websense®

# Getting Started

Websense® Web Security v7.1
with Riverbed Steelhead Appliance 1050

v7.1

Published 2009 Revision C
Printed in the United States of America and Ireland

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

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

## Trademarks

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

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

Novell, Novell Directory Services, eDirectory, and ZENworks are trademarks or registered trademarks of Novell, Inc., in the United States and other countries.

Pentium and Xeon are registered trademarks of Intel Corporation.

This product includes software developed by the Apache Software Foundation (www.apache.org).

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

## WinPcap

# Contents

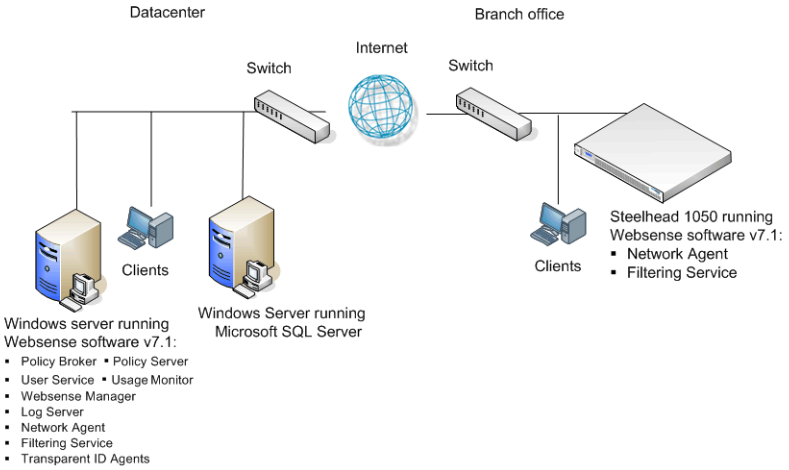
# 1 Websense® Web Security with the Riverbed® Steelhead™ 1050

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 1050 appliance at branch offices and Windows servers 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 1050 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 Windows server.

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 Windows server also 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 Windows servers. Others are optional, such as a directory service, which allows you to apply Web filtering policy to individual users and groups in your organization.

## Windows servers

Your data center must have a Windows server machine that meets the requirements listed below. This is the machine where you install centralized Websense components, such as 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), and your policy 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 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 (any listed)

- 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 required 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

The following recommendations apply to the machine running the database engine, especially if it runs on the same Windows server as Websense 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 data center.

## 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*.

# 2 Setting up the Riverbed Steelhead 1050

Setting up Websense software integrated with the Steelhead 1050 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. *Set up the appliance hardware*.
3. *Perform initial command line configuration* on the appliance.
4. Update the Steelhead 1050 to the latest image (RiOS - Base OS).
5. *Configure the Steelhead 1050* for use with Websense software.
6. Install two components of Websense software on the Steelhead 1050. See *Install Websense components at the branch office*

## Set up the appliance hardware

Follow the Riverbed Steelhead hardware setup guide for model 1050 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.

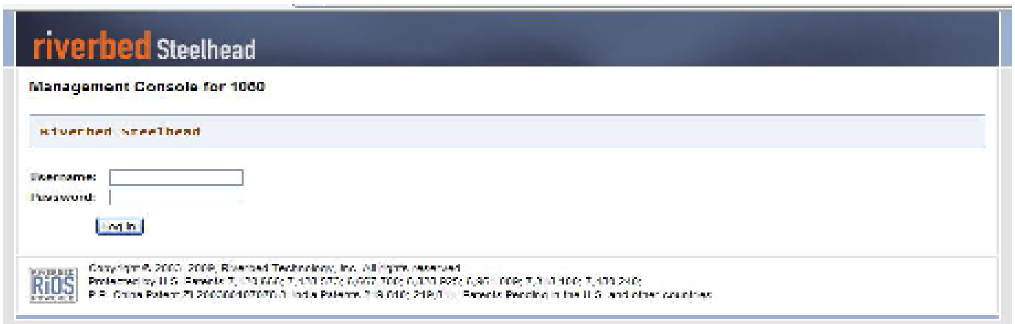
1. Access the appliance through the a USB keyboard and monitor or a serial port connection.

   > **Note**
   > To configure the appliance, connect through the serial port or the keyboard/video ports and complete the jump-start script.

2. To run the initial script, enter the following commands:

   ```
   en
   config t
   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 1050 Console. See *Configure the Steelhead 1050*, page 11.



Copyright © 2003 - 2009, Riverbed Technology, Inc. All rights reserved
[illegible]
[illegible] Patents Pending in the U.S. and other countries

# Configure the Steelhead 1050

The Steelhead 1050 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 1050 administration tasks.

After completing the initial configuration required by the jump-start script, use the Steelhead 1050 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 1050 configuration

Gather the following information before running the Steelhead 1050 console. Some of this information may have been gathered during hardware setup.

| | |
|---|---|
| User name and password for accessing the Riverbed Support Web site | |
| IP address assigned to the network interface for the Steelhead 1050 console manager | |
| RSP license key from Riverbed | |
| IP address for network interface Inpath 0_0 | |
| Subnet mask for network interface Inpath 0_0 | |
| Default gateway for network interface Inpath 0_0 (IP address) | |

See the Steelhead 1050 help system for detailed instructions on any field or area, or for information about other available settings.

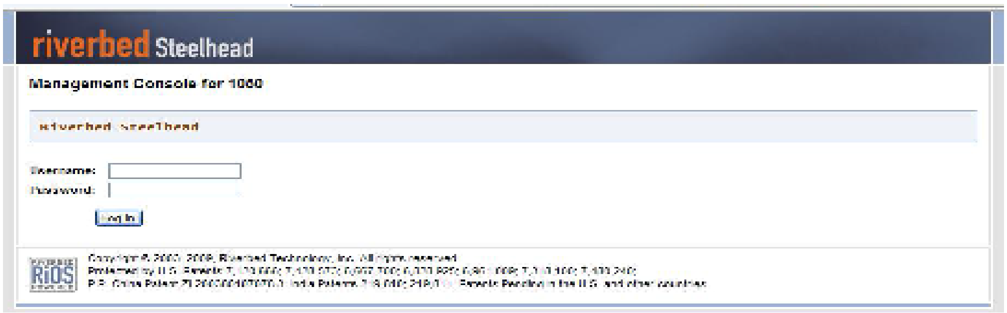
## Upgrading to the latest appliance image

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 1050.

2. Log on with the user name **admin** and the password assigned during initial configuration of the Steelhead 1050.



Management Console for 1050

Riverbed Steelhead

Username:

Password:

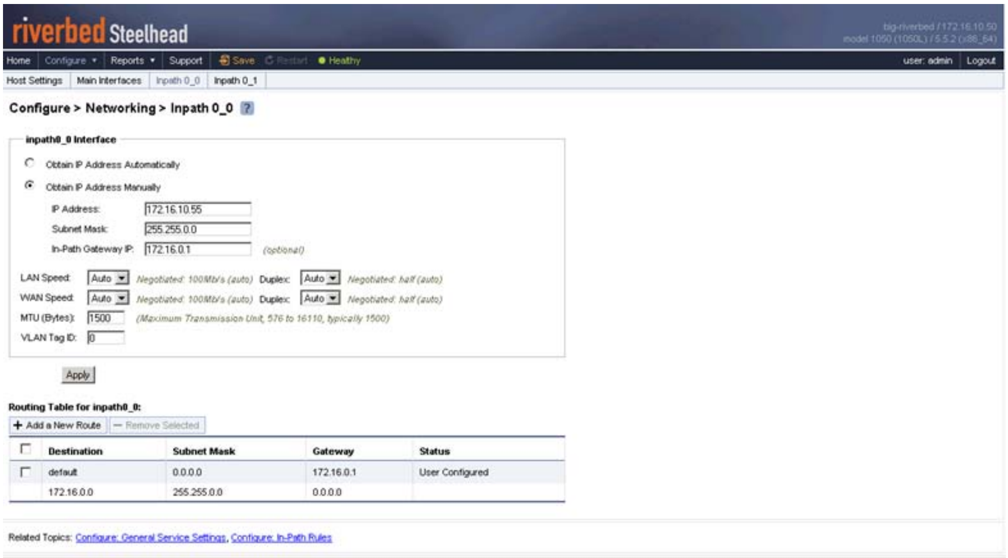
Copyright © 2003 - 2009, Riverbed Technology, Inc. All rights reserved
Protected by U.S. Patents [illegible]
P.R. China Patent [illegible] India Patents [illegible] Patents Pending in the U.S. and other countries

3. Upgrade the Steelhead 1050 software to the latest image:
   a. Open a supported browser, and enter the following URL in the address bar:

      `http://www.riverbed.com/support`

   b. Download the latest software image (RiOS - Base OS) available from the support site. Please download the version specific to Steelhead 1050. You can also sign up for upgrades with Riverbed at this time.

4. Configure the inpath0_0 Interface by navigating to **Configure > Networking > Inpath0_0**.



Configure > Networking > Inpath 0_0 ?

inpath0_0 Interface

○ Obtain IP Address Automatically

● Obtain IP Address Manually

IP Address: 172.16.10.55

Subnet Mask: 255.255.0.0

In-Path Gateway IP: 172.16.0.1 (optional)

LAN Speed: Auto *Negotiated: 100Mb/s (auto)* Duplex: Auto *Negotiated: half (auto)*

WAN Speed: Auto *Negotiated: 100Mb/s (auto)* Duplex: Auto *Negotiated: half (auto)*

MTU (Bytes): 1500 *(Maximum Transmission Unit, 576 to 16110, typically 1500)*

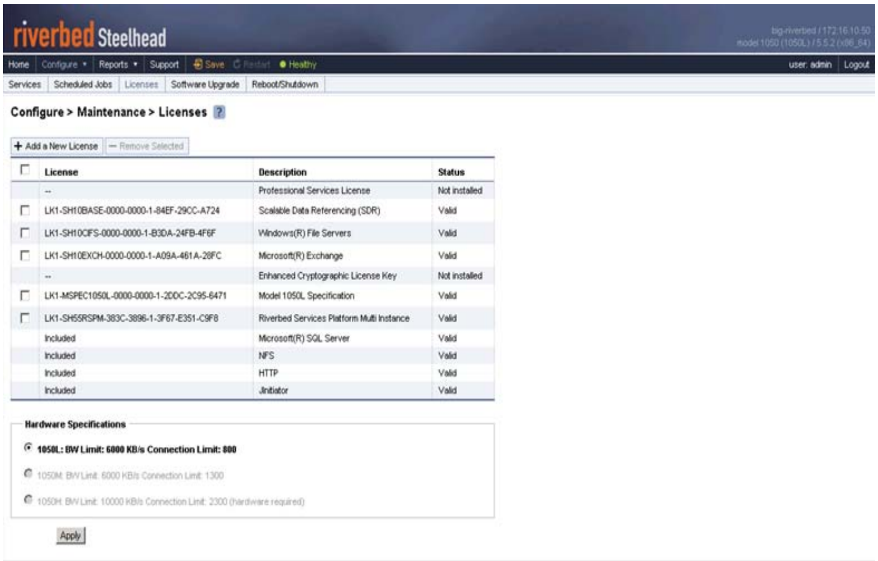
VLAN Tag ID: 0

Routing Table for inpath0_0:

| □ | Destination | Subnet Mask | Gateway | Status |
|---|---|---|---|---|
| □ | default | 0.0.0.0 | 172.16.0.1 | User Configured |
|  | 172.16.0.0 | 255.255.0.0 | 0.0.0.0 |  |

Related Topics: Configure: General Service Settings, Configure: In-Path Rules

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



| □ | License | Description | Status |
|---|---|---|---|
|  | -- | Professional Services License | Not installed |
| □ | LK1-SH10BASE-0000-0000-1-84EF-29CC-A724 | Scalable Data Referencing (SDR) | Valid |
| □ | LK1-SH10CIFS-0000-0000-1-B3DA-24FB-4F6F | Windows(R) File Servers | Valid |
| □ | LK1-SH10EXCH-0000-0000-1-A09A-461A-28FC | Microsoft(R) Exchange | Valid |
|  | -- | Enhanced Cryptographic License Key | Not installed |
| □ | LK1-MSPEC1050L-0000-0000-1-2DDC-2C95-6471 | Model 1050L Specification | Valid |
| □ | LK1-SH55RSPM-383C-3896-1-3F67-E351-C9F8 | Riverbed Services Platform Multi Instance | Valid |
|  | Included | Microsoft(R) SQL Server | Valid |
|  | Included | NFS | Valid |
|  | Included | HTTP | Valid |
|  | Included | Jinitiator | Valid |

Hardware Specifications

● **1050L: BW Limit: 6000 KB/s Connection Limit: 800**

○ 1050M: BW Limit: 6000 KB/s Connection Limit: 1300

○ 1050H: BW Limit: 10000 KB/s Connection Limit: 2300 (hardware required)

6. Upgrade the RSP to the latest image (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 latest RSP image available from the support site. Please download the version specific to Steelhead 1050.

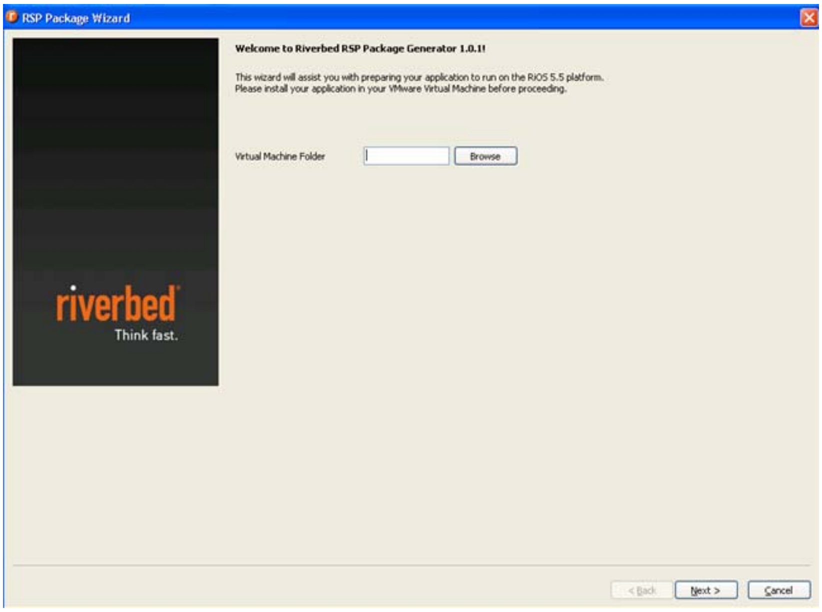
## Generating the package at the VMware workstation

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 using VMware Workstation Version 6.5.0 build-118166. For complete details about this process, see the topic *Reconfiguring the Virtual Machine for RSP* in the “Riverbed Services Platform Installation and Configuration Guide.”
   a. Browse to your Windows Virtual Machine folder.
   b. Allocate 2 Gigabytes of RAM for the image. Allocate all disk space at once. The generator does not allow you to increase the disk space later.
   c. Under **Edit Virtual Machine Settings**, choose **Add Multiple Network Adapters**.
   d. 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.

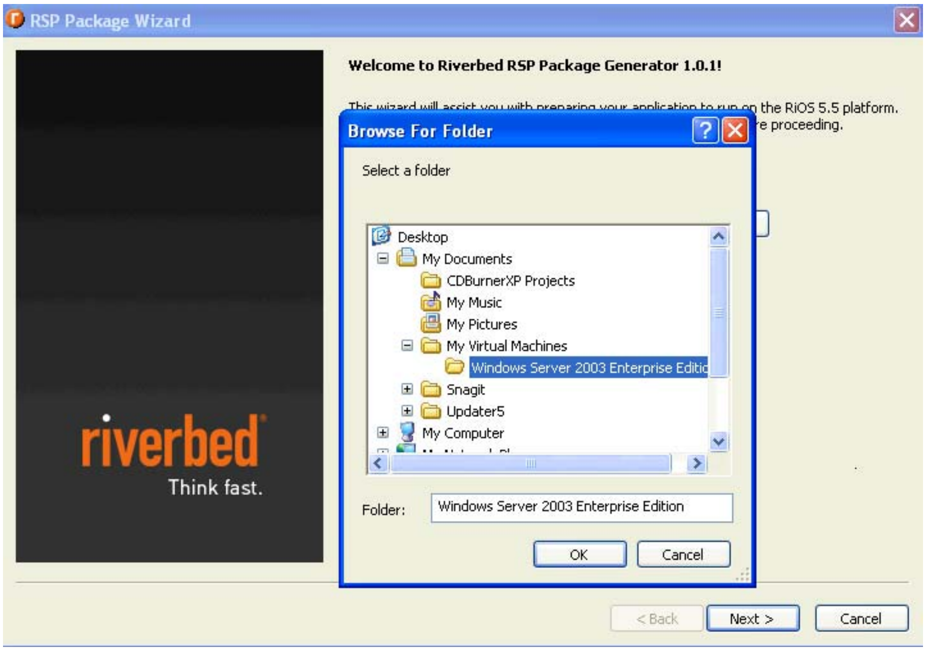


**Welcome to Riverbed RSP Package Generator 1.0.1!**

This wizard will assist you with preparing your application to run on the RiOS 5.5 platform.
Please install your application in your VMware Virtual Machine before proceeding.

Virtual Machine Folder

5. Point the RSP Package Generator to the VM directory.



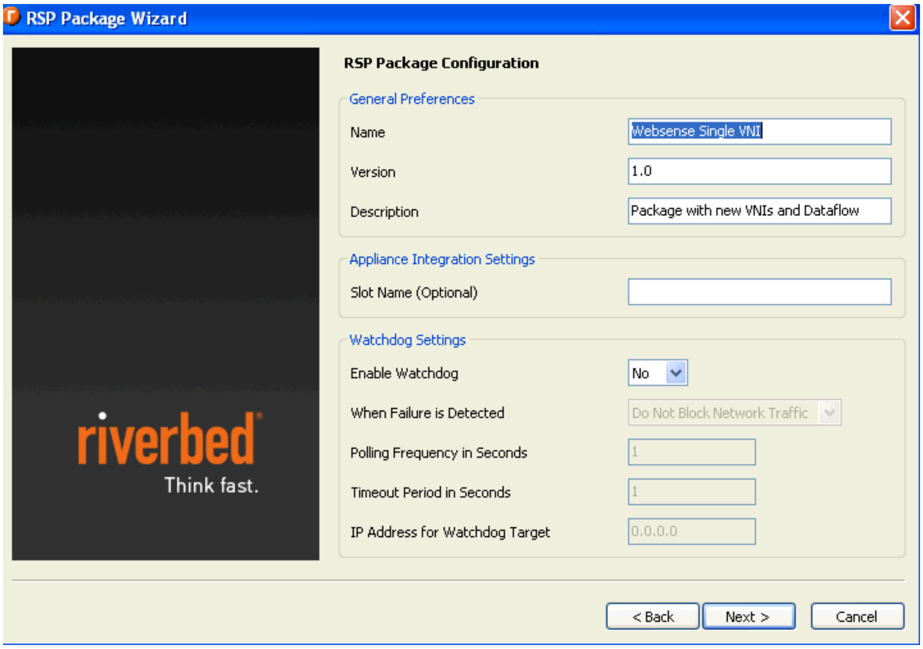
**Welcome to Riverbed RSP Package Generator 1.0.1!**

This wizard will assist you with preparing your application to run on the RiOS 5.5 platform.
re proceeding.

Select a folder

Folder: Windows Server 2003 Enterprise Edition

6. Configure the RSP package details, and then click **Next**.



RSP Package Wizard

RSP Package Configuration

General Preferences

Name: Websense Single VNI

Version: 1.0

Description: Package with new VNIs and Dataflow

Appliance Integration Settings

Slot Name (Optional):

Watchdog Settings

Enable Watchdog: No

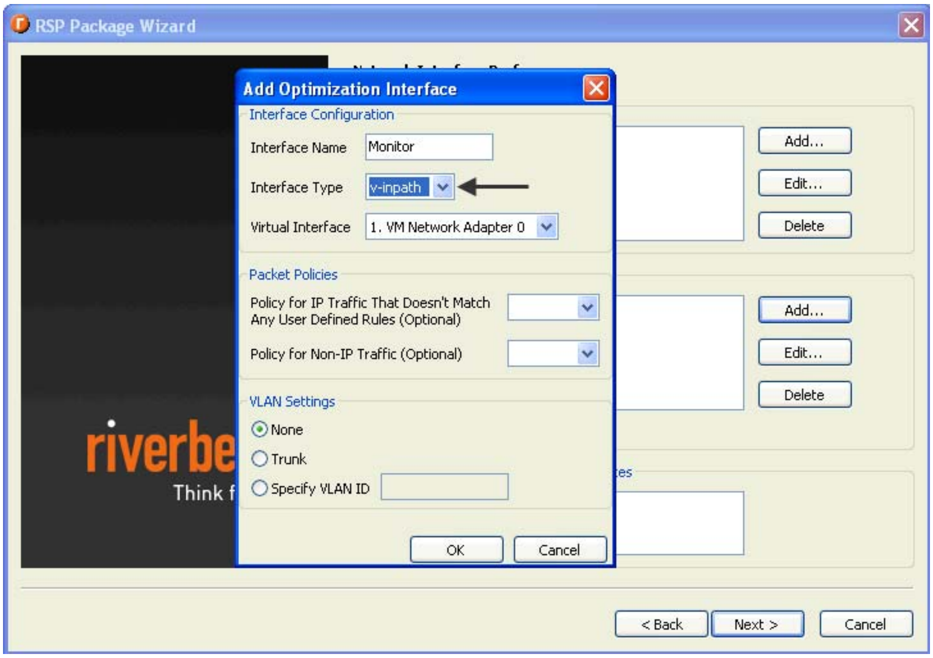
When Failure is Detected: Do Not Block Network Traffic

Polling Frequency in Seconds: 1

Timeout Period in Seconds: 1

IP Address for Watchdog Target: 0.0.0.0

7. Add a single v-inpath VNI by clicking **Add** under Optimization Interfaces.



RSP Package Wizard

Add Optimization Interface

Interface Configuration

Interface Name: Monitor

Interface Type: v-inpath

Virtual Interface: 1. VM Network Adapter 0

Packet Policies

Policy for IP Traffic That Doesn't Match Any User Defined Rules (Optional):

Policy for Non-IP Traffic (Optional):

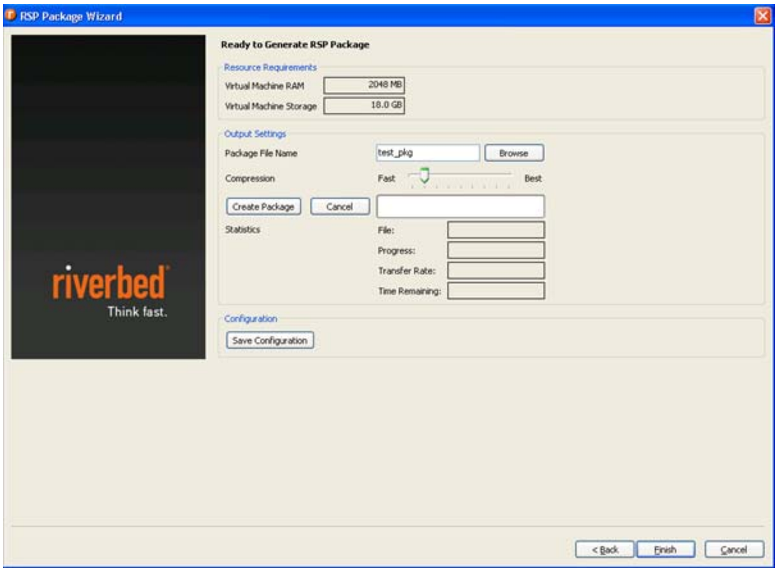
VLAN Settings

● None

○ Trunk

○ Specify VLAN ID

8. Ensure that Resource Requirements are sufficient.
   a. Virtual Machine RAM must be at least 2048 megabytes.
   b. Virtual Machine Storage must be at least 18 gigabytes.
9. Fill in the Output settings, and then click **Create Package**. Your package is now ready.
10. After creating the RSP package, save the package by clicking **Save Configuration**.
11. Copy the package to a location that can be accessed by the RSP platform, or copy it to the Riverbed local file system. You can use a flash drive that has at least 1 GB of free space.



RSP Package Wizard

Ready to Generate RSP Package

Resource Requirements

Virtual Machine RAM: 2048 MB

Virtual Machine Storage: 18.0 GB

Output Settings

Package File Name: test_pkg

Compression: Fast – Best

Statistics

File:

Progress:

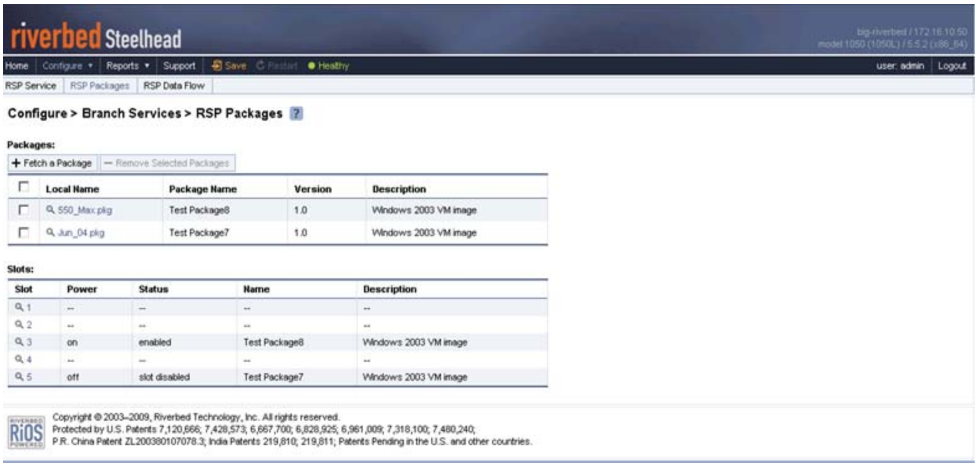
Transfer Rate:

Time Remaining:

Configuration

12. If you use a flash drive, insert the flash drive into a USB port in a client machine anywhere in the network.

13. To begin the process of uploading the RSP package from a client machine to the Steelhead 1050 appliance, navigate to **Configure** > **Branch Services** > **RSP Packages**.



Configure > Branch Services > RSP Packages

Packages:

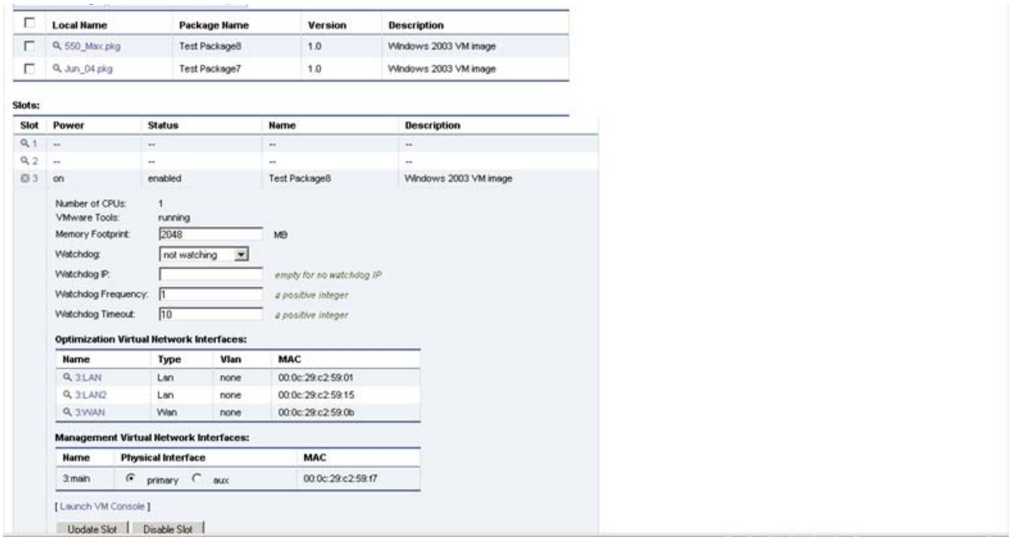
| □ | Local Name | Package Name | Version | Description |
|---|---|---|---|---|
| □ | 550_Max.pkg | Test Package8 | 1.0 | Windows 2003 VM image |
| □ | Jun_04.pkg | Test Package7 | 1.0 | Windows 2003 VM image |

Slots:

| Slot | Power | Status | Name | Description |
|---|---|---|---|---|
| 1 | -- | -- | -- | -- |
| 2 | -- | -- | -- | -- |
| 3 | on | enabled | Test Package8 | Windows 2003 VM image |
| 4 | -- | -- | -- | -- |
| 5 | off | slot disabled | Test Package7 | Windows 2003 VM image |

Copyright © 2003–2009, Riverbed Technology, Inc. All rights reserved.
Protected by U.S. Patents 7,120,666; 7,428,573; 6,667,700; 6,828,925; 6,961,009; 7,318,100; 7,480,240;
P.R. China Patent ZL200380107078.3; India Patents 219,810; 219,811; Patents Pending in the U.S. and other countries.

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



| □ | Local Name | Package Name | Version | Description |
|---|---|---|---|---|
| □ | 550_Max.pkg | Test Package8 | 1.0 | Windows 2003 VM image |
| □ | Jun_04.pkg | Test Package7 | 1.0 | Windows 2003 VM image |

Slots:

| Slot | Power | Status | Name | Description |
|---|---|---|---|---|
| 1 | -- | -- | -- | -- |
| 2 | -- | -- | -- | -- |
| 3 | on | enabled | Test Package8 | Windows 2003 VM image |

Number of CPUs: 1
VMware Tools: running
Memory Footprint: 2048 MB
Watchdog: not watching
Watchdog IP: *empty for no watchdog IP*
Watchdog Frequency: 1 *a positive integer*
Watchdog Timeout: 10 *a positive integer*

Optimization Virtual Network Interfaces:

| Name | Type | Vlan | MAC |
|---|---|---|---|
| 3:LAN | Lan | none | 00:0c:29:c2:59:01 |
| 3:LAN2 | Lan | none | 00:0c:29:c2:59:15 |
| 3:WAN | Wan | none | 00:0c:29:c2:59:0b |

Management Virtual Network Interfaces:

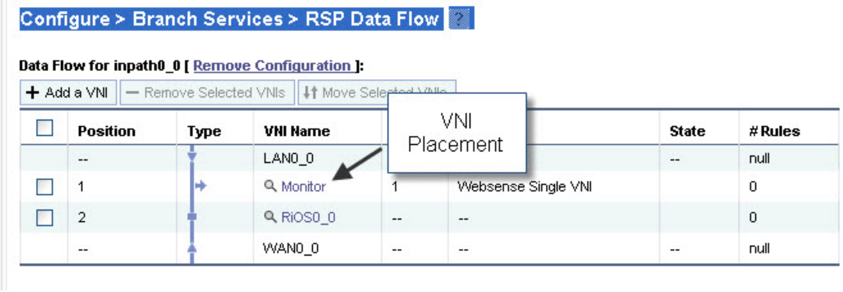
| Name | Physical Interface | MAC |
|---|---|---|
| 3:main | ● primary ○ aux | 00:0c:29:c2:59:f7 |

## 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.



Configure > Branch Services > RSP Data Flow

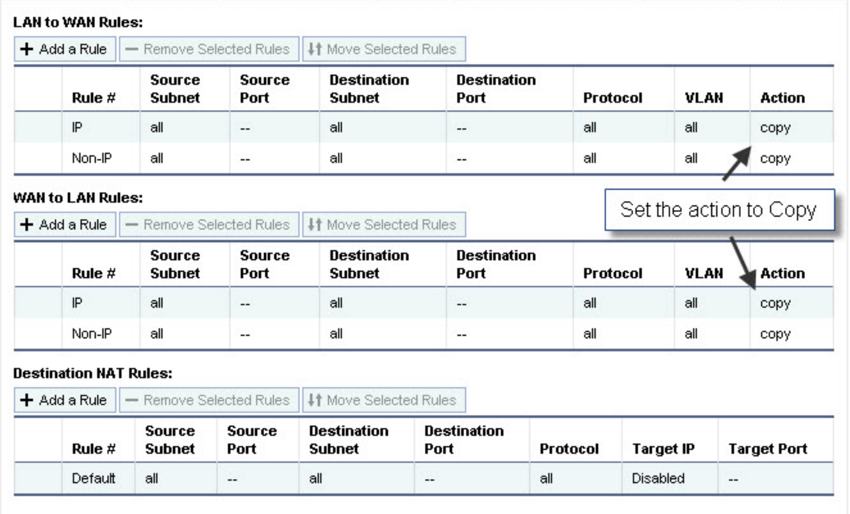
Data Flow for inpath0_0 [ Remove Configuration ]:

+ Add a VNI | — Remove Selected VNIs | Move Sele

| ☐ | Position | Type | VNI Name | | | State | # Rules |
|---|---|---|---|---|---|---|---|
| | -- | | LAN0_0 | | | -- | null |
| ☐ | 1 | | Monitor | 1 | Websense Single VNI | | 0 |
| ☐ | 2 | | RiOS0_0 | -- | -- | | 0 |
| | -- | | WAN0_0 | -- | -- | -- | null |

VNI Placement

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



LAN to WAN Rules:

+ Add a Rule | — Remove Selected Rules | Move Selected Rules

| Rule # | Source Subnet | Source Port | Destination Subnet | Destination Port | Protocol | VLAN | Action |
|---|---|---|---|---|---|---|---|
| IP | all | -- | all | -- | all | all | copy |
| Non-IP | all | -- | all | -- | all | all | copy |

WAN to LAN Rules:

+ Add a Rule | — Remove Selected Rules | Move Selected Rules

| Rule # | Source Subnet | Source Port | Destination Subnet | Destination Port | Protocol | VLAN | Action |
|---|---|---|---|---|---|---|---|
| IP | all | -- | all | -- | all | all | copy |
| Non-IP | all | -- | all | -- | all | all | copy |

Destination NAT Rules:

+ Add a Rule | — Remove Selected Rules | Move Selected Rules

| Rule # | Source Subnet | Source Port | Destination Subnet | Destination Port | Protocol | Target IP | Target Port |
|---|---|---|---|---|---|---|---|
| Default | all | -- | all | -- | all | Disabled | -- |

Set the action to Copy

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 should be 192.168.1.x/24.

4. Ping the Websense Web Security Gateway server, to make certain that both the Virtual Machine and the Web Security Gateway server 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 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.
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, the data center must configure the Network Agent running at the branch office to monitor the branch subdomain(s). See the next chapter for specifics.

# 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 1050 appliance at the branch offices.

## Install Microsoft SQL Server at the data center

Websense components and the database engine at the data center must be installed and running on a Windows server, before you install the Websense components at any branch offices.

The supported database engine at the data center must be installed first. It may be installed either on the same Windows server machine where Websense 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 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

Before installing Websense policy and reporting components, be sure your server machine meets the hardware and software requirements provided in Chapter 1 of this guide.

Be sure that ports used by Websense software do not conflict with ports already in use at your data center. Websense Knowledge Base article 3365 at www.mywebsense.com provides a complete list of port numbers used by Websense software.

Gather the following information before running the Websense installer.

| | |
|---|---|
| User name and password for use on the MyWebsense Web site | You can set up credentials at www.mywebsense.com |
| Websense Subscription key | |
| Database engine location<br>(IP address or machine name) | |
| Database user name | |
| Database password | |

The following procedure summarizes the steps for installing the required components at the data centerdata center. See the Websense *Installation Guide* for more detailed instructions.

1. Log on to the installation machine with administrative privileges.

   If you plan to 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. Download the installation package from www.mywebsense.com.
3. Close all applications and stop any anti-virus software on the server.
4. Double-click the installation package to extract the files and start the installation.
5. Follow the onscreen instructions to the Subscription Agreement screen.
6. Select **Yes**, and click **Next**.
7. Select **Websense Web Security with Reporting**, and click **Next**

   **Websense Web Security with Reporting**: Available for a Windows installation only. Installs Filtering Service, Policy Broker, Policy Server, Websense Manager, User Service, Usage Monitor, and Network Agent together on the same machine. The installer gives you the option of installing the following transparent identification agents: DC Agent (Windows only), eDirectory Agent, Logon Agent, and RADIUS Agent, and installs Log Server to provide reporting.

   > **Important**
   >
   > Make sure that the database engine is running before installing reporting components.

8. If you are installing on Windows Server 2008:
   a. Indicate whether you are using Active Directory to authenticate users in your network.
   b. If you are using Active Directory, select an option for turning on the Windows Computer Browser service.

The Computer Browser service is a Windows utility that must be set to Automatic and Start in the Windows Services dialog box for Websense components to communicate with Active Directory.

If you choose not to have the installer turn it on, or if the installer is unable to turn it on, you must turn it on manually after installation. You must also turn on the Computer Browser service on the Active Directory machine, if you use Active Directory 2008 to authenticate users.

9. Select an Integration Option, and click **Next**.

   Select **Stand-alone** to use Network Agent to detect Internet requests.

10. You are prompted to provide the location of the database engine and an access method, and then asked to specify a location for creating the Websense Log Database.

    a. **Database Engine**: A database engine must be present to continue with the installation of reporting components. Do one of the following:

       - Specify that you want to connect to an existing database engine, and then continue to **step b**.
       - Use the link to find out more about installing the free MSDE database, and then exit setup. Run the installer again once a supported database engine has been configured.

    b. **Database Engine Location**: Enter the name or IP address of the machine on which a supported database engine is running. If a database engine is not available, you must install one before reporting components can be installed.

    c. Select an access method:

       - **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 be blank, or begin or end with a hyphen (-).

       - **Windows trusted connection**—Uses a Windows account to log into the database. This account must be a trusted account with local administration privileges on the database machine. Websense, Inc., recommends **against** using a trusted connection if you use MSDE as your database engine.

    d. Accept the default location for the Log Database, or select a different location. Then, click **Next**.

11. The installer assigns default port numbers to Policy Server (55806) and Filtering Service (15868).

If either of these default ports is in use, the installer requests an alternate port. Enter an unused port number between 1024 and 65535, and click **Next** to continue.

✓ **Note**

Record any port numbers that you change from the default settings. These port numbers may be requested when installing Websense components on other machines.

12. Select the network interface card (NIC) that Network Agent will use to communicate with other Websense software components. All enabled NICs with an IP address are listed.
13. Select a **Network Agent Feedback Option**, and click **Next**.

    Selecting **Yes** allows 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 any information to Websense, Inc., that would identify specific users, no matter which Network Agent feedback option is selected.

14. Select an optional **Transparent User Identification** agent allow Websense software to identifies users without prompting them for logon information, and then click **Next**.

✓ **Note**

It is possible to configure Websense software to use multiple transparent identification agents in the same network. eDirectory Agent, however, cannot be used in combination with either DC Agent or Logon Agent.

See the Websense Manager Help or *Transparent Identification of Users* technical paper for complete information about supported configurations.

- **eDirectory Agent**: Use eDirectory Agent to identify users transparently with Novell eDirectory Service.
- **DC Agent** (*Windows only*): Use DC Agent to identify users transparently with a Windows-based directory service.
- **Logon Agent**: Use Logon Agent to identify users transparently when they log on to the domain.

  Logon Agent receives its user information from a logon application (LogonApp.exe) that must be run by a logon script in your network.
- **DC Agent and Logon Agent** (*Windows only*): Use both DC Agent and Logon Agent to identify users transparently. This combination increases the accuracy of user identification in some networks.

- **None**: Do not install a Websense transparent identification agent. Select this option if your integration product provides user identification, if you do not plan to apply user and group policies, or if you want users to be prompted for logon information before accessing the Internet.

15. If you have remote users that are authenticated by a RADIUS server, select **Yes** to install the optional RADIUS Agent to transparently identify these users, and then click **Next**.
16. If you selected DC Agent for transparent identification, enter a **Domain/User Name** and **Password** with administrator privileges on the domain, and then click **Next**.

✓ **Note**

This ensures that User Service and DC Agent have the domain administrator privileges required to enable user-based filtering. Administrator privileges also can be set after installation. See *Troubleshooting > User Identification* in the Websense Manager Help.

17. Because you are installing reporting components on Windows, the Minimizing Database Management screen allows you to set options that affect the size of the Log Database used to generate reports.
    - **Logging Web Page Visits**: 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.
    - **Consolidating Log Records**: Combine multiple visits by the same user to the same Internet domain (see the Websense Manager Help for details). 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.
18. 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:

    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 installation's system requirements with the machine's resources.

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

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

If you have elected to integrate Websense software with a product that requires a plug-in (like Microsoft ISA Server), you will be prompted to stop and start the firewall at appropriate points in the installation process.

19. Click **Next** to start the installation. An installation progress screen is displayed.
20. Click **Next** on the Installation Complete screen.

    On Windows machines, when the installer finishes running, a Web page provides instructions for launching Websense Manager.
21. If you stopped your anti-virus software, restart it.
22. If your network uses Active Directory 2008 to authenticate users, you must turn on the Windows Computer Browser service on the Active Directory machine.

See the appropriate Websense *Installation Guide Supplement* for any additional setup instructions for your integration.

> ✓ **Note**
>
> If you want to change the location of a Websense component, or add a component, run the Websense installer again and select the appropriate option. The installer detects the presence of Websense components and offers the option of adding components.

## Configure Websense Manager at the data center

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.

| | |
|---|---|
| User name | WebsenseAdministrator (default) |
| Password | |
| Subscription key | |

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 among 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:

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.

   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 the Websense Manager Help system 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. 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 your data center is ready for default operations. See the Websense Manager Help for details on the variety of features and options available for Websense Web Security.

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

## 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 ensure that the Websense software 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, Websense software 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.
3. On the Directory Service page, select **Active Directory (Native Mode)**.
4. Configure the global catalog servers and other settings for your directory service. See Websense Manager Help for assistance.

# Test and refine your policies at the data center

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 Websense Web Security.
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**

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

3. Access Websense Manager by entering the following address:

   ```
   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.

# Install Websense components at the branch office

The following steps explain how to log on to the uploaded VM image on the Steelhead 1050 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 1050 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 the data center server and the Policy Server port number (port 55806 by default).

The following ports need to be open and available for communication with the Windows server 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

  Used for Secure Manual Authentication.
- 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.

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 1050 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 1050 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.
   - 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.

   Select a Network Agent feedback option, and click **Next**.
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:
   - **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 1050 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 in 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.

## 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.

| Location | Contact information |
|---|---|
| North America | +1-858-458-2940 |
| France | Contact your Websense Reseller. If you cannot locate your Reseller: +33 (0) 1 5732 3227 |
| Germany | Contact your Websense Reseller. If you cannot locate your Reseller: +49 (0) 69 517 09347 |
| UK | Contact your Websense Reseller. If you cannot locate your Reseller: +44 (0) 20 3024 4401 |
| Rest of Europe | Contact your Websense Reseller. If you cannot locate your Reseller: +44 (0) 20 3024 4401 |
| Middle East | Contact your Websense Reseller. If you cannot locate your Reseller: +44 (0) 20 3024 4401 |
| Africa | Contact your Websense Reseller. If you cannot locate your Reseller: +44 (0) 20 3024 4401 |
| Australia/NZ | Contact your Websense Reseller. If you cannot locate your Reseller: +61 (0) 2 9414 0033 |
| Asia | Contact your Websense Reseller. If you cannot locate your Reseller: +86 (10) 5884 4200 |
| Latin America and Caribbean | +1-858-458-2940 |

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