websense®

Websense Appliance Manager Help

Websense® V-Series Appliance

Models: V10000, V10000 G2, V5000 G2

v7.6

Trademarks

Contents

1 | V-Series Overview

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

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

◆ Instantly categorizes new sites and dynamic content, proactively discovering security risks, and blocking malware.

◆ 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.

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

◆ Integrates with Websense Data Security solutions to help you monitor and restrict transmission of sensitive or inappropriate information via email.

Security best practices

- ◆ 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.

- ◆ 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

Appliance Manager is the name of the management console for the V-Series appliance. This is a graphical interface for configuring the appliance, checking the status of the software modules, updating passwords, troubleshooting, and applying patches to the appliance.

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

Perform configuring tasks for the software modules on the appliance (such as setting up users and defining and applying filtering policies) through the module's management console, as shown below.

Software module	Description	Console name
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

To launch Content Gateway Manager directly, go to:

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

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

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

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.

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

```
http://<IP-address-of-interface-C>
```

Appliance Manager and the TRITON Unified Security Center support the following browsers:

◆ Microsoft Internet Explorer 7, 8, and 9
◆ Firefox 3.5.x, 3.6.x, and 4.

Logging on to Appliance Manager

You can log onto 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.

The user name is **admin**.

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

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

Logs and reporting

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 hosts 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, the **Today** page shows the operating status of Websense software, 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** are interactive reports that 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 by the Filtering Service instances associated with a Policy Server, and what action is applied to each request.

Databases used with V-Series appliances

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 anti-spam and antivirus databases. The software checks for updates to these databases at a regular interval. You can initiate updates manual from within TRITON - Email Security.

Navigating in Appliance Manager

Appliance Manager opens showing the **Status > General** page in the content pane. The appliance platform, Appliance Controller host name, and a Log Off button are displayed in the banner at the top of the page.

◆ 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	◆ *Patch management*
	◆ *Using the backup utility*
	◆ *Logs*
	◆ *Toolbox*
	◆ *Account management*

Clustering multiple Web Security Gateway appliances

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).

On a V-Series appliance there is one additional step to complete configuration. A dedicated route must be added.

1. Complete all configuration steps in Content Gateway Manager.
2. Log in to Appliance Manager and go to **Configuration > Routing**.
3. Add a Static Route rule for multicast cluster traffic through interface P1.
   a. Click **Add**.
   b. Select **Add individual route**.
   c. For **Destination network**, enter the multicast IP address. For example: 224.0.1.37
   d. Specify a Subnet mask.
   e. Specify a Gateway.
   f. Select P1 from the Interface drop down list.
   g. Click **Add Route**.

Add a dedicated route on every Content Gateway node in the cluster.

General system status

The **Status > General** page appears 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. You can choose to monitor the status pages even after the 30-minute timeout is reached.
>
> To do this, mark the box labeled **Monitor status without timing out** in the Appliance Controller section on this page.
>
> Information on all Status pages then continues to update normally until you close the browser or navigate away from the Status pages. Be sure to **Save** all changes; these are lost if not saved before 30 minutes of inactivity.

Modules on the 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 > Patch Management** 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.
Disable Module (Network Agent)	Sets a flag to indicate that the Network Agent software on this appliance should be shut down and not restarted the next time the appliance is restarted (rebooted). When you click this button, you are prompted to restart the appliance to reallocate the resources (CPU and memory) previously allocated to Network Agent. You can restart later if you wish. Once Network Agent has been successfully disabled, the button on this page changes to Enable Module.
Stop Services Start Services (Network Agent)	Causes the Network Agent service on this appliance to be stopped. Or, if services are stopped, Start Services causes all services to be started.

Button or Link	Description
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.

CPU and memory status

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 seconds, in megabytes

Disk use by module

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 technology 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

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 on 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

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

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

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

◆ Set the appliance **hostname**, or system name (1 - 32 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, the hostname cannot exceed 11 characters (excluding the domain name). 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, **Save** applies and saves new values in that section. **Cancel** discards all changes entered since the last save and restores entry fields in the section to their current settings.

Network interface configuration

Use the **Configuration > Network Interfaces** page 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)*
◆ *Interface bonding*
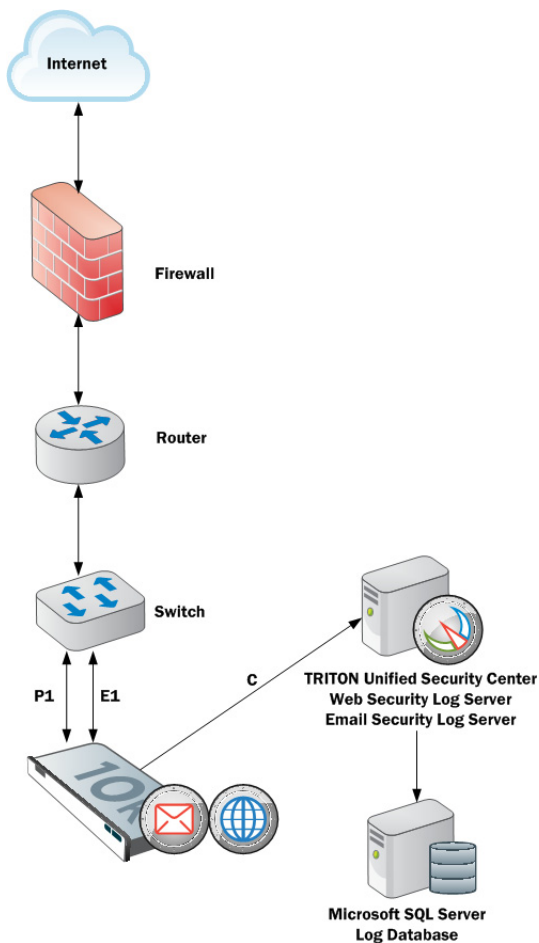
Click **Save** to save and apply new values in each section.

Appliance Controller Interface (C)

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).

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 23.
>
> 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)

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 may 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 may 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)

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 and 443.
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)

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 for both inbound and outbound traffic; E2 is not used.
- ◆ Another option is to configure E1 to accept inbound and E2 to send outbound traffic.

> **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.

Interface bonding

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.

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, truck 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, truck 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

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 completed. 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 effected 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 4: One appliance, Web Security and Email Security with off-box TRITON Unified Security Center and off-box Log Server

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

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

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, reregister Content Gateway with 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, reregister with 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, reregister 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 Server

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 service.

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, reregister with Data Security Management Server.

10. If Web DLP is used, reregister with 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 secondary 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, reregister with 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 appliances to Filtering only, 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, reregister with 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

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

◆ Static routes from subnets and client computers through any active appliance interface, except N.

◆ Module routes from appliance modules through appliance interface C to subnets.

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.

◆ 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 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	Required. The subnet mask for the network where the clients reside (such as 255.255.0.0)

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.

   ```
   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.

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 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 separated, 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 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

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 32.

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 **Save**.

   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 **Privacy password** used for encryption.

7. Click **Save** 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 **Save** to implement your changes. See *Enable specific alerts*, page 32, 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, also enter and confirm the **Password** for the selected user name, 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 **Privacy password** used for encryption.

8. To verify your configuration, click **Send Test Trap**. If the test trap succeeds, click **Save** to implement your changes. See *Enable specific alerts*, page 32, 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 and the SNMP manager.

Enable specific alerts

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.

When have finished configuring which events will trigger an alert for a module, click **Save** to implement the changes.

Configuring Web Security components

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?*).
2. If you selected a mode other than full policy source, provide the **Policy source IP address**. This may be the IP address of another appliance, or the IP address of the server where Websense Policy Broker is installed.
3. Click **Save** to save and apply your changes.
4. If this is a 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.

5. 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, as some settings may not be preserved during migration.

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

What is a policy source?

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.

  ■ Policy Database
  ■ Policy Broker
  ■ Policy Server
  ■ Filtering Service
  ■ User Service
  ■ Usage Monitor
  ■ Control Service
  ■ Directory Agent
  ■ TRITON - Web Security (optional)
    • Investigative Reports Scheduler
    • Manager Web Server
    • Reporting Web Server
    • Reports Information Service
    • 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.

◆ 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.

If you are configuring an appliance that is not the full policy source machine, then it must point to the policy source.

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**. An appliance in either of these modes must point to a policy source appliance or server.

◆ A **user directory and filtering** appliance is a secondary appliance, 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 **filtering only** appliance does not run Policy Server. It runs only:
  ■ Filtering Service
  ■ Control Service
  ■ Websense Content Gateway module
  ■ Network Agent module (optional)

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

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

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

User directory with V-Series appliances

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

Preparing for a hybrid configuration

In Websense 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:

◆ Your **supported LDAP-based directory service** (Windows Active Directory [Native Mode], Oracle [Sun Java] Directory Server, or 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 secondary 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

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

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

The Administration pages enable you to:

- Install software patches (see *Patch 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

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

Go to the **Administration > Patch Management** page to check for, download, and install patches.

- ◆ Appliances automatically check for patches once a day. The time of the check is randomized, cannot be configured, and is different for every appliance.
- ◆ To manually check for patches at any time, 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.
- ◆ When a new patch is available, 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 and efficiently 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 an immediate history of patches that have been applied to the appliance.

See:

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 random time, or manually with the **Check for Patches** button.

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

- ◆ Use the **Administration > Patch Management** 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 **Patch Management** page, the "Appliance current version" number is the current appliance version (the number of the latest patch installed).
- ◆ Be sure that all Websense modules running off the appliance, such as Log Server, are upgraded to the appropriate level each time you patch the appliance. 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

◆ 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.
	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.

Proxy Settings

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.

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.

Patch history

The **Patch History** table on the **Administration > Patch Management** page displays all patches installed on the appliance. For each patch, you see:

◆ Version number

◆ Date and time of patch installation

◆ Confirmation of successful installation

◆ Link to patch log file, showing patch details

Using the backup utility

Related topics:

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 47.

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). 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 that Content Gateway backups are performed in Content Gateway Manager. Backups 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 45).

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 those components.

  ▪ **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

> Related topics:
>
> ◆ *Using the backup utility*, page 43
> ◆ *Full appliance configuration backups*, page 46
> ◆ *Module configuration backups*, page 47
> ◆ *Restoring a backup file*, page 47

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 **Save** 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

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

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

Related topics:

◆ *Using the backup utility*, page 43
◆ *Scheduling backups*, page 45
◆ *Full appliance configuration backups*, page 46
◆ *Module configuration backups*, page 47

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. 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

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

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

- *Web Security block pages*
- *Appliance command line*
- *Command line utility*
- *Technical Support tools*

Web Security block pages

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:
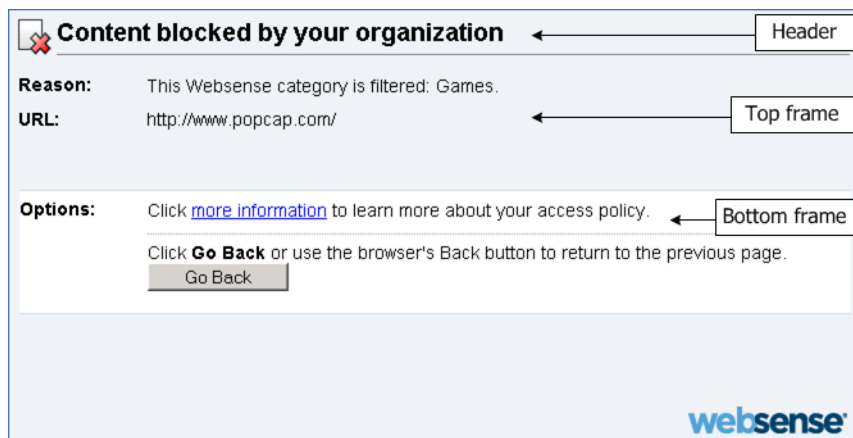
- The header explains that the site is blocked.
- The top frame contains a block message showing the requested URL and the category of the URL.
- The bottom frame presents any options available to the user (go back to the previous page, continue to the site, use quota time to access the site, use different 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.
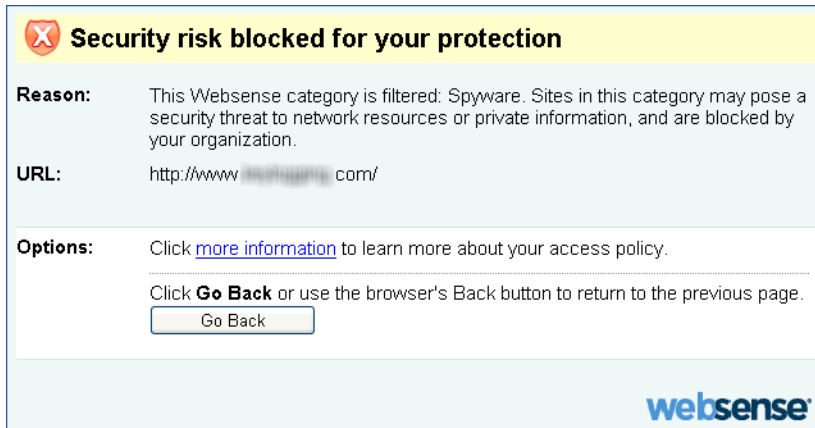
To verify the behavior and appearance of Web Security block pages, use the links at testdatabase.websense.com to attempt to access test sites in categories that your organization blocks.

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 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.

File Name	Contents
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.
policyViolationDefault page.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	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 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

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.

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

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 patch

show patch history

show platform

show policy-source

show remote-access

show remote-access history

show security-mode

show ssh

shutdown

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	Pertains only to the Websense Web Security module. Use it to turn on, turn off, or query the status the 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	Pertains only to the Websense Content Gateway module. 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.]

Command	Description	Parameters
content-line -s	Pertains only to the Websense Content Gateway module. 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 his 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.]
content-line -x	Pertains only to the Websense Content Gateway module. 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.
directory-agent-service	Pertains only to the Web Security module. 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	Pertains only to the Email Security Gateway module. 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. **-k** Change the checksumming parameters of the specified ethernet device.	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 NIC, including but not limited to: • IP and broadcast address • subnet mask • number of packets received and transmitted • number of bytes received and transmitted	[Interface]: Enter the NIC for which you want settings. Click the information icon for valid NIC values. Enter **all** to display all interface status. Example: eth0 or eth1

Command	Description	Parameters
nc -uvz	Attempts to read and write data across a network using user datagram protocol (UDP) to the specified server. Use it for functional tests of components and verification of connectivity. Use it to check data going across a UDP network. If you are having problems loading a Web page, or are getting a block, this command can help determine the problem. 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	Checks that a hostname or IP address exists, can accept requests from the selected module, and that DNS is resolving. Use this to test connectivity to another host— for example, the Data Security Management Server or TRITON - Web Security machine—and determine response time.	[Destination]: Enter the hostname (for example myintranet.com) or IP address of the host you want to test.
ping -I	Checks that a network interface can communicate with a hostname or IP address and that DNS is resolving. Use this to test connectivity to another host— for example, the Data Security Management Server or TRITON - Web Security machine—from one of the appliance NICs.	[Interface]: Enter the name of the NIC you want to test. Click the information icon for valid NIC values. **Example**: eth0 [Destination]: Enter the hostname or IP address of the host you want to test.

Command	Description	Parameters
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.
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.
route -n	Display the current contents of the selected module's kernel IP routing table in numeric format. This is useful in complex network environments—for example, those with proxy chaining—to show if the environment is set up properly.	None.
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

Command	Description	Parameters
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.
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.

Command	Description	Parameters

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

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.

Command	Description	Parameters
traceroute	Use this to determine the route taken by packets across a network to a particular host. If some machines are not getting filtered or blocked, or if traffic is not even getting to the appliance, this shows the devices (or hops) that are between the machines that may be blocking access to the host. Use **tcpdump** to get a packet capture from each device. If you are having latency issues, **traceroute** can also help identify the causes. (Note that **traceroute** is of limited utility if an IP is being spoofed.)	[Destination]: Enter the hostname or IP address of the host destination you are investigating
triton-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.

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

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

◆ *Troubleshooting ports*

◆ *Appliance Configuration summary*

◆ *Remote access*

Troubleshooting ports

Websense Web Security provides the option to open troubleshooting ports temporarily, so that various troubleshooting tests can be run. (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

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

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

Use the **Administration > Account Management** page to change the password for accessing Appliance Manager or Content Gateway Manager. In some circumstances, the page also includes a section for resetting TRITON - Web Security passwords.

◆ *Changing the Appliance Manager password*
◆ *Resetting the TRITON - Web Security password*
◆ *Content Gateway Manager password reset*

Changing the Appliance Manager password

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

Save applies and saves new values in the pane.

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

Resetting the TRITON - Web Security password

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

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.

4 | Copyrights and trademarks

Trademarks

Other acknowledgements

Portions of this Websense Software may utilize the following copyrighted material, the use of which is hereby acknowledged.

CentOS 5.x

CentOS-5 EULA

CentOS-5 comes with no guarantees or warranties of any sorts, either written or implied.

The Distribution is released as GPL. Individual packages in the distribution come with their own licences.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of

Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files,

plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance

on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING

RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Xen 3.2.4

Copyright © 2005 XenSource, Inc. All use and distribution of this copyrighted material is governed by and subject to terms and conditions as licensed by XenSource, Inc. All other rights reserved. Unless otherwise specified, this software is licensed under the terms of the GNU General Public License, version 2. This software comprises a compilation work of XenSource, Inc., and is released under the terms of the GNU General Public License as a whole. Trademarks, service marks, and logos ("Trademarks") displayed are registered and unregistered Trademarks of XenSource, Inc. or of third parties.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable.

However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or

she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD

PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

XML-RPC For C/C++ License v. 1.15

Copyright (C) 2001 by First Peer, Inc. All rights reserved.

Copyright (C) 2001 by Eric Kidd. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

SUN JDK 1.6

Copyright © 2005 Sun Microsystems, Inc.,

4150 Network Circle, Santa Clara, California 95054, U.S.A.

All rights reserved. U.S.

Government Rights - Commercial software. Government users are subject to the Sun Microsystems, Inc. standard license agreement and applicable provisions of the FAR and its supplements. Use is subject to license terms. This distribution may include materials developed by third parties. Sun, Sun Microsystems, the Sun logo, Java, Jini, Solaris and J2SE are trademarks or registered trademarks of Sun Microsystems, Inc.

in the U.S. and other countries. This product is covered and controlled by U.S. Export Control laws and may be subject to the export or import laws in other countries. Nuclear, missile, chemical biological weapons or nuclear maritime end uses or end users, whether direct or indirect, are strictly prohibited.

Export or reexport to countries subject to U.S. embargo or to entities identified on U.S. export exclusion lists, including, but not limited to, the denied persons and specially designated nationals lists is strictly prohibited.

Copyright © 2005 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, Etats-Unis. Tous droits réservés.L'utilisation est soumise aux termes du contrat de licence.

Cette distribution peut comprendre des composants développés par des tierces parties.Sun, Sun Microsystems, le logo Sun, Java, Jini, Solaris et J2SE sont des marques de fabrique ou des marques déposées de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays. Ce produit est soumis à la législation américaine en matière de contrôle des exportations et peut être soumis à la règlementation en vigueur dans d'autres pays dans le domaine des exportations et importations. Les utilisations, ou utilisateurs finaux, pour des armes nucléaires, des missiles, des armes biologiques et chimiques ou du nucléaire maritime, directement ou indirectement, sont strictement interdites.

Les exportations ou réexportations vers les pays sous embargo américain, ou vers des entités figurant sur les listes d'exclusion d'exportation américaines, y compris, mais de manière non exhaustive, la liste de personnes qui font objet d'un ordre de ne pas participer, d'une façon directe ou indirecte, aux exportations des produits ou des services qui sont régis par la législation américaine en matière de contrôle des exportations et la liste de ressortissants spécifiquement désignés, sont rigoureusement interdites.

Sun Microsystems, Inc. Binary Code License Agreement for the JAVA 2 PLATFORM STANDARD EDITION DEVELOPMENT KIT 5.0

SUN MICROSYSTEMS, INC. ("SUN") IS WILLING TO LICENSE THE SOFTWARE IDENTIFIED BELOW TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS BINARY CODE LICENSE AGREEMENT AND SUPPLEMENTAL LICENSE TERMS (COLLECTIVELY "AGREEMENT"). PLEASE READ THE AGREEMENT CAREFULLY. BY DOWNLOADING OR INSTALLING THIS SOFTWARE, YOU ACCEPT THE TERMS OF THE AGREEMENT. INDICATE ACCEPTANCE BY SELECTING THE "ACCEPT" BUTTON AT THE BOTTOM OF THE AGREEMENT. IF YOU ARE NOT WILLING TO BE BOUND BY ALL THE TERMS, SELECT THE "DECLINE" BUTTON AT THE BOTTOM OF THE AGREEMENT AND THE DOWNLOAD OR INSTALL PROCESS WILL NOT CONTINUE.

1. DEFINITIONS. "Software" means the identified above in binary form, any other machine readable materials (including, but not limited to, libraries, source files, header files, and data files), any updates or error corrections provided by Sun, and any user manuals, programming guides and other documentation provided to you by Sun under this Agreement. "Programs" mean Java applets and applications intended to run

on the Java 2 Platform Standard Edition (J2SE platform) platform on Java-enabled general purpose desktop computers and servers.

2. LICENSE TO USE. Subject to the terms and conditions of this Agreement, including, but not limited to the Java Technology Restrictions of the Supplemental License Terms, Sun grants you a non-exclusive, non-transferable, limited license without license fees to reproduce and use internally Software complete and unmodified for the sole purpose of running Programs. Additional licenses for developers and/or publishers are granted in the Supplemental License Terms.

3. RESTRICTIONS. Software is confidential and copyrighted. Title to Software and all associated intellectual property rights is retained by Sun and/or its licensors. Unless enforcement is prohibited by applicable law, you may not modify, decompile, or reverse engineer Software. You acknowledge that Licensed Software is not designed or intended for use in the design, construction, operation or maintenance of any nuclear facility. Sun Microsystems, Inc. disclaims any express or implied warranty of fitness for such uses. No right, title or interest in or to any trademark, service mark, logo or trade name of Sun or its licensors is granted under this Agreement. Additional restrictions for developers and/or publishers licenses are set forth in the Supplemental License Terms.

4. LIMITED WARRANTY. Sun warrants to you that for a period of ninety (90) days from the date of purchase, as evidenced by a copy of the receipt, the media on which Software is furnished (if any) will be free of defects in materials and workmanship under normal use. Except for the foregoing, Software is provided "AS IS". Your exclusive remedy and Sun's entire liability under this limited warranty will be at Sun's option to replace Software media or refund the fee paid for Software. Any implied warranties on the Software are limited to 90 days. Some states do not allow limitations on duration of an implied warranty, so the above may not apply to you. This limited warranty gives you specific legal rights. You may have others, which vary from state to state.

5. DISCLAIMER OF WARRANTY. UNLESS SPECIFIED IN THIS AGREEMENT, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT THESE DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

6. LIMITATION OF LIABILITY. TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL SUN OR ITS LICENSORS BE LIABLE FOR ANY LOST REVENUE, PROFIT OR DATA, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, HOWEVER CAUSED REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF OR RELATED TO THE USE OF OR INABILITY TO USE SOFTWARE, EVEN IF SUN HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

In no event will Sun's liability to you, whether in contract, tort (including negligence), or otherwise, exceed the amount paid by you for Software under this Agreement. The foregoing limitations will apply even if the above stated warranty fails of its essential purpose. Some states do not allow the exclusion of incidental or consequential damages, so some of the terms above may not be applicable to you.

7. TERMINATION. This Agreement is effective until terminated. You may terminate this Agreement at any time by destroying all copies of Software. This Agreement will terminate immediately without notice from Sun if you fail to comply with any provision of this Agreement. Either party may terminate this Agreement immediately should any Software become, or in either party's opinion be likely to become, the subject of a claim of infringement of any intellectual property right. Upon Termination, you must destroy all copies of Software.

8. EXPORT REGULATIONS. All Software and technical data delivered under this Agreement are subject to US export control laws and may be subject to export or import regulations in other countries. You agree to comply strictly with all such laws and regulations and acknowledge that you have the responsibility to obtain such licenses to export, re-export, or import as may be required after delivery to you.

9. TRADEMARKS AND LOGOS. You acknowledge and agree as between you and Sun that Sun owns the SUN, SOLARIS, JAVA, JINI, FORTE, and iPLANET trademarks and all SUN, SOLARIS, JAVA, JINI, FORTE, and iPLANET-related trademarks, service marks, logos and other brand designations ("Sun Marks"), and you agree to comply with the Sun Trademark and Logo Usage Requirements currently located at http://www.sun.com/policies/trademarks. Any use you make of the Sun Marks inures to Sun's benefit.

10. U.S. GOVERNMENT RESTRICTED RIGHTS. If Software is being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), then the Government's rights in Software and accompanying documentation will be only as set forth in this Agreement; this is in accordance with 48 CFR 227.7201 through 227.7202-4 (for Department of Defense (DOD) acquisitions) and with 48 CFR 2.101 and 12.212 (for non-DOD acquisitions).

11. GOVERNING LAW. Any action related to this Agreement will be governed by California law and controlling U.S. federal law. No choice of law rules of any jurisdiction will apply.

12. SEVERABILITY. If any provision of this Agreement is held to be unenforceable, this Agreement will remain in effect with the provision omitted, unless omission would frustrate the intent of the parties, in which case this Agreement will immediately terminate.

13. INTEGRATION. This Agreement is the entire agreement between you and Sun relating to its subject matter. It supersedes all prior or contemporaneous oral or written communications, proposals, representations and warranties and prevails over any conflicting or additional terms of any quote, order, acknowledgment, or other communication between the parties relating to its subject matter during the term of this Agreement. No modification of this Agreement will be binding, unless in writing and signed by an authorized representative of each party.

SUPPLEMENTAL LICENSE TERMS

These Supplemental License Terms add to or modify the terms of the Binary Code License Agreement. Capitalized terms not defined in these Supplemental Terms shall have the same meanings ascribed to them in the Binary Code License Agreement . These Supplemental Terms shall supersede any inconsistent or conflicting terms in the Binary Code License Agreement, or in any license contained within the Software.

A. Software Internal Use and Development License Grant. Subject to the terms and conditions of this Agreement and restrictions and exceptions set forth in the Software "README" file, including, but not limited to the Java Technology Restrictions of these Supplemental Terms, Sun grants you a non-exclusive, non-transferable, limited license without fees to reproduce internally and use internally the Software complete and unmodified for the purpose of designing, developing, and testing your Programs.

B. License to Distribute Software. Subject to the terms and conditions of this Agreement and restrictions and exceptions set forth in the Software README file, including, but not limited to the Java Technology Restrictions of these Supplemental Terms, Sun grants you a non-exclusive, non-transferable, limited license without fees to reproduce and distribute the Software, provided that (i) you distribute the Software complete and unmodified and only bundled as part of, and for the sole purpose of running, your Programs, (ii) the Programs add significant and primary functionality to the Software, (iii) you do not distribute additional software intended to replace any component(s) of the Software, (iv) you do not remove or alter any proprietary legends or notices contained in the Software, (v) you only distribute the Software subject to a license agreement that protects Sun's interests consistent with the terms contained in this Agreement, and (vi) you agree to defend and indemnify Sun and its licensors from and against any damages, costs, liabilities, settlement amounts and/or expenses (including attorneys' fees) incurred in connection with any claim, lawsuit or action by any third party that arises or results from the use or distribution of any and all Programs and/or Software.

C. License to Distribute Redistributables. Subject to the terms and conditions of this Agreement and restrictions and exceptions set forth in the Software README file, including but not limited to the Java Technology Restrictions of these Supplemental Terms, Sun grants you a non-exclusive, non-transferable, limited license without fees to reproduce and distribute those files specifically identified as redistributable in the Software "README" file ("Redistributables") provided that: (i) you distribute the Redistributables complete and unmodified, and only bundled as part of Programs, (ii) the Programs add significant and primary functionality to the Redistributables, (iii) you do not distribute additional software intended to supersede any component(s) of the Redistributables (unless otherwise specified in the applicable README file), (iv) you do not remove or alter any proprietary legends or notices contained in or on the Redistributables, (v) you only distribute the Redistributables pursuant to a license agreement that protects Sun's interests consistent with the terms contained in the Agreement, (vi) you agree to defend and indemnify Sun and its licensors from and against any damages, costs, liabilities, settlement amounts and/or expenses (including attorneys' fees) incurred in connection with any claim, lawsuit or action by any third party that arises or results from the use or distribution of any and all Programs and/or Software.

D. Java Technology Restrictions. You may not create, modify, or change the behavior of, or authorize your licensees to create, modify, or change the behavior of, classes, interfaces, or subpackages that are in any way identified as "java", "javax", "sun" or similar convention as specified by Sun in any naming convention designation.

E. Distribution by Publishers. This section pertains to your distribution of the Software with your printed book or magazine (as those terms are commonly used in the industry) relating to Java technology ("Publication"). Subject to and conditioned

upon your compliance with the restrictions and obligations contained in the Agreement, in addition to the license granted in Paragraph 1 above, Sun hereby grants to you a non-exclusive, nontransferable limited right to reproduce complete and unmodified copies of the Software on electronic media (the "Media") for the sole purpose of inclusion and distribution with your Publication(s), subject to the following terms: (i) You may not distribute the Software on a stand-alone basis; it must be distributed with your Publication(s); (ii) You are responsible for downloading the Software from the applicable Sun web site; (iii) You must refer to the Software as JavaTM 2 Platform Standard Edition Development Kit 5.0; (iv) The Software must be reproduced in its entirety and without any modification whatsoever (including, without limitation, the Binary Code License and Supplemental License Terms accompanying the Software and proprietary rights notices contained in the Software); (v) The Media label shall include the following information: Copyright 2004, Sun Microsystems, Inc. All rights reserved. Use is subject to license terms. Sun, Sun Microsystems, the Sun logo, Solaris, Java, the Java Coffee Cup logo, J2SE , and all trademarks and logos based on Java are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries. This information must be placed on the Media label in such a manner as to only apply to the Sun Software; (vi) You must clearly identify the Software as Sun's product on the Media holder or Media label, and you may not state or imply that Sun is responsible for any third-party software contained on the Media; (vii) You may not include any third party software on the Media which is intended to be a replacement or substitute for the Software; (viii) You shall indemnify Sun for all damages arising from your failure to comply with the requirements of this Agreement. In addition, you shall defend, at your expense, any and all claims brought against Sun by third parties, and shall pay all damages awarded by a court of competent jurisdiction, or such settlement amount negotiated by you, arising out of or in connection with your use, reproduction or distribution of the Software and/or the Publication. Your obligation to provide indemnification under this section shall arise provided that Sun: (i) provides you prompt notice of the claim; (ii) gives you sole control of the defense and settlement of the claim; (iii) provides you, at your expense, with all available information, assistance and authority to defend; and (iv) has not compromised or settled such claim without your prior written consent; and (ix) You shall provide Sun with a written notice for each Publication; such notice shall include the following information: (1) title of Publication, (2) author(s), (3) date of Publication, and (4) ISBN or ISSN numbers. Such notice shall be sent to Sun Microsystems, Inc., 4150 Network Circle, M/S USCA12-110, Santa Clara, California 95054, U.S.A , Attention: Contracts Administration.

F. Source Code. Software may contain source code that, unless expressly licensed for other purposes, is provided solely for reference purposes pursuant to the terms of this Agreement. Source code may not be redistributed unless expressly provided for in this Agreement.

G. Third Party Code. Additional copyright notices and license terms applicable to portions of the Software are set forth in the THIRDPARTYLICENSEREADME.txt file. In addition to any terms and conditions of any third party opensource/freeware license identified in the THIRDPARTYLICENSEREADME.txt file, the disclaimer of warranty and limitation of liability provisions in paragraphs 5 and 6 of the Binary Code License Agreement shall apply to all Software in this distribution.

For inquiries please contact: Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. (LFI#141623/Form ID#011801)

Tomcat 6.0.29

Copyright © 2007 Apache Software Foundation (ASF)

Apache License
Version 2.0, January 2004
http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form

of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

a.You must give any other recipients of the Work or Derivative Works a copy of this License; and

b.You must cause any modified files to carry prominent notices stating that You changed the files; and

c.You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

d.If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational

purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

Anaconda 11.1.2.87

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991 Copyright (C) 1989, 1991 Free Software Foundation, Inc. 675 Mass Ave, Cambridge, MA 02139, USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms

and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Libcli

GNU LESSER GENERAL PUBLIC LICENSE

Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated

straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library,

the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not.Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include

anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice. This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS