Getting Started

Websense Web Security Gateway on the Websense® V10000 Appliance with Riverbed Steelhead 250 branch office appliances
# Contents

## Topic 1

**Web Security Gateway and Riverbed® Steelhead™ 250**

- Deployment overview ........................................... 5
- Data center hardware and software requirements .......... 6
  - Websense V10000 appliance .................................. 6
  - Windows server .............................................. 7
  - Database engine ............................................. 8
  - Directory service ............................................ 8
  - Other ............................................................ 9

## Topic 2

**Setting up the Riverbed Steelhead 250**

- Prerequisites .................................................. 11
- Set up the appliance hardware ................................ 12
- Perform initial command line configuration ............... 12
  - Prepare to run jump-start ................................... 12
- Configure the Steelhead 250 ................................ 13
  - Preparing for Steelhead 250 configuration ............... 14
  - Upgrading to RiOS (Riverbed IOS) and RSP Version 5.5.x 14
  - Generating, uploading, and starting the Windows RSP package. 16
  - Setting up data flow ......................................... 21
  - Adding Websense software to Riverbed RSP VM at branch 23

## Topic 3

**Installing Websense Components**

- Install Microsoft SQL Server at the data center .......... 25
- Install Websense components at the data center .......... 25
- Set up the Websense appliance hardware ................. 26
- Perform initial command line configuration ............... 26
- Configure the V10000 ......................................... 27
- Install Websense Manager and Log Server ............... 30
- Configure Websense Manager ................................ 34
  - Special directory service considerations ................. 37
- Configure Websense Content Gateway ....................... 38
- Test and refine your policies ................................ 39
- Recovering the V10000 appliance ............................ 40
- Install Websense components at the branch office ....... 41
  - Installation procedure: branch components ............. 42
  - Configuring branch copy of Network Agent, at data center ... 43
- Known Issues .................................................. 43
Contents

Quota time cannot be determined precisely ......................... 43
HTTPS block page not displayed in non-proxy environment ... 44
Quota/Confirm HTTPS URL permitted if no proxy ............... 44
Online Help .................................................. 44
Technical Support .............................................. 45
Websense® Web Security Gateway with the Riverbed® Steelhead™ 250

Websense Web Security software and Riverbed Steelhead appliances provide fast, flexible Web security and WAN optimization in a variety of configurations. This guide explains how to set up and configure the Websense Web Security v7.1 components when you are using a Steelhead 250 appliance at branch offices and the Websense V10000 appliance at the data center.

Deployment overview

Distributed organizations with remote and branch offices can integrate Websense Web Security software with Riverbed appliances by deploying two key components of the software on a Steelhead 250 appliance in the branch offices. All Web security policies are hosted and configured centrally, at the data center. This provides local Web security at the branch offices, with persistent policy management and reporting from the corporate data center, where Websense Web Security software runs on a Websense V10000 appliance.

In this deployment, the administrator can use a PAC file to control how branch traffic is filtered. Any HTTP/HTTPS/FTP traffic passing from the branch office through the V10000 appliance, and then to the Internet, is filtered by the V10000. The remaining HTTP/HTTPS/FTP traffic from the branch may go to the Internet directly from the local network and would be filtered by the Websense Web Security components on the Riverbed Steelhead 250. In addition, all other branch traffic (such as IM, P2P, File Transfer) is also filtered by Websense components on the Riverbed Steelhead 250.
Typically, the components are deployed as shown below.

A Windows server at the data center houses Websense Manager (the configuration interface for Websense Web Security) and Log Server (which processes filtering log records into a separate Microsoft SQL Server database for reporting). The Websense V10000 appliance houses the central policy database that serves all branches, as well as other key Websense software components.

**Data center hardware and software requirements**

In the data center, the integrated solution uses the hardware and software specified below. Some elements are required, such as the Websense V10000 appliance and one Windows server. Others components are optional, such as a directory service, which allows you to apply Web filtering policy to individual users and groups in your organization.

**Websense V10000 appliance**

The Websense V10000 appliance is a high-performance platform for Websense Web Security Gateway, combining Websense Web Security filtering and Websense Content Gateway proxy on a single, high-powered machine. The V10000 solution requires a separate Windows 2003 or Windows 2008 Server in the network, which houses Websense Manager, the configuration interface for Websense Web Security, and Log Server, which processes filtering log records into a separate Microsoft SQL Server database.
This security solution offers:

- **V10000 Console**, a Web-based configuration interface that offers appliance management features like:
  - System dashboard, with up-to-the-minute status of the software modules and system resources
  - Appliance configuration and network settings
  - System administration, including patch management and backup and restore
- Events related to appliance configuration and patching are logged. The log entries can be viewed in the V10000 Console, or the entire log file can be downloaded.
- Command line interface for basic appliance settings, available through a USB keyboard and monitor or a serial port connection, that provides basic appliance control commands
- Basic proxy caching and Web filtering after minimal initial configuration
- Full customization of proxy caching and Web filtering available through these separate Web-based configuration interfaces:
  - Websense Content Manager — proxy caching
  - Websense Manager — Web filtering

### Windows server

Your data center must have a Windows server machine that meets the requirements listed below. This is the machine where you install Websense Manager (the configuration interface for Web filtering) and Log Server (the component that receives Internet activity information and processes it into the Log Database).

**Important**

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

Please set the appliance time in your branches, the time on the Websense V10000, and the time on the Windows server machine, before installing Websense Manager and Log Server.

### Hardware

- Quad-Core Intel Xeon processor, 2.5 GHz or higher
- 4-16 GB RAM
- 100 GB free disk space utilizing a disk array
- High speed disk access
Operating System
- Windows Server 2008 (Standard, Enterprise, and Datacenter) installed in 32-bit native mode
- Windows Server 2003, R2 (Standard or Enterprise)
- Windows Server 2003, SP1 or SP2 (Standard or Enterprise)
- Windows Server 2003 (Standard or Enterprise)

Additional Software
- Internet Explorer 7 or Firefox 2 or 3
- Common Desktop Environment (CDE)
- Apache Tomcat 6.0.13 (installed automatically with Websense Manager)
- Adobe Flash Player 8 or later

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

One of these databases:
- Microsoft SQL Server 2005 SP2 or SP 3 (Workgroup, Standard, or Enterprise edition) (recommended)
- Microsoft SQL Server 2000 SP4
- MSDE 2000 SP4 - suitable for smaller networks running Windows Server 2003

The following recommendations apply to the machine running the database engine, especially if it runs on the same Windows server as Websense Manager and Log Server.
- You can improve I/O performance by installing the Log Database on a disk array running RAID level 1+0.
- The amount of required RAM depends on the total number of requests being stored and the number of requests per second being processed. To optimize RAM usage, use the Enterprise Edition of Microsoft SQL Server on a machine running Windows Server 2003 Enterprise Edition or Windows Server 2008 Enterprise Edition or Datacenter.

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

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

**Note**

If your network uses a Windows NTLM directory service, or Active Directory in mixed mode, you must create Websense accounts for any administrators who must log on to Websense Manager (see Websense Manager Help for instructions). This configuration does not support logging on to Websense Manager with network credentials.

- Windows Active Directory
- Windows NT Directory
- Novell eDirectory 8.51 or later
  - NMAS authentication is supported.
  - Recommend Novell Client v4.83 or v4.9 (v4.81 and later are supported)
- Other LDAP-based directory services
- Most standard RADIUS servers
  The following RADIUS servers have been tested:
  - Livingston (Lucent) 2.x
  - Cistron RADIUS server
  - Merit AAA
  - Microsoft IAS

**Other**

Optionally, you can deploy the Websense Remote Filtering Server in the data center, to enable filtering of laptops and other computers that are outside the organization’s network. A client agent is required for each laptop.

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


Setting up the Riverbed Steelhead 250

Setting up Websense software integrated with the Steelhead 250 involves the following tasks, which are detailed in this guide.

1. Set up the Websense software in the data center first, before setting up the branch software. See *Install Websense components at the data center* for instructions.
2. Ensure that all *Prerequisites* have been completed.
3. Set up the appliance hardware.
4. Perform initial command line configuration on the appliance.
5. Configure the Steelhead 250 for use with Websense software.
6. Install two components of Websense software on the Steelhead 250. See *Install Websense components at the branch office*.

**Prerequisites**

Satisfy these requirements before you set up the Riverbed Steelhead 250:

- Upgrade RAM to at least 3GB.
  
The default RAM for the Steelhead 250 appliance is 1GB. But at least 3GB of RAM are required when Websense Web Security is deployed on the Riverbed Services Platform (RSP). 1G is required for the Riverbed System, 2GB for the Websense RSP virtual machine. Insert at least an additional 2GB of RAM into the RAM slot.
  
  For instructions on upgrading memory on the Steelhead 250, please see the *Riverbed Upgrade and Maintenance Guide*.

- Obtain a valid RSP license from Riverbed.
  
The Riverbed Services Platform (RSP) provides customers with the ability to run up to five additional services and applications in virtual memory on VMware in a protected partition on the Steelhead 250 appliance. The RSP function must be enabled by a valid RSP license before you install Websense Web Security components.
  
  For more information about an RSP license, please contact Riverbed.

- Websense Web Security can be installed only on Riverbed RIOS version 5.5.x and RSP version 5.5.x.
Websense and Riverbed have certified that Websense Web Security 7.1 components can integrate with RIOS version 5.5.x and RSP version 5.5.x. Unpredictable results may occur if other versions of Websense Web Security or RSP are used.

Set up the appliance hardware

Follow the Riverbed Steelhead hardware setup guide for model 250 hardware setup. Connect all power sources, the network cables, and the serial cable.

Perform initial command line configuration

The first time you start the appliance, a brief script (jump-start) prompts you to supply basic settings for the appliance.

Prepare to run jump-start

The jump-start script prompts you for the following information [defaults shown in brackets]. Gather needed data before you start the script.

Riverbed Steelhead configuration wizard.
Step 1: Hostname? [example]
Step 2: Use DHCP on primary interface? [no]
Step 3: Primary IP address? [ ]
Step 4: Netmask? [ ]
Step 5: Default gateway? [ ]
Step 6: Primary DNS server? [ ]
Step 7: Domain name? [example.com]
Step 8: Admin password?
Step 9: SMTP server? [exchange]
Step 10: Notification email address? [examplem@riverbed.com]
Step 11: Set the primary interface speed? [auto]
Step 12: Set the primary interface duplex? [auto]
Step 13: Would you like to activate the in-path configuration? [yes]
Step 14: In-Path IP address? [ ]
Step 15: In-Path Netmask? [ ]
Step 16: In-Path Default gateway?
Step 17: Set the in-path:LAN interface speed? [auto]
Step 18: Set the in-path:LAN interface duplex? [auto]
Step 19: Set the in-path:WAN interface speed? [auto]
Step 20: Set the in-path:WAN interface duplex? [auto]

After you gather the information, run the initial command line configuration, as follows.
1. Access the appliance through a serial port connection.

   **Note**
   To configure the appliance, connect through the serial port and complete the jump-start script.

2. To run the initial script, enter the following command:
   ```
   enable
   configure terminal
   configuration jump-start
   ```

3. Configure the network with the information assembled earlier. Accept the default value for all Yes/No questions.

4. After the jump-start script has been completed successfully, go to a different machine and use a supported Web browser to access the Steelhead 250 Console. See *Configure the Steelhead 250*, page 13.

---

**Configure the Steelhead 250**

The Steelhead 250 console is a Web-based configuration interface for the appliance. Through it you can view system status, configure network and communication settings, and perform general Steelhead 250 administration tasks.

After completing the initial configuration required by the jump-start script, use the Steelhead 250 console to configure important settings for network interfaces and upload the RSP package.

You need a flash drive with at least 1 GB of free space to hold the latest RSP package for upload.
Preparing for Steelhead 250 configuration

Gather the following information before running the Steelhead 250 console. Some of this information may have been gathered during hardware setup.

<table>
<thead>
<tr>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name and password for accessing the</td>
</tr>
<tr>
<td>Riverbed Support Web site</td>
</tr>
<tr>
<td>IP address assigned to the network interface for</td>
</tr>
<tr>
<td>the Steelhead 250 console manager</td>
</tr>
<tr>
<td>RSP license key from Riverbed</td>
</tr>
<tr>
<td>IP address for network interface Inpath 0_0</td>
</tr>
<tr>
<td>Subnet mask for network interface Inpath 0_0</td>
</tr>
<tr>
<td>Default gateway for network interface Inpath 0_0 (IP address)</td>
</tr>
</tbody>
</table>

See the Steelhead 250 help system for detailed instructions on any field or area, or for information about other available settings.

Upgrading to RiOS (Riverbed IOS) and RSP Version 5.5.x

1. Open a supported browser, and enter this URL in the address bar:
   https://<IP address>

   Replace <IP address> with the address assigned to the console during initial configuration of the Steelhead 250.

2. Log on with the user name admin and the password assigned during initial configuration of the Steelhead 250.

3. Upgrade the Steelhead 250 software to version 5.5.x. (requires an account with Riverbed):
   a. Open a supported browser, and enter the following URL in the address bar:
      http://www.riverbed.com/support
   b. Download the version 5.5.x software image (RiOS - Base OS) available from the support site. Please download the version specific to Steelhead 250. You can also sign up for upgrades with Riverbed at this time.
   c. Use the console to upload and install the software:
• Navigate to **Configure > Maintenance > Software Upgrade**.
• Upload the downloaded 5.5.x RiOS from the local directory, and then click **Install Upgrade** to upgrade.
• Riverbed Steelhead will reboot and apply the new 5.5.x RiOS successfully.

4. Configure the inpath0_0 Interface by navigating to **Configure > Networking > Inpath0_0**.
5. Apply the RSP license key (provided by Riverbed) by navigating to **Configure > Maintenance > Licenses** and choosing **Add a New License**.

6. Upgrade the RSP to v5.5.x (requires an account with Riverbed):
   a. Open a supported browser, and enter the following URL in the address bar:
      
      https://support.riverbed.com/software/rsp.htm
   b. Download the v5.5.x RSP image from the support site. Please download the version specific to Steelhead 250.
   c. Install the RSP image:
      
      • Navigate to **Configure > Branch Services > RSP Service**
      • Click the down arrow to drop down the menu for **Install RSP From**. Select either **URL**, **Local File**, or **Existing Image**, and then provide the path or point to the image.
      • Click **Install**.
      • Click **Start** to start RSP.

**Generating, uploading, and starting the Windows RSP package**

1. Move to a computer running VMware Workstation or VMware ESX server.
2. Download the Package Generator Wizard from the Riverbed Support Site:

   https://support.riverbed.com/software/rsp.htm

   (Downloading this Package Generator requires an account with Riverbed.)
3. Create a custom VMware image for Websense Web Security components using VMware Workstation or VMware ESX server. For complete details about this process, see the chapter *Creating an RSP Package for a Windows Server* in the *Riverbed Services Platform Installation and Configuration Guide* for RiOS Version 5.5.x.
   
a. Allocate 1.8 Gigabytes of RAM for the image.
   
b. Browse to your Windows Virtual Machine folder. If you find a folder named .vmx.lck in that location, remove the .vmx.lck folder before proceeding.

4. Generate an RSP package by running the Package Generator Wizard.
5. Point the RSP Package Generator to the VM directory.

6. Configure the RSP package details, and then click Next.
7. Keep the default configuration for **Watchdog**, and then click **Next**.

8. Add a single v-inpath VNIC by clicking **Add** under Optimization Interfaces, and then click **OK** and **Next**.
9. Ensure that Resource Requirements are sufficient.
   a. Virtual Machine RAM must be 1.8 gigabytes.
   b. Virtual Machine Storage must be at least 18 gigabytes.
10. Fill in the Output settings, and then click **Create Package**. Your package is now ready.
11. After creating the RSP package, save the package by clicking **Save Configuration**.
12. Copy the package to a location that can be accessed by the RSP platform. You can use a flash drive that has at least 1 GB of free space.

13. If you use a flash drive to copy the package, insert the flash drive into a USB port in a client machine anywhere in the network.
14. To begin the process of uploading the RSP package from a client machine to the Steelhead 250 appliance, navigate to **Configure > Branch Services > RSP Packages**. Then click **Fetch a Package** to upload the RSP package from a local PC or remote http/https/scp/ftp server.

15. Click a Slot number, and then click **Enable Slot**.

### Setting up data flow

1. Navigate to **Configure > Branch Services > RSP Data Flow**.

   The RSP package has one VNI (Virtual Network Interface), which we named
Monitor when we added it in this example. Find the interface you added, and add this interface in position 1 in the data flow, between LAN0_0 and RiOS0_0 from the Interface drop-down menu.

2. Set the action for IP and Non-IP Rules for this VNI to copy traffic to slot. This is similar to spanning a port off a switch.

3. Make sure that this interface (within the VM) is within the same subnet as the inpath0_0 address on the Steelhead appliance. For example, if the inpath0_0 address is 192.168.1.11/24, then the Monitor interface address on the RSP virtual machine should be 192.168.1.x/24.
4. Ping the Websense Web Security Gateway server, to make certain that both the VM and the Gateway are reachable.

5. Navigate to **Configure > Branch Services > RSP Packages** and launch the VM Console.

6. Log on to VMware Infrastructure.

7. Download and install the plug-in to enable the browser to see the VMware image software.
   a. Choose defaults during the installation process.
   b. After the installation completes, log on again to the VMware Infrastructure.

**Adding Websense software to the Riverbed RSP virtual machine at the branch office**

1. Ensure that your data center is running Microsoft SQL Server, and that the Websense server at the data center is running the Websense components. See *Install Websense components at the data center*, page 25 in the next chapter for specifics.

2. Log on to the uploaded VM image and install Websense Network Agent and Filtering Service in Stand-alone mode. See *Install Websense components at the branch office* in the next chapter for specifics.

3. After installation, use Websense Manager running in the data center to configure the Network Agent running at the branch office so that it monitors the branch subdomain(s). See the next chapter for specifics.
Setting up the Riverbed Steelhead 250

Websense Web Security and Riverbed Steelhead
3

Installing Websense Components

Websense software components and your database management system must be installed and running at the data center before you install Websense components on the Riverbed Steelhead 250 appliance at branch offices.

Install Microsoft SQL Server at the data center

Install a supported database engine at the data center first. It may be installed either on the same Windows server machine where Websense reporting components will be installed, or on a different machine in the network.

---

**Important**

The database engine must be installed and running before you install Websense Log Server.

---

If you do not have a supported database engine, you can download and install MSDE for free. Refer to the Websense Knowledge Base on the Websense Support Portal, [www.websense.com/kb](http://www.websense.com/kb) for a download link and further instructions. Search for the exact phrase: *Installing MSDE with Websense software, version 7*.

See the Websense *Installation Guide* for more details on configuring the database engine, including prerequisites such as setting up user roles, and the database rights needed for the account specified during Log Server installation.

Install Websense components at the data center

Setting up the Websense V10000 appliance involves the following tasks, which are detailed in this chapter.

1. *Set up the Websense appliance hardware*, page 26
3. *Configure the V10000*, page 27.
5. *Configure Websense Manager*, page 34.

**Set up the Websense appliance hardware**

The Quick Start guide, which comes in the box with your appliance, provides information on the contents of the Websense V10000 box, how to set up the hardware, and how to connect the cables to the appliance and to your network.

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

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

After hardware setup, connect directly to the appliance through the serial port or the monitor, keyboard, and mouse ports. The activation script, called firstboot, runs when you start the appliance.

**Perform initial command line configuration**

The first time you start the appliance, a brief script prompts you to supply settings for the network interface labeled C and a few other general items.

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td></td>
</tr>
<tr>
<td>IP address for network interface C</td>
<td></td>
</tr>
<tr>
<td>Subnet mask for network interface C</td>
<td></td>
</tr>
<tr>
<td>Default gateway for network interface C</td>
<td>(IP address)</td>
</tr>
<tr>
<td>Primary DNS server for network interface C</td>
<td>(IP address)</td>
</tr>
<tr>
<td>Secondary DNS server for network interface C</td>
<td>(IP address)</td>
</tr>
<tr>
<td>Tertiary DNS server for network interface C</td>
<td>(IP address)</td>
</tr>
<tr>
<td>Unified password to be used for the three consoles: V10000 Console, Websense Manager, and Content Manager.</td>
<td>(8 to 15 characters, at least 1 letter and 1 number)</td>
</tr>
</tbody>
</table>
When you have gathered the necessary information, run the initial command line configuration, as follows.

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

   **Note**
   To configure the appliance, you must connect through the serial port or the keyboard/video/mouse ports and complete the firstboot script.

2. Accept the subscription agreement when prompted.
3. When asked if you want to begin, enter `y` to launch the firstboot activation script. If the activation script does not launch automatically, enter the following command:
   ```
   firstboot
   ```
4. Follow the onscreen instructions to provide the information collected above.
5. After the activation script has been completed successfully, go to a different machine and use a Web browser to access the V10000 Console.

## Configure the V10000

The V10000 Console is the Web-based configuration interface for the Websense appliance. Through it you can view system status, configure network and communication settings, and perform general V10000 administration tasks.

After completing the initial configuration required by the firstboot script, use the V10000 Console to configure important settings for network interfaces N and P1 (and optionally P2), which are used for communications by Network Agent and Websense Content Gateway.

Gather the following information before running the V10000 Console. Some of this information may have been gathered on the Quick Start during hardware setup.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary NTP server, (domain)</td>
<td>Optional</td>
</tr>
<tr>
<td>Secondary NTP server, (domain)</td>
<td>Optional</td>
</tr>
<tr>
<td>Tertiary NTP server, (domain)</td>
<td>Optional</td>
</tr>
<tr>
<td>IP address for network interface P1</td>
<td></td>
</tr>
<tr>
<td>Subnet mask for network interface P1</td>
<td></td>
</tr>
<tr>
<td>IP address for network interface P2</td>
<td>Required only if P2 is enabled</td>
</tr>
<tr>
<td>Subnet mask for network interface P2</td>
<td>Required only if P2 is enabled</td>
</tr>
</tbody>
</table>
After collecting the information needed, access the V10000 Console through a supported browser.

The following procedure summarizes the settings that must be configured to enable default proxy caching and filtering. See the V10000 Console Help for detailed instructions on any field or area, or for information about other available settings.

1. Open a supported browser, and enter the following URL in the address bar:
   
   `https://<IP address>:9447/appmng`

   Replace `<IP address>` with the address assigned to network interface C during initial configuration of the V10000.

2. Log on with the user name `admin` and the password set during initial appliance configuration.
3. In the left navigation pane, click **Configuration > General**.
   a. Set the time zone.
   b. Select Internet Network Time Protocol (NTP) servers for time synchronization, or specify the system time and date. (Use of an NTP server is recommended, to ensure that database downloads and time-based policies are handled precisely.)
   c. Click **Save** in the Time and Date area.

4. In the left navigation pane, click **Configuration > Network Interfaces**.
   a. Configure network interfaces P1 (and optional P2) for Websense Content Gateway. Then, click **Save** in the Websense Content Gateway Interface area.

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

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

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

   One common configuration is to use P1 for traffic into and out of the proxy module. Another common configuration uses P1 for inbound traffic and P2 for outbound traffic. To enable this configuration, be sure to set an appropriate routing rule for P1 and P2 on the **Configuration > Routing** page. For example, you might set inbound traffic to come through P1 and outbound traffic to go through P2.

   Additionally, you can use P2 as a communication channel for multiple proxy servers in a cluster. In this scenario, P2 cannot be used for outbound traffic. For additional information on clusters, see the Websense Content Gateway Administrator’s Guide.

   b. Configure network interface N for Network Agent. Then, click **Save** in the Network Agent Interface area.

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

   **Note**
   The V10000 appliance does not send block messages to users who are blocked from non-HTTP and non-HTTPS protocols.

5. In the left navigation pane, click **Configuration > Routing**.
Installing Websense Components

30 Websense Web Security and Riverbed Steelhead

- Use the appropriate Add Route button to specify customized, static routes from client computers to the Websense Content Gateway software module.
- Use the Edit and Delete buttons to modify existing routes, as needed.

6. In the left navigation pane, click Configuration > Policy Source.
   - Specify the location of Websense Web Security policy information.
     - Choose This V10000 appliance if the policy for your deployment is located on the V10000 being configured.
     - Choose Another V10000 appliance or server on your network if the V10000 currently being configured is not the location of the policy information. Then, enter the IP address of the other server (network interface C if the policy source is another V10000 appliance that is configured as primary).
   - Click Save.

7. Click Log Off, at the top right, to close the Websense V10000 Console.


Install Websense Manager and Log Server

Deploying the Websense V10000 appliance requires installing Websense Manager and Log Server on a separate Windows server machine in the network. A supported database engine must also be installed, either on the same Windows server machine or a different machine in the network.

Websense Manager is the interface for Websense Web Security configuration and policy management.

Log Server receives records of Internet filtering activity and sends them to the Log Database, which is installed on a database engine.

---

**Important**

The database engine must be installed and running before you install Log Server.

---

Gather the following information before running the installer. Some of this information may have been gathered on the Quick Start during hardware setup.

<table>
<thead>
<tr>
<th>Policy Server IP address</th>
<th>(IP address of the policy source machine. Typically, this is the IP address for network interface C on the appliance)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database engine location</td>
<td>(IP address or machine name)</td>
</tr>
</tbody>
</table>

30 Websense Web Security and Riverbed Steelhead
### Installing Websense Components

<table>
<thead>
<tr>
<th><strong>Policy Server IP address</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>(IP address of the policy source machine. Typically, this is the IP address for network interface C on the appliance)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Database user name</strong></th>
<th></th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th><strong>Database password</strong></th>
<th></th>
</tr>
</thead>
</table>

The following procedure summarizes the steps required to install the required components. See the Websense *Installation Guide* for more detailed instructions.

1. Log on to the installation machine with administrative privileges.
   
   If you will use a Windows trusted connection to communicate with the database engine, your logon user account must also be a trusted account with local administration privileges on the database machine.

2. Make sure the date and time are synchronized with the date and time on the V10000 appliance.

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

   Please set the appliance time and the time on the Windows server machine before installing Websense Manager and Log Server.

3. Download the installation package from [www.mywebsense.com](http://www.mywebsense.com).

4. Close all applications and stop any anti-virus software.

5. Double-click the installation package to extract the files and start the installation.

6. Follow the onscreen instructions to the Subscription Agreement screen.

7. Select **Yes**, and click **Next**.

8. Select a **Custom** installation, and click **Next**.

9. In the list of components, mark the check boxes for **Log Server** and **Websense Manager** and any other optional components to be installed on this machine.

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

   Go to the Websense Knowledge Base, and search for the article titled *v7: Changing the Policy Server (or Policy Broker) IP address*. 
See the Websense Deployment Guide and Installation Guide for descriptions of the available components, and associated installation requirements.

10. Clear all other check boxes, and then click Next.

Important
Be sure to clear the check boxes for these components:

- Policy Broker
- Policy Server
- Filtering Service
- User Service
- Usage Monitor
- Remote Filtering Server
- Remote Filtering Client

11. When asked for the IP address of the Policy Server machine, enter the IP address of the policy source machine (typically, this is the IP address for network interface C on the V10000 appliance).

12. Accept the default port number (55806), and click Next.

13. For the Database Engine Location, enter the name or IP address of the machine on which a supported database engine is running.

14. Select a database access method, and then click Next.

- SQL database account—Enter the user name and password for a SQL Server account that has administrative access to the database. This is the recommended method.

Note
The SQL Server password cannot begin or end with a hyphen (-).

- Windows trusted connection—Uses the Windows account that is currently logged on to access the database. This account must have administrative access to the database. Websense, Inc., recommends against using a trusted connection if you run MSDE.

15. On the Minimizing Database Management screen, select options that affect the size of the Log Database used to generate reports.

- Logging Web Page Visits—Select this option to log a record of each Web page requested. This selection creates a smaller database and faster reporting. Deselect this option to log a record of each separate file that is part of a Web page request, including graphic images and advertisements. This selection results in more precise reports, but creates a much larger database and causes reports to generate more slowly.

Important
- **Consolidating Log Records**—Select this option to combine multiple visits by the same user to the same Internet domain (see Websense Manager Help for details of how records are combined). This selection creates a smaller database, but decreases reporting precision.
  
  Deselect this option to record each visit or hit separately. This selection provides greater reporting precision, and a larger database.

16. Provide other information requested if you are installing optional components.
  
  The information requested depends on the components being installed. See the Websense Installation Guide for details on optional components.

17. Accept the default installation path or click **Browse** to locate another path, and then click **Next**. The default installation path is:

   C:\Program Files\Websense

   The installer creates this directory if it does not exist.

   **Important**

   The full installation path must use only ASCII characters.
   Do not use extended ASCII or double-byte characters.

   The installer compares the system requirements for the selected components with the machine’s resources.

   - Insufficient disk space prompts an error message. The installer quits when you click **OK**.
   - Insufficient RAM prompts a warning message. The installation continues when you click **OK**. To ensure optimal performance, increase the machine’s memory to the recommended amount after installation.

18. On the summary screen, click **Next**.

19. In the message stating that features like protocol management and Bandwidth Optimizer cannot be used unless Network Agent is installed, click **Next**.

   After installation, use Websense Manager to configure the Network Agent running on the V10000 appliance to use these features. See *Configure Websense Manager*, page 34.

20. Click **Next** in the Installation Complete screen.

   When the installer finishes running, a Web page provides instructions for launching Websense Manager.

21. If you stopped your anti-virus software, restart it.
Configure Websense Manager

Websense Manager is the central configuration and management interface for Websense Web Security. Use it to customize filtering behavior, monitor Internet usage, generate Internet usage reports, and manage Websense software configuration and settings. This Web-based tool runs on Microsoft Internet Explorer 7 and Mozilla Firefox 2 and 3.

Gather the following information before configuring Websense Manager. Some of this information may have been gathered on the Quick Start during hardware setup.

<table>
<thead>
<tr>
<th>User name</th>
<th>WebsenseAdministrator (default)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>Unified password created when you configured the V10000 (during firstboot)</td>
</tr>
<tr>
<td>Subscription key</td>
<td></td>
</tr>
<tr>
<td>Proxy server IP or name</td>
<td></td>
</tr>
<tr>
<td>Proxy server port</td>
<td></td>
</tr>
</tbody>
</table>

Use the following steps to configure default filtering.

1. On the installation machine, launch Websense Manager by double-clicking the Websense Manager desktop icon, or going to Start > Programs > Websense > Websense Manager.
   Access to Websense Manager is secured with an SSL security certificate issued by Websense, Inc. Because the browser does not recognize Websense, Inc., as a known Certificate Authority (CA), a security warning is displayed.
   For instructions on launching Websense Manager from a remote machine, see Websense Manager Help.

2. To access Websense Manager, do one of the following:
   - Select the option to ignore the warning and continue. (The exact phrasing of this option varies between browsers.)
   - Permanently accept or install the certificate. (See Accepting the Websense Manager security certificate in the Websense Knowledge base for instructions).

3. Log on with the following credentials:
   User name: WebsenseAdministrator
   Password: (enter the unified password set up during V10000 configuration)

4. You are offered the option of launching a Quick Start tutorial. Quick Start tutorials provide an excellent method for becoming familiar with Websense software. To continue following the steps in this guide, click Skip to continue to Websense Manager.
   Websense Manager opens, showing the Status > Today page. Because you have not yet entered a subscription key, the Health Alert Summary at the top of the page shows a series of errors and warnings.
5. Click the *Settings* tab of the left navigation pane. The *Settings > Account* page is displayed.

6. Enter your *Subscription key* exactly as you received it.

7. Create a new, secure password in the *Change Password* area, and then click *OK*.

8. Click *Save All* at the top of the right shortcut pane to save the key and the new password, and start downloading the Websense Master Database.

### Note

The Riverbed Steelhead 250 is designed for a small branch office. Due to capacity limitations, the daily downloads of the Websense Master Database can consume all CPU resources on the Steelhead 250. If this occurs, the Riverbed Steelhead administrator receives several alert emails about high CPU usage.

For best results, configure Websense Web Security to download the Master Database only in the evening or at another time when high CPU usage does not interrupt your production environment.

To set the database download schedule in Websense Manager, please see the embedded Help system.

No filtering occurs until you enter a subscription key. Downloading the database ensures full and accurate filtering.

The Master Database, which contains the category and protocol definitions that provide the basis for Internet filtering, begins to download automatically.

If Websense software must go through a proxy to perform the download, also use the *Settings > Database Download* page to configure proxy settings (see Websense Manager Help for instructions).

The process of downloading the full database may take a few minutes or more than 60 minutes, depending on factors such as Internet connection speed, bandwidth, available memory, and free disk space.

For more information about Master Database downloads, see Websense Manager Help.

9. If you plan to apply filtering policies to individual users, groups, and domains in your network:

   a. Go to *Settings > Directory Service*.

   b. Select the directory service used in your network, and configure its settings. See Websense Manager Help for assistance.

### Important

If your network uses a Windows NT directory or Active Directory (Mixed Mode), or you use Logon Agent to transparently identify users in Active Directory (Native Mode), see *Special directory service considerations*, page 37, for important configuration steps.
10. Go to **Settings > Network Agent > Global**. After making any changes, click **OK**, and then click **Save All**.

Initially, Websense Network Agent uses these guidelines to identify the machines in your network and start filtering requests.

- Machines in the following IP address ranges are assumed to be internal machines. Requests sent to these machines, and messages sent between these machines, are ignored.
  
  10.0.0.0 - 10.255.255.255
  172.16.0.0 - 172.31.255.255
  192.168.0.0 - 192.168.255.255
  224.0.0.0 - 239.255.255.255

- Requests sent to the Internet from all internal machines visible to Network Agent are monitored.

If this basic configuration is adequate for your network, no additional configuration is necessary.

If, however, you want to configure Network Agent to monitor requests sent to some internal machines (like an internal Web server), or to ignore Internet requests sent from certain machines, you can make those changes in Websense Manager, under **Settings > Network Agent > Global**. See Websense Manager Help for details.

11. If you are using explicit proxy, click the IP address under **Settings > Network Agent** in the left navigation pane.

12. Click **Add** in the Proxies and Caches area.

13. Enter the IP address assigned to the network interface used for inbound traffic on the V10000 appliance (usually P1, but some organizations may use P2 for inbound traffic).

**Note**

On the V10000 appliance, Websense sends blocking information for non-HTTP protocols through the N network interface if it is connected to a bidirectional span port, and that port is identified and configured in the V10000 console. Otherwise, blocking information is sent through the C interface.

Configuration settings or changes for the blocking NIC in Websense Manager are disregarded by the V10000. (See the Websense Manager Help topic on Configuring NIC settings for information about the blocking NIC.)

14. Click **OK** to cache your changes. Changes are not implemented until you click **Save All**.

These are the steps required to configure Websense Web Security so that the Websense V10000 is ready for default operations. See the Websense Manager Help for details on the variety of features and options available for Websense Web Security.
Special directory service considerations

If you plan to apply filtering policies to individual users and groups in your network, special configuration steps are required to assure that the Websense V10000 can identify users successfully in networks that:

- Use Windows NT Directory or Active Directory (Mixed Mode)
- Plan to use Websense Logon Agent to transparently identify users in Active Directory (Native Mode).

In these environments, the Websense V10000 appliance must be configured to communicate with a Windows Internet Name Server (WINS) to resolve domain names to domain controller IP addresses. The precise steps vary, depending on your environment.

If your network uses Windows NT Directory or Active Directory (Mixed Mode):

1. In Websense Manager, go to the Settings > Directory Service page.
2. Select Windows NT Directory / Active Directory (Mixed Mode), which is the default.
3. Enter the name and password for the administrative user.
4. Enter the Domain name.
   - If your organization uses multiple domains, enter the name of a domain that is trusted by all domains that authenticate your users.
5. Enter the IP address of a Windows Internet Name Server (WINS) that can resolve the domain name entered above to a domain controller IP address.
6. Click OK to cache your changes. Changes are not implemented until you click Save All.

If your network uses Active Directory (Native Mode), and uses Logon Agent to transparently identify users for filtering:

1. In Websense Manager, go to the Settings > Directory Service page.
2. Provide administrative credentials and identify the Windows Internet Name Server (WINS), as follows.
   a. Select Windows NT Directory / Active Directory (Mixed Mode), which is the default.
   b. Enter the name and password for the administrative user.
   c. Enter the Domain name.
      - If your organization uses multiple domains, enter the name of a domain that is trusted by all domains that authenticate your users.
   d. Enter the IP address of a Windows Internet Name Server (WINS) that can resolve the domain name entered above to a domain controller IP address.
   e. Click OK to cache your changes.
   f. Click Save All to implement these changes.
4. Configure the global catalog servers and other settings for your directory service. See Websense Manager Help for assistance.
5. Click OK to cache your changes. Changes are not implemented until you click Save All.

Configure Websense Content Gateway

Content Manager is the Web-based configuration interface for Websense Content Gateway. Use it to enter the subscription key and download associated databases as part of your initial setup for the Websense V10000 appliance.

Gather the following information before configuring Websense Content Gateway. Some of this information may have been gathered on the Quick Start during hardware setup.

<table>
<thead>
<tr>
<th>User name</th>
<th>admin (default)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>Unified password specified when you configured the V10000 (during firstboot)</td>
</tr>
<tr>
<td>Subscription key</td>
<td>(same as entered in Websense Manager)</td>
</tr>
<tr>
<td>New password</td>
<td></td>
</tr>
</tbody>
</table>

Use the following steps to enter the configuration required to enable default proxy caching.

1. Browse to:
   
   https://<IP address>:8081
   
   Replace <IP address> with the address for network interface C, configured during firstboot (visible in the V10000 Console).
   
   An SSL connection is used for secure, browser-based communication with Content Manager. This connection uses a security certificate issued by Websense, Inc. Because the supported browsers do not recognize Websense, Inc., as a known Certificate Authority, a certificate error is displayed when you launch Content Manager in a new browser session.

2. To access Content Manager, do one of the following:
   
   - Select the option to ignore the warning and continue. (The exact phrasing of this option varies between browsers.)
   - Permanently accept or install the certificate by using procedures appropriate for your browser.

3. Log on with the following credentials:
   User name: admin
   Password: (unified password set up during V10000 configuration)

4. Click the Configure tab in the left navigation pane.
5. Click **My Proxy > Subscription > Subscription Management**.
6. Enter your **Subscription key**, then click **Apply**.
7. Click **My Proxy > UI Setup > Login**.
8. Set a new password for the administrator account, then click **Apply**.
9. Still on the Configure tab, go to **My Proxy > Basic**, and click the **Restart** button.

These are the steps required to configure Websense Content Gateway so that the Websense V10000 is ready for default operations. See the Content Manager Help for details on the variety of features and options available for Websense Content Gateway.

**Test and refine your policies**

After performing the procedures outlined in this document, run the following tests to verify that the system is configured and operating properly.

1. Go to another computer in the network that is monitored by the Websense V10000 appliance.
2. Open a Web browser, and browse to several different sites to generate Internet traffic.
   
   If possible, browse to sites that would likely fall into several different categories; for example, Games, Education, Entertainment, Sports, Shopping, Travel, and Vehicles.

   **Note**

   Since the Default policy enforces the Monitor Only category filter, all sites are permitted.

3. Access Websense Manager by entering the following address:

   ```text
   https://<IP address>:9443/mng
   ```

   Replace `<IP address>` with the IP address of the Websense Manager machine.
4. Log on as WebsenseAdministrator, with the password you set during installation.
5. Observe the charts on the Today page to verify that they reflect the traffic you just generated.

   **Note**

   Charts on the Today page are refreshed every 2 minutes. If they reflect the sites that you browsed to after the next refresh, your configuration is correct.

   If the correct data is not shown, verify that you have correctly entered the configuration information, as described in this document.

After you verify that the system is operating according to the default settings:
1. In Websense Manager, go to Help > Quick Start Tutorials > New User. Work through the lessons to become familiar with the Websense Manager interface, and learn to configure and manage Web filtering policies.

2. Configure policies suitable to your organization’s specific needs, and assign them to the appropriate clients.
   See Websense Manager Help for detailed instructions.

3. Open Content Manager, and customize proxy caching to meet your organization’s specific needs.
   See Websense Content Manager Help for detailed instructions.

4. Open the V10000 Console to view system status, modify the configuration, or manage the appliance.
   See the V10000 Console Help for detailed instructions.

---

### Recovering the V10000 appliance

The Websense V10000 appliance comes with a recovery DVD that can be used to restore the appliance to its factory image, in the event of a serious problem.

1. If possible, back up any information you want preserve.
   a. Log on to the V10000 Console for the primary V10000 appliance.
   c. Go to Administration > Backup Utility, and create a backup for Websense Web Security. See online Help for assistance.
   d. Contact Technical Support for assistance in creating a backup of your Websense Content Gateway configuration.
      For additional information about creating a snapshot (backup) of your Content Gateway configuration, see the Websense Content Gateway Administrator’s Guide.

2. Insert the recovery DVD into the drive.

3. Turn off the power, and then turn it on again.

4. When the list of function keys appears during reboot, press F11, and then select Boot from DVD-ROM.

5. When asked whether you want to reload the system, enter y.
   Restoring the image can take 20 minutes or more.

6. When prompted to begin, enter y.
   This begins the firstboot script.

7. Follow the onscreen instructions to provide the necessary information.
   See Perform initial command line configuration, page 26, for details of what information is requested.
8. Restore the backed up configuration.
   a. Log on to the V10000 Console for the primary V10000 appliance.
   b. Go to Administration > Backup Utility.
   c. Restore the Websense Web Security configuration from the backup created earlier. See online Help for assistance.
   d. Contact Technical Support for assistance in restoring the backup of your Websense Content Gateway configuration.

Install Websense components at the branch office

The following steps explain how to log on to the uploaded VM image on the Steelhead 250 at the branch office and install Websense Network Agent and Filtering Service in Stand-alone mode.

Websense Policy Server must be running in the data center when you start this installation at the branch. In other words, the components you install on the Steelhead 250 need to be able to locate and communicate with Policy Server during installation. To enable this, you are prompted to provide an IP address for Policy Server and the port number for Policy Server (port 55806 by default).

The following ports need to be open and available for communication with the Windows server and the Websense V10000 appliance at your data center that is running the Websense components:

- **Websense Manager - Ports 9443 and 9444**
  These ports are used to enable secure browser connections to Websense Manager (including reporting features). Both the Apache2Websense and ApacheTomcatWebsense services use port 9443. The Tomcat service also uses port 9444.

- **Filtering Service - Port 15868**
  Websense Filtering Service listens on this port for requests. If the port is blocked, you will not be able to filter user traffic.
  Websense Filtering Service may also use this port for communication with Network Agent.

- **Block Messages - Port 15871**
  Websense Filtering Service uses this port to transmit block pages, continue pages, and quota pages to users who try to access restricted sites.

- **Block Message Authentication - Port 15872**

- **Log Server - Port 55805**
  Log Server listens on this port. The Filtering Service sends records about Internet and protocol activity to the Log Server, which then transmits the data to the Log Database for reporting.
Installing Websense Components

Websense Knowledge Base article 3365 at MyWebsense.com provides a complete list of port numbers used by Websense software.

Installation procedure: branch components

Use these steps to install Websense software components on the Steelhead 250 at any branch office. The sections that follow provide additional, component-specific details.

1. Preparation:
   - Log on to the uploaded VM image on the Steelhead 250 at the branch office with appropriate permissions.
   - Close all applications and stop any anti-virus software on the Steelhead appliance.
   - Download and start the Websense installer, if needed.
2. Click Next on the Welcome screen.
3. Select Yes to accept the Subscription Agreement, and then click Next.
4. On the next screen, select Custom, and then click Next again.
   A list of components is displayed.
5. Select only two components to install (Filtering Service and Network Agent only), and then click Next.
6. Be prepared to provide the following information, when prompted:
   - Because Policy Server is installed on a different machine, provide the Policy Server IP address and configuration port (55806, by default), when prompted. Typically, the IP address of Policy Server is the IP address for network interface C on the V10000 appliance.
   - The installer asks you to confirm that you want to install Network Agent on this machine, and that the machine is not running a firewall. Select Yes to install Network Agent, and click Next. Installation continues.
   - The installer prompts you to select the NIC that Network Agent can use for communicating. All enabled NICs with an IP address are listed. Do not choose a NIC without an IP address. Select a NIC and click Next to continue.
   - The installer asks if you want to allow Websense, Inc., to gather information about the use of Websense-defined protocols. This information is used to enhance protocol filtering.

   ![Note]

   Network Agent never sends Websense, Inc., any information that would identify specific users, no matter which Network Agent feedback option is selected.

7. Accept the default installation path or click Browse to locate another path, and then click Next. The installation path must be absolute (not relative). The default installation path is:

42 Websense Web Security and Riverbed Steelhead
Installing Websense Components

- **Windows**: `C:\Program Files\Websense`
  The installer creates this directory if it does not exist.

---

**Important**

- The full installation path must use only ASCII characters.
- Do not use extended ASCII or double-byte characters.

The installer compares its system requirements with the machine's resources. Click **OK** if you see either of these messages. They are likely to appear on the Steelhead 250 but can be safely bypassed:

- Insufficient disk space prompts an error message. Click **OK**.
- Insufficient RAM prompts a warning message. Click **OK**.

A summary shows the installation path and size, and the components to be installed.

8. Click **Next** to start the installation.
9. Click **Next** on the Installation Complete screen.
   When the installer finishes running, a Web page provides instructions for launching Websense Manager.
10. If you stopped your anti-virus software, restart it.

### Configuring the branch copy of Network Agent at the data center

Note that each copy of Network Agent installed in a branch office needs to be assigned IP address ranges (for the client machines it monitors at the branch office).

After branch office installation, configure Network Agent by using Websense Manager at the data center. See the *Network Configuration* topic in Websense Manager Help for detailed instructions. Be sure to choose the correct Network Agent NIC before making assignments for each branch office.

### Known Issues

For installations where a portion of the branch office Internet traffic passes through the Websense Content Gateway proxy (located in the data center), and other branch office traffic does not pass through the Websense proxy (is filtered locally), you may notice some apparent inconsistencies in Web filtering. These differences are expected behavior when the same users are filtered in two different ways (with and without proxy), and are explained below.

#### Quota time cannot be determined precisely

Quota time used by each user each day is tracked by Websense Filtering Service. Because there are two instances of Filtering Service (one on the Websense V10000 in the data center, and one on the Riverbed Steelhead 250) handling URL requests from the same users in the branch office, this means that two quota user maps are maintained for each branch user.
In this situation, assume that a branch user has consumed all assigned quota time for the day by browsing URLs accessed through the proxy in the data center. That same user would still be able to access URLs that have quota, if they are accessed by the local network directly.

**HTTPS block page cannot be displayed in non-proxy environment**

The application layer data is encrypted by SSL, so Filtering Service categorizes a requested URL by IP address, not by URL (such as www.casino.com). The SSL symmetric key is generated between the branch client and the HTTPS server, and is not available to the component that typically serves up the block page.

Therefore, a user would not see HTTPS block pages in a non-proxy environment.

The software instead resets the HTTPS connection between the branch user and the requested HTTPS server. (See exception below for Quota and Confirm.)

**Quota/Confirm HTTPS URL permitted in non-proxy environment**

As mentioned above, an HTTPS block page cannot be displayed in a non-proxy environment. Thus, the filtering software cannot offer a Quota or Confirm page to users who request these URLs. The software instead permits all quota and confirm HTTPS URLs in a non-proxy environment.

However, the HTTPs block page is displayed in the proxy environment. Therefore, Quota/Confirm HTTPS sites see a block page (as expected) in the proxy environment, and the user can choose whether to continue accessing the Web site on the block page.

**Online Help**

Select the **Help** option within the program to display detailed information about using the product.

---

**IMPORTANT**

Default Microsoft Internet Explorer settings may block operation of the Help system. If a security alert appears, select **Allow Blocked Content** to display Help.

If your organization’s security standards permit, you can permanently disable the warning message on the Advanced tab of the **Tools > Internet Options** interface.

(Check **Allow active content to run in files on My Computer** under Security options.)
Technical Support

Technical information about Websense software and services is available 24 hours a day at:

www.websense.com/support/

- the latest release information
- the searchable Websense Knowledge Base
- Customer Forums
- Support Webinars
- show-me tutorials
- product documents
- answers to frequently asked questions
- Top Customer Issues
- in-depth technical papers

For additional questions, click the Contact Support tab at the top of the page.

If your issue is urgent, please call one of the offices listed below. You will be routed to the first available technician, who will gladly assist you.

For less urgent cases, use our online Support Request Portal at ask.websense.com.

For faster phone response, please use your Support Account ID, which you can find in the Profile section at MyWebsense.

<table>
<thead>
<tr>
<th>Location</th>
<th>Contact information</th>
</tr>
</thead>
<tbody>
<tr>
<td>North America</td>
<td>+1-858-458-2940</td>
</tr>
<tr>
<td>France</td>
<td>Contact your Websense Reseller. If you cannot locate your Reseller: +33 (0) 1 5732 3227</td>
</tr>
<tr>
<td>Germany</td>
<td>Contact your Websense Reseller. If you cannot locate your Reseller: +49 (0) 69 517 09347</td>
</tr>
<tr>
<td>UK</td>
<td>Contact your Websense Reseller. If you cannot locate your Reseller: +44 (0) 20 3024 4401</td>
</tr>
<tr>
<td>Rest of Europe</td>
<td>Contact your Websense Reseller. If you cannot locate your Reseller: +44 (0) 20 3024 4401</td>
</tr>
<tr>
<td>Middle East</td>
<td>Contact your Websense Reseller. If you cannot locate your Reseller: +44 (0) 20 3024 4401</td>
</tr>
<tr>
<td>Africa</td>
<td>Contact your Websense Reseller. If you cannot locate your Reseller: +44 (0) 20 3024 4401</td>
</tr>
<tr>
<td>Australia/NZ</td>
<td>Contact your Websense Reseller. If you cannot locate your Reseller: +61 (0) 2 9414 0033</td>
</tr>
</tbody>
</table>
Installing Websense Components

<table>
<thead>
<tr>
<th>Location</th>
<th>Contact information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asia</td>
<td>Contact your Websense Reseller. If you cannot locate your Reseller: +86 (10) 5884 4200</td>
</tr>
<tr>
<td>Latin America and Caribbean</td>
<td>+1-858-458-2940</td>
</tr>
</tbody>
</table>

For telephone requests, please have ready:

- Websense subscription key
- Access to the machine running reporting tools and the database server (Microsoft SQL Server or MSDE)
- Familiarity with your network’s architecture, or access to a specialist