Websense Appliance Manager Help

Websense® V-Series Appliance

Models: V10000, V10000 G2, V5000 G2

v7.7

©1996–2012, Websense Inc.
All rights reserved.
10240 Sorrento Valley Rd., San Diego, CA 92121, USA

R150612770

Published 2012
Printed in the United States and Ireland

The products and/or methods of use described in this document are covered by U.S. Patent Numbers 5,983,270; 6,606,659; 6,947,985; 7,185,015; 7,194,464 and RE40,187 and other patents pending.

This document may not, in whole or in part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form without prior consent in writing from Websense Inc.

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

Websense is a registered trademark of Websense, Inc., in the United States and certain international markets. Websense has numerous other unregistered trademarks in the United States and internationally. All other trademarks are the property of their respective owners.

Microsoft, Windows, Windows NT, Windows Server, and Active Directory are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Sun, Sun Java System, and all Sun Java System based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc., in the United States and other countries.

Mozilla and Firefox are registered trademarks of the Mozilla Foundation in the United States and/or other countries.

eDirectory and Novell Directory Services are a registered trademarks of Novell, Inc., in the U.S and other countries.

Adobe, Acrobat, and Acrobat Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Pentium is a registered trademark of Intel Corporation.

Red Hat is a registered trademark of Red Hat, Inc., in the United States and other countries. Linux is a trademark of Linus Torvalds, in the United States and other countries.

This product includes software distributed by the Apache Software Foundation (http://www.apache.org).
Copyright (c) 2000. The Apache Software Foundation. All rights reserved.

Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are the sole property of their respective manufacturers.

Contents

1 V-Series Overview

Help | V-Series Appliance | Version 7.7.x

The Websense® V-Series™ appliance analyzes Web traffic, email traffic, or both in real-time and applies security policy.

When Websense Web Security Gateway modules are enabled, the appliance:

- Instantly categorizes new sites and dynamic content, proactively discovering security risks, and blocking unwanted content and malware per administrator configured policy.
- Provides advanced analytics—including rules, signatures, heuristics, and application behaviors—to detect and block proxy avoidance, hacking sites, adult content, botnets, keyloggers, phishing attacks, spyware, and many other types of unsafe content.
- Closes a common security gap: decrypting and scanning SSL traffic before it enters the network.

These real-time capabilities on the V-Series appliance integrate with industry-leading Websense Web Security software to provide Web filtering with over 90 default URL categories and more than 120 network and application protocols.

- Software on the appliance can be linked with Websense Data Security solutions, to give data security software access to both Master Database URL categorization and user information collected by Websense Web filtering services.
- Software on the appliance can also be synchronized with Websense hybrid Web filtering, an on-demand, cloud-based service, to apply your organization's policies to off-site users, or to branch offices, remote campuses, and so on.

When Websense Email Security Gateway is enabled, the appliance:

- Scans and filters incoming email messages to block spam or virus content per administrator configured policy.
- Integrates with Websense Data Security solutions to help you monitor and restrict transmission of sensitive or inappropriate information via email.

When the subscription is Websense Email Security Gateway Anywhere, the appliance also:

- Provides a hybrid solution that allows the bulk of spam content to be filtered out before the messages reach your network.

Security best practices

Help | V-Series Appliance | Version 7.7.x

- Lock the appliance inside an IT closet or data center and enable a BIOS password. Physical access to the appliance can be a security risk for your network.
- Physical access to the appliance via serial console (KVM) to access the command line interface is protected after **firstboot** is run, by the administrator credentials.
- Ensure that administrator credentials are restricted to a select few persons. This helps prevent unauthorized access to the system.
- Enable troubleshooting ports and permit remote access only when requested to do so by Websense Technical Support. Return these settings to the disabled state immediately after the Websense specialist logs off.

Management consoles

Help | V-Series Appliance | Version 7.7.x

Related topics:

- *Managing appliances in TRITON Unified Security Center*, page 3
- *Accessing Appliance Manager and other consoles*, page 3
- *Logging on to Appliance Manager*, page 5
- *Configuring two-factor authentication*, page 5
- *Disabling and enabling password logon*, page 6

Appliance Manager is the name of the management console for the V-Series appliance.

Use Appliance Manager to:

- Monitor the status of software modules and appliance resources
- Establish assignments and routes for network interfaces
- Apply patches and hotfixes
- Change passwords
- Perform troubleshooting
- More

TRITON™ Unified Security Center is the name of the management console for TRITON Web, data, email, and mobile security modules. It also provides access to Appliance Manager and Content Gateway Manager (the Web proxy component).

You will use TRITON Unified Security Center to perform such activities as setting up users and defining and applying Web and email filtering policies.

This table lists the TRITON security modules and their related console.

Software module	Description	Console name
TRITON Unified Security Center	Manages configuration and settings common to all modules. Provides centralized access to consoles.	TRITON Unified Security Center
Websense Web Security	Uses policies to filter Internet requests from clients.	TRITON - Web Security
Network Agent	Internet traffic sniffer. Enforces filtering for protocols other than HTTP, HTTPS, and FTP.	TRITON - Web Security
Websense Content Gateway	Includes proxy software and advanced analytics.	Content Gateway Manager
Websense Email Security Gateway	Filters inbound and outbound email messages.	TRITON - Email Security
Websense Data Security	Provides data loss prevention management.	TRITON - Data Security
Websense Mobile Security	A cloud-based service for Apple iOS mobile devices that provides remote device management features and protection against Web threats.	TRITON - Mobile Security

Managing appliances in TRITON Unified Security Center

Help | V-Series Appliance | Version 7.7.x

The TRITON Unified Security Center (TRITON console) provides a facility for managing Websense appliances in your network. Appliances that are part of your TRITON installation are registered automatically on the TRITON console **Appliances** > **Manage Appliances** page. Information for each appliance includes:

- C interface IP address
- Host name
- Security Mode (Web Security, Email Security, or both Web and Email Security)
- If Web Security is enabled, Policy source (Full, Limited, or Filtering Only)
- Software version (for example 7.7.0)
- Hardware platform (for example V5000, V10000, V10000 G2)
- Appliance description

See TRITON Unified Security Center online Help for complete details.

Accessing Appliance Manager and other consoles

Help | V-Series Appliance | Version 7.7.x

How you access Appliance Manager depends on how access has been configured in the TRITON console. There are 3 modes:

- If no special configuration has been performed, you can access Appliance Manager via a link on the **Manage Appliances** page in the TRITON console, or directly via the appliance's C interface IP address and port number (described below). You are prompted for credentials.
- If single sign-on is configured for you in the TRITON console, you can access Appliance Manager via the Single Sign-On button on the **Manage Appliances** page. You are not prompted for credentials. Alternatively, you can go direct to the C interface IP address and port number; you will be prompted for credentials.
- If two-factor authentication (certificate authentication) has been configured on TRITON console, you must also be configured with single sign-on privileges to access Appliance Manager. To get to the Appliance Manager, log on to the TRITON console using your two-factor authentication and then use the Single Sign-On button on the **Manage Appliances** page. Direct access via the C interface IP address is disabled when two-factor authentication is configured. See *Configuring two-factor authentication*.

For information about configuring single sign-on, see *Configuring an existing appliance for single sign-on* in TRITON console online Help.

Direct access

As stated above, if two-factor authentication is not configured, consoles can be accessed directly or through the TRITON console.

To launch a combined Logon Portal that offers access to Appliance Manager, Content Gateway Manager, and the TRITON Unified Security Center, go to:

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

To launch the TRITON Unified Security Center directly, go to:

```
https://<IP-address-of-TRITON-machine>:9443/triton/
```

To launch Content Gateway Manager directly, go to:

```
https://<IP-address-of-interface-C>:8081/
```

All consoles support the following browsers:

- Microsoft Internet Explorer 8 and 9
- Mozilla Firefox versions 5 and later
- Google Chrome 13 and later

Note

If you are using Internet Explorer, ensure that Enhanced Security Configuration is switched off.

If you are using Internet Explorer 8, Compatibility View is not supported.

When you log on to the TRITON console, you are taken to the Web Security module (TRITON - Web Security) by default. Select Email Security or Data Security from the TRITON toolbar to switch to another module.

If you are not using Websense Web Security solutions, you are taken directly to the Email Security or Data Security module at logon. Use the buttons in the TRITON toolbar to switch between modules.

Logging on to Appliance Manager

Help | V-Series Appliance | Version 7.7.x

If two-factor authentication is not configured, you can log on to the Appliance Manager by pointing a browser to the Logon Portal (described above), or by going directly to:

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

You can also log on to the Appliance Manager of any V-Series appliance registered with your TRITON Unified Security Center by clicking **Appliances** in the TRITON toolbar and clicking the Single Sign-On button, if configured, or the hyperlink IP address.

The user name is **admin**.

The password was set on your appliance when the **firstboot** script was run, or subsequently by an administrator.

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

Configuring two-factor authentication

Help | V-Series Appliance | Version 7.7.x

Two-factor authentication:

- Is configured for and applies to TRITON console log on.
- Requires administrators to perform certificate authentication to log on.
- Can be made to apply to Appliance Manager and Content Gateway Manager by forcing administrators to log on to TRITON console before accessing other consoles.
- Requires single sign-on to be configured for administrators allowed access to Appliance Manager and Content Gateway Manager.
- Requires that the password logon capability be **disabled** using an appliance command line interface command. This prevents administrators not configured for single sign-on from accessing the Appliance Manager and Content Gateway Manager.

Configuration is described in detail in *Configuring Certificate Authentication* in TRITON console online Help.

Disabling and enabling password logon

Help | V-Series Appliance | Version 7.7.x

Appliance Manager password logon can be disabled to permit only two-factor authentication or single sign-on access from the TRITON console.

To disable appliance password logon:

1. Set up single sign-on in the TRITON console.
2. If two-factor authentication will be used, set up two-factor authentication in the TRITON console.
3. Access the appliance Command Line Interface and log on with the admin credentials.
4. At the command line enter:

   ```
   password-logon disable
   ```

5. Log off and verify that direct log on is disabled by entering the IP address of the Logon Portal in your browser. The Logon Portal should not include links to Appliance Manager or Content Gateway Manager.

To re-enable password logon for all administrators:

1. Access the appliance Command Line Interface and log on with the admin credentials.
2. At the command line enter:

   ```
   password-logon enable
   ```

> **Note**
> If for some reason the appliance loses its registration with TRITON Unified Security Center, password login is automatically re-enabled.

Logs and reporting

Help | V-Series Appliance | Version 7.7.x

V-Series appliances keep detailed logs of activity on the system. These logs are designed to assist you and Websense Technical Support when there is unexpected behavior or a problem. For more information about V-Series logs, see *Logs*.

Modules on the V-Series by default generate detailed reporting records (usually called "log records") of module usage and actions. This requires installing a Windows-only reporting component (**Log Server** for Web Security and **Email Log Server** for Email Security) on another machine.

To add either Log Server component to your deployment:

- Download the TRITON software installer, available from www.mywebsense.com.
- Install Log Server on a Windows server with access to:
  - The Microsoft SQL Server instance that will host the Log Database
  - The appliance, so that it can retrieve filtering data from Web Security or Email Security components to create log records

Management reports based on filtering log records can be generated using the reporting tools included in the Web Security and Email Security modules of the TRITON Unified Security Center.

Depending on which appliance modules are active, TRITON - Web Security, TRITON - Email Security, or both may be pre-installed on the V-Series appliance. This is intended to help customers evaluate the available Websense solutions in a test environment. Websense, Inc., does not recommend using the pre-installed TRITON modules in a production environment.

Important

Except in rare cases in which only TRITON - Web Security is installed on an appliance and the network includes a small number of users, the TRITON Unified Security Center should be installed on a separate Windows Server 2008 R2 64-bit machine.

Web Security and Email Security reports

- When you launch TRITON - Web Security or Email Security, a dashboard shows the operating status of Websense software.
  - In TRITON - Web Security, the Threats dashboard provides information about advanced malware threat detection. Additional Risks, Usage, and System dashboards provide additional security tools, Internet activity monitoring, and system status information.
  - In TRITON - Email Security, the Today page shows current status, and can display charts of Web or email filtering activities in the network since midnight. The History page shows charts of Web or email filtering activities in the network for up to 30 days.
- **Presentation reports** provide customizable graphical and tabular reports of client Internet activity or message filtering activity.
- Websense Web Security **investigative reports** allow you to drill-down into your data to find the information of most interest to your organization.
- Websense Web Security **Real-Time Monitor** allows you to see what traffic is being analyzed by the Filtering Service instances associated with a Policy Server, and what action is applied to each request.

Databases used on V-Series appliances

Help | V-Series Appliance | Version 7.7.x

Websense software filters Internet and email activity based on your active policies **and** information stored in filtering databases that must be updated at regular intervals.

- The Websense Web Security **Master Database** contains URL category information and protocol definitions. It is managed by Filtering Service. Administrators can control how often the database is updated, and whether or not partial, real-time updates are applied between full updates, in TRITON - Web Security. (See The Websense Master Database for details.)

  A limited, initial version of the filtering database is pre-installed on the appliance, so that filtering can begin as soon as you enter a subscription key. Download the full Master Database as soon as possible to enable comprehensive Internet filtering capabilities. See the *V-Series Appliance Getting Started Guide* after you complete initial setup of the appliance.
- Websense Content Gateway scanning and categorization options rely on a set of databases installed with Websense software. The software checks for updates to these databases at a regular interval. Updates to these databases occur independently of all Master Database updates.

  Every time you restart the appliance or the Content Gateway module, a download of these small databases is initiated. If that download fails, a new download is attempted every 15 minutes until a successful download occurs.
- Websense Email Security Gateway email filtering uses a configurable set of antispam and antivirus databases. The software checks for updates to these databases at a regular interval. You can initiate updates manually from within TRITON - Email Security.
- When Websense Email Security Gateway is deployed with Websense Web Security, Email Security Gateway can also query the Web Security URL Master Database to get the category of URLs embedded in email content.

Navigating in Appliance Manager

Help | V-Series Appliance | Version 7.7.x

Appliance Manager opens showing the **Status > General** page in the content pane. The banner at the top of the page displays the appliance platform, Appliance Controller hostname, icons that indicate the security mode, and a Log Off button.

- To see another page, select an entry in the left navigation pane.
- To get a detailed explanation of the options on any page, go to **Help > Explain This Page**.

Appliance Manager offers access to the following pages:

Status

- *General system status*
- *CPU and memory status*
- *Disk use by module*
- *Network bandwidth*

Configuration

- *System configuration*
- *Network interface configuration*
- *Routing configuration*
- *Alerting*
- *Configuring Web Security components*

Administration

- Patches / Hotfixes – (*Patch management*, *Hotfix management*)
- Backup utility – (*Using the backup utility*)
- *Logs*
- *Toolbox*
- *Account management*

Clustering multiple Web Security Gateway appliances

Help | V-Series Appliance | Version 7.7.x

Content Gateway is the Web proxy component of Web Security Gateway. An important feature of Content Gateway is its ability to link together multiple instances of Content Gateway to form a *managed cluster*. This allows Web Security Gateway appliances to quickly scale to increase capacity and system performance while system administration remains simple and can be performed from a single cluster node. Management clustering is fully described in the Content Gateway online Help system.

To configure clustering, open Content Gateway Manager, click **Get Help!**, and select the **Clusters** topic from the **Contents** tab. If your are using **SSL Manager**, be sure to read the section on SSL clustering. Also be sure to read the section titled **Adding nodes to a cluster**. Fully familiarize yourself with the feature before enabling it. There are several essential requirements, including that all nodes must be on the same version of Content Gateway, and that clustering must be enabled on each node separately (although, once enabled, all can be administered on any node).

General system status

Help | V-Series Appliance | Version 7.7.x

The **Status > General** page displays first when you log on to Appliance Manager. It presents the current status of each software module on the appliance.

Use this page to:

- Check for system alerts, including information about new patches.
- Gauge resource use by each module, including:
  - How many CPUs are dedicated to the module.
  - How much memory (RAM) is allocated.
  - Which appliance interfaces are used by the module (for example, C, P1).
  - Which services (daemons), if any, are included in the module.
- Stop and start software services, or restart or disable an entire software module.
- Restart or shut down the appliance itself.

Important

For security purposes, an Appliance Manager session ends after 30 minutes of inactivity.

However, you can choose to monitor the **Status** pages even after the 30-minute timeout is reached. To do this, in the **Appliance Controller** section, mark the box labeled **Monitor status without timing out**. You are prompted to confirm your selection. Information on all **Status** pages then continues to update normally until you close the browser.

Modules on the V-Series may include:

- The **Appliance Controller** software operates behind the scenes. It manages appliance configuration, downloads and applies patches, accesses the backup utility, requests module restarts, initiates shutdowns, and handles other appliance management tasks.
- **Websense Content Gateway** contains the Websense proxy software and Web content scanning and analysis. Several services (daemons) comprise this software.
- **Websense Web Security** is the software that handles Web filtering. Several services (daemons) comprise this software.
- **Network Agent** is the Web Security component that monitors Internet traffic and filters non-HTTP protocols such as instant messaging.
- **Websense Email Security** is the software that handles email filtering. Several services (daemons) comprise this software.

The links and buttons on the page allow you to perform the following tasks:

Button or Link	Description
View Patch	Appears when an alert indicates that a new patch is available. Click the button to go to the **Administration > Patches / Hotfixes** page where you can view a list of available patches and access the patch management facility.
Restart Appliance	Causes this appliance to be rebooted. All modules are stopped. Modules are then restarted. Modules that are flagged as Disabled are not restarted.
Shutdown Appliance	Causes this appliance and all software modules to be shut down in an orderly fashion.
Restart Module (Websense Content Gateway)	Causes the Websense Content Gateway module on this appliance (all of its services) to be stopped and then restarted.
Launch (Content Gateway Manager)	Launches Content Gateway Manager. See *Management consoles*.
Stop Services Start Services (Websense Content Gateway)	Causes all proxy services and content analysis on this appliance to be stopped. Or, if services are stopped, Start Services causes all services to be started.
Restart Module (Websense Web Security)	Causes the Websense Web Security module on this appliance (all services in use) to be stopped and then restarted.
Launch (TRITON - Web Security)	Launches TRITON - Web Security. See *Management consoles*.
Stop Services Start Services (Websense Web Security)	Causes all Websense Web Security services running on this appliance to be stopped. [If this appliance is not designated to be the Full policy source for your network, some services may not be in use.] Or, if services are stopped, Start Services causes all services to be started.
Restart Module (Network Agent)	Causes the Network Agent service on this appliance to be stopped and then restarted.

Button or Link	Description
Disable Module Enable Module (Network Agent)	The Disable Module button for Network Agent displays only when Network Agent is provisioned and running on a Web Security Gateway or Web Security Gateway Anywhere appliance. Network Agent cannot be disabled on a Web Security (no Gateway) appliance. Clicking the Disable Module button causes the Disable Network Agent dialog box to display. The dialog offers 2 options: 1) permanently disable the module, or 2) temporarily disable the module. Not all deployments use Network Agent and disabling it redistributes system resources -- CPU and memory -- to other modules provisioned on the appliance. However, when Network Agent is permanently disabled, the appliance must be **re-imaged** in order to regain the ability to use Network Agent on the appliance. See *Re-enabling Network Agent if permanently disabled*. When Network Agent is temporarily disabled, a flag is set to indicate that Network Agent should be shut down on the appliance and not restarted the next time the appliance is restarted. **Note:** An important side effect of temporarily disabling Network Agent is that it must be re-enabled before changing the policy source, C interface IP address, or applying a patch. On average, it takes 10 minutes to re-enable Network Agent. When Network Agent is in the temporarily disabled state, both the Enable Module and Permanently Disable buttons display. For an introduction to the purpose of Network Agent, see *Network Agent Interface (N)*, page 25.
Stop Services Start Services (Network Agent)	Causes the Network Agent service on this appliance to be stopped. Or, if the service is stopped, Start Services causes the service to be started.
Restart Module (Websense Email Security Gateway)	Causes the Websense Email Security Gateway services on this appliance to be stopped and then restarted.
Stop Services Start Services (Websense Email Security Gateway)	Causes all Websense Email Security Gateway services running on this appliance to be stopped. Or, if services are stopped, Start Services causes all services to be started.

Disabling Network Agent

Help | V-Series Appliance | Version 7.7.x

The Network Agent **Disable Module** option is offered only when Network Agent is provisioned and running on a Web Security Gateway or Web Security Gateway Anywhere appliance. Network Agent cannot be disabled on a Web Security (no Gateway) appliance

When Network Agent is enabled, CPU and memory is allocated to it. If Network Agent is not used, those resources are unavailable to other modules on the appliance.

If you do not plan to use Network Agent, you can disable it, thereby reallocating its resources to other modules.

When disabling Network agent, you can disable it either temporarily or permanently.

When Network Agent is permanently disabled, the appliance must be **re-imaged** in order to regain the ability to use Network Agent on the appliance.

When Network Agent is temporarily disabled, a flag is set to indicate that Network Agent should be shut down and not restarted the next time the appliance is restarted. When the appliance is restarted, Network Agent resources are reallocated to other modules on the appliance.

Important

A side effect of temporarily disabling Network Agent is that it must be re-enabled before changing the policy source, C interface IP address, or applying a patch. On average, it takes 10 minutes to re-enable Network Agent.

When Network Agent is in the temporarily disabled state, both the Enable Module and Permanently Disable buttons display.

For an introduction to Network Agent, see *Network Agent Interface (N)*, page 25.

Re-enabling Network Agent if permanently disabled

Help | V-Series Appliance | Version 7.7.x

If Network Agent is permanently disabled and you want to re-enable it, you must re-image the appliance. This wipes the current system and restores the original, unconfigured system image. See *Restoring to factory image* in the V-Series Getting Started guide.

After re-imaging, you can apply patches and restore a full backup or module-level backups. If you restore a full backup, the backup must have been made when Network Agent was enabled, otherwise the restore will fail because the configured systems are incompatible.

CPU and memory status

Help | V-Series Appliance | Version 7.7.x

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

- **CPU Usage** displays:

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

Disk use by module

Help | V-Series Appliance | Version 7.7.x

The **Status > Disk Usage** page provides a summary of the previous 60 seconds of disk activity, as well as information about overall disk space availability, for each module on this appliance.

- **Disk Activity** shows average input/output operations per second (IOPS) and charts the previous 60 seconds of activity.
- **Usage Statistics** shows disk space used and available within the module.

The sections for the Appliance Controller, Websense Web Security, and Network Agent modules show one summary of information for all components within the module. This is represented as **system** disk activity or usage.

The section for the Websense Content Gateway module may also show information for cache and PreciseID disk activity and usage.

- The cache consists of a high-speed object database called the **object store**. The object store indexes objects according to URLs and associated headers, enabling Websense Content Gateway to store, retrieve, and serve Web pages, and also parts of Web pages, providing optimum bandwidth savings. If the cache disk fails, Websense Content Gateway goes into proxy-only mode (no caching).
- When Websense Content Gateway integrates with Websense Data Security, PreciseID Fingerprinting is used to detect sensitive information despite manipulation, reformatting, or other modification.

In addition to overall system information, the Email Security Gateway section also shows disk activity and usage information for MTA, the mail transfer agent responsible for sending, receiving, and directing email messages.

Network bandwidth

Help | V-Series Appliance | Version 7.7.x

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

- **Appliance Controller Interface** (C)
- **Websense Content Gateway Interface** (P1) or (P1 and E1)
- **Websense Content Gateway Interface** (P2) or (P2 and E2)
- **Network Agent Interface** (N)
- **Websense Email Security Gateway** (E1) or (E1 and P1)
- **Websense Email Security Gateway** (E2) or (E2 and P2)

Interfaces E1 and E2 are included on the V-10000 and V-10000 G2 models only. The disposition of P1, P2, E1 and E2 is dependent on the modules installed or the configuration applied. For information about configuring the interfaces, see *Network interface configuration*. The bandwidth display includes them only if they are enabled.

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

Inbound/Outbound

- current megabits per second, inbound and outbound, on the interface
- maximum bandwidth capacity in megabits per second

Bandwidth Statistics

- total megabits of data received and sent
- total number of packets received and sent
- packets dropped, inbound and outbound
- total errors, inbound and outbound
- rate in megabits per second, inbound and outbound

System watchdog

Help | V-Series Appliance | Version 7.7.x

V-Series appliances implement a system watchdog daemon to monitor critical system processes and conditions. Should one of the monitored processes or conditions fail or fault, the watchdog service performs a reset or restart.

Monitored processes and states include:

- Appliance kernel -- is the kernel active.

- Domain Agent -- is the Domain Agent running. This is an essential process that is responsible for communicating between the user interface and appliance back end processes.
- Journal Commit I/O -- detect a “journal commit I/O” error.
- File table -- detect a file table overflow condition.

Watchdog actions are recorded in the system log file, which can be viewed in the Appliance Manager on the **Administration > Logs** page.

2 Configuration

Help | V-Series Appliance | Version 7.7.x

Use the Configuration section of Appliance Manager to:

- Set the appliance time and date, host name, and description (see *System configuration*).
- Define the network interfaces for the appliance (see *Network interface configuration*). Depending on your model, this may include C, P1, P2, N, E1, and E2.
- Optionally specify static routes for the Content Gateway or Email Security module, or for the appliance itself (see *Routing configuration*).
- Set up SNMP alerting (see *Alerting*).
- Identify which computer is hosting filtering configuration and policies for the network (*Configuring Web Security components*).

System configuration

Help | V-Series Appliance | Version 7.7.x

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

- Review basic appliance information, including the current appliance hostname, security mode (Web security, Email security, or Web and Email security mode), version number, hardware platform, system date and time, and uptime.
- See which software modules are installed on the appliance and get their version numbers.

- Set the system **time and date**.

  Important

  If any Websense services are running, stop all Websense services before changing the time. Then, reset the time **and** make certain that the time is consistent across all servers running Websense services. Finally, restart Websense services.

  If you do not stop the services first, client updates and policy changes entered after the time reset are not saved.

  - Use the **Time zone** list to select the time zone to be used on this system.

    GMT (Greenwich Mean Time), the default, is also known as UTC (Universal Time, Coordinated). Other time zones are calculated by adding or subtracting from GMT. GMT is sometimes chosen to provide a common time stamp for geographically distributed systems.
  - Use the **Time and date** radio buttons to indicate how you want to set the date.

    Time is set and displayed using 24-hour notation.

    - To synchronize with an Internet Network Time Protocol (NTP) server (www.ntp.org.), select the **Automatically synchronize** option and enter the address of a primary NTP server. The secondary and tertiary fields are optional.

      Important

      If you synchronize the system clock with an NTP server, NTP protocol packets and their response packets must be allowed on any firewall or NAT device between the appliance and the NTP server. Ensure that you have outbound connectivity to the NTP servers. Add a firewall rule that allows outbound traffic to UDP port 123 for the NTP server.

      If interface C on this appliance is not connected to the Internet, then you must provide a way for interface C to reach an NTP server. One solution is to install an NTP server on the local network where interface C can reach it.
    - To set the time yourself, select the **Manually set** option and change the value in the Date and Time fields. Use the format indicated below the entry field.
  - Click **OK** to apply and save the changes.
- Set the appliance **hostname**, or system name (1 - 60 characters long).
  - The first character must be a letter.
  - Other characters can be letters, numbers, dashes, or periods.

- The name cannot end with a period.

Important

If this is a Web Security Gateway appliance and Content Gateway will be configured to perform Integrated Windows Authentication (IWA), the hostname cannot exceed 11 characters, excluding the domain name.

In addition, hostname should not be changed after the domain is joined. If it is changed, IWA will immediately stop working and will not work again until the domain is unjoined and then re-joined with the new hostname.

For more information, see the section titled *Integrated Windows Authentication* in Content Gateway Manager Help.

- Create or edit a unique **appliance description** to help you identify and manage the system, particularly when there are multiple appliances deployed in a cluster.

  The description is displayed in the appliance list in the TRITON Unified Security Center when the appliance is added there.

In each section that allows changes, **OK** saves and applies the new values. **Cancel** discards changes and restores entry field values to their current settings.

V-Series 7.7.0 support for IPv6

Help | V-Series Appliance | Version 7.7.x

Version 7.7 of TRITON Enterprise, including 7.7 V-Series appliances, provides incremental support for IPv6.

V-Series support is provided in combination with Web Security and Web Security Gateway (Anywhere).

IPv6 is not supported with Email Security Gateway.

Important

To use IPv6 with Web Security Gateway (Anywhere) the Content Gateway proxy must be configured as an **explicit proxy**. IPv6 is **not** supported in transparent proxy deployments.

For Web Security, IPv6 support includes:

- Dual IP stack implementation on interfaces C and N

- IPv6 traffic to the Internet or clients on interfaces C and N, including Block pages sent on C or N
- IPv6 static routes
- SNMP traps and counters for IPv6 data
- Network diagnostic tools in the Command Line Utility and Command Line Interface

For Web Security Gateway (Anywhere), support includes all of the above, plus:

- Dual IP stack implementation on interfaces P1 and P2
- Traffic to the Internet or clients on interfaces P1 and P2, and their bonded interface (E1/E2), if configured

Limits and restrictions:

- IPv6-only internal networks are not supported
- IPv4 must be used to communicate among V-Series appliances and with TRITON components

See TRITON – Web Security Help and Content Gateway Manager Help for detail pertinent to those components.

IPv6 configuration summary

Help | V-Series Appliance | Version 7.7.x

IPv6 support is disabled by default.

IPv6 is enabled in the Appliance Manager at the top of the **Configuration > Network Interfaces > IPv6** page. When it is enabled, all IPv6 support is enabled for all affected capabilities on the appliance.

In any field that accepts an IPv6 address, the address can be entered in any format that conforms with the standard. For example:

- Leading zeros within a 16-bit value may be omitted
- One group of consecutive zeros may be replaced with a double colon

Disabling IPv6 support requires a full restart of the appliance.

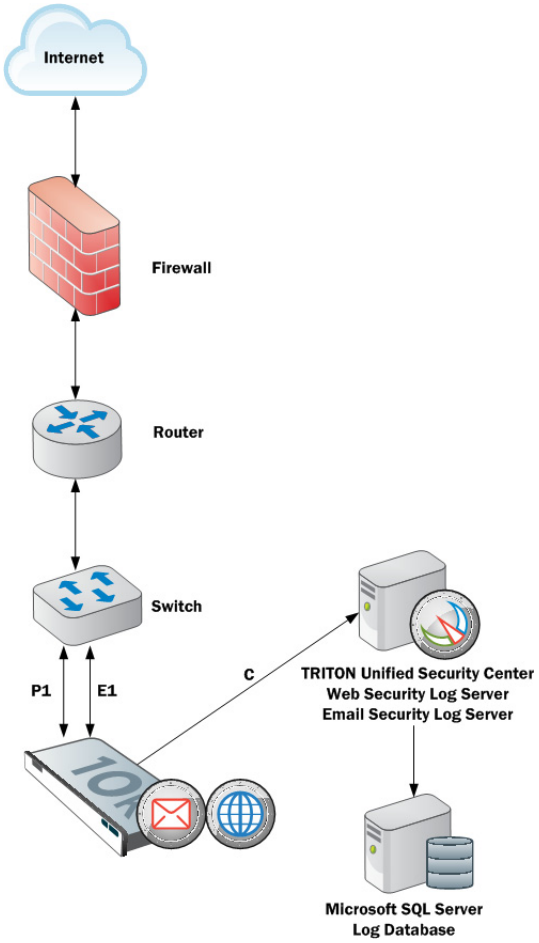
When IPv6 is disabled, IPv6 values remain in the configuration files, but are not editable.

Network interface configuration

Help | V-Series Appliance | Version 7.7.x

Use the **Configuration > Network Interfaces IPv4** and **IPv6** pages to specify the IP address, subnet mask, default gateway, and DNS addresses for each network interface on the appliance.

- *Appliance Controller Interface (C)*
- *Websense Content Gateway Interfaces (P1 and P2)*
- *Network Agent Interface (N)*
- *Email Security Gateway Interfaces (E1 and E2, or P1 and P2)*
- *Interface bonding*



Appliances with Web Security Gateway (Anywhere) support IPv6 addresses for C, P1, P2, and N.

Appliances with Email Security Gateway **do not** support IPv6 addresses for E1 and E2.

For more information about IPv6 support, see *V-Series 7.7.0 support for IPv6*.

Click **OK** to save and apply new values in each section.

Appliance Controller Interface (C)

Help | V-Series Appliance | Version 7.7.x

The Appliance Controller interface (C):

- Communicates with all Websense management interfaces
- Communicates with the Websense Data Security server
- Provides inter-appliance communication
- Transports (optionally) non-HTTP and non-HTTPS protocol enforcement
- Handles Websense Master Database downloads via the Internet (unless your site uses P1 for database downloads; for configuration information, go to www.websense.com/support and search for "V-Series Master Database download").

Initial configuration of the C interface is completed when the appliance is first powered on; a script called **firstboot** prompts you for the values needed to configure interface C.

Important

Changing the C interface IP address significantly impacts the deployment and may require reinstallation of some components.

If your appliance is in production and you need to change the C interface IP address, see *Changing the C interface IP address*, page 30.

To enable the C interface IP address entry field, place the mouse pointer over the iHelp icon and click "Enable IP field" in the pop-up.

Guidelines for configuring network interface C

IP address (C interface)	Required. This interface typically requires continual access to the Internet, though some sites use P1 for all communication with the Internet. If you change the IP address of the C interface, the update process may take about 10 minutes. After the IP address is changed, you are redirected to a logon page. Enter your user name and password. The **Status > General** page will show that the services are starting up. Wait for all services to start.
Subnet mask (C)	Required.
Default gateway (C)	Optional. IP address of the router that allows traffic to be routed outside of the subnet.

Primary DNS (C)	Required. IP address of the domain name server.
Secondary DNS (C)	Optional. Serves as a backup in case the primary DNS is unavailable.
Tertiary DNS (C)	Optional. Serves as a backup in case the primary and secondary DNSes are unavailable.

Websense Content Gateway Interfaces (P1 and P2)

Help | V-Series Appliance | Version 7.7.x

The Websense Content Gateway Interfaces (P1 and P2) handle traffic directed to and from the Websense Content Gateway proxy module.

- Both the P1 and P2 proxy interfaces can be used to accept users' Internet requests (inbound traffic) and communicate with Web servers (outbound traffic). In other words, both interfaces can be configured to handle traffic into and out of the proxy module.
- A typical configuration is to use P1 for both inbound and outbound traffic; P2 is not used.
- Another option is to configure P1 to accept users' Internet requests (inbound only). In this case, P2 is configured to communicate with Web servers (outbound).

Important

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 the General tab of the **Configure > Networking > WCCP** page).

Guidelines for configuring network interfaces P1 and P2

General guideline	If you use both P1 and P2, they must be located in the same subnet. The default gateway is automatically assigned to P2 (which is bound to eth1). Ensure that outbound packets can reach the Internet.
IP address (P1 or P2 interface)	Required.
Subnet mask	Required.

Default gateway	Required. The gateway must be in the same subnet as the IP address of the interface (P1 or P2) used for communicating with the Internet (outbound traffic). If you use both P1 and P2, they must be located in the same subnet. The default gateway is automatically assigned to P2 (which is bound to eth1). Ensure that outbound packets can reach the Internet.
Primary DNS	Required. IP address of the domain name server.
Secondary DNS	Optional. Serves as a backup in case the primary DNS is unavailable.
Tertiary DNS	Optional. Serves as a backup in case the primary and secondary DNSes are unavailable.

Network Agent Interface (N)

Help | V-Series Appliance | Version 7.7.x

Network Agent is a software component used to filter protocols other than HTTP and HTTPS. It provides bandwidth optimization data and enhanced logging detail.

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

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

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

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

Guidelines for configuring network interface N

Select an interface to use to send blocking information for non-HTTP and HTTPS traffic	• Select **Interface C** only if you want to use interface C to send blocking information. • Select **Interface N** if network interface N is connected to a bidirectional span port, and you want to use N to transport blocking information. Blocking NIC settings configured in TRITON - Web Security do not override the settings you enter in this pane. The settings in Appliance Manager take precedence.
IP address of interface N	Required. Network Agent should be able to see the outbound and inbound traffic in your network. Network Agent ignores ports 80, 443, 8070, and 8080.
Subnet mask	Required if interface N is selected. Otherwise the subnet mask has a fixed value of 255.255.255.255.
Default gateway	Required if Interface N is checked. Otherwise, the field is disabled.
Primary DNS	Required. IP address of the domain name server.
Secondary DNS	Optional. Serves as a backup in case the primary DNS is unavailable.
Tertiary DNS	Optional. Serves as a backup in case the primary and secondary DNSes are unavailable.

Network Agent can instead be installed on a different server in the network. See the *V-Series Appliance Getting Started Guide* for requirements.

Email Security Gateway Interfaces (E1 and E2, or P1 and P2)

Help | V-Series Appliance | Version 7.7.x

Websense Email Security Gateway Interfaces handle traffic into and out of the Websense Email Security Gateway module.

Note

The names of the interfaces vary depending on the model of V-Series appliance.

- On V10000 G2, E1 and E2 are used.
- On V5000 G2, P1 and P2 are used.

- Both the E1 and E2 interfaces can be used to accept inbound traffic and send outbound traffic. On V5000 G2, use P1 and P2.

- A typical configuration is to use E1 (P1) for both inbound and outbound traffic; E2 (P2) is not used.
- Another option is to configure E1 (P1) to accept inbound and E2 (P2) to send outbound traffic.
- When you need to support a large volume of outbound traffic, you can configure virtual interfaces on E1 or E2 (P1 or P2). See *Email Security virtual interfaces*, page 28.

Important

On the V10000 G2, if you use the E2 interface, the E1 interface is bound to eth0, and the E2 interface is bound to eth1. Keep this in mind when you configure Websense Email Security Gateway.

On the V5000 G2, 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 Email Security Gateway.

Guidelines for configuring network interfaces E1 and E2

Note

On a V5000 G2 substitute P1 for E1 and P2 for E2.

If you use both E1 and E2, and you locate them in the same subnet, then the default gateway is automatically assigned to E2 (which is bound to eth1). Ensure that outbound packets can reach the Internet.

IP address (E1 or E2 interface)	Required.
Subnet mask	Required.
Default gateway	Required. The gateway must be in the same subnet as the IP address of the interface (E1 or E2) used for communicating with the Internet (outbound traffic). If you use both E1 and E2, and you locate them in the same subnet, then the default gateway is automatically assigned to E2 (which is bound to eth1). Ensure that outbound packets can reach the Internet.
Primary DNS	Required. IP address of the domain name server.

Secondary DNS	Optional. Serves as a backup in case the primary DNS is unavailable.
Tertiary DNS	Optional. Serves as a backup in case the primary and secondary DNSes are unavailable.

Email Security virtual interfaces

Help | V-Series Appliance | Version 7.7.x

Multiple virtual IP addresses can be configured on E1 or E2.

- Virtual IP addresses are used for outbound traffic only.
- Virtual IP addresses are bound to the specified physical interface.
- Virtual IP addresses must be in the same subnet as the specified physical interface.
- A maximum of 10 virtual IP addresses can be specified for each physical interface (E1 and E2).

Multiple virtual interfaces can be helpful to support multiple domains and/or a large volume of outbound traffic.

To add virtual IP addresses to E1 or E2:

1. Go to **Configure > Network Interfaces > Virtual Interfaces** and click **Add**.
2. Select E1 or E2. If E2 has not been configured, it is not offered.
3. In the Virtual IP address entry field enter one IPv4 address per line.
4. Click **Add Interfaces**.

To remove virtual IP addresses:

1. On the **Configure > Network Interfaces > Virtual Interfaces** page, select the check box to the left of the entries you want to remove and then click **Delete**.
2. Confirm your action.

Interface bonding

Help | V-Series Appliance | Version 7.7.x

V10000 appliances (Websense Web Security only) and V10000 G2 appliances that run one module only—Websense Web Security **or** Websense Email Security Gateway—can bond interfaces for failover or load balancing. Configuration details are provided below.

Interface bonding is not supported on V5000 G2 appliances.

Important

Do **not** bond interfaces that have different speeds or duplex modes. Doing so can result in performance problems.

V10000/V10000 G2 with Websense Web Security only

Interfaces E1 and E2 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 the switch or router that is directly connected to the V10000/ V10000 G2 supports load balancing (etherchannel, trunk group, or similar), then traffic to and from the primary interface can be 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.

If you do bond an interface (P1 or P2), choose one mode for that bonding (either active/standby or load balancing). You do not have to choose the same bonding mode for both.

Ensure that all interfaces are cabled properly before bonding.

V10000 G2 with Websense Email Security Gateway only

Interfaces P1 and P2 can be cabled to your network and then bonded through software settings to a Websense Email Security Gateway interface, with P1 optionally bonded to E1, and P2 optionally bonded to E2. No other pairing is possible.

Interface bonding provides these alternatives:

- Active/Standby mode: E1 (or E2) is active, and P1 (or P2) is in standby mode. Only if the primary interface fails would its bonded interface (P1 or P2) become active.
- Load balancing: If the switch or router that is directly connected to the V10000/ V10000 G2 supports load balancing (etherchannel, trunk group, or similar), then traffic to and from the primary interface can be balanced between the primary interface and its bonded interface (P1 or P2).

You can choose to bond or not bond each Websense Email Security Gateway interface (E1 and E2) independently. You do not have to bond at all.

If you do bond an interface (E1 or E2), choose one mode for that bonding (either active/standby or load balancing). You do not have to choose the same bonding mode for both.

Ensure that all interfaces are cabled properly before bonding.

Changing the C interface IP address

Help | V-Series Appliance | Version 7.7.x

Sometimes it is necessary to change the C interface IP address. What is affected and what must be done depends on the configuration of your appliances and the details of your deployment. **The number of activities that must be performed and the service disruption can be significant. If possible, retain the current C interface IP address.**

In most cases, off-box components that depend on or directly service an appliance should be uninstalled prior to changing the C interface IP address and reinstalled after the IP address change is complete. These components include:

- Off-box TRITON Unified Security Center
- Filtering Service
- Network Agent
- Real Time Monitor
- DC Agent
- Logon Agent
- eDirectory Agent
- Radius Agent
- Remote Filtering Service
- Sync Service
- Linking Service

Important

It is strongly recommended that you back up your appliance and affected off-box components before making any changes.

Follow the steps in the scenario below that matches your deployment.

Scenario 1: One appliance, Web Security only with on-box TRITON Unified Security Center and off-box Log Server

Scenario 2: One appliance, Web Security only with off-box TRITON Unified Security Center and off-box Log Server

Scenario 3: One or many appliances, Email Security Gateway only with off-box TRITON Unified Security Center and off-box Log Server

Scenario 1: One appliance, Web Security only with on-box TRITON Unified Security Center and off-box Log Server

This configuration is for small deployments and Proof of Concept projects.

Summary of steps:

1. If Web DLP is configured, unregister Content Gateway with the Data Security Management Server.
2. On the Log Server host, stop the Log Server service.
3. On the appliance, change the C interface IP address.
4. On the Log Server host, change the IP address of the Policy Server entry in websense.ini to the new C interface IP address and restart Log Server.
5. If Web DLP is used, in Content Gateway Manager manually re-register with the Data Security Management Server.

For detailed step-by-step instructions, go to the Websense Technical Library and search for the article titled *Changing the C interface IP address: step-by-step*.

Scenario 2: One appliance, Web Security only with off-box TRITON Unified Security Center and off-box Log Server

Summary of steps:

1. If Web DLP is configured, unregister Content Gateway with the Data Security Management Server.
2. On the Log Server host, stop the Log Server service.
3. On the TRITON Unified Security Center host, uninstall TRITON Unified Security Center and associated components (see the component list, above). Make a list of uninstalled components.
4. On the appliance, change the C interface IP address.
5. Reinstall TRITON Unified Security Center and associated components.
6. On the Log Server host, change the IP address of the Policy Server entry in websense.ini to the new C interface IP address and restart Log Server.
7. If Web DLP is used, restart the Content Gateway module to automatically re-register with the Data Security Management Server.

For detailed step-by-step instructions, go to the Websense Technical Library and search for the article titled *Changing the C interface IP address: step-by-step*.

Scenario 3: One or many appliances, Email Security Gateway only with off-box TRITON Unified Security Center and off-box Log Server

Summary of steps:

1. If Email DLP is used, unregister Email DLP.
2. On the appliance, change the C interface IP address.
3. In TRITON - Email Security, change the appliance IP address to the new value.
4. If Email DLP is used, re-register Email DLP.

For detailed step-by-step instructions, go to the Websense Technical Library and search for the article titled *Changing the C interface IP address: step-by-step*.

Scenario 4: One appliance, Web Security and Email Security with off-box TRITON Unified Security Center and off-box log servers

Summary of steps:

1. If Web DLP is used, unregister Content Gateway with the Data Security Management Server.
2. If Email DLP is used, unregister Email DLP with the Data Security Management Server.
3. On the Log Server host, stop the Log Server and Email Log Server services.
4. On the TRITON Unified Security Center host, uninstall TRITON Unified Security Center and associated components (see the component list, above). Make a list of uninstalled components.
5. On the appliance, change the C interface IP address.
6. Reinstall TRITON Unified Security Center and associated components.
7. On the Log Server host, change the IP address of the Policy Server entry in websense.ini to the new C interface IP address and restart Log Server.
8. In TRITON - Email Security, change the appliance IP address to the new value.
9. If Email DLP is used, re-register with Data Security Management Server.
10. If Web DLP is used, restart the Content Gateway module to automatically re-register with the Data Security Management Server.

For detailed step-by-step instructions, go to the Websense Technical Library and search for the article titled *Changing the C interface IP address: step-by-step*.

Scenario 5: Multiple appliances in a cluster, Web Security only, off-box TRITON Unified Security Center and off-box Log Server

Covered under this scenario:

1. Changing the C interface of the Full policy source appliance
2. Changing the C interface of User directory and filtering appliances
3. Changing the C interface of Filtering only appliances

Summary steps for changing the C interface of the Full policy source appliance:

1. If Web DLP is configured, unregister Content Gateway with the Data Security Management Server.
2. On the Log Server host, stop the Log Server service.
3. On the TRITON Unified Security Center host, uninstall TRITON Unified Security Center and associated components (see the component list, above). Make a list of uninstalled components.
4. Document the Policy Source settings of all appliances in the cluster and then on the User directory and filtering and Filtering only appliances change the policy source setting to Full policy source.
5. On the original Full policy source appliance, change the C interface IP address.
6. On each of the User directory and filtering and Filtering only appliances, change the policy source setting from Full policy source to the original setting, pointing the appliance to the new Full policy source C interface IP address.
7. Reinstall TRITON Unified Security Center and associated components.
8. On the Log Server host, change the IP address of the Policy Server entry in websense.ini to the new C interface IP address and restart Log Server.
9. If Web DLP is used, restart the Content Gateway module to automatically re-register with the Data Security Management Server.

Summary steps for changing the C interface of the User directory and filtering appliance:

1. Uninstall off-box components that are registered to the User directory and filtering appliance whose C interface IP address will change (e.g. Network Agent).
2. Temporarily make Filtering only appliances that depend on the User directory and filtering appliance whose C interface IP address will change, Full policy source appliances.
3. Change the C interface IP address of the User directory and filtering appliance.
4. Return the policy source setting of the Filtering only appliance, pointing them to the new User directory and filtering C interface IP address.
5. Reinstall off-box components that are registered to the User directory and filtering appliance.

Summary steps for changing the C interface of the Filtering only appliance:

1. Uninstall off-box components that are registered to the Filtering only appliance whose C interface IP address will change (e.g. Network Agent).
2. Change the C interface IP address.
3. Reinstall off-box components that are registered to the Filtering only appliance.

For detailed step-by-step instructions, go to the Websense Technical Library and search for the article titled *Changing the C interface IP address: step-by-step*.

Scenario 6: Multiple appliances in a cluster, Web Security only,

off-box Policy Broker, off-box TRITON Unified Security Center and off-box Log Server

> **Note**
> No appliance is set to Full policy source.

Summary of steps:

1. If Web DLP is configured, unregister Content Gateway with the Data Security Management Server.
2. Uninstall off-box components that are registered to the appliance(s) whose C interface IP address will change (e.g. Network Agent).
3. Document the Policy Source settings of all appliances in the cluster and then change the policy source setting of each to Full policy source.
4. Change the C interface IP address (or addresses, if more than one appliance must change).
5. Return the policy source settings of the appliances to their original mode, pointing them to the new C interface IP address of a changed appliance if appropriate (if the appliance is a Filtering only appliance and the C interface change was to the User directory and filtering appliance it pointed to).
6. Reinstall off-box components that are registered to appliances in the cluster.
7. If Web DLP is used, restart the Content Gateway module to automatically re-register with the Data Security Management Server.

For detailed step-by-step instructions, go to the Websense Technical Library and search for the article titled *Changing the C interface IP address: step-by-step*.

Routing configuration

Help | V-Series Appliance | Version 7.7.x

Use the **Configuration > Routing** page to specify:

- Static routes from subnets and client computers through any active appliance interface, except N. If IPv6 is enabled, static IPv6 routes can also be added and imported.
- Module routes from appliance modules through appliance interface C to subnets. IPv6 module routes are **not** supported.

Configuring static routes

- Static routes can be specified for any active interface on the appliance, except N, which is dedicated to Network Agent and cannot be routed.

- The same route cannot be added for 2 different interfaces on the same module. If attempted, the appliance displays an error.
- Static routes that are defined for an interface that is later made inactive remain in the routing table, and are displayed in gray to indicate that the routes are inactive.
- Static routes that become invalid because the IP address of the interface changes are disabled and displayed in red.
- Static routes can be added and deleted, but not modified. To modify a route, delete it and add a new route specifying the new values.
- When a static route is added, imported, or deleted, the services associated with the module that manage the specified interface must be restarted. For example, if static routes are added to interface P1, when the additions are complete, all Content Gateway services must be restarted.
- The static route table has a maximum limit of 5000 entries.

Adding static routes

Static routes can be added one at a time, or many at time using an import file.

When a static route is added, data entered in each field is validated by the appliance, and an error message is displayed if there is an inconsistency in the route.

To add static routes:

1. Go to the **Configuration > Routing** page, select the IPv4 or IPv6 tab, and click **Add/Import** under **Static Routes**.
2. **To manually add a single route**, select the **Add individual route** radio button, enter values for all fields, and then click **Add Route**.

Destination Network	Required. Specify the subnet IP address for which traffic will be routed.
Subnet Mask (IPv4) or Subnet prefix length (IPv6)	Required. The subnet mask or prefix for the network where the clients reside (such as 255.255.0.0, or 64)
Gateway	Required. IP address providing access from the proxy subnet to the client subnet. This address must be on the same subnet as the appliance.
Interface	Required. The appliance interface to be used for the static route. Only active interfaces are offered in the drop down list.

3. **To add multiple routes using an import list file**:
   a. Prepare the import file. See **Import file specifications**, below.
   b. Select the **Import route file** radio button.
   c. Specify the full path and file name, or **Browse** to locate the file. Click **Import Route** to import the routes specified in the file.

The appliance reads the file, validates each route, and reports errors for lines that are invalid.

Duplicate route entries are ignored; duplicate entries are not created.

If the number of routes in the file, combined with the number of existing routes exceeds the 5000 route table limit, the import fails. No routes are added and an error message displays.

Import file specifications:

1. The file must be a plain text file. (Most routers export route tables to a plain text file.)
2. The file can contain comment lines. Comment lines begin with "#".
3. A line that defines a route must include the following 4 fields in the order shown. Each field must be separated by a space.

   For IPv4:

   ```
   destination netmask default-gateway interface
   ```

   Destination is a subnet address or host IP address.

   Netmask determines the proper value of *destination*.

   Default-gateway is the next hop.

   Interface is the appliance interface through which traffic is routed. The specified interface must be enabled. If it is disabled, the appliance reports an error and does not add the route.

   For IPv6:

   ```
   destination prefix-length default-gateway interface
   ```

   Destination is a subnet address or host IP address.

   Prefix-length determines the proper value of *destination*.

   Default-gateway is the next hop.

   Interface is the appliance interface through which traffic is routed. The specified interface must be enabled. If it is disabled, the appliance reports an error and does not add the route.

Deleting static routes

1. In the Static Routes table, select the routes to be deleted:
   - To select 1 route, click the box to the left of the entry you want to delete.
   - To select multiple entries, click the box to the left of each entry you want to delete.
   - To delete all routes, click the box to the left of the label **Destination Network**.
2. Click **Delete**.

Exporting the route table

To export the route table to a text file, click **Export Table**. Use the Browse dialog to specify a location and name for the file.

All routes in the table, whether enabled or disabled, are exported.

The file is formatted as described above for import files.

Configuring module routes

In some deployments it is necessary or desirable to route some Web Security or Email Security traffic through the appliance C interface (typically Web and email traffic is routed through separate, dedicated interfaces (P1/P2, E1/E2) and C is reserved for management traffic). However, some sites might want to route authentication (or other) traffic through the C interface. This is accomplished by defining module routes on the **Configuration > Routing** page.

The module route table has a maximum limit of 5000 entries.

Adding a module route

1. In the Module Route section of the **Configuration > Routing** page, click **Add**.
2. Specify a value for each field and click **Add Route**.

Module	Required. Select a module from the drop down list. The list displays only modules installed on the appliance. The Network Agent module may be installed, but will not appear in the list.
Destination subnet	Required. Specify the subnet IP address for which traffic will be routed.
Subnet mask	Required. The subnet mask for the destination subnet.

Note

It is the responsibility of the administrator to verify that the endpoint is available on the subnet.

Deleting a module route

1. In the Module Routes section, select the routes to be deleted.
   - To select 1 route, click the box to the left of the entry you want to delete.
   - To select multiple entries, click the box to the left of each entry you want to delete.
   - To delete all routes, click the box to the left of the label **Module**.
2. Click **Delete**.

Alerting

Help | V-Series Appliance | Version 7.7.x

Use the **Configuration > Alerting** page to enable and configure SNMP alerting.

There are 2 methods of SNMP alerting that you can enable on the **Setup** tab:

- Allow your SNMP manager to poll the appliance for standard SNMP counters (see *Enable SNMP polling (monitoring)*).
- Configure the appliance to send SNMP traps for selected events to your SNMP manager (see *Enable SNMP traps*).

  After enabling the SNMP trap server on the appliance, use the **Alerts** tab to configure which events cause a trap to be sent. See *Enable specific alerts*, page 39.

Enable SNMP polling (monitoring)

1. Under Monitoring Server, click **On**.
2. Select the **SNMP version** (v1, v2c, or v3) used in your network.
   - With SNMP v1 and v2c, a suffix (-wcg, -wws, -na, or -esg) is appended to the community name to indicate the originating module for the counter.
   - With SNMP v3, you can specify the context name (WCG, WWS, NA, or ESG) to poll counters for each module.
3. If you selected v1 or v2c, provide the **Community name** for the appliance, and then click **OK**.

   You have completed your SNMP monitoring configuration.
4. If you selected v3, select the **Security level** (None, Authentication only, or Authentication and Encryption) used in your network, and the **User name** to associate with SNMP communication.
5. If you selected a security level that includes authentication, also enter and confirm the **Password** for the selected user name, then select the **Authentication protocol** (MD5 or SHA).
6. If you selected authentication and encryption, select the **Encryption protocol** (DES or AES), and then enter and confirm the **Encryption key** used for encryption.
7. Click **OK** to implement your changes.

Enable SNMP traps

Before enabling the appliance to send SNMP traps, download the **appliance MIB file** using the link in the Trap Server section of the **Configuration > Alerting** page. The MIB file must be installed in your SNMP manager before it can interpret traps sent by the appliance.

When you are ready for the appliance to start sending SNMP traps:

1. Under Trap Server, click **On**, and then select the SNMP version (v1, v2c, or v3) used in your network.
2. For SNMP v1 or v2c, provide the following information:
   - The **Community name** to associate with traps sent by the appliance

- The IP address and port used by your SNMP manager.

3. To verify your configuration, click **Send Test Trap**. If the test trap succeeds, click **OK** to apply and save your changes. See *Enable specific alerts*, page 39, to configure which events cause a trap to be sent.

   If there is a problem sending the test trap, verify the community name, IP address, and port, and make sure that the network allows communication between the appliance C interface and the SNMP manager.
4. For SNMP v3, enter the **Engine ID** and **IP address** of your SNMP manager, as well as the **Port** used for SNMP communication.
5. Select the **Security level** (None, Authentication only, or Authentication and Encryption) used in your network, and the **User name** to associate with SNMP communication.
6. If you selected a security level that includes authentication, enter the **Password** for the selected user name, and then select the **Authentication protocol** (MD5 or SHA).
7. If you selected authentication and encryption, select the **Encryption protocol** (DES or AES), and then enter the **Encryption key** used for encryption.
8. To verify your configuration, click **Send Test Trap**. If the test trap succeeds, click **OK** to implement your changes. See *Enable specific alerts*, page 39, to configure which events cause a trap to be sent.

   If there is a problem sending the test trap, verify the engine ID and authentication settings and values, and verify that the network allows communication between the appliance and the SNMP manager.

Enable specific alerts

Help | V-Series Appliance | Version 7.7.x

The appliance can send traps for each of its modules: Appliance Controller, Websense Content Gateway, Websense Web Security, Network Agent, and Email Security Gateway. The Alerts tab of the **Configuration > Alerting** page lists the alerts associated with only the modules that you have enabled.

A table for each module lists:

- The hardware or software **Event** that triggers the alert (for example, a network interface link going down or coming up, or a Websense service stopping).
- The **Threshold**, if applicable, that defines the alert condition (for example, CPU usage exceeding 90%, or free disk space reaching less than 10% of the total disk size).
- The **Type** of alert (system resource or operational event).
- Whether or not an SNMP trap is sent when the event occurs or the threshold is reached.

To enable all alerts for a module, select the check box next to **SNMP** in the table header. All check boxes in the column are selected.

Otherwise, mark the check box next to an event name to enable SNMP alerts for that event. To disable alerts for an event, clear the associated check box.

Time-based thresholds: Most of the events that have a configurable threshold also have a configurable time-based threshold, specified in minutes. When the time-based threshold is set and **both thresholds** are exceeded, an alert is sent. To enable time-based thresholds, select the **Enable time-based thresholds** check box at the top of the page. The time-based threshold is enabled on every event for which it is configurable.

Event-cleared alerts: In addition to generating event condition alerts, you can configure alerts to be sent when conditions return below the threshold. These are called **event-cleared alerts**. To enable event-cleared alerts, select the **Generate event-cleared alerts** check box at the top of the page.

The following events do not generate event-cleared alerts:

- Hostname change
- IP address change
- Scheduled backup failure
- SNMP authentication failure

When you have finished configuring alerts, click **OK** to implement the changes.

Configuring Web Security components

Help | V-Series Appliance | Version 7.7.x

Use the **Configuration > Web Security Components** page to specify which Web Security components are active on the appliance, and where the appliance gets Web Security global configuration and filtering policy information. Also define the TRITON - Web Security location.

1. Under **Policy Source**, select which Web Security configuration is used on this appliance: **Full policy source** (default; see *What is a policy source?*), **User directory and filtering**, or **Filtering only** (see *What if an appliance is not the policy source?*). If this is a Full policy source appliance, it acts as both the Policy Broker and a Policy Server. There can be only 1 Full policy source appliance in your network.
2. If this is a User directory and filtering appliance, it also acts as a Policy Server. Enter the IP address of the Policy Broker appliance or server.
3. If this is a Filtering only appliance, enter the IP address of a Policy Server. It does not have to be the IP address of the Policy Broker machine.
4. Click **OK** to save and apply your changes.

5. If this is a Websense Web Security or Websense Web Security Gateway only appliance running as a Full policy source, under **TRITON - Web Security**, specify whether to use the TRITON instance installed **On** the appliance, or whether to use an **Off**-appliance instance.

   Note
   When you upgrade from an earlier version of the appliance, your previous settings are preserved. If you do not have an off-appliance management console location already established, the system uses TRITON - Web Security on the policy source appliance by default.

   - If you are using Websense Data Security or Email Security Gateway in conjunction with Websense Web Security Gateway, the TRITON Unified Security Center must be installed on an Windows Server 2008 R2 64-bit machine.
   - Generally, the on-appliance installation of TRITON - Web Security is intended for evaluations and small deployments. Most production sites are advised to download the TRITON installer from mywebsense.com and install the TRITON console on a separate Windows server.

6. If you are moving from using an off-appliance TRITON - Web Security instance to using the on-appliance instance, make sure you have backed up your original TRITON console. Then expand **Import Configuration** and browse to the location of your backup file.

   This allows you to move much of your existing configuration and policy information to the appliance, rather than having to recreate your settings.

   As always, be sure to verify the configuration in the new TRITON console, because some settings may not be preserved during migration.

   Important
   The on-appliance instance is recommended only for proof of concept demonstrations and when the number of users is small and the traffic load is light. Otherwise, the TRITON console should remain on the Windows 2008 R2 server.

7. Click **OK** to save and apply your changes.

What is a policy source?

Help | V-Series Appliance | Version 7.7.x

Every Websense Web Security deployment must include a single **policy source**. This is an appliance or other server that hosts 2 components: Websense Policy Broker and Websense Policy Database. All other Websense appliances or other servers point to

this machine and receive regular updates from it. This appliance (or other server) is called the **policy source**.

- When a Websense Web Security Gateway only appliance is configured as a policy source, all available Websense Web Security components run on that appliance, including.
  - Filtering Service
  - Policy Database
  - Policy Broker
  - Policy Server
  - User Service
  - Directory Agent (required for hybrid service)
  - State Server (optional; disabled by default)
  - Multiplexer (disabled by default; unavailable when the appliance is Filtering only)
  - Usage Monitor
  - Control Service
  - TRITON - Web Security (appliance-based; optional)
    - Reports Information Service
    - Investigative Reports Scheduler
    - Manager Web Server
    - Reporting Web Server
    - Central Access
    - Unified Security Center
    - Settings Database
  - Websense Content Gateway module
  - Network Agent module (optional)

  Windows-only services, like Log Server, and optional services, like transparent identification agents, still run on other machines.
- When a policy source appliance runs in **Web and Email** security mode (hosting Websense Web Security Gateway and Email Security Gateway), the TRITON services are disabled by default and must be located on a Windows 2008 R2 server.
- A non-appliance policy source is a server hosting **Policy Broker**. The Policy Database is automatically created and run on the Policy Broker machine. This machine typically also includes a Policy Server instance, and may include additional Websense software components.

The Policy Database holds all filtering policies (including client definitions, filters, and filter components) for all appliances and all domains in the network. It also holds global configuration information that applies to the entire deployment.

What if an appliance is not the policy source?

A Websense V-Series appliance that is not serving as the policy source can be designated to run either **User directory and filtering** or **Filtering only**.

- A **User directory and filtering** appliance is a lightweight version of the policy source machine. It runs:
  - Policy Server
  - User Service
  - Usage Monitor
  - Filtering Service
  - Control Service
  - Directory Agent
  - Websense Content Gateway module
  - Network Agent module (optional)

  Having User Service and Policy Server on remote appliances means that you are able to obtain local network user names. Latency between User Service and Policy Server is eliminated, because both run on the same appliance.

  Whenever you make a policy change, that change is immediately updated on the policy source appliance. The change is pushed out to User directory and filtering appliances within 30 seconds.

  These appliances can continue filtering for as long as 14 days if their connection with the policy source machine is interrupted. So even if a network connection is poor or is lost, filtering continues as expected.

  A **User directory and filtering** appliance is configured to point to the Full policy source for updates.
- A **Filtering only** appliance does not run Policy Server. It runs only:
  - Filtering Service
  - Control Service
  - Websense Content Gateway module
  - Network Agent module (optional)

  A **Filtering only** appliance is configured to point to a Policy Server. This works best when the appliance is close to the Policy server and on the same network.

  These appliances require a continual connection to the centralized policy server, not only to stay current, but also to continue filtering. If the connection to the policy server becomes unavailable for any reason, filtering on a Filtering only appliance can continue for up to 3 hours.

  If the policy server machine is on a remote network, with a WAN connection, it can be difficult to obtain user name/IP address maps for the local users.

User directory with V-Series appliances

Help | V-Series Appliance | Version 7.7.x

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

Preparing for a hybrid configuration

In Web Security Gateway Anywhere environments, some users may be filtered by the hybrid (SaaS) service. In this situation, an interoperability component on the appliance called **Directory Agent** is required to enable user-, group-, and domain- (OU) based filtering.

Directory Agent must be able to communicate with:

- A supported LDAP-based directory service:
  - Windows Active Directory® (Mixed Mode)
  - Windows Active Directory (Native Mode®)
  - Oracle (Sun Java™) System Directory
  - Novell eDirectory
- Websense **Sync Service**

After deployment, use TRITON - Web Security to configure User Service and Directory Agent.

- User Service configuration is performed on the Settings > General > Directory Services page.
- Directory Agent configuration is performed on the Settings > Hybrid Configuration > Shared User Data page.
  - You can have multiple Directory Agent instances.
  - Each Directory Agent must use a unique, non-overlapping root context.
  - Each Directory Agent instance must be associated with a different Policy Server.
  - All Directory Agent instances must connect to a single Sync Service. (A deployment can have only one Sync Service instance.)
  - You must configure the Sync Service connection manually for all supplemental Directory Agent instances (these are the Directory Agents running on User Directory and filtering, and Filtering only appliances). Communication is configured automatically for the Directory Agent instance that connects to the same Policy Server as Sync Service. See the TRITON - Web Security Help for details.

You can configure Directory Agent to use a different root context than User Service, and to process its directory data differently than User Service. Also, with Windows Active Directory, if User Service is configured to communicate with multiple global catalog servers, Directory Agent can communicate with all of them.

Redundancy

Help | V-Series Appliance | Version 7.7.x

Internet usage filtering requires interaction between several Websense software components:

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

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

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

3 Administration

Help | V-Series Appliance | Version 7.7.x

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

As a best practice, create your MyWebsense account when you first set up the appliance, so that you can:

- Immediately apply any patches made available since your appliance was assembled.
- Get access whenever you need support or updates.

Administration options

Help | V-Series Appliance | Version 7.7.x

The Administration pages enable you to:

- Install software patches (see *Patch management*).
- Install software hotfixes (see *Hotfix management*).
- Prepare and restore backups of your appliance configuration, Web Security modules, and Email Security module (see *Using the backup utility*).
- Access system logs for all active modules (see *Logs*).
- Customize block pages, enable remote access to the appliance command-line interface, and launch the command-line utility (see *Toolbox*).
- Change the Appliance Manager or Content Gateway Manager **admin** password (see *Account management*).

Patch management

Help | V-Series Appliance | Version 7.7.x

V-Series appliances are kept up to date with an easy-to-use patch management facility.

Go to the **Administration > Patches / Hotfixes > Patches** page to check for, download, and install patches.

- Appliances automatically check for new patches once a day. The time of the check is randomized, cannot be configured, and is different for every appliance.
- To manually check for new patches, use the **Check for Patches** button.
- When a new patch is available, the patch version number, description, and status are displayed in the **Available patches** table and an alert is displayed on the **Status > General** page.
- After a patch is downloaded it can be copied to another location on your network where it can be easily uploaded to multiple appliances.
- If the appliance management interface (C) does not directly connect to the Internet, you can configure a proxy server through which the appliance checks for patches.
- The Patch History table provides a history of patches that have been applied to the appliance.

See:

Patch update options, page 47

Patch history, page 48

Best practices for appliance patches

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

Patch process for appliances

Patch discovery is performed automatically every 24 hours at a random time, or manually with the **Check for Patches** button.

Patch download and installation is initiated manually by the appliance administrator.

- Use the **Administration > Patches / Hotfixes** page to download and install each patch on the appliance, during a low-activity period on your network.
- Install patches in consecutive sequence.
- On the **Patches** page, the "Appliance current version" number is the current appliance version (reflects the latest patch installed).
- Be sure that all Websense modules running off the appliance, such as Log Server, are upgraded to the appropriate level each time you patch the appliance. See the patch release notes for details
- The online V-Series Compatibility Matrix shows a table of the Websense software module versions that are compatible with each appliance version.

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

Patch update options

Help | V-Series Appliance | Version 7.7.x

- Available patches are listed in the **Available patches** table.
- For each available patch, a version number, description, and status is given. There is also a link to the patch release notes.

Important

It is very important to read the release notes. In addition to a summary of changes contained in the patch, there is information about impacts to other modules and an estimate of the time it will take to apply the patch.

The following options are available:

Download	Click **Download** to start downloading an available patch. In the Status field, a progress bar displays the progress of the download. Another patch can be selected, and the download initiated, while the first download is underway. Such requests form a sequential download queue. When the patch download is complete: • The **Download** button is replaced by **Install** and **Delete** buttons. (See below.) • A **Save to network location** link is included after the patch description. Click the link to copy the patch file to another location on your network. This can be helpful if you have multiple appliances and do not want to download the patch from Websense separately for every appliance. Instead, on each appliance simply use the **Upload Patch Manually** function to upload the patch from the network location. It is recommended that patches be downloaded and applied in numeric sequence. In many cases, this is a requirement.
Pause	When a download is underway, a **Pause** button displays. Click **Pause** to temporarily halt the download.
Cancel	When a download is underway, a **Cancel** button displays. Click **Cancel** to end the download process.
Resume	When a patch download has been paused, a **Resume** button displays. Click **Resume** to continue a paused download.

Install	When a patch has been downloaded and verified (a checksum is performed as part of the download process), and is ready for installation, the **Install** button is enabled. **IMPORTANT:** Before installing a patch, it is important that you **read the patch release notes**. **IMPORTANT:** If Network Agent is temporarily disabled and you **do not** want to permanently disable it (which requires re-imaging the appliance to regain its use), you must re-enable Network Agent before installing the patch. See *Re-enabling Network Agent before installing a patch*, page 49. Click **Install** to install the patch. A series of pages prompt for confirmation and provide status. You are notified if a restart is required after installation. After the restart, the patch is removed from the patch queue and logged in the Patch History table. The new appliance version number is reflected in the **Appliance version** field. If an earlier patch has not been installed but is required, you receive a message in the **Status** column indicating which earlier patch is required, and the **Install** button for the dependent patch is disabled. Install the earlier patch first. If a patch installation fails, any installed files from that patch are immediately uninstalled and a message displays indicating that the patch installation failed. You can try installing it again. If that fails, delete the patch, then download it again and re-attempt the installation.
Delete	Click **Delete** if you want to delete a patch.
Check for Patches	Click the **Check for Patches** button to manually check for new patches.
Upload Patch Manually	Click **Upload Patch Manually** to upload a patch from another location on your network. This can be a convenient and efficient method of distributing a patch among multiple appliances in a cluster or where multiple appliances have access to a local network. For instructions on copying a patch file from an appliance to another location in the network, see the entry for **Download**, above.

Patch history

Help | V-Series Appliance | Version 7.7.x

The **Patch History** table on the **Administration > Patches / Hotfixes > Patches** page displays a list of all patches installed on the appliance. For each patch, you see:

- Version number
- Date and time of patch installation
- Comments that confirm the success or failure of patch installation
- A link to patch log file, showing patch details

Re-enabling Network Agent before installing a patch

Help | V-Series Appliance | Version 7.7.x

Follow these steps if Network Agent is temporarily disabled, you don't want to permanently disable it, and you want to install a patch. (For more information about temporarily and permanently disabling Network Agent, see *Disabling Network Agent*, page 12.

1. If you have initiated an installation on the **Patches** page, and the **Network Agent Disable** dialog box has displayed, and you **do not** want to permanently disable Network Agent, select **Cancel** to close the dialog box and then go to the **Status > General** page. In the **Network Agent** area, click **Enable Module** and then **OK** to confirm the action. The appliance automatically restarts.
2. If you have **not** initiated an installation on the **Patches** page, go to the **Status > General** page and in the **Network Agent** area click **Enable Module** and then **OK** to confirm the action. The appliance automatically restarts.
3. After the appliance has restarted, log on, go to the **Administration > Patch / Hotfixes > Patches** page, and perform the patch installation.
4. When the patch installation is complete, if you want to again temporarily disable Network Agent, return to the **Status > General** page and disable Network Agent.

The reason that Network Agent must be re-enabled prior to patch installation (if it is not permanently disabled) is that if Network Agent is stopped and the patch includes updates to Network Agent, the updates are not made to the stopped module and when it is re-enabled some time in the future it may be incompatible with other modules on the system.

Hotfix management

Help | V-Series Appliance | Version 7.7.x

Related topics:

- *Hotfix application process*, page 50
- *Hotfix installation*, page 51
- *Hotfix history*, page 52

When necessary, Websense, Inc. releases a targeted *hotfix* to address a specific issue in an appliance module. In most cases, you receive notification of hotfixes in a Websense Technical Alert email, or, in response to a specific problem that you have reported, a Technical Support Agent recommends a specific hotfix.

The Appliance Manager **Hotfixes** page is your facility for finding, installing, uninstalling, and maintaining a history of hotfix application.

Go to the **Administration > Patches / Hotfixes > Hotfixes** page to manage hotfixes.

- In the majority of cases, you are notified of hotfixes through:
  - A Websense Technical Alert email, or
  - A Websense Technical Support Agent. The Agent will provide the name of a specific hotfix to address the problem you reported.
- A hotfix may address an issue on any module running on your appliance.
- A hotfix should not be recommended to you for a module that you have not configured or are not running on your appliance.
- As a best practice, unless otherwise instructed by a Websense Technical Support Agent, do not install a hotfix for an issue that you have not run into.
- Hotfix names are constructed: *XXX*-#.#.#-###:

  For example: WCG-7.7.4-001
- The Hotfix facility will not install a hotfix that is not valid for the module versions on your appliance.
- A hotfix may have dependencies on one or more other hotfixes, in which case the hotfix facility will not allow the installation of the hotfix until after its dependents are installed.

Hotfix application process

Following is a summary. For complete details, see *Hotfix installation*.

1. In the **Hotfix Installation** area, enter the name of the hotfix and click **Find**. If the hotfix is not found, review the notification from Websense and check that the name is entered correctly. If the name repeatedly returns not found, contact Websense Technical Support.
2. When a hotfix is found, a pop-up displays that includes a description of the hotfix and other pertinent information. If the description is what you expect, click **Download** to download the hotfix to the appliance. Otherwise, click **Cancel**.
3. After the hotfix is downloaded, a description and status display in the **Downloaded hotfixes** table. Confirm that the hotfix has no dependencies and is ready for installation. If the hotfix is dependent on another hotfix, you must download and install that hotfix first.
4. Click **Install** to install the hotfix.

If you have several appliances and do not want to download the hotfix from Websense.com multiple times, you can use the **Save to network location** link to copy the downloaded hotfix to a convenient location on your network, and then, on each appliance, use the **Upload Hotfix Manually** button to upload the file to the appliance.

For procedural information, see:

Hotfix installation, page 51

Hotfix history, page 52

Hotfix installation

Help | V-Series Appliance | Version 7.7.x

Related topics:

- *Hotfix management*, page 49
- *Hotfix application process*, page 50
- *Hotfix history*, page 52

Use the Hotfix Installation area to:

- Search for and download a hotfix
- Install a hotfix
- Delete a hotfix that has not yet been installed
- Copy a hotfix to a network location
- Upload a hotfix from a network location

The following options are available:

Hotfix ID entry field	Specify the exact name of the hotfix to be searched for in the Websense.com hotfix repository. Inclusion of leading or trailing zeros is required. The format is: *XXX*-#.#.#-### For example: WCG-7.7.0-001
Find button	After the hotfix name has been entered, click **Find** to direct the Appliance Manager to go to Websense.com to search for the hotfix. If the hotfix is found, a **Hotfix Details** pop-up dialog box displays with a description of the hotfix, and a **Download** and **Cancel** button.
Downloaded hotfixes table	This tables maintains a complete list of hotfixes downloaded to the appliance but not yet installed. A record of installed hotfixes is maintained in the Hotfix History section.
Hotfix ID	The hotfix ID.

Description	A high-level description of the hotfix that usually includes: • The name • A short description of the problem that the hotfix addresses • The module the hotfix applies to • Relative severity (high, moderate, low) • The release date • A link to the official **Release notes** (hosted on Websense.com) • A **Save to network location** link that opens a dialog that allows you to save the hotfix to a location on your network.
Status	States whether the hotfix is ready for installation or has a dependency on another hotfix that must be installed first.
Action	Includes the **Install** button to initiate installation, and a **Delete** button to remove the hotfix from the appliance prior to installation. To uninstall and remove a hotfix, see the uninstall function that is accessed from the Hotfix History area.
Upload Hotfix Manually	Use this button to upload a hotfix from the appliance to a location on your network.

Hotfix history

Help | V-Series Appliance | Version 7.7.x

Related topics:

- *Hotfix management*, page 49
- *Hotfix application process*, page 50
- *Hotfix installation*, page 51

Use the Hotfix History section to:

- View the current appliance version
- View a record of installed hotfixes
- Uninstall hotfixes
- View a record of uninstalled hotfixes

The following options are available:

View drop down list	From the drop down list, select **Installed hotfixes** to populate the table with a list of hotfixes that have been installed, and that were attempted to be installed but failed. Select **Uninstalled hotfixes** to populate the table with a list of hotfixes that have been uninstalled, or were attempted to be uninstalled but failed.
When **Installed hotfixes** is selected from the **View** drop down list	
Radio button adjacent to the **Hotfix ID**	Select the radio button to activate the **Uninstall** button. If the hotfix has dependencies that prevent it from being uninstalled, a message is displayed below the table.
Hotfix ID	The hotfix ID.
Name	The name of the hotfix and a link to the Release Notes.
Module	The name of the effected appliance module.
Date Installed	The day and year that the hotfix was installed.
Status	Indication of whether the installation succeeded or failed. If the installation failed, a link is provided to the installation log file.
Uninstall button	Use this button to initiate uninstallation of the selected hotfix.
When **Uninstalled hotfixes** is selected from the **View** drop down list	
Hotfix ID	The name of the hotfix.
Reason	A reason that you provide for uninstalling the hotfix. It is easy to lose track of why a hotfix was uninstalled. Recording a clear description here can save repeated errors and lost time in the future.
Date Uninstalled	The day and year that the hotfix was uninstalled.
Status	Success or failure status of the uninstall action. Occasionally a hotfix may fail to uninstall. One reason may be that uninstallation is dependent on uninstalling another hotfix or set of hotfixes.

Patches and hotfixes proxy settings

Help | V-Series Appliance | Version 7.7.x

If the appliance management interface (C) does not directly connect to the Internet, you can configure a proxy server through which the appliance checks for patches and hotfixes.

Use proxy server	Select the check box to enable or disable the option.
Proxy IP address and port	Specify the IP address and port number of the proxy to be used.
User name/ password (optional)	Optionally, authenticate the proxy connection with a user name and password.
Test Connection	Click **Test Connection** to test the connection to the specified proxy.

Using the backup utility

Help | V-Series Appliance | Version 7.7.x

Related topics:

- *Scheduling backups*, page 55
- *Full appliance configuration backups*, page 56
- *Module configuration backups*, page 57
- *Restoring a backup file*, page 58

Use the Backup tab of the **Administration > Backup Utility** page to initiate configuration backups, schedule recurring backups, or manage existing backup files. To restore an appliance or module configuration from an existing backup file, click the Restore tab, and then see *Restoring a backup file*, page 58.

Two types of backup are available on the V-Series appliance:

- A **full appliance configuration** backup saves all appliance settings, as well as configuration and policy information for all active modules (for example, Web Security Gateway and Email Security Gateway). Websense, Inc., recommends running a full backup on every appliance in your network on a regular basis.

  Note that the full backup file may be smaller than the module backup files, because it is compressed.

- A **module configuration** backup (Web Security Configuration or Email Security Configuration) saves all configuration information for the selected module. This includes any client and policy data stored on the selected appliance.

> **Note**
> Module configuration backup does not include a Content Gateway option.
>
> Content Gateway only backups (snapshot) can be performed in Content Gateway Manager. Snapshots must be performed manually; there is no scheduling facility.

Backup types and backup status information are shown in the Perform Backup list. To start or schedule a backup, first select the backup type, and then click either **Run Backup Now** or **Configure Backup Schedule** (for information about scheduling backups, see *Scheduling backups*, page 55).

You must initially set up the backup function; it is not automatic. Once you schedule backups, however, those backups will continue to run at regular intervals without requiring further intervention. To stop a scheduled backup from recurring, click **Cancel Scheduled Backup**.

The Local Backup Files list shows all backup files stored on the current appliance. Select a backup type from the **View backups for** list to change the type of backup file shown.

Each entry in the list includes the following information:

- The date and time of the backup
- The name of the backup file

For full appliance configuration backup files, the following information is also included:

- The patch version of the appliance on which the backup was run. When you restore from a backup, the backup file must be the same version as the appliance you are restoring.
- The host name of the backup source.
- A comment on the policy information in each backup file.
  - **Email security mode** indicates a full backup of an Email Security Gateway appliance.
  - **Full policy source** (Web Security Gateway mode) or **Web (policy source) and Email Security** (Web and Email Security mode) is the default comment if the backup was generated on the policy source appliance.
  - **User directory and filtering** (Web Security Gateway mode) or **Web (user/filtering) and Email Security** (Web and Email Security mode) is the default comment if the backup was generated on an appliance configured to run Filtering Service and User Service.

- **Filtering only** (Web Security Gateway mode) or **Web (filtering only) and Email Security** (Web and Email Security mode) is the standard comment if the backup was generated on a Filtering only appliance.

Up to 20 appliance backup files and 20 backup files for each module can be stored on the appliance. When the twenty-first backup file is created, the oldest file is automatically deleted.

To download a backup file to another machine, click the file name, then browse to path where you want to save the file.

To delete local backup files manually, mark the checkbox next to the backup file name in the Local Backup Files list, and then click **Delete**.

Scheduling backups

Help | V-Series Appliance | Version 7.7.x

Related topics:

- *Using the backup utility*, page 53
- *Full appliance configuration backups*, page 56
- *Module configuration backups*, page 57
- *Restoring a backup file*, page 58

Use the **Backup Utility > Configure Backup Schedule** page to specify how frequently and at what time of day the selected backup type is performed, and to select a location for storing backup files. Schedule each applicable backup type (full appliance, Web Security, or Email Security) separately.

To schedule backups:

1. Select a **Backup frequency**: daily, weekly, or monthly.
   - For weekly backups, select which day of the week the backup is run.
   - For monthly backups, select which day of the month the backup is run. You cannot schedule backups to run on the 29th, 30th, or 31st day of the month, because not all months have those days.
2. Specify a **Start time** for the backup process. Ideally, select a time when the appliance is unlikely to be under heavy load.

   Enter the time in 24-hour format (where 00:00 indicates midnight, and 12:00 indicates noon).
3. Provide a **Storage location** for the backup files. Only one remote backup location can be configured for each backup type.
   - Select **Appliance** to have the file stored locally. A maximum of 20 backup files can be saved, and the backup file directory cannot be renamed, moved, or deleted.

Backup files saved to the appliance can be viewed on the Backup Utility page, under Local Backup files.

- Select **Remote machine** to store the backup file on another machine in the network, then indicate whether to use a **Samba file share** or **FTP server** and provide the following connection information:
  a. The **IP address/hostname** of the remote machine, and the connection **Port** to use.
  b. The **Default directory** in which backup files will be created. A different subdirectory will be created automatically for each backup file type.

  Important
  If you want to create backup files for multiple appliances on the same remote machine, be sure to use a separate directory for each appliance's backup files.

  This avoids the possibility of conflicts that could lead to files being mistakenly overwritten or deleted.

  c. The **User name** and **Password** to use when connecting to the remote machine. If a network logon is used, also provide the **Domain** in which the account resides.
  d. Click **Test Connection** to make sure the appliance can communicate with the remote machine and write to the specified location.
  e. If you want remote backup files to be automatically deleted after a specified time period, mark the **Delete backup files that are older than** check box, and then select a time period from the list.

4. Click **OK** to save your changes and return to the Backup Utility page. The new backup schedule is displayed in the Perform Backup list.

Full appliance configuration backups

Help | V-Series Appliance | Version 7.7.x

A full appliance configuration backup saves all appliance settings, as well as saving configuration and policy data for all active modules (Web Security, Email Security, or both) on the appliance. If you have multiple appliances, run backups on each one. The backup file includes data for only the appliance on which it is created.

Note
If you have Websense software components installed off the appliance—like Log Server or the TRITON Unified Security Center—Websense, Inc., recommends that you run the Backup Utility on those machines at approximately the same time that you back up your appliance. When you restore the system, this allows you to restore from a time-compatible set of backups on all machines.

Full appliance configuration backup files for Web Security appliances include:

- All configuration files for the appliance on which the backup is run, including configuration files for the Appliance Manager
- A snapshot, including all configuration data, of Websense Content Gateway
- All configuration settings for Websense Web Security, including:
  - Global configuration information, stored in the Policy Database (if Policy Broker is running on the selected appliance)
  - Local configuration information, such as Filtering Service and Log Server settings, stored in the **config.xml** file (if Policy Server is running on the selected appliance)
  - Websense component initialization (.ini) and configuration (.cfg) files

Full appliance configuration backup files for Email Security appliances include:

- All configuration files for the appliance on which the backup is run, including configuration files for the Appliance Manager
- Policy and configuration data for Websense Email Security

For appliances running in Web and Email security mode, both sets of information are included in backup files.

Module configuration backups

Help | V-Series Appliance | Version 7.7.x

Module configuration backups save all configuration information, including policy data, for the selected module.

- Web Security configuration backups performed on the *full policy source* appliance include all information stored in the Policy Database.
- Email Security configuration backups can be performed only if the Email Security module is enabled on the selected appliance.
- Backup operations for Content Gateway are managed through Content Gateway Manager. Click the Content Gateway Manager link at the top of the Backup Utility page to open the console and initiate backups.

Restoring a backup file

Help | V-Series Appliance | Version 7.7.x

Related topics:

- *Using the backup utility*, page 53
- *Scheduling backups*, page 55
- *Full appliance configuration backups*, page 56
- *Module configuration backups*, page 57

When you initiate the restore process, all current settings for the appliance or module are erased. Backup files stored on the appliance are not affected. When restoring the full appliance configuration, at the end of the restore process, the appliance restarts. The appliance is not restarted after restoring a module.

To restore an appliance or module to a saved configuration:

1. Stop all Websense software components running off the appliance.

   For example, stop Log Server, Sync Service, Linking Service, transparent identification agents, all components associated with the TRITON Unified Security Center, and the integrated Data Security Management Server.
2. Open Appliance Manager on the appliance whose configuration you want to restore and go to the **Administration > Backup Utility** page.
3. Click the **Restore** tab, then select the configuration type that you want to restore from the **Select restore mode** list. Note that when you restore a full appliance configuration:
   - The current appliance version must match the version associated with the backup file. (The appliance version is displayed on the **Restore** tab.) Thus, a version 7.5 backup can be restored only to an appliance that is at version 7.5.
   - The current appliance policy source mode (Full policy source, User directory and filtering, or Filtering only) must match the policy source mode in effect when the backup file was created.
   - In most circumstances, the current appliance mode (Email Security, Web Security, Web and Email Security) must match that of the backup file. (For example, a backup from an Email Security-only appliance must be used to restore an Email Security-only appliance.)

     There is one exception. If you are running in Web and Email security mode on a V10000 G2 appliance, you can restore a Web Security Gateway full backup.
   - The hardware model of the current appliance must be the same as the model that was backed up. (For example, a backup from model V10000 G2 must be used to restore a model V10000 G2 appliance.)
   - The original appliance that was backed up cannot also be running elsewhere in the network. Restoring a full configuration re-creates the original appliance and makes use of unique ID numbers from that appliance.
4. Click **Run Restore Wizard**. The restore wizard opens.
5. Select a radio button to indicate where the backup file is stored, and then click **Next**.
   - **This remote machine: <***host name or IP address***>**: Retrieve the file from the default location on the specified machine. The default location is the path specified in the backup schedule for the selected backup type.
   - **This appliance**: Use a backup file that was saved locally.
   - **Another location (browse for file)**: Use a file saved on any accessible machine in the network.
6. Select or specify the file to use.

- If you selected the default local or remote backup file location, you are given a list of available backup files to use. Select an entry in the list, and then click **Next**.
- If you selected another location, browse to the path on the remote machine where the backup file is located, and then click **Next**.

7. Verify the details on the Confirm page, and then click **Restore Now**. The appliance is restored to the selected configuration.

   If you have initiated a full appliance configuration restore, the appliance is restarted during the restore process.

8. Before starting the off-box components, ensure that the system time of all TRITON component hosts is synchronized. On the appliance, either set the time manually, or, if an NTP server is configured, click OK to trigger an update with the NTP server.
9. Start the Websense components that are running off the appliance.

   Note that if the restore process changed appliance IP addresses, you may need to reconfigure or reinstall off-box components to re-establish communication between on-box and off-box components.

Logs

Help | V-Series Appliance | Version 7.7.x

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

Note

Network Agent generates a log file only if you have enabled logging in TRITON - Web Security.

If you want to examine Network Agent log files in the Appliance Manager, first log on to TRITON - Web Security and navigate to **Settings > Network Agent > Global**. Then scroll down to **Additional Settings** to enable logging of protocol traffic and specify a logging interval.

Select the module for which you want to view logs:

- Appliance Controller
- Websense Content Gateway
- Websense Web Security
- Network Agent
- Websense Email Security Gateway

If you are reviewing the Appliance Controller log, next select the date range.

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

Then select the view option. Select either:

- View last __ lines

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

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

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

If you are downloading the entire log file, use the **File Download** dialog box to navigate to the save location.

Toolbox

Help | V-Series Appliance | Version 7.7.x

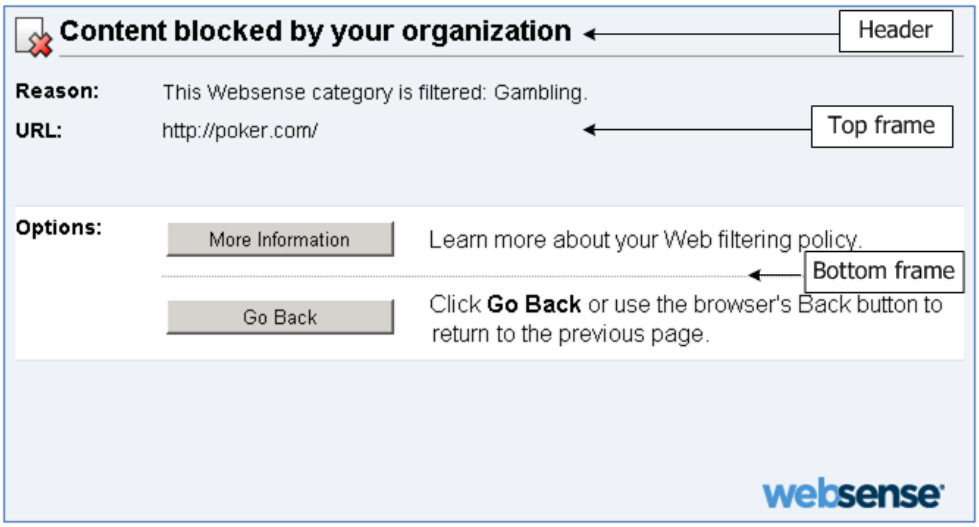
Use the **Administration > Toolbox** page to set up customized block pages, access basic Linux commands, and assist with troubleshooting.

Web Security block pages

Help | V-Series Appliance | Version 7.7.x

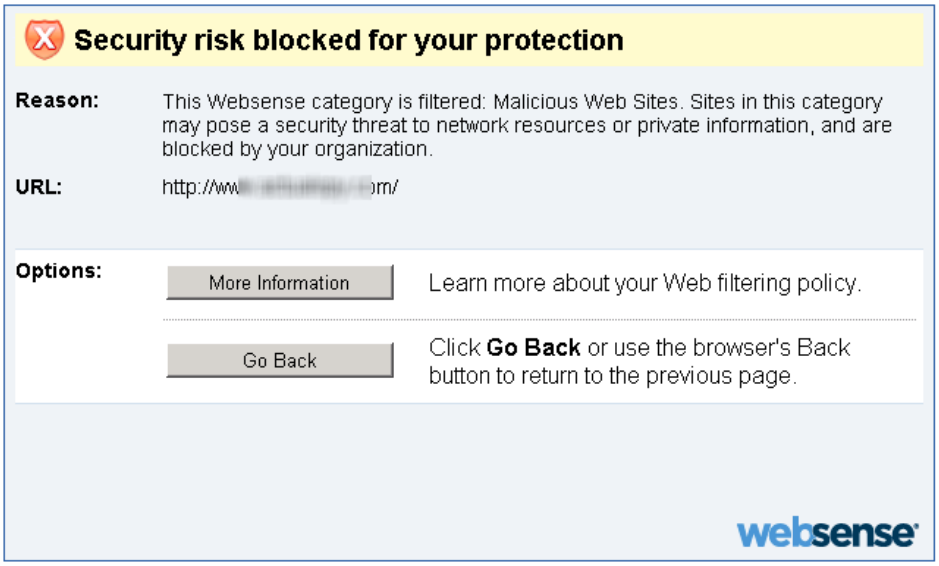
The appliance hosts a set of default Web Security block pages. These are displayed to end users each time a Web request is blocked.

Block pages are constructed from HTML and JavaScript files. By default, the block page has 3 main sections:



- The header explains that the site is blocked.
- The top frame contains a block message showing the requested URL and the category of the URL.
- The bottom frame presents any options available to the user (go back to the previous page, continue to the site, use quota time to access the site, use different credentials to try to access the site).

If the site is blocked because it belongs to a category in the Security Risk class, a special version of the block page is displayed.



To verify the behavior and appearance of Web Security block pages, use the links at testdatabase.websense.com to attempt to access test sites in categories that your organization blocks.

Use the **Administration > Toolbox** page to determine whether to:

- Use the block pages (both standard and security) provided with your Websense Web Security software (**Default block page**).
- Edit the block page files to suit the needs of your organization (**Custom block page**).

Customizing block pages

When you select **Custom block page**, a copy of the default block page files is created in an editable directory on the appliance. The default block page files are neither moved nor deleted, so that you can revert to them at any time.

After selecting the custom block page option:

1. Select the files you want to change, and then click **Download File(s)**. The files are copied to a location on your computer that you specify. The available files are:

File Name	Contents
block.html	Contains the text for the top frame of the block message, which explains that access is restricted, lists the requested site, and describes why the site is restricted.
blockFrame.html	Text and button (Go Back option) for sites in blocked categories.
blockStyle.css	Cascading style sheet containing most block page styles.
continueFrame.html	Text and buttons for sites in categories to which the **Confirm** action is applied.
master.html	Constructs the information frame for the block page, and uses one of the following files to display appropriate options in the bottom frame.
messagefile.txt	Contains text strings used in block pages
moreInfo.html	Content for the page that appears when a user clicks the **More information** link on the block page.
webDLPPolicyViolation.html	Provides block page content when Websense Data Security components block content from being posted to or downloaded from the Web.
quotaFrame.html	Text and buttons for sites in categories to which the **Quota** action is applied.
security.js	A JavaScript file used in construction of a security block page.

   - When you select a single file, its details are displayed, including its default use, last modification date, and size.
   - If you select more than one file to download, the files are packaged into a single ZIP file.

2. Make modifications locally.

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

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

3. Click **Upload File(s)** to place the modified files and any supporting graphics files on the appliance.
   - The edited files can refer to custom graphics files (like logos). If you use custom graphics, be sure to upload these additional graphics files to the editable directory.
   - If you have more than 5 files to upload, select the first 5 files to be uploaded, and then click **Add More Files**. You can upload a maximum of 10 files at a time.
4. Click **Apply Changes**. This restarts Filtering Service.
5. To test the customized block pages, go to testdatabase.websense.com and try to access test sites in categories blocked by your organization's policies.
6. Return to Step 2 if adjustments are needed.

Changing the block page logo

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

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

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

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

The result will look something like this:

```
<img title="ABC_Corporation" src="/en/Custom/
myimage.png" ...>
```

Note that parameter and folder names are case-sensitive.

4. Save and close the file.
5. Upload both the image file (containing your logo) and the edited copy of **master.html** to your V-Series appliance, and then click **Apply Changes**.

Changing the size of the message frame

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

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

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

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

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

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

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

Starting over

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

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

Appliance command line

Help | V-Series Appliance | Version 7.7.x

On the appliance **Toolbox** page, the **Appliance command line** section provides:

- The ability to turn on and off SSH remote access to the appliance **command line interface** (the same shell used to run the **firstboot** script). SSH access allows administrators to log on to the appliance command line shell from machines on the network that have a route to the appliance.

- Access to a **command line utility** that is embedded within Appliance Manager. The command line utility provides convenient access to common troubleshooting commands.

SSH Remote Access

Use the **Remote Access** option to enable and disable SSH access to the appliance command line interface.

To connect to the appliance command line shell when SSH access is enabled:

- Use a terminal emulator that supports SSH.
- SSH to the IP address of the C interface.
- Use your Appliance Manager administrator logon credentials when prompted.
- Run the "help" command to see the available commands.

Following is a list of command line commands. The debug-util sub commands are also available in the Appliance Manager in the *Command line utility* and are described in detail there.

admin email
debug-util controller
debug-util esg
debug-util na
debug-util view
debug-util wcg
debug-util wse
firstboot
help
history
ip address
ip dns
ip gateway
local-access
module disable
module enable
module restart
module start
module stop
password-logon disable
password-logon enable
patch delete
patch list

policy-source
quit
reload
remote-access disable
remote-access enable
reset password
show cpu
show disk-io
show disk-space
show interface c
show memory
show module
show module service
show password-logon
show patch
show patch history
show platform
show policy-source
show remote-access
show remote-access history
show security-mode
show smtp server
show ssh
shutdown
smtp server
ssh disable
ssh enable

Command line utility

Use the **Command Line Utility** to run troubleshooting, debugging, and utility commands. Results are displayed in the **Console output** section of the page. You can download the output file for the command last executed.

Click **Launch Utility** to open the command utility.

The **Module** drop down list includes an entry for each module installed on the appliance. Select the module that you want to work with:

- Appliance Controller
- Websense Content Gateway
- Websense Web Security

- Network Agent
- Websense Email Security Gateway

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

Command	Description	Parameters
arp	Displays the kernel ARP table for the selected module.	None.
cache-user-names	Applies to the Websense Web Security module only. Use it to turn on, off, or query the status of caching of user names resolved from IP addresses by Content Gateway. Cached entries are valid for 10 minutes.	[Action]: Enter **enable** to turn on user name caching. Enter **disable** to turn off user name caching. Enter **status** to display the status of user name caching.
content-line -r	Applies to the Websense Content Gateway module only. Use it to display the current value of a configuration variable in Content Gateway's records.config file.	[Variable Name]: Enter the name of the configuration variable for which you want to retrieve a value. **Example**: `proxy.config.vmap.enabled` This variable returns "0" or "1". "0" indicates that the virtual IP manager is disabled; "1" indicates that it is enabled. For a complete list of valid configuration variables, click the link **Websense Content Gateway variables** and navigate to the records.config topic. [You may be asked for credentials if you have not logged on to the proxy console earlier in the session.]
content-line -s	Applies to the Websense Content Gateway module only. Use it to set the value of a configuration variable in Content Gateway's records.config file. With this command, you can make changes to Content Gateway variables without restarting the proxy. To activate the changes, run `content_line -x` (see below).	[Variable Name]: Enter the name of the variable you want to modify. [Value]: Enter the value you want to supply the variable. **Example**: Enter the variable name **proxy.config.arm.enabled** and the value "1" or "0". This enables or disables the ARM, which is used for transparent proxy caching, IP spoofing, and ARM security. For a complete list of valid configuration variables, click the link **records.config**. [You may be asked for credentials if you have not logged on to the proxy console earlier in the session.]

Command	Description	Parameters
content-line -x	Applies to the Websense Content Gateway module only. Use it to read and apply the values of all configuration variables in Content Gateway's records.config file. If you have used `content_line -s` to change the setting of any variables in the file records.config, you can activate your changes immediately (without restarting the proxy) by running this command.	None.
copy-MasterCA	Applies to the Websense Web Security module only. When TRITON console is located on the appliance and a new master certificate is created following changes to the certificate authentication root certificate, use this command to copy the new Master CA to the Websense Web Security module. **Note:** If you are logged on to TRITON console, you will be logged off.	None
directory-agent-service	Applies to the Websense Web Security module only. This command disables and enables the directory agent service.	[Action]: Enter **enable** to enable the directory agent service. Enter **disable** to disable the directory agent service.
esg-license-reset	Applies to the Email Security Gateway module only. This command clears all Email Security Gateway subscription information. After the command is run, the user must re-enter the subscription key to use Email Security Gateway. **Note**: If the network is unreachable, the command takes 30 minutes to timeout.	None

Command	Description	Parameters
ethtool	Displays the current ethernet card settings of the specified network interface (NIC) device. This includes: • Supported ports • Supported link modes • Auto-negotiation support • Advertised link modes • Advertised auto-negotiation • Speed • Duplex • Port • PHYAD • Transceiver • Auto-negotiation setting • Wake-on support • Wake-on status • Link detection Use **ethtool** to verify local network connectivity. For example, if the ping command fails, use this to determine if you are using the right IP address.	None.
ethtool -k	Displays offload parameters, including checksum, for the selected network interface (NIC) device. This can be used to investigate a variety of problems. For example, if your NIC settings are right, but you are having duplex issues, you know you need to change your duplex settings.	None.
ifconfig	Use to troubleshoot network interface issues. Helps you identify IP issues and check subnets and network interfaces. Displays status information about the specified network interface (NIC), including but not limited to: • IP and broadcast address • subnet mask • number of packets received and transmitted • number of bytes received and transmitted	[Interface]: Enter the NIC for which you want settings. Click the information icon for valid NIC values. Enter **all** to display all interface status. Example: eth0 or eth1
multiplexer	Enables and disables the Multiplexer service that supports SIEM integrations. See TRITON – Web Security Help. Multiplexer service will not run on a Filtering only appliance. Instead it transparently uses the Multiplexer service running on the Policy source machine.	[Action]: Enter **enable** to enable the Multiplexer service. Enter **disable** to disable the Multiplexer service.

Command	Description	Parameters
nc -uvz	The netcat (nc) utility. Attempts to read and write data across a network using user datagram protocol (UDP) to the specified server. Use it for functional tests of components and verification of connectivity. Use it to check data going across a UDP network. If you are having problems loading a Web page, or are getting a block, this command can help determine the problem. If you see a reset coming from the proxy, you can determine which DOM/module it is coming from. **-u** Run netcat in UDP mode **-v** Run netcat in verbose mode. **-z** Run netcat in zero I/O mode (used for scanning).	[Destination]: Enter the IP address of the server with which you want to communicate. [Port]: Enter the port number of that server.
nc -vz	The netcat (nc) utility. Attempts to read and write data across a network using transmission control protocol (TCP) to the specified server. Use it for functional tests of components and verification of connectivity. **-v** Run netcat in verbose mode. **-z** Run netcat in zero I/O mode (used for scanning)	[Destination]: Enter the IP address of the server with which you want to communicate. [Port]: Enter the port number of that server.

Command	Description	Parameters
netstat -neatup	Displays a list of open sockets on the selected module, appended with the process column. **-n** Displays active TCP connections. However, addresses and port numbers are expressed numerically, and no attempt is made to determine names. **-e** Displays ethernet statistics, such as the number of bytes and packets sent and received. **-a** Displays all active TCP connections and the TCP and UDP ports on which the computer is listening. **-t** Indicates which open ports are using TCP. **-u** Indicates which open ports are using UDP. **-p** Limits display of statistics or state of all sockets to those applicable to protocol.	None.
netstat -ng	Displays multicast group membership information about the selected module. **-n** Displays active TCP connections. However, addresses and port numbers are expressed numerically, and no attempt is made to determine names. **-g** Shows the multicast group memberships for all interfaces.	None.

Command	Description	Parameters
netstat - nItup	Use one of the netstat commands if you are having network connection and routing issues. **netstat -nItup** displays the following: • the amount of traffic in your network. • all active TCP connections and the TCP and UDP ports on which the computer is listening. Addresses and port numbers are expressed numerically, and no attempt is made to determine names. • Ethernet statistics, such as the number of bytes and packets sent and received. **-n** Displays active TCP connections and the ports they use when they connect. (This is useful if, for example, Filtering Service is not filtering. You can look at the connection the module is using here. If it is not the IP and port of the Filtering Service machine, you have found the source of the problem.) **-I** Shows the state of a particular interface, such as eth0 or eth1. **-t** Indicates which open ports are using TCP. **-u** Indicates which open ports are using UDP. **-p** Limits display of statistics or state of all sockets to those applicable to protocol.	None.

Command	Description	Parameters
netstat -s	Displays summary statistics for each protocol on the selected module. By default, statistics are shown for the IP, ICMP, TCP, UDP, and TCPEXT protocols. This includes such things as: • IP - the number of packets received, forwarded, and discarded for each protocol. • ICPM - the number of messages received, failed, sent. • TCP - the number of active and passive connection openings and failed connection attempts. • UDP - the number of packets received and set. • TCPEXT - statistics about SYN cookies, ACKs, packets received and queued, retransmits, and DSACKs. This is just a sampling. Many more statistics are shown.	None.
nslookup	Use this for DNS resolution problems. For example, if a particular Web site is not loading, perform an nslookup on it to view its IP address. **nslookup** lets you query DNS servers to find DNS details, including IP addresses of a particular computer, MX records for a domain, and the DNS servers of a domain.	[Host]: Enter the hostname (for example myintranet.com) or IP address of the host for which you want DNS information. [DNS server]: Enter the hostname or IP address of the DNS server for the appliance.
ping, ping6	Checks that a hostname or IP address exists, can accept requests from the selected module, and that DNS is resolving. Use this to test connectivity to another host— for example, the Data Security Management Server or TRITON - Web Security machine—and determine response time. Use **ping** for IPv4 addresses, and **ping6** for IPv6 addresses. **Note:** ping6 is not supported in the Websense Web Security module.	[Destination]: Enter the hostname (for example myintranet.com) or IP address of the host you want to test.

Command	Description	Parameters
ping -I, ping6 -I	Checks that a network interface can communicate with a hostname or IP address and that DNS is resolving. Use this to test connectivity to another host— for example, the Data Security Management Server or TRITON - Web Security machine—from one of the appliance NICs. Use **ping** for IPv4 addresses, and **ping6** for IPv6 addresses. **Note:** ping6 -I is not supported in the Websense Web Security module.	[Interface]: Enter the name of the NIC you want to test. Click the information icon for valid NIC values. **Example**: eth0 [Destination]: Enter the hostname or IP address of the host you want to test.
policy-broker-token	Pertains only to the Web Security module. Use this command to retrieve the Policy Broker token for this appliance. This may be needed to configure support for Remote Filtering. See the Websense Technical Library for more information.	None.
print-bypass	This command applies only to the Websense Content Gateway module. When Content Gateway is in transparent proxy caching mode, use this command to see which source and destination IPs the proxy is bypassing. If sites are not loading correctly, this helps you identify if a site is loading from your cache or going directly to the site for download. All entries in the source and destination bypass tables for the proxy are printed to the output console. For more information on source and destination bypass, see the **Configuration Files > bypass.config** section of the Content Gateway Manager Help system.	None.
route -A inet6 -n	Display the contents of the selected module's kernel IP routing table IPv6 entries in numeric format. This is useful in complex network environments—for example, those with proxy chaining—to see if the environment is set up properly.	None.
route -n	Display the contents of the selected module's kernel IP routing table in numeric format. This is useful in complex network environments—for example, those with proxy chaining—to see if the environment is set up properly.	None.

Command	Description	Parameters
show-triton-admin-email	Pertains only to the Web Security module. Displays the email address to which alerts, password resets, and other TRITON administrator messages are sent.	None.
show-triton-smtp-settings	Pertains only to the Web Security module. Displays the SMTP server information and sender email settings used when notifications are sent from TRITON.	None
state-server	Applies to Websense Web Security module when the appliance is configured as a Full policy source or User directory and filtering system. In multiple Filtering Service deployments, Websense State Server is required for proper application of time-based filtering actions (Quota, Confirm, Password Override, and Account Override). See **Policy Server, Filtering Service, and State Server** in TRITON - Web Security Help.	[Action]: Enter **enable** to enable the state server service. Enter **disable** to disable the state server service.
sysctl-tcp-timestamps	Pertains only to the Websense Content Gateway module. View or change the setting for TCP time stamps. Edit this setting if you are experiencing performance problems with specific Web sites that do not properly support TCP time stamps. The operating system sets this kernel setting during installation. If the setting was changed and you are experiencing site latency with other sites—those that work best with TCP time stamps— return the setting to its default value and consider routing traffic to the problematic sites around the proxy. Be sure to choose a setting that works well for the sites that are most important to you. The setting affects the use of time stamps by the kernel for all TCP connections.	[Value]: Enter “0” to disable the current time stamp setting, and restore it to its default. Enter “1” to re-enable a custom setting. Enter “view” to view the current setting.

Command	Description	Parameters
sysctl-tcp-window-scaling	Pertains only to the Websense Content Gateway module. View or change the setting for TCP window scaling. Edit this setting if you are experiencing performance problems with specific Web sites that do not properly support TCP windows scaling. The operating system sets this kernel setting during installation. If the setting was changed and you are experiencing site latency with other sites—those that work best with TCP windows scaling— return the setting to its default value and consider routing traffic to the problematic sites around the proxy. Be sure to choose a setting that works well for the sites that are most important to you. The setting affects the use of windows scaling by the kernel for all TCP connections.	[Value]: Enter "0" to disable the current window scaling setting, and restore it to its default. Enter "1" to re-enable a custom setting. Enter "view" to view the current setting.

tcpdump	Use for any Web traffic issues to get packet captures—for example, if a site will not load or if you are having authentication problems.
	tcpdump intercepts and displays packets being transmitted or received by the specified network interface. Use the Expression field to select which packets are displayed.
	The output from **tcpdump** can help you determine whether all routing is occurring properly, to and from the interface. The output is verbose; it displays the data of each package in both hex and ASCII; and it includes a link-level header on each line.
	Note: If you do not stop the tcpdump command manually, 10,000 packets are captured, the maximum allowed.
		[Interface]: Enter the name of the NIC you are debugging. Click the information icon for valid NIC values.
		Example: eth0
		[Expression]: Enter a boolean expression that filters the packets to those of interest. Click the information icon for examples.
		Example 1: To capture all TCP traffic to and from the proxy on port 8080, enter this expression:
		`tcp port 8080`
		Example 2: To capture all TCP traffic to the site google.com, enter this expression:
		`tcp and dst host google.com`
		Example 3: To capture all TCP traffic from a specific end-user machine, enter this expression:
		`tcp and src host user.websense.com`
		Note: You can enter a hostname if it is resolvable by a DNS server, but the output uses IP addresses either way.

Command	Description	Parameters
tcpdump -w	Use this to dump traffic (raw packets) from the specified NIC to a file. To download the file, click the link, **Download output file for last command**, after running the command. This link is under the console output window. Websense Technical Support may request this file on occasion.	[Interface]: Enter the name of the appliance NIC you are debugging. Click the information icon for valid NIC values. [Expression]: Enter a boolean expression that filters the packets to those of interest. Click the information icon for examples. Enter **all** to capture all packets. **Note:** You can enter a host name if it is resolvable by a DNS server, but the output uses IP addresses either way.
top -bn1	Displays all operating system tasks that are currently running on the selected module. Use this to help troubleshoot CPU and memory issues. **-b** Run in batch mode. **-n** Update the display for a number of iterations, then exit. **-1** Do not display idle processes.	None.
traceroute, traceroute6	Use this to determine the route taken by packets across a network to a particular host. If some machines are not getting filtered or blocked, or if traffic is not even getting to the appliance, this shows the devices (or hops) that are between the machines that may be blocking access to the host. Use **tcpdump** to get a packet capture from each device. If you are having latency issues, **traceroute** can also help identify the causes. Use **traceroute** for IPv4 addresses, and **traceroute6** for IPv6 addresses. **Note: traceroute** is of limited utility if an IP address is being spoofed. **Note: traceroute6** is not supported in the Websense Web Security module.	[Destination]: Enter the hostname or IP address of the host destination you are investigating

Command	Description	Parameters
triton-admin-email	Pertains only to the Websense Web Security module, and only when TRITON - Web Security is running on the appliance. Use this to set the email address to which alerts, password reset notifications, and other administrator communication is sent.	[Email address]: The email address of the administrator.
triton-smtp-settings	Pertains only to the Websense Web Security module, and only when TRITON - Web Security is running on the appliance. Use it to configure the SMTP server and sender settings. **Note**: Typically these settings are made in the TRITON Unified Security Center on the **Settings > Notifications** page.	[SMTP server IP]: The IP address or host name of the SMTP server through which email alerts should be routed. [Port]: The SMTP port. [From email address]: The email address to use as the sender for email alerts. [Sender name]: The name of the sender of the alerts.
triton-websecurity-services	Pertains only to the Websense Web Security module. Use it to start, stop, restart, and query the status of TRITON - Web Security services.	[Action]: Enter **start** to start TRITON - Web Security services. Enter **stop** to stop TRITON - Web Security services. Enter **restart** to restart TRITON - Web Security services. Enter **status** to display the status of TRITON - Web Security services.
user-group-ip-precedence	Applies to the Web Security module only. Use this command to change the precedence of identification attributes applied to: filtering policy, Delegated Administrator (DA) role identification, protocol policy, and quota time available. By default, the precedence attributes are, in descending order: User > Computer > Network > Group > Domain When user-group-ip-precedence is enabled, the precedence order is: User > Group > Domain > Computer > Network	[Action]: Enter **enable** to modify the precedence order to: User > Group > Domain > Computer > Network Enter **disable** (default) to set the precedence order to: User > Computer > Network > Group > Domain Enter **status** to display the current setting. **WARNING:** Changing the state of user-group-ip-precedence causes Filtering Service to stop and restart.

Command	Description	Parameters
wcg-net-check	This command applies only to the Websense Content Gateway module. Use it to display diagnostics for Websense Content Gateway, such as: • interface status • connection to DNS name servers • connection to Policy Server • gateway packet loss • ping statistics for various modules • Internet connectivity • filtering status This command is useful for investigating latency issues, outages, or filtering problems, among other things.	None.
wget	Use to initiate a non-interactive download of files from the Web, so you can diagnose connectivity issues. Use **wget**, for example, if you have configured the proxy, but cannot access the Web. **wget** simulates the proxy going out and retrieving the Web site. This command supports HTTP, HTTPS, and FTP protocols.	[URL]: Enter the URL of the Web site from which you want to download files.
wget-proxy	Use to test connectivity between the specified URL and the proxy (file download not supported). Use **wget**, for example, if you have configured the proxy, but cannot access the Web. **wget** simulates the proxy going out and retrieving the Web site. This command supports HTTP, HTTPS, and FTP protocols.	[URL]: Enter the URL of the Web site to which you want to test connectivity. [Proxy IP]: Enter the proxy IP address. This is the IP address of the P1 interface on most appliance configurations. [Port]: Enter the port on which the proxy expects this traffic. 8080 is configured for HTTP by default. 8070 is configured for HTTPS by default. [User name]: Enter the user name of the client, if required for authentication. [Password]: Enter the password of the client, if required for authentication. Enter 'none' in both fields if user name and password are not applicable.

Technical Support tools

Help | V-Series Appliance | Version 7.7.x

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

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

Troubleshooting ports

Help | V-Series Appliance | Version 7.7.x

Websense Web Security provides the option to open troubleshooting ports temporarily, so that various troubleshooting tests can be run. (This facility is not available for Websense Email Security Gateway.)

Use this tool only when directed to do so by Websense Technical Support.

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

Important

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

Appliance Configuration summary

Help | V-Series Appliance | Version 7.7.x

The configuration summary tool gathers data from the appliance and generates an archive file that can be sent to Websense Technical Support for analysis and debugging. The process takes 1 to 2 minutes.

When Websense Technical Support requests this file:

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

Remote access

Help | V-Series Appliance | Version 7.7.x

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

- When you click **On** and then click **Save**, a passcode is generated and displayed on screen.

- Provide the passcode to your Websense Technical Support technician. This enables SSH, so that the technician can log on to your appliance.
- Each time you allow remote access to the appliance and a Websense technician logs on, a record is added to the **Remote access logon history** at the bottom of the **Toolbox** page.
- When the technician is done, be sure to click **Off** and click **Save** to disable the access.

Account management

Help | V-Series Appliance | Version 7.7.x

Use the **Administration > Account Management** page to:

- Change the password for accessing Appliance Manager (*Changing the Appliance Manager password*)
- Change the password for accessing Content Gateway Manager (*Content Gateway Manager password reset*)
- When TRITON - Web Security runs on the appliance, you can reset the TRITON - Web Security password (*Resetting the TRITON - Web Security password*)
- Specify the admin notification email address and SMTP server for password recovery email messages (*Setting the admin notification email address*)
- From the list of available languages, select the language in which the Help system will display (*Help system language*).

Changing the Appliance Manager password

Help | V-Series Appliance | Version 7.7.x

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

Click OK to save the new password.

Cancel discards all changes entered since the last **OK** action and restores the entry fields to the last saved values.

Setting the admin notification email address

Help | V-Series Appliance | Version 7.7.x

Use these settings to define and validate the email address and SMTP server used when Appliance Manager password recovery is performed. For a description of the password recovery mechanism, see *Appliance Manager password reset*.

1. Specify the email address to which password recovery email messages are sent.

2. Specify the SMTP server IP address and port.
3. If the SMTP connection requires authentication, provide the account name and password.
4. Validate the SMTP settings with the Test Connection button.

Click OK to save the new values.

Cancel discards all changes entered since the last **OK** action and restores the entry fields to the last saved values.

Resetting the TRITON - Web Security password

Help | V-Series Appliance | Version 7.7.x

Administrators can change their own TRITON console password at any time from the TRITON Settings > My Account page.

For administrators who have forgotten their TRITON - Web Security password, when TRITON - Web Security runs on the appliance, the **Administration > Account Management** page includes a section to facilitate resetting the administrator password.

Click the **logon page** link, and then click **Forgot my password**.

Note

In most deployments, the TRITON Unified Security Center, including TRITON - Web Security, is installed on a separate machine. In such cases:

- The **TRITON - Web Security Password Reset** section is not displayed.
- To reset the password, launch the TRITON console, and then click **Forgot my password** on the logon page.

The password reset process sends a temporary password to the email address associated with your administrator account. The temporary password is valid for only 30 minutes. If more than 30 minutes elapses before you attempt to log on with the temporary password, you must request a new password again.

You are prompted to enter a new password when you log on using the temporary password.

If the email SMTP settings and administrator email address are not configured for TRITON - Web Security, you must use the **triton-smtp-settings** and **triton-admin-email** commands in the **Websense Web Security** category of the **Toolbox > Command Line Utility** to configure the settings. See *Command line utility*.

Content Gateway Manager password reset

Help | V-Series Appliance | Version 7.7.x

This option is only available when Content Gateway is run on the appliance.

1. Click **Reset Password** to reset your proxy password.
2. The new password appears at the bottom of the screen. Write it down.
3. As soon as you navigate away from the **Account Management** page in Appliance Manager, your reset password is no longer displayed.
4. Log on to Content Gateway Manager with the new password.
5. Go to **Configure > My Proxy > UI Setup > Login** to change the new password to the desired string.

Appliance Manager password reset

Help | V-Series Appliance | Version 7.7.x

Should you forget or misplace the Appliance Manager logon password, there are 2 ways to establish a new password, both are initiated on the logon portal.

Click **Forgot my password**.

- If a notification email address and SMTP server have been configured, a temporary password is mailed to the email address. Log on using the temporary password within 1 hour and reset your password. See, *Setting the admin notification email address*.
- If a notification email cannot be sent, an error message displays and you are advised to contact Websense Technical Support. A security code is also provided. Make a note of it, it is required by Websense Technical Support to generate a new password.

Help system language

Help | V-Series Appliance | Version 7.7.x

From the **Language** drop down list, select the language in which you would like Help system information to be displayed, and click OK to apply your selection.