virtual machines that you have created on a single, physical Windows machine with a supported version of VMware, if desired.

Database management software

You are required to have a Windows database server running a supported version of Microsoft SQL Server. This is where the Log Database is built. Log Database provides the information for Websense Web Security reporting.

TRITON - Web Security

The **TRITON - Web Security** management console is pre-installed on the appliance as a convenience for evaluations and small installations. Organizations with high traffic volume or large reporting needs should install and run **TRITON - Web Security** on a ***separate Windows server***, to optimize performance.

TRITON - Web Security services include:

- Investigative Reports Scheduler
- Manager Web Server
- Reporting Web Server
- Reports Information Service

Recovering the V-Series appliance from DVD

The Websense V-Series appliance comes with a recovery disk 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. Note that all Websense components running off the appliance must be stopped before you use the recovery disk.

1. Stop all Websense components that are running off the appliance. For example, stop Log Server, Sync Service, Linking Service, transparent ID agents, **TRITON - Web Security** and all components on the **Data Security Management Server**.
2. If possible, back up any information you want preserve.
   a. Log on to the Appliance Manager for the primary V-Series appliance.
   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.
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 either:
   - **Boot from Embedded SATA** drive (models V10000 G2 and V5000 G2)
   - **Boot from IDE CD-ROM device** (model 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 onscreen instructions at the terminal and provide the necessary information.

   See *Perform initial command-line configuration* for details of what information is requested.

10. Restore the backed up configuration via the Appliance Manager.

    a. Point a browser to the Logon Portal and log on to the Appliance Manager for the primary V-Series appliance.

    b. Go to **Administration > Backup Utility**.

    c. Choose **Restore**.

11. Upload your Full Configuration backup file to the appliance, and then select **Restore**. The appliance will be rebooted automatically after the **Restore** is completed. Appliance and software module settings are restored.

12. Ensure that the appliance time and date are synchronized with other servers.

13. Restart the components that run off the appliance.

14. On occasion, a manual download of the Websense Web Security Master Database should be initiated after a Recovery. Do this in the TRITON - Web Security console if you receive a warning message about the Master Database.