Installation Guide

for use with

Squid Web Proxy Cache

Websense Enterprise®
Websense® Web Security Suite™

v6.3.2

Trademarks

WinPcap

Contents

CHAPTER 1 | Introduction

Thank you for choosing Websense® web filtering and web security software. This guide covers installation and initial setup of Websense Enterprise® or Websense® Web Security Suite™ integrated with the Squid Web Proxy Cache.

Websense, Inc., strongly recommends that your users be informed of your organization's policies concerning internet access, and that Websense software has been installed as a tool for monitoring activity and/or enforcing your internet use policies.

About this Guide

This guide can be used with the following Websense products:

◆ Websense Enterprise®

◆ Websense® Web Security Suite™

The installation and initial setup information provided in this guide applies to the *web filtering* components of these products. These components are labelled **Websense Enterprise** in the Websense Enterprise installers, and **Websense Web Security Suite components** in the Web Security Suite installers.

For additional information about the web filtering components in the Websense Enterprise and Web Security Suite products:

◆ See the *Deployment Guide* for Websense Enterprise and Web Security Suite before installing the web filtering components to learn how to deploy these components in your network.

◆ See the *Administrator's Guide* for Websense Enterprise and Web Security Suite after installing the web filtering components for information about configuring and customizing web filtering and web security features.

The rest of the components available in the Websense Enterprise and Web Security Suite products are documented as follows:

- ◆ *Reporting Tools for web filtering* (available in all six Websense products listed above): These components are labelled **Websense Enterprise Reporting** in the Websense Enterprise installers, and **Web Security Suite Reporting components** in the Web Security Suite installers. For information about installing, configuring, and using these web filtering reporting components, see the Websense Reporting documentation set. For information about planning deployment of web filtering reporting components in your network prior to installation, see the *Deployment Guide* for Websense Enterprise and Web Security Suite.

- ◆ *Desktop filtering* and *desktop filtering reporting* is available with Websense Client Policy Manager™ (CPM). For information about installing, configuring, and using desktop filtering and desktop filtering reporting, see the CPM documentation set.

Document Conventions

References to "Websense software" in this guide apply to both Websense Enterprise and Websense Web Security Suite, unless specifically stated otherwise. The sample Websense installer screens included in this guide are from the Windows version of the Websense Enterprise installer, unless specifically stated otherwise. When the content of a Web Security Suite screen differs significantly from the displayed Websense Enterprise screen, it is noted in the text.

Where to Find More Information

Websense product documentation, including all documents referenced in this guide, is available on the Websense website at:

www.websense.com/SupportPortal/

Websense Components

The following list provides an overview of the Websense Enterprise and Websense Web Security Suite web filtering components, and includes brief descriptions of the Reporting Tools for web filtering.

- ◆ **Policy Server**: Stores all Websense configuration information, including filtering policies, and communicates this data to other Websense services.

◆ **Filtering Service**: Interacts with the Squid Web Proxy Cache and Network Agent to filter internet requests. Filtering Service either permits the internet request or sends an appropriate block message to the user.

◆ **Websense Manager**: Administrative interface that allows you to configure and manage Websense functionality through the Policy Server. Websense Manager is used to define and customize internet access policies, add or remove clients, configure Policy Server, and much more.

◆ **User Service**: Communicates with directory services in your network to allow you to apply filtering policies based on users, groups, domains, and organizational units.

◆ **Network Agent**: Manages the internet protocols that are not managed by the Squid Web Proxy Cache. Detects HTTP network activity and instructs the Filtering Service to log this information. You must install Network Agent and configure it properly to use the Bandwidth Optimizer, Protocol Management, and IM Attachment Manager features, and to log the number of bytes transferred and duration of transfer. Network Agent is also used to manage HTTP, HTTPS, and FTP filtering for a Stand-Alone (non-integrated) Websense installation.

◆ **Usage Monitor**: Tracks users' internet activity and sends alerts to Websense administrators when configured threshold values are crossed.

◆ **DC Agent**: An optional component that transparently identifies users who authenticate through a Windows® directory service. DC Agent enables filtering of internet requests according to policies assigned to particular users or groups.

◆ **RADIUS Agent**: An optional component that works through a RADIUS Server to transparently identify users and groups who access your network using a dial-up, Virtual Private Network (VPN), Digital Subscriber Line (DSL), or other remote connections.

◆ **eDirectory Agent**: An optional component that works together with Novell® eDirectory™ to transparently identify users so that Websense can filter them according to particular policies assigned to users or groups.

◆ **Logon Agent**: An optional component that works with a Websense client application (`LogonApp.exe`) to transparently identify users as they log on to a Windows domain via client machines. Logon Agent can be used with a Windows NT®-based directory service or with Active Directory®, which is LDAP-based. Logon Agent receives its user information from

the logon application, `LogonApp.exe`, which must be run by a logon script in your network.

◆ **Real-Time Analyzer™ (RTA)**: Displays the real-time status of all the traffic filtered by Websense Enterprise or Web Security Suite. RTA graphically displays bandwidth information and shows requests by category or protocol.

◆ **Remote Filtering Server**: An optional component that provides web filtering for machines located outside your organization's network firewall or internet gateway. In order to be filtered through the Remote Filtering Server, a remote workstation must be running the Remote Filtering Client. The Remote Filtering Server is enabled only if you subscribe to the remote filtering service.

◆ **Remote Filtering Client**: An optional component installed on client machines, such as notebook computers, that will be used outside your organization's network firewall or internet gateway. This component connects with a Remote Filtering Server inside the network firewall to enable web filtering of the remote workstation. The Remote Filtering Client is enabled only if you subscribe to the Remote Filtering service.

> **Note**
>
> The Remote Filtering Client is also available as part of the Client Agent in the Websense Client Policy Manager™ (CPM). For more information, see your Websense Client Policy Manager documentation.

◆ **Websense Master Database**: Contains a collection of millions of internet sites, each categorized by content. In addition, the Master Database contains protocols for such things as streaming media, peer-to-peer file sharing, and instant messaging.

◆ **Websense Enterprise Reporter**: This reporting tool is available free of charge with your Websense Enterprise or Web Security Suite subscription. Its Log Server component records internet activity on your network. Using this log information, Reporter can generate a wide variety of reports and charts depicting your network's internet usage trends. These reports can be used to refine internet filtering strategies, helping to maximize network resources and employee productivity. For installation procedures, see the *Reporting Installation Guide* for Websense Enterprise and Web Security Suite.

- ◆ **Websense Enterprise Explorer**: This reporting tool is available free of charge with your Websense Enterprise or Web Security Suite subscription. Explorer is a web-based reporting application that provides a customizable view into the Log Database. It displays summary information, as well as specific detail about users' internet activity. For installation procedures, see the *Reporting Installation Guide* for Websense Enterprise and Web Security Suite.

- ◆ **Websense Enterprise Explorer for Unix**: This reporting tool is available free of charge with your Websense Enterprise or Web Security Suite subscription. It is provided in a separate installer from the rest of the Websense Enterprise and Web Security Suite components. Explorer for Unix is a web-based reporting application that provides the same functionality as Websense Enterprise Explorer, but for Solaris and Linux operating systems. For installation procedures, see the *Explorer for Unix Administrator's Guide* for Websense Enterprise and Web Security Suite.

How Websense Filtering Works

The Websense Filtering Service is the engine by which internet content filtering is enforced. With its flexible, policy-based filtering approach, Websense software allows you to apply different filtering policies to different clients (users, groups, domains/organizational units, workstations, or networks).

When the Squid Web Proxy receives an internet request from a client, it queries the Websense Filtering Service to find out whether the requested site should be blocked or not. To make this determination, Filtering Service consults the policy assigned to the client. Each policy delineates specific time periods during the week and lists the category sets that are in effect during those time periods. After it determines which categories are blocked, Filtering Service consults its comprehensive database of internet addresses (URLs). If the site is assigned to a blocked category, the user receives a block page instead of the requested site. If the site is assigned to a permitted category, Filtering Service notifies the Squid Web Proxy that the site is not blocked, and the site is returned to the user.

Websense Enterprise and Web Security Suite filter network applications that use TCP-based protocols and measure bandwidth usage of UDP-based messages as well. If an initial internet request is made with TCP, and the request is blocked by the Websense software, all subsequent UDP traffic will

also be blocked. UDP protocols such as RTSP and RTP are monitored and logged.

The Quota feature is an alternative to full blocking. It gives employees time each day to visit sites in categories you deem appropriate. Quotas can be a powerful tool for internet access management. Quotas help you control how much time your employees spend on personal surfing and the types of sites they are able to access. For more information, see the *Administrator's Guide* for Websense Enterprise and Web Security Suite.

The Protocol Management feature allows Websense software to filter internet protocols other than HTTP. This includes protocols, applications, or other data transfer methods such as those used for instant messaging, streaming media, file sharing, file transfer, internet mail, and various other network or database operations. You must install Network Agent to use protocol management.

If you have a subscription that includes the Bandwidth Optimizer module and have installed Network Agent, your Websense software can filter internet sites, protocols, or applications based on available network bandwidth. You can specify filtering settings to limit user access to sites, protocols, or applications based on bandwidth usage.

If you have a subscription that includes the Instant Messaging (IM) Attachment Manager and have installed Network Agent, you can configure your Websense software to restrict file attachment sending and file sharing with IM clients. This feature enhances the default IM controls in Websense Enterprise and Web Security Suite by allowing you to permit certain IM traffic while blocking the transfer of attachments by those IM clients.

Steps for a Successful Websense Deployment

The following sequence is recommended for installing Websense Enterprise or Web Security Suite and configuring it to filter internet traffic in conjunction with the Squid Web Proxy.

1. **Plan the Websense deployment**: Websense components can be deployed in various combinations, depending upon the size and architecture of your network. Deciding which Websense components to install and where to put them is your first task. The information required to make this decision can be found in the *Deployment Guide* for Websense Enterprise and Web

Security Suite. For an overview of basic deployment in a small network (< 500 users), and deployment information specific to your integration product, see *Chapter 2: Network Configuration*.

2. **Install Websense filtering components**: Once you have decided how to deploy Websense software in your network, install the selected web filtering components. See *Chapter 4: Installing Websense Enterprise or Web Security Suite* for installation procedures.

> ✓ **Note**
>
> Be sure to install the Squid Plug-in on each Squid Web Proxy Cache machine so that Websense Filtering Service and Squid can communicate.

3. **Perform initial setup tasks**: Perform the post-installation setup tasks in *Chapter 5: Initial Setup*.

4. **Configure user authentication**: Configure authentication of users. See *Chapter 6: Authentication* for instructions.

5. Once you have completed the previous tasks to set up default global web filtering, you can customize your filtering policies, configure user- and group-based filtering, and learn to use more advanced Websense features by following the instructions in the *Administrator's Guide* for Websense Enterprise and Web Security Suite.

After the Websense filtering components have been successfully installed, install and configure the web filtering reporting components (Reporting Tools) so you can analyze and report on internet usage in your network. Use the information in the reports to tailor filtering policies for your organization. See the Websense Reporting documentation for instructions.

Network Configuration

Websense components can be installed in a number of possible configurations, depending upon the nature of your network and your filtering requirements. To determine the appropriate deployment for your network, and for a complete list of system requirements, see the *Deployment Guide* for Websense Enterprise and Web Security Suite.

The information in this chapter provides an overview of where Websense components can be installed, with specific information about where to install Websense components in relation to your integration product.

Websense Enterprise and Web Security Suite Components

When deciding how to deploy Websense Enterprise and Web Security Suite components in your network, consider the following installation dependencies:

- **Filtering Service**: Typically installed on the same machine as Policy Server and may be installed on the same machine as Websense Manager. The Filtering Service can be installed on a different operating system than the Policy Server, as long as they are properly configured to communicate with each other. This is an unusual deployment. Filtering Service installs on Windows, Solaris™, and Linux®. You can install a maximum of 10 Filtering Services for each Policy Server if they employ quality network connections. For additional information, see the *Deployment Guide* for Websense Enterprise and Web Security Suite.

- **Policy Server**: Typically installed on the same machine as the Filtering Service, but may be installed on a separate machine, depending upon the configuration of your network. There must be only one Policy Server installed for each *logical* installation. An example would be a Policy Server that delivers the same policies and categories to each machine in a subnet. The Policy Server installs on Windows, Solaris, and Linux.

◆ **Websense Manager**: May be installed on the same machine as Policy Server, and/or on one or more different machines in your network. Websense Manager machine needs network access to the Policy Server machine, but the two machines do not need to have the same operating system. Websense Manager installs on Windows, Solaris, and Linux.

◆ **User Service**: Installed in networks using a directory service for authentication. User Service is unnecessary if you intend to filter and log internet requests based on client workstation IP addresses only. User Service can be installed on the same operating systems supported by the Policy Server and is typically installed on the same machine; however, you may install User Service on a different operating system than the Policy Server. If the Policy Server is installed on Linux, for example, you can install User Service separately on a Windows machine. User Service installs on Windows, Solaris, and Linux.

> **Important**
>
> You can have only one User Service installation for each Policy Server in your network.

For systems providing multilingual support, User Service produces correct results for one *locale* only. The locale of the Policy Server determines the language it supports for directory services. Organizations with multilingual support requirements must install the product suite (User Service, Policy Server, and Filtering Service) for each supported language on machines configured for that language.

◆ **Network Agent**: Can be installed on the Filtering Service machine or separately, depending upon your needs and the configuration of your network. Network Agent installs on Windows, Solaris, and Linux. When planning the deployment of Network Agent consider the following:

■ Network Agent must be able to directly *see* 2-way internet traffic from your internal network to filter and log effectively. Make sure your network configuration routes both the internet request *from* the workstation and the response from the internet back *to* the workstation past Network Agent.

■ The simplest deployment is to connect the Network Agent machine to an unmanaged, unswitched hub that is located between an external router and your network.

- If the Network Agent machine is connected to a switch or router, configure the switch or router to use bi-directional port spanning (mirroring).

  If the span port on the switch or router is not capable of bi-directional communication, two network interface cards (NICs) are required in the installation machine: one NIC that can be configured for monitoring, attached to the span port; and a second NIC that can be configured for blocking, attached to a regular port. In this scenario, one NIC is receiving data, and one NIC is transmitting data, so the required two-way communication is provided by the two NICs in combination. After installation, the NICs must be configured for monitoring and blocking, respectively. For instructions, see the Network Agent chapter in the *Administrator's Guide* for Websense Enterprise and Web Security Suite.

  If you are installing Network Agent in a network that employs switches, see the Switched Configuration section in the Deploying Network Agent chapter of the *Deployment Guide* for Websense Enterprise and Web Security Suite for additional information.

- For small to medium sized organizations, Network Agent can be installed on the same server machine as the other Websense web filtering components, assuming that the server meets the minimum system requirements. For larger organizations, you may want to put Network Agent on a separate, dedicated server to increase the amount of traffic that can be managed.

- On larger networks, you may need to install multiple Network Agents and assign them to monitor various IP address ranges in your network. Make sure that the IP address ranges for each instance of Network Agent do not overlap. Overlapping IP ranges result in double logging. Deploy the Network Agents so that they can filter the entire network. Partial deployment results in incomplete filtering by protocol and bandwidth, as well as the loss of log data from network segments not watched by Network Agent. To define IP address ranges for multiple Network Agents, follow the instructions in the Network Agent chapter of the *Administrator's Guide* for Websense Enterprise and Web Security Suite.

- Avoid deploying Network Agent across different LANs. If you install an instance of Network Agent on 192.x.x.x and configure it to communicate with a Filtering Service on 10.x.x.x through a variety of switches and routers, communication may be slowed enough to prevent Network Agent from blocking an internet request in time.

- Do *not* install Network Agent on a machine running any type of firewall. Network Agent uses a packet capturing utility which will not work properly when installed on a firewall machine. The only exception is a blade server or appliance with separate processors or virtual processors to accommodate Network Agent and the firewall software.

◆ **Usage Monitor**: Typically installed on the same machine as the Policy Server, but may be installed on a separate machine in your network that has access to the Policy Server machine. The Usage Monitor installs on Windows, Solaris, and Linux.

> **Important**
>
> You can have only one installation of Usage Monitor for each Policy Server in your network.

◆ **Real-Time Analyzer (RTA)**: Can be installed on the same machine as Filtering Service or on a separate machine. The Real-Time Analyzer installs on Windows only.

Real-Time Analyzer (RTA) can be memory and CPU demanding, depending on desired system settings and network load conditions. RTA should not be installed on real-time critical machines. For more information, see the *Deployment Guide* for Websense Enterprise and Web Security Suite.

> **Important**
>
> You can have only one installation of RTA for each Policy Server in your network.

One of these web servers must be installed on the same machine as RTA

- Apache HTTP Server
- Microsoft IIS

> **Note**
>
> If you do not have one of the supported web servers on your system, the Websense installer provides the option of installing the Apache HTTP Server.

For information about supported versions of these web servers, see the *Deployment Guide* for Websense Enterprise and Web Security Suite.

◆ **Websense Transparent Identification Agents**: If you want to apply user- and group-based filtering policies, Websense software must be able to identify a user making a request, given the originating IP address. Installing a Websense transparent identification agent allows Websense software to filter internet requests from users in your directory service, without prompting users to log on to the browser. A transparent identification agent can be used if your integration product does not send user information for some or all users to the Websense Filtering Service.

DC Agent, eDirectory Agent, Logon Agent, and RADIUS Agent are the available Websense transparent identification agents. The following descriptions provide information about selecting and installing the appropriate agent(s) to identify users in your network.

▪ **DC Agent**: Installed in networks using a Windows directory service (NTLM-based or Active Directory). DC Agent can be installed on any Windows or Linux machine in the network, either on the same machine as other Websense components, or on a different machine.

- For small to medium networks, Websense, Inc., recommends that you install only one DC Agent per domain. If you have a large, distributed network with many domain controllers on the same domain, you can install multiple DC Agents. Installing DC Agent on the domain controller machine is *not* recommended. DC Agent can be installed on any network segment as long as NetBIOS is allowed between the DC Agent and the domain controllers. Setting up the DC Agent in the DMZ is not recommended.

- You may install DC Agent and RADIUS Agent together on the same machine or on separate machines in your network.

- DC Agent and eDirectory Agent can be installed in the same network, but cannot be active at the same time, since Websense software does not support communication with both Windows and Novell directory services simultaneously. Do not install DC Agent and eDirectory Agent on the same machine.

- If DC Agent is not identifying all your users as anticipated, you may install Logon Agent as well to improve user authentication in your network. For example, this might be necessary in a network that uses Windows 98 workstations. DC Agent uses workstation *polling* to get user information from workstations as they make internet requests; however, polling cannot retrieve user information from a Windows 98 workstation.

- If you are installing DC Agent, be sure that the machine names of any Windows 9x workstations in your network do not contain any spaces. This situation could prevent DC Agent from receiving a user name when an internet request is made from that workstation.

For configuration information, see the User Identification chapter in the *Administrator's Guide* for Websense Enterprise and Web Security Suite. For detailed deployment information, see the white paper titled *Transparent Identification of Users in Websense Enterprise*, available at: www.websense.com/SupportPortal/

■ **eDirectory Agent**: Can be installed on the same machine as the rest of the Websense filtering software, or installed on a separate machine in your network. You can install multiple eDirectory Agents on the same network, each configured to communicate with the Filtering Service. You can install eDirectory and RADIUS Agent on the same machine or on separate machines in your network. The eDirectory Agent can be installed in the same network as DC Agent or Logon Agent, but cannot be active at the same time, since Websense software does not support communication with Windows and Novell directory services simultaneously. Do not install eDirectory Agent on the same machine as DC Agent or Logon Agent. The eDirectory Agent installs on Windows, Solaris, and Linux.

For configuration information, see the User Identification chapter in the *Administrator's Guide* for Websense Enterprise and Web Security Suite. For detailed deployment information, see the white paper titled *Transparent Identification of Users in Websense Enterprise*, available at: www.websense.com/SupportPortal/

■ **Logon Agent**: Can be installed on the same machine as the rest of the Websense filtering software, or installed on a separate machine in your network. Logon Agent may be installed together with DC Agent to improve the accuracy of user authentication in your network. Logon Agent installs on Windows, Linux, or Solaris and works

together with the User Service and Filtering Service. Logon Agent can be used with a Windows NT-based directory service or with Active Directory, which is LDAP-based. `LogonApp.exe`, the client application that passes user logon information to Logon Agent, runs only on Windows client machines. You must create a logon script to run `LogonApp.exe` in your network; see *Creating and Running the Script for Logon Agent*, page 189 for instructions. Logon Agent and eDirectory Agent can be installed in the same network, but cannot be active at the same time, since Websense software does not support communication with both Windows and Novell directory services simultaneously. Do not install Logon Agent and eDirectory Agent on the same machine.

For configuration information, see the User Identification chapter in the *Administrator's Guide* for Websense Enterprise and Web Security Suite. For detailed deployment information, see the white paper titled *Transparent Identification of Users in Websense Enterprise*, available at: www.websense.com/SupportPortal/

- **RADIUS Agent**: Can be installed on the same machine as the rest of the Websense filtering software, or installed on a separate machine in your network. You may install multiple RADIUS Agents on the same network, each configured to communicate with the Filtering Service. RADIUS Agent can be used in conjunction with either Windows- or LDAP-based directory services. You can install RADIUS Agent and eDirectory Agent on the same machine or on separate machines in your network. The RADIUS Agent installs on Windows, Solaris, and Linux.

  For configuration information, see the User Identification chapter in the *Administrator's Guide* for Websense Enterprise and Web Security Suite. For detailed deployment information, see the white paper titled *Transparent Identification of Users in Websense Enterprise*, available at: www.websense.com/SupportPortal/

- **Websense Filtering Plug-in**: A special Websense component, the Squid Plug-in, must be installed on the Squid Web Proxy Cache machine to allow the Squid Web Proxy Cache to communicate with Websense Filtering Service. The Squid Plug-in must be installed on the same machine with every Squid Web Proxy Cache that communicates with Filtering Service. The Squid Plug-in is supported on Solaris and Linux.

◆ **Remote Filtering components**

The Remote Filtering components are required only if you need to enable web filtering on user workstations located outside your organization's network firewall or internet gateway. They can be installed from a **Custom** installation only.

✔ **Note**

To enable the Remote Filtering components, you must subscribe to the remote filtering service.

■ **Remote Filtering Server**: Should be installed on a separate, dedicated machine. This machine must be able to communicate with the Filtering Service and with Remote Filtering Clients on user workstations that may be used both inside and outside the network firewall. The Remote Filtering Server installs on Windows, Linux, and Solaris.

The Remote Filtering Server automatically detects whether clients are inside or outside of the network firewall. If it determines that a client is inside the firewall, the user is filtered just like other internal clients. Remote Filtering is only activated if the client is outside the firewall.

To provide failover protection for the primary Remote Filtering Server, you can install secondary and tertiary Remote Filtering Servers. If a Remote Filtering Client on a remote workstation cannot connect with the primary Remote Filtering Server, it will try to connect with the secondary, then the tertiary, then the primary again, and so on.

• Install only one primary Remote Filtering Server for each Filtering Service in your network.

• Do not install the Remote Filtering Server on the same machine as the Filtering Service or Network Agent.

• The Remote Filtering Server machine does not have to be joined to a domain.

Remote Filtering components are not included in the deployment diagrams provided in this chapter. For deployment information and network diagrams, see the Remote Filtering section in the *Deployment Guide* for Websense Enterprise and Web Security Suite.

■ **Remote Filtering Client**: Can be installed on user machines that you want to filter outside the network firewall. To deploy this client application, you can use the provided installer, called the **Remote**

Filtering Client Pack, and a third-party deployment tool. A Remote Filtering Client must be able to communicate with a Remote Filtering Server inside the network firewall to enable web filtering on the remote workstation. The Remote Filtering Client Pack and the Remote Filtering Client install only on Windows.

Note

The Remote Filtering Client is also available as part of the Websense Client Policy Manager™ (CPM). If you are using CPM to manage application filtering on employee desktops, the Remote Filtering Client is provided as part of the CPM Client Agent. For more information, see your Websense Client Policy Manager documentation.

Remote Filtering components are not included in the deployment diagrams provided in this chapter. For detailed deployment information and network diagrams, see the Remote Filtering section in the *Deployment Guide* for Websense Enterprise and Web Security Suite.

Important

Do not install the Remote Filtering Client on a Remote Filtering Server machine.

◆ **Websense Reporting components**: Should be installed on a separate machine from the Websense Enterprise or Web Security Suite web filtering components, except when evaluating Websense software, or in a small network (see the *Deployment Guide* for detailed system requirements and recommendations). The Log Server receives and saves information about internet requests filtered by Websense Enterprise or Web Security Suite. Reporter and Explorer then use this information to create reports on users' internet activity. See the Websense Enterprise and Web Security Suite Reporting documentation for installation and administrative information.

Note

To properly generate reports, you must use the same version of the Websense Reporting Tools as the Websense Enterprise or Web Security Suite software.

Deploying Websense Components with your Integration Product

Before beginning installation, read the *Deployment Guide* for Websense Enterprise and Web Security Suite to learn about system requirements and how best to deploy Websense Enterprise or Web Security Suite components, as well as the Websense Reporting Tools, in your network.

Websense components can be installed on a dedicated server machine, or widely distributed across a network on various operating systems. The recommended deployment depends on a number of factors, including the size and complexity of your network, the amount of traffic being handled, and the types of hardware available. Wherever you decide to deploy Websense components, make sure that the installation machine can handle the expected traffic load.

The information in this section is not intended to be a comprehensive discussion of all available deployment options. The network architecture shown represents a small network, with 500 users or fewer. The network diagrams are intended primarily to show the recommended location of your **integration product** relative to the Websense components.The network architecture represents a small network, with 500 users or fewer. The network diagram is intended primarily to show the recommended location of your **integration product** relative to the Websense components. In some cases, Websense filtering software can be installed on the same machine as your integration product, if the machine has adequate resources. For detailed information about where to deploy individual Websense components in networks of all sizes, see the *Deployment Guide* for Websense Enterprise and Web Security Suite.

Websense Filtering Service communicates with the Squid Web Proxy Cache through a Websense filtering plug-in called the Squid Plug-in. The Squid Plug-in must be installed on each Squid Web Proxy Cache machine.

Single Squid Web Proxy Cache Configuration

The following diagram shows the main Websense filtering components, the Squid Plug-in, and the Squid Web Proxy Cache running on the same machine.
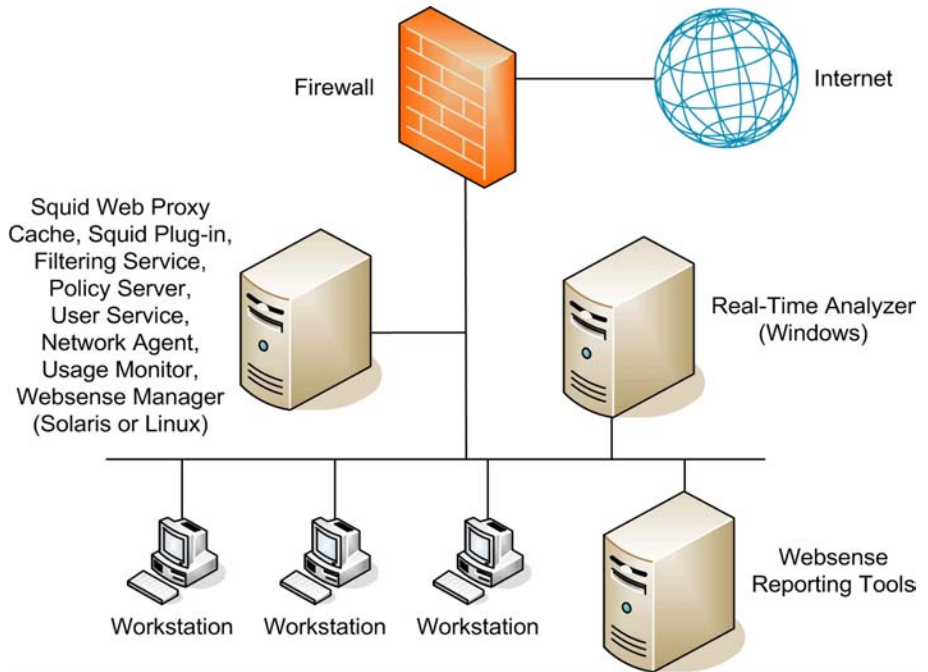
Filtering Service Installed on the Same Machine as Squid Web Proxy

In this configuration, the Websense filtering components are installed with the Squid Web Proxy on a Solaris or Linux machine. You can also install a Websense transparent identification agent on the same machine as the Filtering Service, or on a separate machine. DC Agent, supported on Windows and Linux, is one choice for networks that use a Windows-based directory service. For networks that use a Novell directory service, eDirectory Agent could be installed instead. The Real-Time Analyzer, which is supported only on Windows, must be installed on a Windows machine. For added flexibility, Websense Manager can also be installed on any Windows, Linux, or Solaris machine that has network access to the Policy Server machine.

An alternate setup places all of the Websense Enterprise or Web Security Suite components together on a Windows machine separate from the Squid Web Proxy machine. In this case, the Squid Plug-in must be installed on the

Squid Web Proxy machine so that it can communicate with Websense Filtering Service.

The following diagram shows this alternate setup.
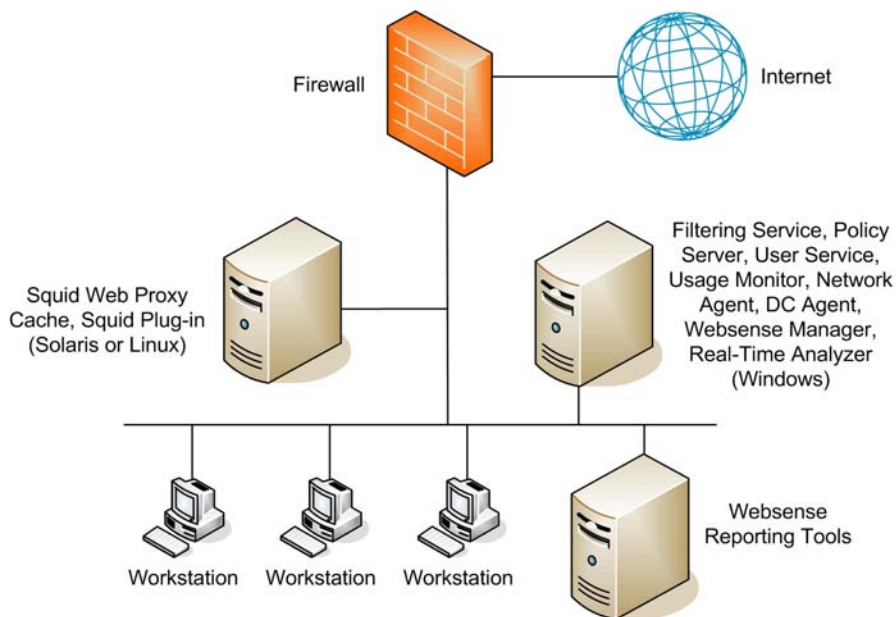
Filtering Service Installed Separately from Squid Web Proxy Machine

This configuration eases the load on the Squid Web Proxy machine by placing Websense filtering components on a separate machine. The Websense Filtering Service and Squid Web Proxy machine must be able to communicate over the network in this setup. DC Agent is shown as the installed transparent identification agent to identify users in a Windows-based directory service. For added flexibility, Websense Manager can also be installed on other Windows, Linux, or Solaris machines that have network access to the Policy Server machine.

Array Configuration

Websense software is compatible with most array configurations, including Cache Array Routing Protocol (CARP) arrays. If the Squid Web Proxy Cache machines in the array can run Websense Enterprise or Web Security Suite without a loss of performance, installing the main Websense filtering components on one of the array machines is recommended. In this

configuration, the two applications will not have to communicate over the network.

The following diagram shows the main Websense filtering components running on a Squid Web Proxy Cache machine, with an additional Websense Manager installed on a workstation that has network access to the Policy Server machine.

Array Configuration—First Option
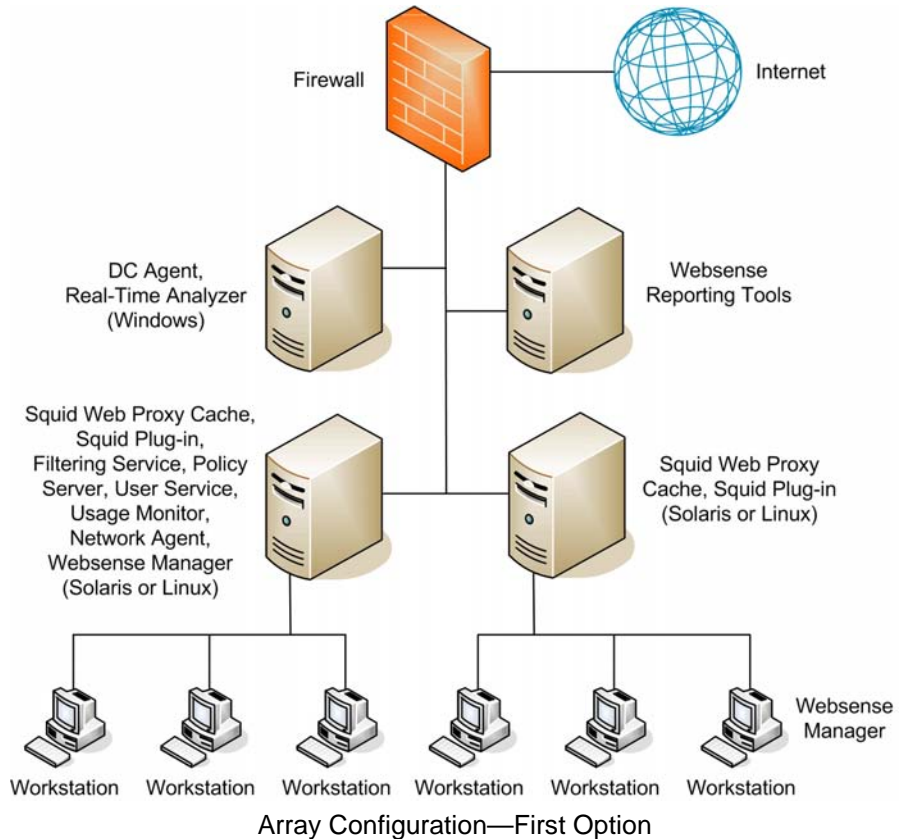
If there is a potential loss of performance by installing the Websense filtering components on the Squid Web Proxy machine, you can install Websense Enterprise or Web Security Suite on a separate machine outside the array, and then install the Squid Plug-in on each member of the array. When Websense

software is installed in this manner, all array members send internet requests to the Filtering Service that is installed outside the array.

Array Configuration—Second Option
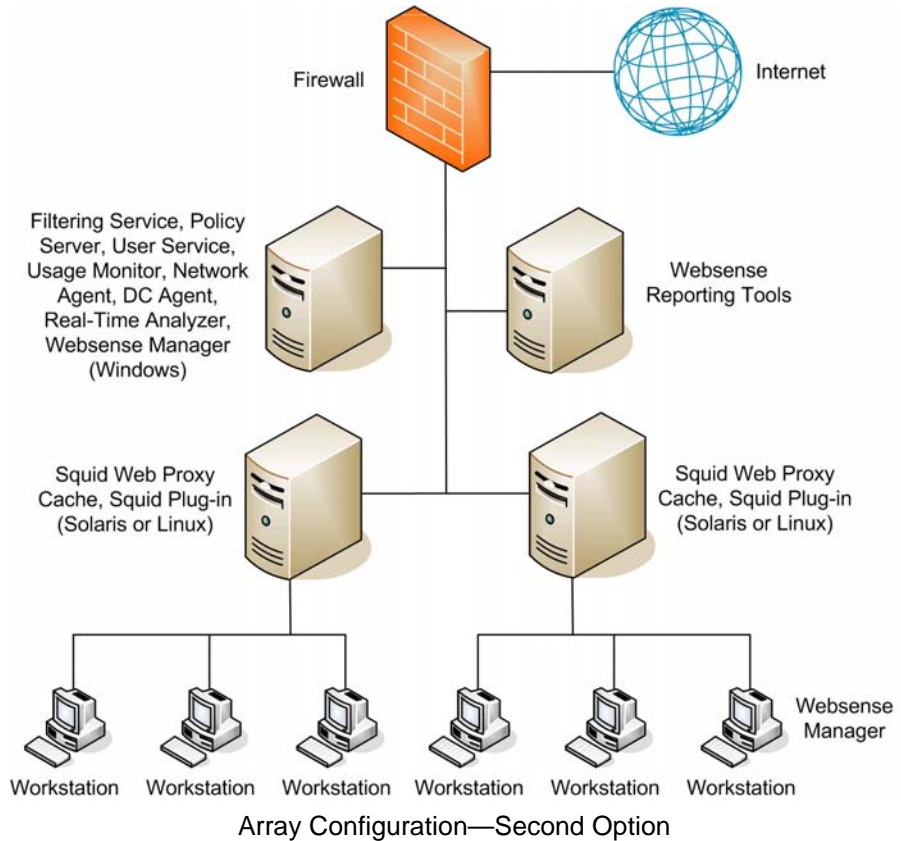
Other configurations are possible. Consult your Squid Web Proxy Cache documentation for information about array configurations.

Websense Reporting Components

Websense, Inc., does not recommend installing Websense Reporting components on the same machine as Websense Enterprise or Web Security Suite. Filtering and logging functions are CPU intensive and could cause operating system errors. Install Websense Enterprise or Web Security Suite and Websense Reporting components on separate machines inside the network, where they will not have to compete for resources. The exception to this is when Websense Enterprise or Web Security Suite is being evaluated on a small network or segment of a larger network.

For detailed information about how to deploy each of the Websense Reporting components in your network, see the *Deployment Guide* for Websense Enterprise and Web Security Suite, and your Websense Enterprise and Web Security Suite Reporting documentation.

Directory Services

If your environment includes a directory service, Websense software allows you to filter internet requests based on individual policies assigned to directory objects. Directory objects identified in a directory service can be added in Websense Manager and assigned specific policies.

Websense software can communicate with the following directory services:

◆ Windows® NTLM-based directories

◆ Windows® Active Directory®

◆ Sun Java™ System Directory Server

◆ Novell Directory Services®/Novell® eDirectory®

For information about supported versions of these directory services, see the *Deployment Guide* for Websense Enterprise and Web Security Suite. For information about configuring directory service access, see the *Administrator's Guide* for Websense Enterprise and Web Security Suite.

> ✔ **Note**
>
> Websense software can communicate with your directory service whether it runs on the same operating system as the Websense components, or on a different system.

Filtering can be based on individual user, group, and domain/organizational unit policies, providing that the Websense software is able to identify the user making an internet request. The authentication method you configure must allow Filtering Service to obtain directory object information from a Windows or LDAP directory. For information about accessing LDAP and

Windows directories, see the *Administrator's Guide* for Websense Enterprise and Web Security Suite.

> **✓ Note**
>
> In any environment, Websense software can filter based on workstation or network policies. Workstations are identified within the Websense software by their IP addresses, and networks are identified as IP address ranges.

Internet requests can be filtered based on policies assigned to individual directory objects after the following tasks have been accomplished:

◆ If you are using the Sun Java System Directory Server or Novell Directory Services/eDirectory:

1. Enable the appropriate directory service in Websense Manager.

2. Enable the Websense software to identify users transparently with Novell by installing and configuring the Websense eDirectory Agent.

3. Enable Websense manual authentication so that if the Websense software is unable to identify users transparently, it will prompt users to manually authenticate.

Detailed instructions for each of these tasks can be found in the User Identification chapter in the *Administrator's Guide* for Websense Enterprise and Web Security Suite.

◆ If you are using a Windows NTLM-based directory or Active Directory:

1. Configure the Windows directory service in Websense Manager.

2. Enable the Websense software to identify users transparently by installing and configuring the Websense DC Agent and/or Logon Agent.

3. Enable Websense manual authentication so that if the Websense software is unable to identify users transparently, it will prompt users to manually authenticate.

Detailed instructions for each of these tasks can be found in the User Identification chapter in the *Administrator's Guide* for Websense Enterprise and Web Security Suite.

> ✔ **Note**
>
> DC Agent on Linux is not supported with LDAP-based directory services. If you are running DC Agent on Linux and are using Windows Active Directory, NTLM authentication must be enabled in Active Directory.

The Websense transparent identification feature allows the Websense software to filter internet requests from users in a Windows or Novell directory service, without prompting users to manually authenticate. Websense software can transparently identify users in a Windows domain if DC Agent and/or Logon Agent is installed. In networks using a Novell directory service, you can transparently identify users by installing the Websense eDirectory Agent. If users access your network through a RADIUS server, you use RADIUS Agent to transparently identify them. RADIUS Agent can be used in conjunction with either Windows- or LDAP-based directory services.

Once the Websense Filtering Service is configured to communicate with the transparent identification agent (DC Agent, Logon Agent, eDirectory Agent, or RADIUS Agent), the agent obtains user information from the directory service and sends the information to Filtering Service. When Filtering Service receives the IP address of a machine making an internet request, Filtering Service matches the address with the corresponding user name provided by the transparent identification agent. This allows the Websense software to transparently identify users whenever they open a browser that sends an internet request to your integration product.

For more information about transparent identification using DC Agent, Logon Agent, eDirectory Agent, and RADIUS Agent, see the User Identification chapter in the *Administrator's Guide* for Websense Enterprise and Web Security Suite. For more detailed information, see the white paper titled *Transparent Identification of Users in Websense Enterprise*, available at: www.websense.com/SupportPortal

Filtering in a Network with Citrix® Server Users

If your network includes some users who access the internet via a Citrix® server, and others who access the internet through another gateway (firewall, caching appliance, or proxy server), you must install two complete instances of Websense software:

◆ One instance of Websense software choosing the Citrix integration, to filter Citrix users. Follow the instructions in the *Installation Guide for use with Integrated Citrix® Servers*.

◆ Another, separate instance of Websense software, to filter the non-Citrix users. This instance of Websense software can be integrated with the other gateway (firewall, caching appliance, or proxy server), or it can be the Websense Stand-Alone Edition. To install this Websense instance, follow the instructions in the Websense Enterprise and Web Security Suite Installation Guide for the integration product you are using, or for the Stand-Alone Edition.

System Requirements

Websense software can be installed on machines with Windows, Solaris, and Linux operating systems (see the *Deployment Guide* for supported versions). Not all Websense components are supported on all three types of operating system. However, you can install Websense components on machines with different operating systems, and they will be able to communicate with one another. For example, an instance of Websense Manager installed on a Windows machine can configure a Policy Server installed on a Windows, Solaris, or Linux machine. For a list of supported operating systems for each Websense Enterprise and Web Security Suite component, see the *Deployment Guide* for Websense Enterprise and Web Security Suite.

Such factors as network size, network configuration, and internet traffic volume can affect the ability of Websense software to filter internet requests. For hardware recommendations for your network, see the *Deployment Guide* for Websense Enterprise and Web Security Suite.

For a complete list of system requirements for installation of Websense Enterprise and Web Security Suite components in your network, see the *Deployment Guide* for Websense Enterprise and Web Security Suite. This section contains system requirements specific to your integration product.

Supported Squid Versions

Websense Enterprise and Web Security Suite v6.3.2 are compatible with Squid v2.5.

The Websense Squid Plug-in for the Squid Web Proxy Cache is supported only on Solaris and Linux.

User Workstations

Websense filtering is based on protocols, not on the operating system of the user workstation being filtered.

To be filtered by the Websense software, a user workstation must access the internet through the Squid Web Proxy Cache.

Browsers must be set for proxy-based connections.

Upgrading Websense Enterprise or Web Security Suite

This chapter contains procedures for upgrading a previous version of Websense Enterprise or Web Security Suite to version 6.3.2. It also contains instructions for upgrading an existing Websense Stand-Alone Edition to a Websense system integrated with Squid Web Proxy Cache.

Before upgrading, make sure your system meets the system requirements listed in the *Deployment Guide* for Websense Enterprise or Websense Web Security Suite.

The Websense Enterprise installer will upgrade all Websense Enterprise components detected on the installation machine, with the exception of the Remote Filtering Client. The Websense Web Security Suite installer will upgrade all Web Security Suite components detected on the machine, with the exception of the Remote Filtering Client.

> **Note**
>
> If the optional Remote Filtering Client application is installed on user workstations in your network, see *Remote Filtering Client*, page 50 for upgrade instructions.

You can also use the Websense Web Security Suite installer to upgrade your Websense Enterprise system to Web Security Suite. See *Upgrading from Websense Enterprise to Web Security Suite*, page 54 for more information.

Direct upgrades from version 6.1 or higher are supported. Websense Enterprise or Web Security Suite "version 6.1 or higher" refers to the following releases:

◆   6.1.x

◆   6.2.x and 6.3.x

During upgrade, the installer will configure v6.3.2 components to use the same network interface cards (NICs) for Websense communications and the

same Network Agent used by the earlier version. The installer will also automatically assign the same port numbers to the v6.3.2 Websense components that the existing Websense components use.

The Websense Master Database will be removed during upgrade. You can either download the new Master Database during upgrade of the Filtering Service, or download it after the upgrade is complete by using Websense Manager. When scheduling the upgrade, be aware that users will not be filtered until the services are restarted and the new Master Database has been successfully loaded. Depending on how your integration product is configured to respond when Websense filtering is unavailable, traffic will either be allowed unfiltered or blocked entirely during the upgrade.

> ✔ **Note**
>
> The upgrade process is for use on properly functioning Websense systems. Upgrading will not repair a non-functional system.

Versions Supported

Support for integration with the Squid Web Proxy Cache was introduced in Websense Enterprise v5.0.1.

Direct upgrades from v6.1 or higher of Websense Enterprise or Web Security Suite integrated with the Squid Web Proxy Cache are supported. If you are running v5.2 or v5.5, an upgrade to v6.3.2 requires two steps: upgrade to v6.1 first, and then upgrade to v6.3.2.

To perform the intermediate upgrade to v6.1, you will need the v6.1 installer for your product and operating system. Download the appropriate installer:

- **Websense Enterprise** v6.1 installer:
    - **Windows**: www.websense.com/Downloads/files/v6.1/full/ Websense61Setup.exe
    - **Solaris**: www.websense.com/Downloads/files/v6.1/full/ Websense61Setup_Slr.tar.gz
    - **Linux**: www.websense.com/Downloads/files/v6.1/full/ Websense61Setup_Lnx.tar.gz
- **Websense Web Security Suite** v6.1 installer:

- **Windows**: www.websense.com/Downloads/files/v6.1/full/ WebSecurity61_Setup.exe
- **Solaris**: www.websense.com/Downloads/files/v6.1/full/ WebSecurity61_Setup_Slr.tar.gz
- **Linux**: www.websense.com/Downloads/files/v6.1/full/ WebSecurity61_Setup_Lnx.tar.gz

If you are running Websense Enterprise v5.0.1 or v5.1 integrated with the Squid Web Proxy Cache, Websense, Inc., recommends that you perform a fresh installation of v6.3.2 rather than upgrading. If you decide to upgrade to v6.3.2, three steps are required: upgrade to v5.5.2 first, then upgrade to v6.1, and finally upgrade to v6.3.2.

The v5.5.2 Websense Enterprise installer for your operating system can be downloaded from:

- **Windows**: www.websense.com/Downloads/files/v5.5.2/full/ Websense552Setup.exe
- **Solaris**: www.websense.com/Downloads/files/v5.5.2/full/ Websense552Setup_Slr.tar.gz
- **Linux**: www.websense.com/Downloads/files/v5.5.2/full/ Websense552Setup_Lnx.tar.gz

Transferring Configuration Data Without Upgrading

The recommended path for upgrading Websense Enterprise or Web Security Suite is through the normal upgrade process, in which all configuration data from the earlier version is retained. In some cases, however, you may decide that an upgrade of your production system is undesirable. Your network policy may not permit upgrades to the production system, or you may want to move your Websense software to a larger machine to accommodate increased network traffic.

If running a normal upgrade is not an option, you can use either of two procedures that will transfer configuration data from the production system to a freshly installed version of Websense Enterprise or Web Security Suite.

These procedures require a test environment and may involve several cycles of installation and upgrade.

> **Warning**
>
> Do not attempt to upgrade an earlier version of Websense Enterprise or Web Security Suite by copying the `config.xml` file into a v6.3.2 system. Configuration files from earlier versions are not compatible with v6.3.2.

The procedures for converting to v6.3.2 without upgrading are described in the technical paper titled *Transferring Configuration Settings to a v6.3.2 System Without Upgrading*, available at: www.websense.com

Before You Upgrade

◆ **Backing up files**: Before upgrading to a new version of Websense Enterprise or Web Security Suite, Websense, Inc., recommends that you perform a full system backup as a fallback strategy. This will allow you to restore your current production system with a minimum of downtime should you encounter any problems with the upgrade. At a minimum, you should back up the latest Websense configuration file and the initialization files. To back up these files, stop the Policy Server and copy the `config.xml` file, the `websense.ini` file, and the `eimserver.ini` file from the `Websense\bin` folder to a safe location.

◆ **Non-English language versions**: In v6.3.2, all Websense installers are available in English and nine other language versions (see *Non-English Language Versions*, page 71). When upgrading, choose the v6.3.2 installer for the language of your current Websense installation. Upgrading your system with the v6.3.2 installer for a non-English language will first convert the system to English. At the end of the upgrade process, the v6.3.2 Language Pack installer will run automatically to convert the upgraded Websense components to your language.

> **Note**
>
> All Websense components in a Websense installation must be in the same language.

◆ **Upgrading distributed components**: To upgrade your system, you must run the Websense installer on each machine on which a Websense component resides. The installer detects all Websense components, including the Squid Plug-in, and upgrades them accordingly.

> **Warning**
>
> Always run the installer on the **Policy Server** machine first. The Policy Server must be successfully upgraded and running before you upgrade or install other Websense components in your network.

◆ **Upgrading the Squid Plug-in**: To upgrade the filtering plug-in for your integration product, run the Websense installer on the Squid Web Proxy Cache machine and follow the onscreen instructions. For proper communication to be established with the Squid Web Proxy Cache, you must upgrade the Websense Filtering Service *before* upgrading the filtering plug-in.

◆ **Remote Control Utilities**: Upgrade of Websense software using a remote control utility such as Terminal Services is not supported.

◆ **Reporting**: To properly generate reports, you must use the same version of Websense filtering software and Websense Reporting Tools.

> **Important**
>
> Upgrade all Websense Enterprise or Web Security Suite components *before* upgrading your existing Websense Enterprise Reporting or Web Security Suite Reporting components.

For information about upgrading Reporting components, see the *Reporting Installation Guide* for Websense Enterprise and Web Security Suite.

◆ **Websense services**: Websense services must be running when the upgrade process begins. The installer will stop and start these services as necessary during the upgrade. If these services have been running uninterrupted for several months, however, the installer may not be able to stop them before the upgrade process times out. To ensure the success

of the upgrade, manually stop and restart all the Websense services before beginning the upgrade.

> **Note**
>
> If you have set the **Recovery** properties of any of your Websense services to restart the service on failure, you must change this setting to **Take No Action** before upgrading.

◆ **Matching locales**: When upgrading a Filtering Service that is installed on a different machine from Websense Manager, you must upgrade the Filtering Service to v6.3.2 in the same locale environment (language and character set) as the Websense Manager.

When upgrading on Solaris or Linux, log on to the Filtering Service machine with the locale appropriate to the Websense Manager.

Once the upgrade is complete, the Websense services can be restarted with any locale setting.

Upgrading on Solaris or Linux

Before upgrading to a new version of Websense Enterprise or Web Security Suite, Websense, Inc., recommends that you perform a full system backup as a fallback strategy. This will allow you to restore your current production system with a minimum of downtime should you encounter any problems with the upgrade.

At a minimum, be sure you have backed up the following files before proceeding:

◆ `config.xml`
◆ `eimserver.ini`
◆ `websense.ini`

> **Important**
>
> If your Websense services have been running uninterrupted for several months, the installer may have difficulty stopping them. To prevent the upgrade process from timing out and failing, stop the services manually and restart them again before beginning the upgrade.

To upgrade Websense Enterprise or Web Security Suite v6.1 or higher to v6.3.2:

1. Close all Websense Managers anywhere in the network that connect to the Policy Server you are upgrading.

2. Log on to the installation machine as the **root** user.

3. Close all applications and stop any antivirus software.

4. Create a setup directory for the installer files.

   For example: `/root/Websense_setup`

5. Obtain an installer package for either Websense Enterprise or Web Security Suite:

   ■ **Web download**: To download an installer package, go to www.websense.com, and then navigate to the Downloads page.

      a. Choose your product, the dynamic (online) or full (offline) installer package, the operating system, and the language.

> **Note**
>
> The **Dynamic** installer is an **online** installer package that requires web access during installation. It downloads the necessary product files from the website as needed after product selections have been made.
>
> The **Full** installer is a complete **offline** installer. It is much larger than the online Dynamic installer package, and contains all the files needed to install the Websense Enterprise or Web Security Suite components. Use this package if you experience difficulties with the online installer.

      b.   Save the selected installer package to the setup directory on the installation machine.

6. In the setup directory, enter the following command to unzip the file:

   `gunzip <download file name>`

   For example: `gunzip Websense632Setup_Slr.tar.gz`

7. Expand the file into its components with the following command:

   `tar xvf <unzipped file name>`

   For example: `tar xvf Websense632Setup_Slr.tar`

   This places the following files into the setup directory:

File	Description
install.sh	Installation program.
Setup	Archive file containing related installation files and documents.
Documentation	Release Notes: An HTML file containing release notes and last minute information about the Websense software. Read this file with any supported browser.

8. Run the installation program from the setup directory with the following command:

   `./install.sh`

   To run the GUI version of the installer, use the following command:

   `./install.sh -g`

   If you are using a non-English based system, the installer will display an error message advising you that the GUI version is not supported.

9. Follow the onscreen instructions through the subscription agreement.

10. Follow the upgrade sequence:

    ■ **Websense upgrade**: The installer detects the earlier version of Websense components and gives you the choice of upgrading the existing installation or exiting Setup. Be sure to close any Websense Managers connected to the Policy Server being upgraded before continuing. Select **Upgrade** and continue.

    ■ **Stopping Websense services**: A list of currently running Websense services from the earlier version appears. A message explains that the installer must stop these services before the upgrade can proceed. Select **Next** to continue.

    ■ **System requirements check**: The installer compares the system requirements for the installation you have selected with the resources of the installation machine. If the machine has inadequate disk space or memory, separate warnings are displayed.

        • If the installation machine has insufficient disk space, the selected components cannot be installed, and the installer will quit.

        • If the installation machine has less than the recommended amount of memory, the installation will continue. To ensure the best performance of the components you are installing, you should upgrade your machine's memory to the recommended amount.

    ■ **Installation summary**: A summary list appears, showing the installation path, installation size, and the components to be upgraded.

11. Select **Next** to begin the upgrade.

    ■ If you are using the online installer, the Download Manager copies the appropriate installer files from the Websense website. Installation begins automatically when the necessary files have been downloaded.

■ **Master Database Download**: The installer asks if you want to download the Websense Master Database now or at a later time using Websense Manager. Select a database download option and then select **Next** to continue.

> ⚠ **Warning**
>
> During upgrade, the installer removes the existing Master Database. Websense filtering cannot resume until the new Master Database has been successfully downloaded, decompressed, and loaded. This 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.

If you have chosen to download the Master Database now, the download begins. The database must first be downloaded from the internet, and then decompressed and loaded into local memory. Downloading the database from the internet can take a few minutes or more than 30 minutes, depending on factors such as internet connectivity, bandwidth, time of day, and your location relative to the download server. Decompressing and loading the database can take a few minutes or more than 30 minutes, depending on factors such as available memory, free disk space, and server process utilization.

When the database has finished loading, a message appears advising you of the status of the download. Select **Next** to continue.

12. When a message announcing successful completion of the installation is displayed:

    ■ If you chose a non-English language installer, select **Next** to continue. The Websense Language Pack installer starts. Follow the onscreen instructions to update Websense components with text in the selected language.

    ■ If you chose an English language installer:

      • If you are installing in GUI mode, and Websense Manager was upgraded, select **Next** to continue. The installer asks if you want to start Websense Manager. Make a choice and select **Finish** to exit the installer.

      • Otherwise, select **Finish** to exit the installer.

13. If you stopped your antivirus software, be sure to start it again.

> **Important**
>
> Make sure you upgrade any other Websense components or products that may have a dependency on the system you just upgraded. This will prevent conflicts caused by incompatible versions.
>
> For example, if you are using Websense Reporting Tools, you must upgrade them to the same version as the Websense filtering components to properly generate reports.

If you decide to change the location of a Websense component, add a feature, or remove a component, run the Websense installer again on the machine you want to modify and select the appropriate option. The installer detects the presence of Websense components and offers you options for modifying your installation.

Upgrading Components on Windows

Run the Windows version of the Websense Enterprise or Web Security Suite installer on each Windows machine on which a Websense component is installed.

> **Important**
>
> Make sure to back up the `websense.ini`, `eimserver.ini`, and `config.xml` files before proceeding. A full system backup is recommended.

To upgrade your v6.1 or higher Windows Websense components to v6.3.2:

1. Close all Websense Managers anywhere in the network that connect to the Policy Server you are upgrading.
2. Log on to the installation machine with **domain** and **local** administrator privileges.

If you are upgrading User Service and DC Agent, this will assure that they have administrator privileges on the domain.

> **Important**
>
> User Service and DC Agent must have administrator privileges on the network to retrieve user login information from the domain controller. Without this information, Websense software cannot filter by users and groups. If you cannot install these components with such privileges, you can configure domain administrator privileges for these services after installation. For instructions, see *Configure Domain Administrator Privileges*, page 202.

3. Close all applications and stop any antivirus software.

> **Warning**
>
> Be sure to close the Windows Event Viewer, or the upgrade may fail.

4. Obtain an installer package for either Websense Enterprise or Web Security Suite:

   - **Web download**: To download an installer package, go to www.websense.com, and then navigate to the Downloads page.

     a. Choose your product, the dynamic (online) or full (offline) installer package, the operating system, and the language.

> **Note**
>
> The **Dynamic** installer is an **online** installer package that requires web access during installation. It downloads the necessary product files from the website as needed after product selections have been made.
>
> The **Full** installer is a complete **offline** installer. It is much larger than the online Dynamic installer package, and contains all the files needed to install the Websense Enterprise or Web Security Suite components. Use this package if you experience difficulties with the online installer.

b. Download the selected installer package to a folder on the installation machine, and double-click to extract the installer files.

A screen displays instructions for extracting the setup program.

Websense Enterprise Installer File Extraction

If you are using the Web Security Suite installer, the default destination folder will be `WebSecuritySuite632Setup`.

5. If you do not want to accept the default location, click **Browse** to select a destination folder, or type in a path.

If the path you enter does not exist, the installer will create it for you.

> **Important**
>
> Do not extract the installer files to a folder on your desktop. This may prevent the Real-Time Analyzer from receiving the IP address of the Policy Server machine. Accept the default location of `C:\temp` or select another appropriate folder.

6. Click **Extract** to begin decompressing the files.

   - If Websense installation files already exist in that location, you may choose to overwrite the existing files.

   - A progress bar shows the status of the extraction, and the view pane scrolls a list of the files as they are decompressed.

   - `Setup.exe` runs automatically after the files are decompressed.

7. Follow the onscreen instructions and click **Next** to advance through the welcome screen and the subscription agreement.

   The installer detects the Websense components from your earlier version and asks how you want to proceed. You can upgrade the current system or exit the installer.

8. Select **Upgrade** and click **Next**.

   A list of currently running Websense services from the earlier version appears. A message explains that the installer must stop these services before the upgrade can proceed.

9. Click **Next** to continue.

   The installer compares the system requirements for the installation you have selected with the resources of the installation machine. If the machine has inadequate disk space or memory, warnings are displayed in separate screens.

   - If the target machine has insufficient disk space, the selected components cannot be installed, and the installer quits.

   - If the installation machine has less than the recommended amount of memory, the installation can continue. To ensure the best performance of the components you are installing, you should upgrade your machine's memory to the recommended amount.

A summary screen appears, listing the installation path, file sizes, and the components that will be upgraded.

10. Click **Next** to begin the upgrade.

   - If you are using the online installer, the Download Manager progress bars are displayed as the necessary files are downloaded from the Websense website. When the download process is complete, the installer stops the Websense services and begins the upgrade. An installation progress bar appears while the installer upgrades your system and restarts the Websense services.

   - If you are using the Apache HTTP Server, you must restart it before using the Real-Time Analyzer on your upgraded system. The installer asks if you want to restart Apache now or wait until later. Select **Yes** or **No** and click **Next** to continue.

11. When a message announcing successful completion of the installation is displayed:

   - If you chose a non-English language installer, click **Next** to continue. The Websense Language Pack installer starts. Follow the onscreen instructions to update Websense components with text in the selected language.

   - If you chose an English language installer:

      • If Websense Manager was not upgraded, no further action is required and you can click **Finish** to exit the installer.

      • If Websense Manager was upgraded, click **Next** to continue. The installer displays a screen asking if you want to launch Websense Manager. If you do not want to launch Manager, clear the checkbox. Click **Finish** to exit the installer.

12. If you stopped your antivirus software, be sure to start it again.

Upgrading the Remote Filtering Components

If the optional Remote Filtering components are installed in your network, you must upgrade them along with the rest of your Websense Enterprise or Web Security Suite components.

> **Important**
>
> You must upgrade Remote Filtering Server to the same version as the rest of your Websense components.
>
> Remote Filtering Server 6.3.2 is backwards compatible with Remote Filtering Client 6.2. You do not have to upgrade your v6.2 Remote Filtering Clients to v6.3.2, but be aware that they will not be able to access the remote filtering features added in version 6.3.2. For information about these features, see the *Websense Enterprise and Websense Web Security Suite v6.3.2 Release Notes*.

Remote Filtering Server

The Remote Filtering Server is upgraded in the same manner as the rest of the Websense components, by running the v6.3.2 Websense installer on the machine where the Remote Filtering Server is installed. See the previous sections of this chapter for detailed instructions.

Remote Filtering Client Pack

The Remote Filtering Client Pack can be upgraded in the same manner as the rest of the Websense components, by running the v6.3.2 Websense installer on the machine where the Remote Filtering Client Pack is installed. See the previous sections of this chapter for detailed instructions.

Remote Filtering Client

The Remote Filtering Clients in your network can be upgraded in two ways:

- ◆ **Manual upgrade**: Use the v6.3.2 Remote Filtering Client Pack installer package to manually uninstall the existing version of the Remote Filtering Client on an individual workstation, and then install the new version. See *Manual Upgrade of Remote Filtering Client*, page 51 for information.

This upgrade method does *not* preserve existing Remote Filtering Client configuration settings; communication information for Remote Filtering Server must be re-entered.

◆ **Automatic upgrade with third-party tool**: Use the v6.3.2 Remote Filtering Client Pack and a third-party deployment tool to automatically uninstall the existing version of Remote Filtering Client on employee workstations, and replace it with the new version. See *Upgrading Remote Filtering Client with a Third-Party Deployment Tool*, page 53 for information.

> ✔ **Note**
>
> If you add Websense Client Policy Manager (CPM) to your network when you upgrade, you do not have to upgrade your Remote Filtering Clients as described in this section. Because the Remote Filtering Client is included as part of the CPM Client Agent, you can simply deploy CPM Client Agent with the appropriate remote filtering settings. For more information, see your Websense Client Policy Manager documentation.

Manual Upgrade of Remote Filtering Client

To manually upgrade an instance of the Remote Filtering Client on a single Windows workstation to v6.3.2:

> ✔ **Note**
>
> This upgrade method does *not* preserve existing Remote Filtering Client configuration settings; communication information for Remote Filtering Server must be re-entered.

1. Run the v6.3.2 Websense installer on the Remote Filtering Client workstation to upgrade or install the Remote Filtering Client Pack:

    ■ If a previous version of the Remote Filtering Client Pack is installed on the machine, the Websense installer will detect it. Follow the onscreen instructions to upgrade it to v6.3.2.

- If no previous version of the Remote Filtering Client Pack exists on the machine, follow the installation instructions in *Remote Filtering Client Pack*, page 122.

2. Navigate to the default installation location of

   ```
   C:\Program Files\Websense\bin\
   RemoteFilteringAgentPack\NO_MSI\CPMClient.msi
   ```

   and double-click on the CPMClient.msi file to run the new Remote Filtering Client installer.

3. When the application detects an existing installation of Remote Filtering Client, it asks if you want to remove it. Click **Next** to continue.

4. When the **Remove the Program** dialog box appears, click **Remove**.

5. When the **InstallShield Wizard Completed** dialog box opens, click **Finish** to complete removal of the existing Remote Filtering Client.

6. Restart the machine.

7. Double-click on the CPMClient.msi file to run the Remote Filtering Client installer again.

8. Click **Next** to continue.

9. Re-enter the connection information for the primary Remote Filtering Server that this client uses for web filtering. If you are not certain of these values, you can view them in Websense files on the Remote Filtering Server machine:

   a. Navigate to the securewispproxy.ini file, located in the /bin subdirectory in the Websense installation directory on the Remote Filtering Server machine.

   b. Open the securewispproxy.ini file with a text editor to view the values of the following Remote Filtering Server parameters:

      • External IP address or host name: ProxyPublicAddress
      • External communication port: ProxyPort
      • Internal IP address or host name: ProxyIP
      • Internal communication port: HeartBeatPort

   c. If you do not remember the pass phrase you defined when installing the Remote Filtering Server, enter the encrypted key instead. The Websense software generates this key automatically by combining the pass phrase you defined with unpublished Websense keys. If you do not know the encrypted key, you can look it up if you have administrator rights on the Remote Filtering Server machine:

- Navigate to the WSSEK.DAT file, located in the `/bin` subdirectory in the Websense installation directory on the Remote Filtering Server machine, and open it with a text editor to view the encrypted key.

10. If secondary and tertiary Remote Filtering Servers are being used, re-enter communication parameters for each of these servers as well.

11. Click **Next** to continue.

12. Click **Install** to begin installation.

    When the installer is finished, a message appears advising you that the procedure was successful.

13. Click **Finish** to exit the installer.

14. If a message appears indicating that you must restart the machine, click **Yes** to restart now. Remote filtering will not function properly until the machine is restarted.

    If no message appears, restarting the machine is not required.

Upgrading Remote Filtering Client with a Third-Party Deployment Tool

This upgrade method allows you to deploy version 6.3.2 of the Remote Filtering Client to user workstations, while preserving the existing configuration settings.

To obtain the installer for version 6.3.2 of the Remote Filtering Client, you can:

◆ Upgrade an existing version of the Remote Filtering Client Pack to version 6.3.2 (see *Remote Filtering Client Pack*, page 50 for instructions).

-OR-

◆ Install version 6.3.2 of the Remote Filtering Client Pack on a Windows machine (see *Remote Filtering Client Pack*, page 122 for instructions).

If you selected the default installation path of `C:\Program Files\Websense`, the installer is placed in the following location:

```
C:\Program Files\Websense\bin\
RemoteFilteringAgentPack\NO_MSI\CPMClient.msi
```

To deploy the new version of the Remote Filtering Client to Windows workstations, use this installer with a third-party deployment tool, such as Microsoft® Systems Management Server (SMS) or Novell® ZENworks®.

Upgrade Syntax

The following is an example of the syntax to upgrade Remote Filtering Client using a third-party deployment tool. This command must be typed on a single line with no returns.

```
msiexec /i cpmclient.msi REINSTALL=ALL
REINSTALLMODE=voums /qn
```

When the installer upgrades an installation of the Remote Filtering Client, the current configuration settings are used. If your remote filtering configuration *has not* changed, no additional parameters are necessary. However, if you have changed your configuration, you must include the appropriate parameters and new values in the command. For a complete list of command line parameters, see *Installing Remote Filtering Client with a Third-Party Deployment Tool*, page 129.

Upgrading from Websense Enterprise to Web Security Suite

Existing Websense Enterprise systems, version 6.1 and higher, can be upgraded directly to Web Security Suite. You must run the Web Security Suite installer on each machine where a Websense component is installed. The installer detects all Websense components of version 6.1 or higher on that machine and upgrades them accordingly.

Make sure to observe the following sequence when upgrading a Websense Enterprise system to a Websense Web Security Suite system:

◆ First, upgrade Websense Enterprise components to Web Security Suite components. Use the same upgrade procedures described previously in this chapter for upgrading an existing Web Security Suite installation to v6.3.2.

◆ Next, upgrade Websense Enterprise Reporting components to Web Security Suite Reporting components. For instructions, see the *Reporting Installation Guide* for Websense Enterprise and Web Security Suite.

If you are running a version of Websense Enterprise prior to v6.1, you must perform an intermediate upgrade first to bring your Websense Enterprise version level up to v6.1. For more information, see *Versions Supported*, page 36.

Initial Setup

If you are an existing Websense Enterprise customer who is upgrading to Websense Web Security Suite, some additional post-installation configuration is required.

You must configure Websense Security PG™ (also known as Websense Security Filtering) and the Security Protocol Groups in your existing policies in order to block access to these sites and protocols. For information, see the Websense Enterprise *Administrator's Guide*.

The rest of the initial setup steps are the same as for a new installation of Web Security Suite. These steps are described in *Chapter 5: Initial Setup*.

Converting a Stand-Alone System to an Integrated System

You can convert an existing Websense Stand-Alone Edition to a Websense system using Squid Web Proxy Cache without losing any configuration settings. The conversion process preserves such settings as port numbers and IP addresses.

✔ **Note**

Microsoft Windows versions of stand-alone Websense systems (Websense Enterprise or Web Security Suite Stand-Alone Edition, Stand-Alone EIM Evaluation, and Websense for Small and Medium Businesses (SMB)) *cannot* be converted to systems integrated with Squid Web Proxy Cache on Solaris or Linux machines. No upgrade path exists that will preserve the configuration settings.

All Websense Filtering Components on the Same Machine

When all Websense Enterprise or Web Security Suite components are installed on the same machine, you can convert a Stand-Alone system to an integrated system by performing the following tasks:

Task 1: Upgrade to the v6.3.2 Stand-Alone Edition:

- If you have Websense v6.1 or higher Stand-Alone Edition installed, perform a direct upgrade to the v6.3.2 Stand-Alone Edition. This will preserve your configuration data and use the settings from your original system. Follow the procedures in *Upgrading to the New Stand-Alone Edition*, page 58.
- If you have an earlier Websense stand-alone version installed, see v6.3.2 of the *Installation Guide for use with Stand-Alone Edition* for upgrade instructions.

Task 2: Restart the installation machine.

Task 3: Convert the v6.3.2 Stand-Alone Edition to a system integrated with Squid Web Proxy Cache.

The procedure depends on where the Websense filtering software is installed:

- If the Websense software is running on the same machine as the Squid Web Proxy Cache, follow the procedures in *Converting to an Integrated System when Squid Web Proxy Cache is on the Websense Machine*, page 62.
- If the Websense software is running on a different machine than the Squid Web Proxy Cache, follow the procedures in *Converting to an Integrated System when Squid Web Proxy Cache is on a Different Machine*, page 65.

Task 4: If the Squid Web Proxy Cache is on a different machine than the Websense Filtering Service, install the Squid Plug-in on that machine. For instructions, see *Installing the Squid Plug-in on the Squid Web Proxy Machine*, page 87.

Task 5: Perform the tasks in *Chapter 5: Initial Setup*.

Distribute Websense Filtering Components

To convert your Websense Stand-Alone Edition to use Squid Web Proxy Cache and move some Websense filtering components to other machines, perform the following tasks:

Task 1: Upgrade to the v6.3.2 Stand-Alone Edition:

- If you have Websense v6.1 or higher Stand-Alone Edition installed, perform a direct upgrade to the v6.3.2 Stand-Alone Edition. This will preserve your configuration data and use the settings from your original system. Follow the procedures in *Upgrading to the New Stand-Alone Edition*, page 58.
- If you have an earlier Websense stand-alone version installed, see v6.3.2 of the *Installation Guide for use with Stand-Alone Edition* for upgrade instructions.

Task 2: Restart the installation machine.

Task 3: Run the Websense installer again and remove those components that you want to move to a different location in your network.

> **Warning**
>
> Removing the Policy Server will delete all existing configuration settings.

Task 4: Convert the v6.3.2 Stand-Alone Edition to a system integrated with Squid Web Proxy Cache.

The procedure depends on where the Websense filtering software is installed:

- If the Websense software is running on the same machine as the Squid Web Proxy Cache, follow the procedures in *Converting to an Integrated System when Squid Web Proxy Cache is on the Websense Machine*, page 62.
- If the Websense software is running on a different machine than the Squid Web Proxy Cache, follow the procedures in *Converting to an Integrated System when Squid Web Proxy Cache is on a Different Machine*, page 65.

Task 5: Run the Websense installer on each machine in your network on which you want to install a separate component. Select a **Custom** installation when prompted and select the component you want to install. Separate installation procedures for individual components can be found in *Installing Websense Components Separately*, page 91.

Task 6: If the Squid Web Proxy Cache is on a different machine than the Websense Filtering Service, install the Squid Plug-in on that machine. For instructions, see *Installing the Squid Plug-in on the Squid Web*

Proxy Machine, page 87.

Task 7: Perform the tasks in *Chapter 5: Initial Setup*.

Upgrading to the New Stand-Alone Edition

Your first task is to upgrade your v6.1 or higher Stand-Alone Edition to the v6.3.2 Stand-Alone Edition.

Important

Websense services must be running when the upgrade process begins. The installer will stop and start these services as necessary during the upgrade. If these services have run uninterrupted for several months, however, the installer may not be able to stop them before the upgrade process times out.

To ensure the success of the upgrade, manually stop and restart all the Websense services before beginning the upgrade. To stop and start Websense services, follow the instructions in *Stopping or Starting Websense Services*, page 176.

Solaris or Linux

The v6.3.2 Websense Enterprise or Web Security Suite installer can upgrade version 6.1 or higher of the Stand-Alone Edition.

1. Back up the following files before proceeding:

   - `websense.ini`
   - `eimserver.ini`
   - `config.xml`

Note

Before upgrading to a new version of Websense Enterprise or Web Security Suite, Websense, Inc., recommends that you perform a full system backup as a fallback strategy. This will allow you to restore your current production system with a minimum of downtime should you encounter any problems with the upgrade.

---

2. Close all Websense Managers anywhere in the network that connect to the Policy Server you are upgrading.

3. Log on to the installation machine as the **root** user.

4. Close all applications and stop any antivirus software.

5. Create a setup directory for the installer files.

   For example: `/root/Websense_setup`

6. Obtain a v6.3.2 Solaris or Linux installer package for either Websense Enterprise or Web Security Suite:

   - **Web download**: To download an installer package, go to www.websense.com, and then navigate to the Downloads page.

     a. Choose your product, the dynamic (online) or full (offline) installer package, the operating system, and the language.

   ✔ **Note**

   The **Dynamic** installer is an **online** installer package that requires web access during installation. It downloads the necessary product files from the website as needed after product selections have been made.

   The **Full** installer is a complete **offline** installer. It is much larger than the online Dynamic installer package, and contains all the files needed to install the Websense Enterprise or Web Security Suite components. Use this package if you experience difficulties with the online installer.

     b. Save the selected installer package to the setup directory on the installation machine.

7. In the setup directory, enter the following command to unzip the file:

   `gunzip <download file name>`

   For example: `gunzip Websense632Setup_Slr.tar.gz`

8. Expand the file into its components with the following command:

    ```
    tar xvf <unzipped file name>
    ```

    For example: `tar xvf Websense63Setup_Slr.tar`

    This places the following files into the setup directory:

File	Description
install.sh	Installation program
Setup	Archive file containing related installation files and documents.
Documentation	Release Notes: An HTML file containing release notes and last minute information about the Websense software. Read this file with any supported browser.

9. Run the installation program from the setup directory with the following command:

    ```
    ./install.sh
    ```

    To run the GUI version of the installer, use the following command:

    ```
    ./install.sh -g
    ```

    If you are using a non-English based system, the installer will display an error message advising you that the GUI version is not supported.

10. Follow the onscreen instructions through the subscription agreement.

11. Follow the upgrade sequence:

    - **Websense upgrade**: The installer detects the earlier version of Websense components and gives you the choice of upgrading the existing installation or exiting Setup. Be sure to close any Websense Managers connected to the Policy Server being upgraded before continuing. Select **Upgrade** and continue.

    - **Stopping Websense services**: A list of currently running Websense services from the earlier version appears. A message explains that the installer must stop these services before the upgrade can proceed. Select **Next** to continue.

    - **System requirements check**: The installer compares the system requirements for the installation you have selected with the resources of the installation machine. If the machine has inadequate disk space or memory, separate warnings are displayed.

- • If the installation machine has insufficient disk space, the selected components cannot be installed, and the installer will quit.
- • If the installation machine has less than the recommended amount of memory, the installation can continue. To ensure the best performance of the components you are installing, you should upgrade your machine's memory to the recommended amount.

■ **Installation summary**: A summary list appears, showing the installation path, file sizes, and the components that will be upgraded.

12. Select **Next** to begin the upgrade.

If you are using the online installer, the Download Manager indicates the progress of the file download from the Websense website. After the files are downloaded, the installer stops all Websense services.

An installation progress bar appears and the Websense services are restarted.

■ **Master Database Download**: The installer asks if you want to download the Websense Master Database now or at a later time using Websense Manager. Select a database download option and then select **Next** to continue.

> ⚠ **Warning**
> During upgrade, the installer removes the existing Master Database. Websense filtering cannot resume until the new Master Database has been successfully downloaded, decompressed, and loaded. This 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.

If you have chosen to download the Master Database now, the download begins. The database must first be downloaded from the internet, and then decompressed and loaded into local memory. Downloading the database from the internet can take a few minutes or more than 30 minutes, depending on factors such as internet connectivity, bandwidth, time of day, and your location relative to the download server. Decompressing and loading the database can take a few minutes or more than 30 minutes, depending on factors such as available memory, free disk space, and server process utilization.

When the database has finished loading, a message appears advising you of the status of the download. Select **Next** to continue.

13. When a message announcing successful completion of the installation is displayed:

   ■ If you chose a non-English language installer, select **Next** to continue. The Websense Language Pack installer starts. Follow the onscreen instructions to update Websense components with text in the selected language.

   ■ If you chose an English language installer:

      • If you are installing in command line mode, select **Finish** to exit the installer.

      • If you are installing in GUI mode, select **Next** to continue. The installer asks if you want to start Websense Manager. Make a choice and select **Finish** to exit the installer.

14. If you stopped your antivirus software, be sure to start it again.

Converting to an Integrated System when Squid Web Proxy Cache is on the Websense Machine

Once you have upgraded your existing Stand-Alone Edition to the v6.3.2 Stand-Alone Edition, you are ready to convert to a system that integrates with Squid Web Proxy Cache.

If the Websense software (Filtering Service) is on the *same* machine as the Squid Web Proxy Cache, follow the instructions in this section.

Solaris or Linux

To convert a Solaris or Linux v6.3.2 Websense Stand-Alone Edition to a v6.3.2 Websense system integrated with Squid Web Proxy Cache when Squid Web Proxy Cache is on the same machine:

> **Important**
>
> If you are converting the Stand-Alone Edition on a machine running Red Hat Enterprise Linux ES 4 with SELinux enabled, and using the version of Squid that is prepackaged with the Red Hat installation, additional steps are necessary for successful Websense filtering.
>
> The SELinux installation packaged with Red Hat Enterprise Linux ES 4, and enabled by default, prevents Squid from launching the Websense Squid Plug-in (`WsRedtor`). If `WsRedtor` does not launch, Websense filtering cannot occur. You can address this issue by configuring SELinux permissions so that `WsRedtor` can launch; see your Red Hat Enterprise Linux documentation for details. For more information and a discussion of other options for addressing this issue, see the troubleshooting topic *Internet requests are not being filtered*, page 230.

1. Back up the following files before proceeding:
   - `websense.ini`
   - `eimserver.ini`
   - `config.xml`
2. Close all Websense Managers anywhere in the network that connect to the Policy Server you are upgrading.
3. Log on to the installation machine as the **root** user.
4. Close all applications and stop any antivirus software.
5. Run the Websense installer from the directory where you unpacked it using the following command:

   `./install.sh`

   To run the GUI version of the installer, use the following command:

   `./install.sh -g`

If you are using a non-English based system, the installer will display an error message advising you that the GUI version is not supported.

6. Make the following selections:

   - **Stand-Alone Edition Detected**: The installer detects the presence of the Websense Stand-Alone Edition and asks what you want to do. Select **Integrate with a firewall, proxy server, or network appliance** and continue.

   - **Stopping Websense services**: A message explains that the installer must stop the Filtering Service before the installation can proceed. Select **Next** to continue.

   - **Integration product**: Select **Squid Web Proxy Cache** from the list of supported integration types.

   - **Squid configuration file**: The installer asks for the path to the Squid configuration file (`squid.conf`). A default path is provided. The installer will attempt to verify this path and will not continue unless it is accurate.

   - **Squid executable**: The installer asks for the file path to the Squid executable (**squid**). The installer shuts down Squid automatically before the installation continues.

   - **System requirements check**: The installer compares the system requirements for the installation you have selected with the resources of the installation machine. If the machine has inadequate disk space or memory, separate warnings are displayed.

     - If the installation machine has insufficient disk space, the selected components cannot be installed, and the installer will quit.

     - If the installation machine has less than the recommended amount of memory, the installation can continue. To ensure the best performance of the components you are installing, you should upgrade your machine's memory to the recommended amount.

   - **Installation summary**: A summary list appears, showing the installation path, file sizes, and the components that will be installed.

7. Select **Next** to begin installation.

   If you are using the online installer, the Download Manager copies the appropriate installer files from the Websense website. Installation begins automatically when the necessary files have been downloaded.

8. When a message announcing successful completion of the installation is displayed:

   - If you chose a non-English language installer, select **Next** to continue. The Websense Language Pack installer starts. Follow the onscreen instructions to update Websense components with text in the selected language.

   - If you chose an English language installer, select **Finish** to exit the installer.

9. If you stopped your antivirus software, be sure to start it again.

Converting to an Integrated System when Squid Web Proxy Cache is on a Different Machine

Once you have upgraded your existing Stand-Alone Edition to the v6.3.2 Stand-Alone Edition, you are ready to convert to a v6.3.2 Websense system that integrates with Squid Web Proxy Cache.

If the Websense Filtering Service is on a *different* machine than the Squid Web Proxy Cache, you must remove the existing Stand-Alone version of the Filtering Service, and re-install it integrated with Squid Web Proxy Cache.

Solaris or Linux

To convert a Solaris or Linux v6.3.2 Websense Stand-Alone Edition to a v6.3.2 Websense system integrated with Squid Web Proxy Cache when Squid Web Proxy Cache is on a different machine:

> **Important**
>
> If you are converting the Stand-Alone Edition on a machine running Red Hat Enterprise Linux ES 4 with SELinux enabled, and using the version of Squid that is prepackaged with the Red Hat installation, additional steps are necessary for successful Websense filtering.
>
> The SELinux installation packaged with Red Hat Enterprise Linux ES 4, and enabled by default, prevents Squid from launching the Websense Squid Plug-in (`WsRedtor`). If `WsRedtor` does not launch, Websense filtering cannot occur. You can address this issue by configuring SELinux permissions so that `WsRedtor` can launch; see your Red Hat Enterprise Linux documentation for details. For more information and a discussion of other options for addressing this issue, see the troubleshooting topic *Internet requests are not being filtered*, page 230.

---

1. Back up the following files before proceeding:
   - `websense.ini`
   - `eimserver.ini`
   - `config.xml`
2. Close all Websense Managers anywhere in the network that connect to the Policy Server you are upgrading.
3. Log on to the installation machine as the **root** user.
4. Close all applications and stop any antivirus software.
5. Run the v6.3.2 Websense Enterprise or Web Security Suite installer from the directory where you unpacked it, using the following command:

   `./install.sh`

   To run the GUI version of the installer, use the following command:

   `./install.sh -g`

If you are using a non-English based system, the installer will display an error message advising you that the GUI version is not supported.

6. Make the following selections:

   ■   **Stand-Alone Edition Detected**: The installer detects the presence of the Websense Stand-Alone Edition and asks what you want to do. Select **Remove Websense components** and continue.

   ■   **Remove components**: The installer provides a list of currently installed components. Select **Filtering Service** for removal.

   ■   **Uninstall summary**: A message states that the Filtering Service will be removed. Select **Next** to continue.

   ■   **Uninstall complete**: The installer displays a message indicating that the selected components have been removed. Select **Finish** to exit the installer.

7. Run the v6.3.2 Websense Enterprise or Web Security Suite installer again by entering the following command in the directory where you unpacked it:

   ```
   ./install.sh
   ```

   Or, to run the GUI version of the installer, use the following command:

   ```
   ./install.sh -g
   ```

8. Make the following selections:

   ■   **Add/Remove/Repair components**: The installer detects the previously installed Websense components and asks how you want to proceed. Select **Add Websense components**.

   ■   **Select components**: The installer asks you to select the components you want to install. Select **Filtering Service**.

   ■   **Integration option**: Select **Integrated** when asked if you want to install Websense software in a stand-alone mode, or in an integrated configuration.

   ■   **Integration product**: Select **Squid Web Proxy Cache** from the list of supported integration types.

   ■   **Initial filtering options**: Select **Yes** to filter internet traffic immediately after installation, based on the existing policies configured in your Policy Server. Select **No** to monitor internet traffic only, while permitting all internet requests.

■ **System requirements check**: The installer compares the system requirements for the installation you have selected with the resources of the installation machine. If the machine has inadequate disk space or memory, separate warnings are displayed.

- If the installation machine has insufficient disk space, the selected components cannot be installed, and the installer will quit.

- If the installation machine has less than the recommended amount of memory, the installation can continue. To ensure the best performance of the components you are installing, you should upgrade your machine's memory to the recommended amount.

■ **Installation summary**: A summary list appears, showing the installation path, installation size, and the Filtering Service as the component that will be installed.

9. Select **Next** to begin installation.

   If you are using the online installer, the Download Manager copies the appropriate installer files from the Websense website. Installation begins automatically when the necessary files have been downloaded.

   The installer asks if you want to download the Websense Master Database now or at a later time using Websense Manager.

10. Select a database download option and click **Next**.

    If you have chosen to download the Master Database now, a progress bar appears. The database must first be downloaded from the internet, and then decompressed and loaded into local memory. Downloading the database from the internet can take a few minutes or more than 30 minutes, depending on factors such as internet connectivity, bandwidth, time of day, and your location relative to the download server. Decompressing and loading the database can take a few minutes or more than 30 minutes, depending on factors such as available memory, free disk space, and server process utilization.

    When the database has finished loading, a message appears advising you of the status of the download.

11. Select **Next** to continue.

12. When a message announcing successful completion of the installation is displayed:

- If you chose a non-English language installer, select **Next** to continue. The Websense Language Pack installer starts. Follow the onscreen instructions to update Websense components with text in the selected language.

- If you chose an English language installer, select **Finish** to exit the installer.

13. If you stopped your antivirus software, be sure to start it again.

Changing IP Addresses of Installed Components

Websense filtering software handles most IP address changes automatically, without any interruption in internet filtering. Changes to the IP address of the machine running the Policy Server result in notification of the change being broadcast to Websense components on other machines. In some cases, however, services need to be restarted or configurations updated after changing an IP address. For a full discussion of the IP address change process, see the *Administrator's Guide* for Websense Enterprise and Web Security Suite.

CHAPTER 4

Installing Websense Enterprise or Web Security Suite

This chapter contains instructions for a new installation of Websense Enterprise or Web Security Suite components. In addition to installation procedures, instructions are provided for modifying an installation, including adding, removing, and repairing installed components.

Websense Installers

Separate Websense installers are available for the Windows, Solaris, and Linux operating systems. There are two different Websense product installers for each operating system:

- **Websense Enterprise**
- **Web Security Suite**

For information about using the product features after you have completed installation, see the *Administrator's Guide* for Websense Enterprise and Web Security Suite.

All Websense installers are available in English and nine other language versions. See *Non-English Language Versions*, page 71 if you plan to use your Websense software in a non-English language environment.

Non-English Language Versions

Separate Websense Enterprise and Web Security Suite v6.3.2 installer packages are available for the following languages:

Language	Code
Chinese (Simplified)	zh_CN
Chinese (Traditional)	zh_TW

Language	Code
English	en
French	fr
German	de
Italian	it
Japanese	ja
Korean	ko
Portuguese (Brazil)	pt_BR
Spanish	es

Go to www.websense.com, navigate to the Downloads page, and then select an installer package for the desired language.

> **Important**
>
> All Websense components in a Websense installation must be in the same language.

Each non-English installer package includes a Language Pack that converts your Websense system to that language. The Language Pack installer launches automatically following completion of the main Websense installer. Simply follow the onscreen instructions to complete the installation of the Language Pack.

> **Note**
>
> **Installer Language**: The Japanese version of the Websense installer and Language Pack installer are in Japanese. The Websense installer and Language Pack installer for all other languages are in English.

The Language Pack makes the following modifications to a Websense Enterprise or Web Security Suite system:

◆ Localized block page files are copied into a new directory created for the selected non-English language on the installation machine. The directory name is the language code shown in the preceding table.

◆ The Websense configuration file (`config.xml`) is edited to localize certain data strings such as warnings and error messages.

◆ Websense category names are updated with localized versions.

◆ Alert messages for Websense Administrators are updated with localized versions.

◆ The Reporting Tools Portal and Real-Time Analyzer are updated with localized versions.

◆ *Japanese only*: The Websense Manager user interface is converted to Japanese.

> ✔ **Note**
>
> For information about the modifications that Language Pack makes to the Websense Reporting components, see the *Reporting Installation Guide* for Websense Enterprise and Web Security Suite.
>
> For information about the modifications that Language Pack makes to Client Policy Manager components, see the *Installation Guide* for Websense Client Policy Manager.

Before Installing

Read the following information before installing Websense Enterprise or Web Security Suite.

◆ **Reporting**: To properly generate reports, you must use the same version of Websense filtering software and Websense Reporting Tools.

> **Important**
>
> Install all Websense Enterprise or Web Security Suite components *before* installing Websense Enterprise Reporting or Web Security Suite Reporting components.

For information about installing Reporting components, see the *Reporting Installation Guide* for Websense Enterprise and Web Security Suite.

◆ **Deployment**: The Squid Plug-in, the Websense filtering plug-in for communication with the Squid Web Proxy Cache, is supported on Solaris

and Linux operating systems only. The Squid Plug-in must be installed on the Squid Web Proxy Cache machine. You can install the main Websense components (Filtering Service, Policy Server, Websense Manager, User Service, Usage Monitor, and Network Agent) along with the Squid Plug-in on the Squid machine by running a Typical installation (see *Typical Websense Installation*, page 76). You can also run a Typical installation on a separate Linux or Solaris machine to install the main components, and then install the Squid Plug-in separately on the Squid machine (see *Installing the Squid Plug-in on the Squid Web Proxy Machine*, page 87).

◆ **Deployment**: *Installing Websense Components Separately*, page 91

You can install Websense components on separate machines that do not have the same operating system. For example, you can install Websense Manager on a Windows machine and use it to configure a Policy Server running on a Linux machine. As long as each Websense component is supported on the operating system of the machine where it is installed, the components will work together. A list of system requirements for each Websense component can be found in the *Deployment Guide* for Websense Enterprise and Web Security Suite.

Be sure to read the *Deployment Guide* for Websense Enterprise and Web Security Suite before beginning installation to determine the appropriate deployment of Websense components in your network. The *Deployment Guide* also contains system requirements, including the supported operating systems for each Websense component and the supported versions of your integration product.

◆ **Computer clock synchronization**: If you are distributing Websense components in your network, synchronize the clocks on all machines on which a Websense component will be installed.

◆ **Remote filtering**: To install the optional Remote Filtering components that allow filtering of workstations located outside the network firewall, you must run the Websense installer and select a **Custom** installation. For information, see *Installing Websense Components Separately*, page 91.

◆ **Network Agent**: Network Agent is included as part of a Typical installation. The machine on which Network Agent is installed must be deployed so that Network Agent is able to monitor all requests sent from user workstations to the internet, as well as all replies from the internet to the requesting workstations. If you install Network Agent on a machine that cannot monitor the targeted traffic, Network Agent features such as Protocol Management, Bandwidth Optimizer, and IM Attachment Manager will not work correctly. For more information about positioning the

Network Agent machine in your network, see the Network Agent chapter in the *Deployment Guide* for Websense Enterprise and Web Security Suite.

> **Important**
>
> *Do not* install Network Agent on a machine running any type of firewall. Network Agent uses a packet-capturing utility which may not work properly when installed on a firewall machine. The only exception is a blade server or appliance that has separate processors or virtual processors to accommodate Network Agent and the firewall software.

◆ **Network Interface Card (NIC)**: The NIC that you designate for use by Network Agent during installation must support *promiscuous* mode. Promiscuous mode allows a NIC to listen to IP addresses other than its own. (Contact the manufacturer of your card to see if it supports promiscuous mode.) If the card supports promiscuous mode, it will be set to that mode by the Websense installer during installation.

> **Note**
>
> If you install Network Agent on a machine with multiple NICs, you can configure Network Agent after installation to use more than one NIC. See *Configuring Network Agent to use Multiple NICs*, page 199 for more information.

After installation, you can run the Traffic Visibility Tool to test whether the selected NIC can see the appropriate user internet traffic. See *Testing Visibility of Internet Traffic to Network Agent*, page 199

◆ **Web server**: To install Real-Time Analyzer (RTA) you must have either Microsoft IIS or Apache HTTP Server installed. If neither supported web server is detected, the installer gives you the option to install the Apache HTTP Server or continue the installation without installing RTA.

◆ **Internet access**: For the Websense Master Database download to occur during installation, the machine running the Websense Filtering Service must have internet access to the download servers at the following URLs:

■ download.websense.com

■ ddsdom.websense.com

■ ddsint.websense.com

- portal.websense.com
- my.websense.com

Make sure that these addresses are permitted by all firewalls, proxy servers, routers, or host files that control the URLs that Filtering Service can access.

◆ **Remote Control Utilities**: Installation of Websense Enterprise or Web Security Suite using a remote control utility such as Terminal Services is not supported.

◆ **Enabling Java interfaces**: If you are installing any Websense components on a Windows 2000 Server machine, you must install DirectX to launch the Java-based GUI installer. If DirectX is not present, you can only install Websense components in the console mode. To enable the console installer in Windows 2000, see the procedure in the troubleshooting topic *Websense splash screen is displayed, but installer does not launch on Windows 2000*, page 229.

If you have performed a console installation on a Windows 2000 Server machine without DirectX, you must install Websense Manager on a Solaris machine or on a Windows or Linux machine capable of displaying a Java interface.

Typical Websense Installation

Follow the procedures in this section to install Websense Enterprise or Web Security Suite on a Solaris or Linux machine. These procedures are for a **Typical** installation, in which the main Websense filtering components are installed on the same machine.

If you plan to distribute the main Websense components on separate machines in your network, you must install Policy Server first. Only Websense Manager can be installed before Policy Server has been successfully installed. To install components separately, run the Websense installer on each machine and select a **Custom** installation. For instructions to install Websense components separately, see *Installing Websense Components Separately*, page 91.

If you decide to change the location of a Websense component, add a component, or remove a component, run the Websense installer again on the machine you want to modify and select the appropriate option. The installer detects the presence of Websense components and offers you options for modifying your installation. For information about adding or removing

Websense components, see *Adding Components*, page 154 and *Removing Components*, page 164.

You can install the supported Websense components on the Squid Web Proxy Cache machine or on a different machine. If you install the Websense Filtering Service and Squid Web Proxy Cache on the same machine, you must also install the Squid Plug-in on that machine. The Squid Plug-in is the Websense component that allows Filtering Service to communicate with Squid.

If you install the Websense Filtering Service on a machine separate from the Squid Web Proxy Cache, you must subsequently install the Squid Plug-in on every Squid Web Proxy Cache machine that will communicate with the Websense Filtering Service. To install the Squid Plug-in separately, follow the instructions in *Installing the Squid Plug-in on the Squid Web Proxy Machine*, page 87.

> **Important**
>
> If you are installing Websense software on a machine running an SELinux-enabled Red Hat Enterprise Linux ES 4 operating system and the version of Squid that is prepackaged with the Red Hat installation, additional steps are necessary for successful Websense filtering.
>
> The SELinux installation packaged with Red Hat Enterprise Linux ES 4, and enabled by default, prevents Squid from launching the Websense Squid Plug-in (WsRedtor). If WsRedtor does not launch, Websense filtering cannot occur. You can address this issue by configuring SELinux permissions so that WsRedtor can launch; see your Red Hat Enterprise Linux documentation for details. For more information and a discussion of other options for addressing this issue, see the troubleshooting topic *Internet requests are not being filtered*, page 230.

A **Typical** installation gives you the opportunity to install the following Websense components together on the same Solaris or Linux machine:

◆ Filtering Service

◆ Policy Server

◆ User Service

- Websense Manager
- Network Agent
- eDirectory Agent
- Logon Agent
- RADIUS Agent
- Usage Monitor
- Squid Plug-in (installed on Squid machine)

If some components need to be installed on separate machines, see *Installing Websense Components Separately*, page 91 for instructions to install individual Websense components.

To install Websense Enterprise or Web Security Suite on a Solaris or Linux machine:

1. Log on to the installation machine as the **root** user.
2. Close all applications and stop any antivirus software.
3. Create a setup directory for the installer files.

   For example: `/root/Websense_setup`

4. Obtain an installer package for either Websense Enterprise or Web Security Suite:

   - **Web download**: To download an installer package, go to www.websense.com, and then navigate to the Downloads page.

     a. Choose your product, the dynamic (online) or full (offline) installer package, the operating system, and the language.

   ✓ **Note**

   The **Dynamic** installer is an **online** installer package that requires web access during installation. It downloads the necessary product files from the website as needed after product selections have been made.

   The **Full** installer is a complete **offline** installer. It is much larger than the online Dynamic installer package, and contains all the files needed to install the Websense Enterprise or Web Security Suite components. Use this package if you experience difficulties with the online installer.

b. Save the selected installer package to the setup directory on the installation machine.

5. In the setup directory, enter the following command to unzip the file:

    `gunzip <download file name>`

    For example: `gunzip Websense632Setup_Slr.tar.gz`

6. Expand the file into its components with the following command:

    `tar xvf <unzipped file name>`

    For example: `tar xvf Websense632Setup_Slr.tar`

    This places the following files into the setup directory:

File	Description
install.sh	Installation program.
Setup	Archive file containing related installation files and documents.
Documentation	Release Notes: An HTML file containing release notes and last minute information about the Websense software. Read this file with any supported browser.

7. Run the installation program from the setup directory with the following command:

    `./install.sh`

    To run the GUI version of the installer, use the following command:

    `./install.sh -g`

    If you are using a non-English based system, the installer will display an error message advising you that the GUI version is not supported.

8. Follow the onscreen instructions through the subscription agreement.

9. Provide the installer with the following information.

    ■   **Product selection** (*Web Security Suite only*): Select the Web Security Suite edition you want to install:

- **Web Security Suite**: Provides web security and reporting features.
- **Web Security Suite and Client Policy Manager**: Provides web security and reporting features, plus desktop security.

The installer displays information about the required installation sequence for the components of this product on your operating system. Installing in the proper sequence is important because of the shared components.

- **Installation type**: You are asked to select an installation type:

  - **Typical**: Installs Filtering Service, 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: eDirectory Agent, Logon Agent, and RADIUS Agent.

  - **Custom**: Allows you to install individual Websense components. You can use this option to install components on separate machines in your network. For more information, see *Installing Websense Components Separately*, page 91

  Select **Typical** to install the listed Websense components.

- **Multiple IP addresses**: If the installation machine is multihomed, all enabled network interface cards (NICs) appear in a list. Select the IP address of the card to use for Websense communications.

> **Important**
>
> Make sure you select a NIC in *normal* mode (cards with an IP address). Interface cards configured for *stealth* mode will appear in this list as well. If you select a stealth mode NIC for Websense communications, Websense services will not work.

- **Integration option**: Select **Integrated**.
- **Integration product**: Select **Squid Web Proxy Cache**.
- **Websense Plug-in**: If you are installing Websense Enterprise or Web Security Suite on the Squid Web Proxy Cache machine, select **Install plug-in and other selected Websense components**. If you are installing Websense components on a different machine, select **Install selected Websense components without plug-in**.

- **Squid configuration file**: If you are installing Websense Enterprise or Web Security Suite on the Squid Web Proxy machine, provide the path to the Squid configuration file (squid.conf). A default path is provided. The installer will attempt to verify this path and will not continue unless it is accurate.

- **Squid executable**: If you are installing Websense Enterprise or Web Security Suite on the Squid Web Proxy machine, provide the file path to the Squid executable (**squid**). The installer shuts down Squid automatically before the installation continues.

- **Port numbers**: The installer automatically assigns default port numbers to the Policy Server (55806) and the Filtering Service (15868). If either of these default ports is in use, the installer asks you to enter an alternate port. Enter an unused port number between 1024 and 65535.

> ✔ **Note**
>
> Record the port numbers if you change them from the defaults. You will need them when installing other Websense components.

- **Subscription key**: You can download the Websense Master Database during installation if you provide a valid subscription key or evaluation key. This will enable the Websense software to begin filtering immediately.

  - **I have a Websense subscription key**: If you have a valid subscription key, select this option and enter your key when prompted. You will be given the option to download the Websense Master Database during installation.

  - **I do not wish to use a key at this time**: Select this option to continue the installation without entering a key. You will not be given the option to download the Websense Master Database during installation. You can download the Master Database after installation by entering your key in Websense Manager. For instructions, see *Subscription Key and Master Database Download*, page 183.

  To request a 30-day evaluation key, go to:

  www.websense.com

■ **Network Interface Card (NIC) selection**: All enabled network interface cards (NICs) appear in a list. If the machine has multiple NICs, select the one to use for Network Agent. Be sure that this card has visibility into the internet traffic you want Network Agent to filter.

> ✔ **Note**
>
> After installation, you can run the Traffic Visibility Tool to test whether the selected NIC can see the appropriate user internet traffic. See *Testing Visibility of Internet Traffic to Network Agent*, page 199.

■ **Network Agent Feedback**: The installer asks if you want to allow Websense, Inc., to gather information about the use of Websense-defined protocols. Information will be used in the development of protocol filtering. Select a Network Agent feedback option and continue.

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

■ **Initial filtering options**: Websense software can be configured to filter internet traffic immediately after installation, based on a predefined default policy, or to monitor internet traffic only. Select **Yes** to filter traffic initially, or **No** if you prefer to evaluate your network traffic before applying any type of filtering. You can install one or more of the Websense Reporting Tools to report on network activity.

■ **Transparent user identification**: Select one of the following:

  • **eDirectory Agent**: Select this option to install eDirectory Agent to authenticate users transparently with Novell eDirectory Service.

  • **Logon Agent**: Select this option to install Logon Agent to authenticate users transparently when they log on to the domain. Logon Agent receives its user information from an application

called `LogonApp.exe` that must be run by a logon script in your network. For instructions, see *Creating and Running the Script for Logon Agent*, page 189.

- **None**: This option does not install a Websense transparent identification agent. Select this option if you plan to configure authentication of users through Squid Web Proxy Cache.

✔ **Note**

You can configure manual authentication in Websense Manager after installation. For instructions, see the *Administrator's Guide* for Websense Enterprise and Web Security Suite.

- **RADIUS Agent**: If you have remote users who are authenticated by a RADIUS server, you can choose to install RADIUS Agent to transparently identify them.

- **Directory Access for DC Agent**: If you selected DC Agent for installation, you must provide a user name and a password with administrative privileges on the domain. DC Agent needs access to directory information to be able to identify users transparently.

✔ **Note**

If you cannot install DC Agent with the appropriate privileges on the domain, you can configure them after installation. For instructions, see *Configure Domain Administrator Privileges*, page 202.

- **Samba Client**: The installer warns that you must install the Samba client (v2.2.8a and later) to display protocol block messages and onscreen alerts on Windows workstations. You may continue Websense installation and download the Samba client later.

✔ **Note**

The Samba client controls the display of protocol block messages and onscreen alerts only:

- ◆ The Samba client must be installed on Linux and Solaris User Service machines in order to display protocol block messages on Windows workstations. However, it is *not* required for protocol blocking to occur.

- ◆ The Samba client must be installed on Linux and Solaris Policy Server machines in order to display onscreen alerts on Windows workstations.

To download the Samba client:
- • *Solaris*: Go to the Sun freeware website at: www.sunfreeware.com
- • *Linux*: Go to: http://rpmfind.net/linux/RPM

- **Web browser**: You must provide the full path to the web browser you want to use when viewing online Help. This information is requested for installing Websense Manager.

- **Installation directory**: Enter the path to the directory where you want to install the Websense components, or accept the default location (`/opt/Websense`). If this directory does not already exist, the installer will create it.

💧 **Important**

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

- **System requirements check**: The installer compares the system requirements for the installation you have selected with the resources of the installation machine. If the machine has inadequate disk space or memory, separate warnings are displayed.

- • If the installation machine has insufficient disk space, the selected components cannot be installed, and the installer will quit.
- • If the installation machine has less than the recommended amount of memory, the installation can continue. To ensure the best performance of the components you are installing, you should upgrade your machine's memory to the recommended amount.

  If a disk space or memory error is displayed, check the *Deployment Guide* for system recommendations.

- ■ **Installation summary**: A summary list appears, showing the installation path, the installation size, and the components that will be installed.

10. Select **Next** to begin the installation.

    If you are using the online installer, the Download Manager copies the appropriate installer files from the Websense website. Installation begins automatically when the necessary files have been downloaded.

    The installer creates the /opt/Websense directory, and the /opt/Websense/Manager directory if you installed Websense Manager. It also sets up the necessary files, including /etc/rc3.d/S11WebsenseAdmin, which enables Filtering Service to start automatically each time the system starts.

    - ■ **Restart Squid**: If you have installed Websense Enterprise or Web Security Suite on the Squid machine, the installer prompts you restart Squid.

    - ■ **Master Database Download**: If you provided a valid subscription key when prompted, you are asked if you want to download the Websense Master Database now or at a later time using Websense Manager. Select a database download option and select **Next** to continue.

    ✔ **Note**

    The Master Database can take a few minutes or more than 60 minutes to download, decompress, and load into local memory.

    If you selected to download the Master Database now, the download begins. The database must first be downloaded from the internet, and then decompressed and loaded into local memory. Downloading the database from the internet can take a few minutes or more than

30 minutes, depending on factors such as internet connectivity, bandwidth, time of day, and your location relative to the download server. Decompressing and loading the database can take a few minutes or more than 30 minutes, depending on factors such as available memory, free disk space, and server process utilization.

When the database has finished loading, a message appears advising you of the status of the download. Select **Next** to continue.

11. When a message announcing successful completion of the installation is displayed:

    ■ If you chose a non-English language installer, select **Next** to continue. The Websense Language Pack installer starts. Follow the onscreen instructions to update Websense components with text in the selected language.

    ■ If you chose an English language installer:

       • If you are installing in command line mode, select **Finish** to exit the installer.

       • If you are installing in GUI mode, select **Next** to continue. The installer asks if you want to start Websense Manager. Make a choice and select **Finish** to exit the installer.

         See the *Administrator's Guide* for instructions on using Websense Manager.

12. If you stopped your antivirus software, be sure to start it again.

13. If you did not install the Filtering Service on the Squid Web Proxy Cache machine, you must install the Squid Plug-in on the Squid Web Proxy Cache machine. This installation allows Filtering Service to communicate with Squid. See *Installing the Squid Plug-in on the Squid Web Proxy Machine*, page 87 for instructions.

14. See *Chapter 5: Initial Setup* to perform post-installation tasks.

15. See *Chapter 6: Authentication* to configure authentication of users.

> ✔ **Note**
>
> If you decide to change the location of a Websense component, add functionality, or repair a component, run the Websense installer again on the machine you want to modify and select the appropriate option. The installer detects the presence of Websense components and offers you options for modifying your installation. For instructions, see *Modifying an Installation*, page 154.

Installing the Squid Plug-in on the Squid Web Proxy Machine

If you installed the Websense Filtering Service on a machine separate from the Squid Web Proxy Cache, you must install the Squid Plug-in on the Squid Web Proxy Cache machine so that the Websense Filtering Service and Squid can communicate. You must install the Squid Plug-in *after* installing the Websense Filtering Service.

The Squid Plug-in is supported on Solaris and Linux.

To install the Squid Plug-in on the Squid Web Proxy Cache machine:

1. Log on to the machine as the **root** user.
2. Stop the Squid Web Proxy Cache.
3. Close all applications and stop any antivirus software.
4. Create a setup directory for the installer files.

   For example: `/root/Websense_setup`
5. Obtain an installer package for either Websense Enterprise or Web Security Suite:

   - **Web download**: To download an installer package, go to www.websense.com, and then navigate to the Downloads page.

    a. Choose your product, the dynamic (online) or full (offline) installer package, the operating system, and the language.

> ✔ **Note**
>
> The **Dynamic** installer is an **online** installer package that requires web access during installation. It downloads the necessary product files from the website as needed after product selections have been made.
>
> The **Full** installer is a complete **offline** installer. It is much larger than the online Dynamic installer package, and contains all the files needed to install the Websense Enterprise or Web Security Suite components. Use this package if you experience difficulties with the online installer.

    b. Save the selected installer package to the setup directory on the installation machine.

6. In the setup directory, enter the following command to unzip the file:

   `gunzip <download file name>`

   For example: `gunzip Websense632Setup_Slr.tar.gz`

7. Expand the file into its components with the following command:

   `tar xvf <unzipped file name>`

   For example: `tar xvf Websense632Setup_Slr.tar`

This places the following files into the setup directory:

File	Description
install.sh	Installation program
Setup	Archive file containing related installation files and documents.
Documentation	Release Notes: An HTML file containing release notes and last minute information about the Websense software. Read this file with any supported browser.

8. Run the installation program from the setup directory with the following command:

   ```
   ./install.sh
   ```

   To run the GUI version of the installer, use the following command:

   ```
   ./install.sh -g
   ```

   If you are using a non-English based system, the installer will display an error message advising you that the GUI version is not supported.

9. Follow the onscreen instructions through the subscription agreement.

10. Provide the installer with the following information.

   - **Product selection** (*Web Security Suite only*): Select the product that you plan to use:

     • **Web Security Suite or Web Security Suite**: Provides web security and reporting features.

     • **Web Security Suite and Client Policy Manager**: Provides web security and reporting features, plus desktop security.

     The installer displays information about the required installation sequence for the components of this product on your operating system.

   - **Installation type**: Choose **Custom**.

   - **Component selection**: Select **Filtering Plug-in** from the list of components to install.

■ **Policy Server**: Provide the IP address and port number of the Policy Server machine.

> **Note**
>
> The displayed configuration port (55806) is the default port number used by the installer to install the Policy Server. If you installed the Policy Server using a different port number, enter that port number.

■ **Filtering Service**: Enter the IP address of the Filtering Service machine, and the port number if it is different from the default.

■ **Installation directory**: Enter the path to the directory where you want to install the Squid Plug-in, or accept the default location (`/opt/Websense`). If this directory does not already exist, the installer will create it.

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

■ **System requirements check**: The installer compares the system requirements for the installation you have selected with the resources of the installation machine. If the machine has inadequate disk space or memory, separate warnings are displayed.

  • If the installation machine has insufficient disk space, the selected components cannot be installed, and the installer will quit.

  • If the installation machine has less than the recommended amount of memory, the installation can continue. To ensure the best performance of the components you are installing, you should upgrade your machine's memory to the recommended amount.

■ **Installation summary**: A summary list appears, showing the installation path, the installation size, and the components that will be installed.

11. Select **Next** to begin the installation.

If you are using the online installer, the Download Manager copies the appropriate installer files from the Websense website. Installation begins automatically when the necessary files have been downloaded. The installer creates the specified installation directory and installs the Squid Plug-in in that location.

If Network Agent was not installed, a message reminds you that features such as Protocol Management and Bandwidth Optimizer cannot be used unless Network Agent is installed on a machine with direct access to internet traffic. Select **Next** to continue.

12. When a message announcing successful completion of the installation is displayed:

   ■ If you chose a non-English language installer, select **Next** to continue. The Websense Language Pack installer starts. Follow the onscreen instructions to update Websense components with text in the selected language.

   ■ If you chose an English language installer, select **Finish** to exit the installer.

13. If you stopped your antivirus software, be sure to start it again.

14. Restart the Squid Web Proxy Cache.

Installing Websense Components Separately

All Websense Enterprise and Web Security Suite components can be installed separately using the **Custom** installation path in the Websense installer. Use a Custom installation if your environment requires you to distribute Websense components on different machines in your network. The Remote Filtering components can be installed only through a Custom installation.

This section describes the procedures for installing the following Websense components separately. It is assumed that Policy Server and Filtering Service are on a different machine.

> **Important**
>
> When installing Websense components separately, Policy Server must be installed first. Only Websense Manager can be installed before Policy Server.

◆ **Websense Manager**: Websense Manager installs on Windows, Solaris, and Linux. It can connect to a Policy Server on the same operating system or on a different operating system.

◆ **Network Agent**: Network Agent can be installed on Windows, Solaris, and Linux machines and must be able to see all internet traffic, both inbound and outbound.

◆ **DC Agent**: DC Agent runs on Windows and is installed in networks that use a Windows directory service (NTLM-based or Active Directory). To retrieve user information from the domain controller, DC Agent must be installed with domain administrator privileges on the network.

◆ **Real-Time Analyzer (RTA)**: RTA installs on Windows only. You can have only one instance of RTA for each Policy Server in your network.

◆ **RADIUS Agent**: RADIUS Agent installs on Windows, Solaris, and Linux. RADIUS Agent can be used in conjunction with either Windows- or LDAP-based directory services; it works together with a RADIUS client and RADIUS server to transparently identify users logging on from remote locations.

◆ **eDirectory Agent**: eDirectory Agent installs on Windows, Solaris, and Linux, and is installed in networks that use Novell eDirectory to identify users.

◆ **Logon Agent**: Logon Agent installs on Windows, Solaris, and Linux. Logon Agent receives user information at logon from a client application called `LogonApp.exe`, which must be run by a logon script. Instructions for creating and running this logon script in your network can be found in *Creating and Running the Script for Logon Agent*, page 189. `LogonApp.exe` runs only on Windows client machines.

✔ **Note**

The installation of these Websense components in the presence of other Websense components requires fewer steps. The installer searches for existing Websense initialization files and automatically uses this configuration information to locate the Policy Server and Filtering Service in the network.

◆ **Remote Filtering components**: The Remote Filtering components— Remote Filtering Server and Remote Filtering Client Pack—are required only if you need to enable web filtering on user workstations located

outside your organization's network firewall. These optional components are only available through a **Custom** installation.

> ✓ **Note**
> To enable the Remote Filtering components, you must subscribe to the remote filtering service.

- **Remote Filtering Server**: The Remote Filtering Server installs on Windows, Solaris, and Linux. It must be able to communicate with the Websense Filtering Service and with the Remote Filtering Clients installed on user workstations.
- **Remote Filtering Client Pack**: The Remote Filtering Client Pack is an installer used to deploy the **Remote Filtering Client** to Windows workstations that will be used outside the network firewall. The Remote Filtering Client Pack installs on Windows only.

Be sure to read the *Deployment Guide* for Websense Enterprise and Web Security Suite before beginning installation to determine the best way to distribute Websense Enterprise and Web Security Suite components in your network.

Windows Procedures

The steps in this section are common to all separate installations of Websense Enterprise and Web Security Suite components on Windows. Start here to download and run the Websense installer, and then refer to the appropriate sections for the component-specific procedures.

To install components separately on Windows:

1. Log on to the installation machine with **local** administrator privileges.

> **Important**
>
> If you are installing User Service or DC Agent, log on with **domain** as well as **local** administrator privileges. User Service and DC Agent must have administrator privileges on the network to retrieve user login information from the domain controller. Without this information, Websense software cannot filter by users and groups. If you cannot install these components with such privileges, you can configure administrator privileges for these services after installation. For instructions, see *Configure Domain Administrator Privileges*, page 202.

2. Close all applications and stop any antivirus software.

3. Obtain an installer package for either Websense Enterprise or Web Security Suite:

   - **Web download**: To download an installer package, go to www.websense.com, and then navigate to the Downloads page.

     a. Choose your product, the dynamic (online) or full (offline) installer package, the operating system, and the language.
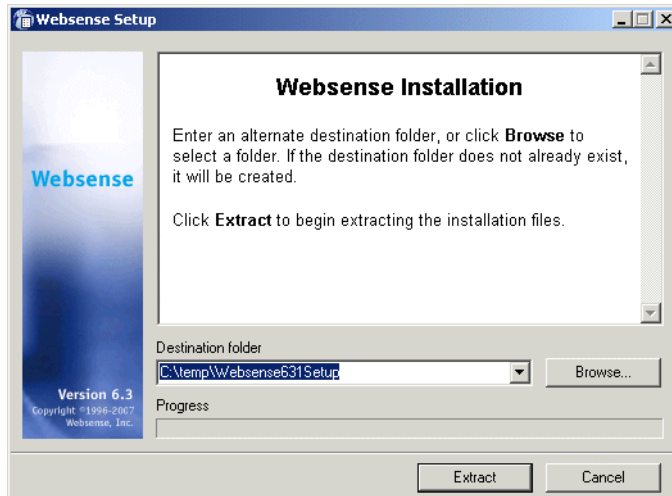
   > **Note**
   >
   > The **Dynamic** installer is an **online** installer package that requires web access during installation. It downloads the necessary product files from the website as needed after product selections have been made.
   >
   > The **Full** installer is a complete **offline** installer. It is much larger than the online Dynamic installer package, and contains all the files needed to install the Websense Enterprise or Web Security Suite components. Use this package if you experience difficulties with the online installer.

b. Download the selected installer package to a folder on the installation machine, and double-click to extract the installer files.

A screen displays instructions for extracting the setup program.

Websense Enterprise Installer File Extraction

If you are installing Web Security Suite, the default destination folder will be `WebSecuritySuite632Setup`.

4. If you do not want to accept the default location, click **Browse** to select a destination folder, or type in a path.

If the path you enter does not exist, the installer will create it for you.

> **Important**
>
> Do not extract the installer files to a folder on your desktop. This may prevent the Real-Time Analyzer from receiving the IP address of the Policy Server machine. Accept the default location of `C:\temp` or select another appropriate folder.

5. Click **Extract** to begin decompressing the files.

   - If Websense installation files already exist in that location, you may choose to overwrite the existing files.

   - A progress bar shows the status of the extraction, and the view pane scrolls a list of the files as they are decompressed.

   - `Setup.exe` runs automatically after the files are decompressed.

6. Click **Next** in the welcome screen and follow the onscreen instructions through the subscription agreement.

7. In the Product Selection screen, select the product to install and click **Next**:

   - *Websense Enterprise installer*: Select **Websense Enterprise**.
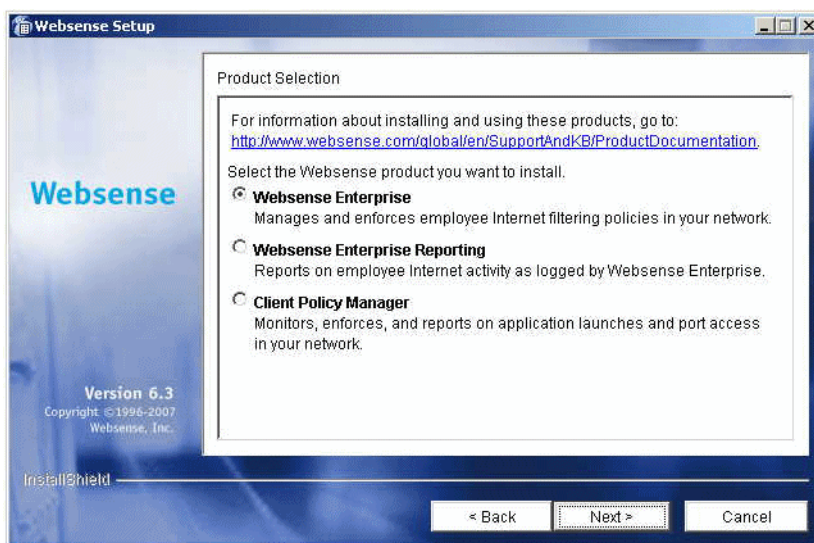
Websense Enterprise Product Selection

■ *Websense Web Security Suite installer*: Select the Web Security Suite edition you plan to use:

- • **Web Security Suite**: Provides web security and reporting features.
- • **Web Security Suite and Client Policy Manager**: Provides web security and reporting features, plus desktop security.
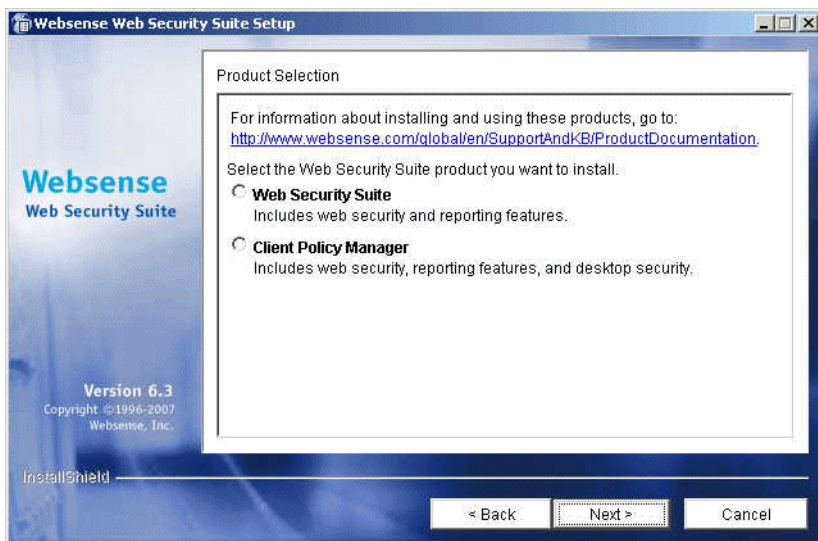
Web Security Suite Product Selection

8. (*Web Security Suite only.*) An information screen appears, listing the order in which the modules of the Web Security Suite must be installed. Click **Next** to continue.

9. (*Web Security Suite only.*) The Component Selection screen appears, displaying the modules for the edition of Web Security Suite that you selected, in the order they must be installed. Select **Web Security Suite components** and click **Next** to continue.

   You are offered a choice of two setup types.

10. Select **Custom** and click **Next**.

11. To continue, proceed to the appropriate component section below.

Websense Manager

Websense Manager, the administrative interface for your Websense software, can be installed in multiple locations in your network for convenient access.

The Websense Manager machine needs network access to the Policy Server machine.

To install Websense Manager on a Windows machine:

1. Download and start the Windows installer using the procedure in *Windows Procedures*, page 93.

2. Following the **Custom** installation path brings you to the component selection screen. Select **Websense Manager** and click **Next**.

   A dialog box appears, asking you to select an installation directory for Websense Manager.

3. Accept the default path (C:\Program Files\Websense) or click **Browse** to locate another installation folder, and then click **Next** to continue.

   The installer compares the system requirements for the installation you have selected with the resources of the installation machine. If the machine has inadequate disk space or memory, separate warnings are displayed:

   - If the installation machine has insufficient disk space, the selected components cannot be installed, and the installer will quit.

   - If the installation machine has less than the recommended amount of memory, the installation can continue. To ensure the best performance of the components you are installing, you should upgrade your machine's memory to the recommended amount.

   A summary list appears, showing the installation path, the installation size, and the components that will be installed.

4. Click **Next** to start the installation.

   If you are using the online installer, the Download Manager progress bars are displayed as the appropriate installer files are downloaded from the Websense website. Installation begins automatically when the necessary files have been downloaded.

   If Network Agent was not installed, a message reminds you that features such as Protocol Management and Bandwidth Optimizer cannot be used unless Network Agent is installed on a machine with direct access to internet traffic. Click **Next** to continue.

   A message announcing the successful completion of the installation is displayed.

5. Click **Next** to continue.

- If you chose a non-English language installer, the Websense Language Pack installer starts. Click **Next** in the welcome screen and follow the onscreen instructions.

- If you chose an English language installer, a screen appears asking if you want to launch Websense Manager. If you do not want to launch Manager, clear the checkbox. Click **Finish** to exit the installer.

6. If you stopped your antivirus software, remember to start it again after Websense components have been installed.

Network Agent

Network Agent must be able to monitor 2-way internet traffic from the internal network. Install Network Agent on a machine that can see the internet requests *from* the internal network as well as the internet response *to* the requesting workstations.

> **Important**
>
> If you install Network Agent on a machine that cannot monitor the targeted traffic, Network Agent features such as Protocol Management, Bandwidth Optimizer, and IM Attachment Manager will not perform as expected.

If this installation is part of a multiple deployment of the Network Agent (for load balancing purposes), you must be sure that the IP address ranges for each instance of the Network Agent do not overlap. Overlapping ranges result in double logging. Deploy the Network Agents so that they can filter the entire network.

Partial deployment results in incomplete filtering by protocol and bandwidth, as well as the loss of log data from network segments not watched by Network Agent.

To define IP address ranges for multiple Network Agents, follow the instructions in the *Administrator's Guide* for Websense Enterprise and Web Security Suite. For detailed information about deploying Network Agent, see the *Deployment Guide* for Websense Enterprise and Web Security Suite.

Do not install Network Agent on a machine running any type of firewall. Network Agent uses a packet capturing utility which may not work properly when installed on a firewall machine.

If you are attempting to install Network Agent on a machine on which the Filtering Service and Policy Server are already installed, see the procedures in *Adding Components*, page 154.

> **Important**
>
> The Websense Filtering Service and the Policy Server must be installed and running prior to installing Network Agent, or installed at the same time as Network Agent. The installer asks for the IP addresses and port numbers of these components and will not install Network Agent if the Policy Server and Filtering Service cannot be located.

To install Network Agent on a Windows machine:

1. Download and start the Windows installer using the procedure in *Windows Procedures*, page 93.

2. Following the **Custom** installation path brings you to the component selection screen. Select **Network Agent** and click **Next**.

   The installer asks you to identify the machine on which the Policy Server is installed.

> **Note**
>
> The configuration port (55806) in this dialog box is the default port number used by the installer to install the Policy Server. If you installed the Policy Server using a different port number, enter that port number in this dialog box.

3. Enter the IP address of the Policy Server machine, and the port number if different from the default, and then click **Next**.

   The installer asks you if this machine is running a firewall. Make sure that the installation machine is not being used as a firewall before continuing.

> **Important**
>
> Network Agent cannot function properly on a machine running a firewall.
>
> The only exception is a blade server or appliance that has separate processors or virtual processors to accommodate Network Agent and the firewall software.

4. Select **Yes** or **No** and click **Next** to continue:

   - Select **Yes** if the installation machine is *not* being used as a firewall. Installation will continue.

   - Select **No** if you are attempting to install Network Agent on a firewall machine, and Setup will exit. Install Network Agent on a machine that is not running a firewall.

   A screen appears asking you to select the network interface card (NIC) that you want Network Agent to use for capturing traffic. All network interface cards enabled in the machine appear in a list.

5. If the machine has multiple NICs, select the one that has visibility into the internet traffic you want Network Agent to filter.

   > **Note**
   >
   > After installation, you can run the Traffic Visibility Tool to test whether the selected NIC can see the appropriate user internet traffic. See *Testing Visibility of Internet Traffic to Network Agent*, page 199.

6. Click **Next** to continue.

   The installer asks you to identify the machine on which the Websense Filtering Service is installed.

   > **Note**
   >
   > The communication port (15868) in this dialog box is the default port number used by the installer to install Filtering Service. If you installed Filtering Service using a different port number, enter that port number in this dialog box.

7. Enter the IP address of the Filtering Service machine, and the port number if different from the default, and then click **Next**.

   A screen appears asking if you want to allow Websense, Inc., to gather information about the use of Websense-defined protocols. Information will be used in the development of 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.

8. Select a Network Agent feedback option and click **Next** to continue.

   The installer asks you to select an installation folder for the Websense components.

9. Accept the default path (C:\Program Files\Websense) or click **Browse** to locate another installation folder, and then click **Next** to continue.

   The installer compares the system requirements for the installation you have selected with the resources of the installation machine. If the machine has inadequate disk space or memory, separate warnings are displayed:

   - If the installation machine has insufficient disk space, the selected components cannot be installed, and the installer will quit.

   - If the installation machine has less than the recommended amount of memory, the installation can continue. To ensure the best performance of the components you are installing, you should upgrade your machine's memory to the recommended amount.

   A summary list appears, showing the installation path, the installation size, and the components that will be installed.

10. Click **Next** to start the installation.

    If you are using the online installer, the Download Manager progress bars are displayed as the appropriate installer files are downloaded from the Websense website. Installation begins automatically when the necessary files have been downloaded.

11. When a message announcing successful completion of the installation is displayed:

- If you chose a non-English language installer, click **Next** to continue.

    The Websense Language Pack installer starts. Click **Next** in the welcome screen and follow the onscreen instructions.

- If you chose an English language installer, click **Finish** to exit the installer.

12. If you stopped your antivirus software, remember to start it again after Websense components have been installed.

13. Configure Network Agent for use in your network. See the instructions for initial configuration of Network Agent in *Chapter 5: Initial Setup*, as well as the Network Agent chapter in the *Administrator's Guide* for Websense Enterprise and Web Security Suite.

DC Agent

DC Agent is a Websense transparent identification agent used in networks that authenticate users with a Windows directory service (NTLM-based or Active Directory). You can choose to install DC Agent during a Typical Websense installation on Windows or Linux. If you did not install it, and you need to authenticate through a Windows-based directory service, you can install DC Agent on a Windows machine with the following procedure.

If your network is large, you may benefit from installing DC Agent on multiple machines. This way, you will have ample space for DC Agent files that are continually populated with user information. For additional information about how to deploy DC Agent, see *Websense Enterprise and Web Security Suite Components*, page 15.

Do not install DC Agent on the same machine as eDirectory Agent, as this can cause conflicts.

To install DC Agent on a Windows machine:

1. Download and start the Windows installer using the procedure in *Windows Procedures*, page 93.

2. Following the **Custom** installation path brings you to the component selection screen. Select **DC Agent** and click **Next**.

    If the installation machine is multihomed, all enabled network interface cards appear in a list.

3. Select the IP address of the card you want DC Agent to use to communicate and click **Next**.

The installer asks you to identify the machine on which the Policy Server is installed.

> ✔ **Note**
>
> The configuration port (55806) in this dialog box is the default port number used by the installer to install the Policy Server. If you installed the Policy Server using a different port number, enter that port number in this dialog box.

4. Enter the IP address of the Policy Server machine, and the port number if different from the default, and then click **Next**.

   The installer asks you to provide a user name and a password with administrative privileges on the domain. DC Agent needs access to directory information to be able to identify users transparently.

5. Enter the domain and user name, followed by the network password for an account with domain administrator privileges, and then click **Next**.

> ✔ **Note**
>
> You can also grant domain administrator privileges to DC Agent after installation. For instructions, see *Configure Domain Administrator Privileges*, page 202.

   The installer asks you to select an installation folder for the Websense components.

6. Accept the default path (C:\Program Files\Websense) or click **Browse** to locate another installation folder, and then click **Next** to continue.

   The installer compares the system requirements for the installation you have selected with the resources of the installation machine. If the machine has inadequate disk space or memory, separate warnings are displayed:

   ■ If the installation machine has insufficient disk space, the selected components cannot be installed, and the installer will quit.

- If the installation machine has less than the recommended amount of memory, the installation can continue. To ensure the best performance of the components you are installing, you should upgrade your machine's memory to the recommended amount.

A summary list appears, showing the installation path, the installation size, and the components that will be installed.

7. Click **Next** to start the installation.

   If you are using the online installer, the Download Manager progress bars are displayed as the appropriate installer files are downloaded from the Websense website. Installation begins automatically when the necessary files have been downloaded.

   If Network Agent was not installed, a message reminds you that features such as Protocol Management and Bandwidth Optimizer cannot be used unless Network Agent is installed on a machine with direct access to internet traffic. Click **Next** to continue.

8. When a message announcing successful completion of the installation is displayed:

   - If you chose a non-English language installer, click **Next** to continue.

     The Websense Language Pack installer starts. Click **Next** in the welcome screen and follow the onscreen instructions.

   - If you chose an English language installer, click **Finish** to exit the installer.

9. If you stopped your antivirus software, remember to start it again after Websense components have been installed.

10. Configure User Service to communicate with DC Agent by following the instructions in the User Identification chapter of the *Administrator's Guide* for Websense Enterprise and Web Security Suite.

Real-Time Analyzer (RTA)

RTA graphically displays bandwidth usage information and shows requests by category or protocol. RTA installs on Windows only. You can have only one instance of RTA for each Policy Server in your network.

To install RTA on a Windows machine:

1. Download and start the Windows installer using the procedure in *Windows Procedures*, page 93.

2. Following the **Custom** installation path brings you to the component selection screen. Select **Real-Time Analyzer** and click **Next**.

   If the installation machine is multihomed, all enabled network interface cards appear in a list.

3. Select the IP address of the card you want RTA to use to communicate and click **Next**.

   The installer asks you to identify the machine on which the Policy Server is installed.

   > ✓ **Note**
   >
   > The configuration port (55806) in this dialog box is the default port number used by the installer to install the Policy Server. If you installed the Policy Server using a different port number, enter that port number in this dialog box.

4. Enter the IP address of the Policy Server machine, and the port number if different from the default, and then click **Next**.

   The installer checks your system for a supported web server (Apache HTTP Server or IIS) for the Real-Time Analyzer and takes the following action:

   - If both supported web servers are detected, a dialog box appears asking you to choose one server for RTA.

   - If one of the supported servers is detected, the installer continues. No notification appears.

■ If neither supported web server is detected, the installer gives you the option to install the Apache HTTP Server or continue the installation without installing RTA.
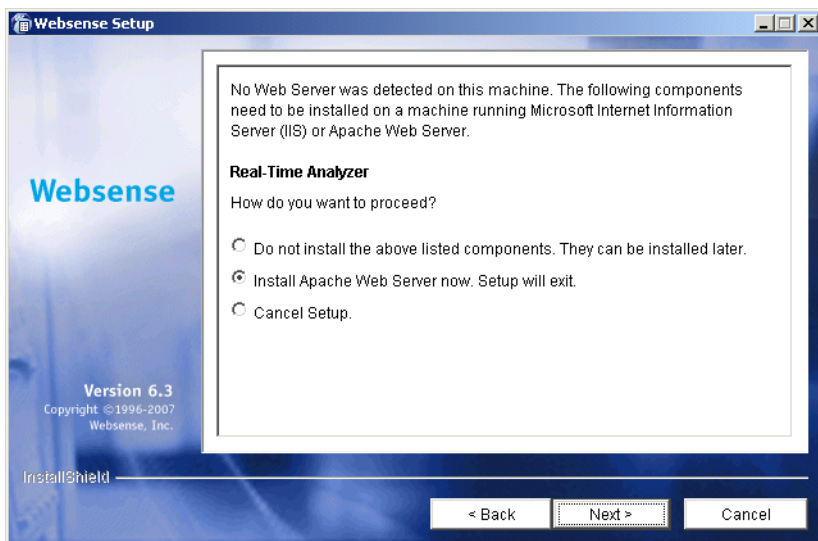
Web Server for Real-Time Analyzer

If you select the Apache HTTP Server installation option, the Websense installer starts the Apache installer and exits without installing any Websense components. You must restart your computer after installing the Apache HTTP Server and run the Websense installer again.

✓ **Note**
Apache HTTP Server documentation is installed in HTML format in the docs/manual/ directory. It is also available at: http://httpd.apache.org/docs/2.0/.

5. Select a web server installation option and click **Next** to continue.

If you are using IIS as your web server, you are prompted to select the name of the website in the IIS Manager under which the installer should create a virtual directory. The default value is **Default Web Site**, which is correct in most instances.
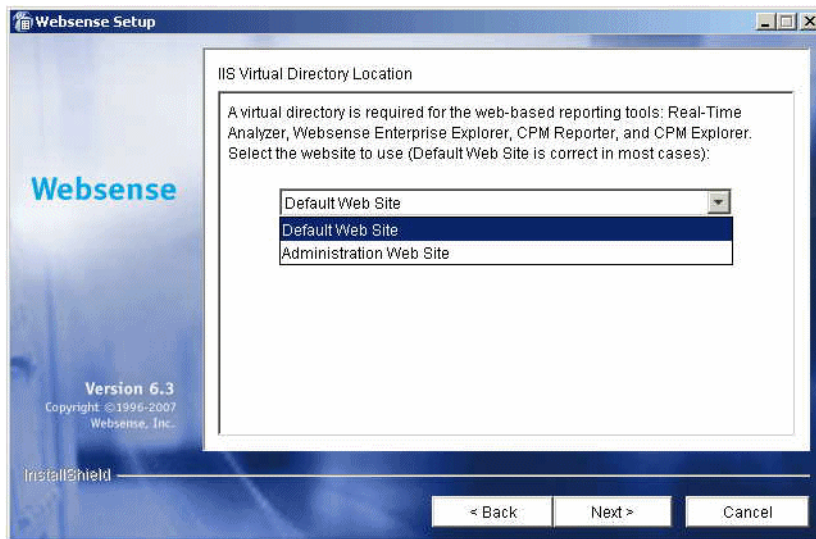
Virtual Directory Selection

6. If you have renamed the default website in the IIS Manager or are using a language version of Windows other than English, select the proper website from the names in the drop-down list, and then click **Next** to continue.

The installer asks you to select an installation folder for the Websense components.

7. Accept the default path (`C:\Program Files\Websense`) or click **Browse** to locate another installation folder, and then click **Next** to continue.

The installer compares the system requirements for the installation you have selected with the resources of the installation machine. If the machine has inadequate disk space or memory, separate warnings are displayed:

■ If the installation machine has insufficient disk space, the selected components cannot be installed, and the installer will quit.

■ If the installation machine has less than the recommended amount of memory, the installation can continue. To ensure the best performance of the components you are installing, you should upgrade your machine's memory to the recommended amount.

A summary list appears, showing the installation path, the installation size, and the components that will be installed.

8. Click **Next** to start the installation.

   If you are using the online installer, the Download Manager progress bars are displayed as the appropriate installer files are downloaded from the Websense website. Installation begins automatically when the necessary files have been downloaded.

   If Network Agent was not installed, a message reminds you that features such as Protocol Management and Bandwidth Optimizer cannot be used unless Network Agent is installed on a machine with direct access to internet traffic. Click **Next** to continue.

9. When a message announcing successful completion of the installation is displayed:

   ■ If you chose a non-English language installer, click **Next** to continue.

      The Websense Language Pack installer starts. Click **Next** in the welcome screen and follow the onscreen instructions.

   ■ If you chose an English language installer, click **Finish** to exit the installer.

   ✔ **Note**

   Before you can access Real-Time Analyzer and other Websense Reporting Tools, you must first log on to Websense Manager and configure user permissions. For more information, see the *Administrator's Guide* for Websense Enterprise and Web Security Suite.

10. If you stopped your antivirus software, remember to start it again after Websense components have been installed.

RADIUS Agent

The Websense RADIUS Agent allows you to integrate your Websense filtering policies with authentication provided by a RADIUS server. RADIUS Agent enables Websense software to transparently identify users who access your network using a dial-up, Virtual Private Network (VPN), Digital Subscriber Line (DSL), or other remote connection.

To install the RADIUS Agent on a Windows machine:

1. Download and start the Windows installer using the procedure in *Windows Procedures*, page 93.

2. Following the **Custom** installation path brings you to the component selection screen. Select **RADIUS Agent** and click **Next**.

   The installer asks you to identify the machine on which the Policy Server is installed.

   > ✔ **Note**
   >
   > The configuration port (55806) in this dialog box is the default port number used by the installer to install the Policy Server. If you installed the Policy Server using a different port number, enter that port number in this dialog box.

3. Enter the IP address of the Policy Server machine, and the port number if different from the default, and then click **Next**.

   If the installation machine is multihomed, all enabled network interface cards (NICs) with an IP address appear in a list.

4. Select the IP address of the card you want RADIUS Agent to use to communicate and click **Next**.

   The installer asks you to select an installation folder for the Websense components.

5. Accept the default path (C:\Program Files\Websense) or click **Browse** to locate another installation folder, and then click **Next** to continue.

   The installer compares the system requirements for the installation you have selected with the resources of the installation machine. If the machine has inadequate disk space or memory, separate warnings are displayed:

   - If the installation machine has insufficient disk space, the selected components cannot be installed, and the installer will quit.

   - If the installation machine has less than the recommended amount of memory, the installation can continue. To ensure the best performance of the components you are installing, you should upgrade your machine's memory to the recommended amount.

A summary list appears, showing the installation path, the installation size, and the components that will be installed.

6. Click **Next** to start the installation.

   If you are using the online installer, the Download Manager progress bars are displayed as the appropriate installer files are downloaded from the Websense website. Installation begins automatically when the necessary files have been downloaded.

   If Network Agent was not installed, a message reminds you that features such as Protocol Management and Bandwidth Optimizer cannot be used unless Network Agent is installed on a machine with direct access to internet traffic. Click **Next** to continue.

7. When a message announcing successful completion of the installation is displayed:

   - If you chose a non-English language installer, click **Next** to continue.

     The Websense Language Pack installer starts. Click **Next** in the welcome screen and follow the onscreen instructions.

   - If you chose an English language installer, click **Finish** to exit the installer.

8. If you stopped your antivirus software, remember to start it again after Websense components have been installed.

9. Configure the RADIUS Agent, and configure your environment for RADIUS Agent. For instructions, see the User Identification chapter in the *Administrator's Guide* for Websense Enterprise and Web Security Suite.

eDirectory Agent

The Websense eDirectory Agent works together with Novell eDirectory to identify users transparently so that Websense software can filter them according to particular policies assigned to users or groups.

Do not install eDirectory Agent on the same machine as DC Agent or Logon Agent, as this can cause conflicts.

To install the eDirectory Agent on a Windows machine:

1. Download and start the Windows installer using the procedure in *Windows Procedures*, page 93.

2. Following the **Custom** installation path brings you to the component selection screen. Select **eDirectory Agent** and click **Next**.

   The installer asks you to identify the machine on which the Policy Server is installed.

   ✓ **Note**

   The configuration port (55806) in this dialog box is the default port number used by the installer to install the Policy Server. If you installed the Policy Server using a different port number, enter that port number in this dialog box.

3. Enter the IP address of the Policy Server machine, and the port number if different from the default, and then click **Next**.

   If the installation machine is multihomed, all enabled network interface cards (NICs) with an IP address appear in a list.

4. Select the IP address of the card you want eDirectory Agent to use to communicate and click **Next**.

   The installer asks for the Novell eDirectory name and password.

5. Enter the full *distinguished name* and a valid password, and then click **Next** to continue.

   The installer asks you to select an installation folder for the Websense components.

6. Accept the default path (`C:\Program Files\Websense`) or click **Browse** to locate another installation folder, and then click **Next** to continue.

   The installer compares the system requirements for the installation you have selected with the resources of the installation machine. If the machine has inadequate disk space or memory, separate warnings are displayed:

   ▪ If the installation machine has insufficient disk space, the selected components cannot be installed, and the installer will quit.

   ▪ If the installation machine has less than the recommended amount of memory, the installation can continue. To ensure the best performance of the components you are installing, you should upgrade your machine's memory to the recommended amount.

A summary list appears, showing the installation path, the installation size, and the components that will be installed.

7. Click **Next** to start the installation.

   If you are using the online installer, the Download Manager progress bars are displayed as the appropriate installer files are downloaded from the Websense website. Installation begins automatically when the necessary files have been downloaded.

   If Network Agent was not installed, a message reminds you that features such as Protocol Management and Bandwidth Optimizer cannot be used unless Network Agent is installed on a machine with direct access to internet traffic. Click **Next** to continue.

8. When a message announcing successful completion of the installation is displayed:

   - If you chose a non-English language installer, click **Next** to continue.

     The Websense Language Pack installer starts. Click **Next** in the welcome screen and follow the onscreen instructions.

   - If you chose an English language installer, click **Finish** to exit the installer.

9. If you stopped your antivirus software, remember to start it again after Websense components have been installed.

10. Configure the eDirectory Agent and Novell eDirectory by following the instructions in the User Identification chapter of the *Administrator's Guide* for Websense Enterprise and Web Security Suite.

Logon Agent

Logon Agent is a Websense transparent identification agent that detects users as they log on to Windows domains in your network via client machines. The Logon Agent receives logon information from LogonApp.exe, a separate client application that runs only on Windows client machines, and must be run by a logon script. For information about setting up this script in your network, see *Creating and Running the Script for Logon Agent*, page 189.

Logon Agent can be run together with DC Agent if some of the users in your network are not being authenticated properly. This might happen if your network uses Windows 98 workstations, which do not permit DC Agent to poll users for their identification when they make an internet request.

Do not install Logon Agent on the same machine as eDirectory Agent, as this can cause conflicts.

To install the Logon Agent on a Windows machine:

1. Download and start the Windows installer using the procedure in *Windows Procedures*, page 93.

2. Following the **Custom** installation path brings you to the component selection screen. Select **Logon Agent** and click **Next**.

   The installer asks you to identify the machine on which the Policy Server is installed.

   > ✓ **Note**
   >
   > The configuration port (55806) in this dialog box is the default port number used by the installer to install the Policy Server. If you installed the Policy Server using a different port number, enter that port number in this dialog box.

3. Enter the IP address of the Policy Server machine, and the port number if different from the default, and then click **Next**.

   If the installation machine is multihomed, all enabled network interface cards (NICs) with an IP address appear in a list.

4. Select the IP address of the card you want Logon Agent to use to communicate and click **Next**.

   The installer asks you to select an installation folder for the Websense components.

5. Accept the default path (C:\Program Files\Websense) or click **Browse** to locate another installation folder, and then click **Next** to continue.

   The installer compares the system requirements for the installation you have selected with the resources of the installation machine. If the machine has inadequate disk space or memory, separate warnings are displayed:

   - If the installation machine has insufficient disk space, the selected components cannot be installed, and the installer will quit.

■ If the installation machine has less than the recommended amount of memory, the installation can continue. To ensure the best performance of the components you are installing, you should upgrade your machine's memory to the recommended amount.

A summary list appears, showing the installation path, the installation size, and the components that will be installed.

6. Click **Next** to start the installation.

If you are using the online installer, the Download Manager progress bars are displayed as the appropriate installer files are downloaded from the Websense website. Installation begins automatically when the necessary files have been downloaded.

If Network Agent was not installed, a message reminds you that features such as Protocol Management and Bandwidth Optimizer cannot be used unless Network Agent is installed on a machine with direct access to internet traffic. Click **Next** to continue.

7. When a message announcing successful completion of the installation is displayed:

■ If you chose a non-English language installer, click **Next** to continue.

The Websense Language Pack installer starts. Click **Next** in the welcome screen and follow the onscreen instructions.

■ If you chose an English language installer, click **Finish** to exit the installer.

8. If you stopped your antivirus software, remember to start it again after Websense components have been installed.

9. Set up the required logon script by following the instructions is *Creating and Running the Script for Logon Agent*, page 189.

10. Configure Logon Agent to communicate with client workstations and the Filtering Service by following the instructions in the User Identification chapter of the *Administrator's Guide* for Websense Enterprise and Web Security Suite.

Remote Filtering Server

The Remote Filtering Server provides web filtering for user workstations located outside the network firewall. In order to be filtered through the Remote Filtering Server, a remote workstation must be running the Remote

Filtering Client. (For Remote Filtering Client installation instructions, see *Remote Filtering Client*, page 123.)

✔ Note

To enable the Remote Filtering components, you must subscribe to the remote filtering service.

The Remote Filtering Server should be installed on a separate, dedicated machine. This machine must be able to communicate with the Websense Filtering Service and with the remote workstations outside the network firewall. The Remote Filtering Server machine does not have to be joined to a domain.

The Remote Filtering Server should be installed inside your organization's outermost network firewall, but in the DMZ outside the firewall that protects the rest of the corporate network. For more information about deploying the Remote Filtering Server in your network, see the *Remote Filtering* section in the *Deployment Guide* for Websense Enterprise and Web Security Suite.

To provide failover capability for the primary Remote Filtering Server, you can install secondary and tertiary Remote Filtering Servers. Each Remote Filtering Client can be configured to connect with a primary, secondary, and tertiary Remote Filtering Server. If the primary server is unavailable, the client attempts to connect with the secondary, then the tertiary, then the primary again, and so on.

Important

◆ Install only one primary Remote Filtering Server for each Filtering Service in your network.

◆ Do not install the Remote Filtering Server on the same machine as the Filtering Service or Network Agent.

◆ Remote Filtering Server is supported on Windows Server® 2003 only if Service Pack 1 has been installed.

◆ Do not enable DHCP on the Remote Filtering Server machine.

To install the Remote Filtering Server on a Windows machine:

1. Download and start the Windows installer using the procedure in *Windows Procedures*, page 93.

2. Following the **Custom** installation path brings you to the component selection screen. Select **Remote Filtering Server** and click **Next**.

   If the installation machine is multihomed, all enabled network interface cards appear in a list.

3. Select the IP address of the card you want the Remote Filtering Server to use to communicate with other Websense components inside the network firewall, and click **Next**.

   Remote Filtering Clients must be able to connect to the Remote Filtering Server, both from inside and from outside the internet gateway or network firewall. The installer asks you to provide connection information for this machine.

Remote Filtering Server Communication

4. In the **External IP Address or Host Name** field, enter an IP address or machine name (in the form of a fully qualified domain name) that is visible from *outside* the network firewall.

5. In the **External Communication Port** field, enter a port number (from 10 to 65535) that is not in use, and that is accessible from *outside* the network firewall. The default value is 80. (If there is a web server installed on the machine, port 80 may already in use, so you may need to change the default value.)

> **Important**
>
> The port entered as the **External Communication Port** must be opened on your network firewall to accept connections from Remote Filtering Clients on workstations located outside the firewall. For more information, see *Firewall Configuration for Remote Filtering*, page 206.

6. In the **Internal Communication Port** field, enter a port number (from 1024 to 65535) that is not in use, and that is accessible only from *inside* the network firewall. The default value is 8800.

> **Important**
>
> Be sure that your network firewall is configured to block connections to the **Internal Communication Port** from workstations located outside the firewall. For more information, see *Firewall Configuration for Remote Filtering*, page 206.

7. Click **Next** to continue.

   The installer asks you to enter a pass phrase of any length for the Remote Filtering Server. This pass phrase will be combined with unpublished keys to create an encrypted authentication key (shared secret) for secure client/server communication.

8. Before selecting a **pass phrase**, consider the following requirements:

   ■ If Websense Client Policy Manager (CPM) is already installed in your network, you must enter the same pass phrase used when installing CPM.

   ■ If you install Websense Client Policy Manager (CPM) in your network in the future, you must use the pass phrase you enter in this screen.

- If you want this installation of the Remote Filtering Server to function as a backup (secondary or tertiary) server for a primary Remote Filtering Server, you must enter the same pass phrase used when installing the primary Remote Filtering Server.

- The pass phrase must include only ASCII characters. Do not use extended ASCII or double-byte characters.

- You must use the pass phrase you enter in this screen when you install the Remote Filtering Clients that will connect with this server. (See *Remote Filtering Server Connection Information*, page 126.)

> **Warning**
>
> Be sure to record your **pass phrase** and keep it in a safe place, as it cannot be retrieved it from the Websense system later.

9. Enter and confirm your **pass phrase**.

10. Click **Next** to continue.

Remote Filtering Server must be able to communicate with the Websense Filtering Service. The installer asks you to identify the machine on which Filtering Service is installed.

Filtering Service Information

11. In the first field, enter the actual (internal) IP address of the Filtering Service machine.

12. Is there a firewall or other network device that performs network address translation between the Filtering Service machine and this machine?

    - If yes, enter the translated (external) IP address of the Filtering Service machine.

    - If no, click to deselect the checkbox and grey out the **Translated (external) IP address of Filtering Service** field.

13. Enter the filter port number for the Filtering Service machine, if it was changed from the default of 15868.

    > ✓ **Note**
    >
    > The filter port is the default communication port used by the installer to install Filtering Service. If you installed Filtering Service using a different communication port, enter that port number.

14. Enter the block page port number for the Filtering Service machine, if it was changed from the default value of 15871.

    > **Important**
    >
    > If there is a firewall between the Filtering Service machine and the Remote Filtering Server machine, be sure to open the filter port (15868) and block page port (15871) on that firewall. Filtering Service must be able to accept connections from the Remote Filtering Server, and serve block pages to remote users. For more information, see *Firewall Configuration for Remote Filtering*, page 206.

15. Click **Next**.

    The installer asks you to select an installation folder for the Websense components.

16. Accept the default path (C:\Program Files\Websense) or click **Browse** to locate another installation folder, and then click **Next** to continue.

The installer compares the system requirements for the installation you have selected with the resources of the installation machine. If the machine has inadequate disk space or memory, separate warnings are displayed:

- If the installation machine has insufficient disk space, the selected components cannot be installed, and the installer will quit.

- If the installation machine has less than the recommended amount of memory, the installation can continue. To ensure the best performance of the components you are installing, you should upgrade your machine's memory to the recommended amount.

A summary list appears, showing the installation path, the installation size, and the components that will be installed.

17. Click **Next** to start the installation.

   If you are using the online installer, the Download Manager progress bars are displayed as the appropriate installer files are downloaded from the Websense website. Installation begins automatically when the necessary files have been downloaded.

   Since the Network Agent was not installed on this machine, a message reminds you that features such as Protocol Management and Bandwidth Optimizer cannot be used unless Network Agent is installed on a machine with direct access to internet traffic. Click **Next** to continue.

18. When a message announcing successful completion of the installation is displayed:

   - If you chose a non-English language installer, click **Next** to continue.

     The Websense Language Pack installer starts. Click **Next** in the welcome screen and follow the onscreen instructions.

   - If you chose an English language installer, click **Finish** to exit the installer.

19. If you stopped your antivirus software, remember to start it again after Websense components have been installed.

For more information about how remote filtering works, see the *Filtering Remote Clients* section in the *Administrator's Guide* for Websense Enterprise and Web Security Suite.

Remote Filtering Client Pack

The Remote Filtering Client Pack is an installer package that allows you to install the Remote Filtering Client. Once you have this installer package, you can use it to deploy the Remote Filtering Client on Windows workstations (see *Remote Filtering Client*, page 123). The Remote Filtering Client Pack can be installed on Windows machines only.

> ✔ **Note**
>
> To enable the Remote Filtering components, you must subscribe to the remote filtering service.

To install the Remote Filtering Client Pack on a Windows machine:

1. Download and start the Windows installer using the procedure in *Windows Procedures*, page 93.

2. Following the **Custom** installation path brings you to the component selection screen. Select **Remote Filtering Client Pack** and click **Next**.

   The installer asks you to select an installation folder for the Remote Filtering Client Pack.

3. Accept the default path (C:\Program Files\Websense) or click **Browse** to locate another installation folder, and then click **Next** to continue.

   The installer compares the system requirements for the installation you have selected with the resources of the installation machine. If the machine has inadequate disk space or memory, separate warnings are displayed:

   - If the installation machine has insufficient disk space, the selected components cannot be installed, and the installer will quit.

   - If the installation machine has less than the recommended amount of memory, the installation can continue. To ensure the best performance of the components you are installing, you should upgrade your machine's memory to the recommended amount.

   A summary list appears, showing the installation path, the installation size, and the components that will be installed.

4. Click **Next** to start the installation.

If you are using the online installer, the Download Manager progress bars are displayed as the appropriate installer files are downloaded from the Websense website. Installation begins automatically when the necessary files have been downloaded.

If Network Agent was not installed on this machine, a message reminds you that features such as Protocol Management and Bandwidth Optimizer cannot be used unless Network Agent is installed on a machine with direct access to internet traffic. Click **Next** to continue.

5. When a message announcing successful completion of the installation is displayed:

   ■ If you chose a non-English language installer, click **Next** to continue.

      The Websense Language Pack installer starts. Click **Next** in the welcome screen and follow the onscreen instructions.

   ■ If you chose an English language installer, click **Finish** to exit the installer.

6. If you stopped your antivirus software, remember to start it again after Websense components have been installed.

7. If you accepted the default installation path in Step 3, the Remote Filtering Client Pack can be found in the following location:

   ```
   C:\Program Files\Websense\bin\
   RemoteFilteringAgentPack\NO_MSI\CPMClient.msi
   ```

8. Use the Remote Filtering Client Pack to install the Remote Filtering Client on user workstations that you want to filter when they are outside the network firewall. See *Remote Filtering Client*, page 123 for details.

Remote Filtering Client

The Remote Filtering Client is installed on workstations that will be used outside the network firewall. This component connects with a Remote Filtering Server located inside the network firewall to enable web filtering on the remote workstation. The Remote Filtering Client installs on Windows only.

> **✔ Note**
>
> To enable the Remote Filtering components, you must subscribe to the remote filtering service.

The Remote Filtering Client can be installed in the following ways:

◆ **Manual installation**: Use the Remote Filtering Client Pack to manually install the Remote Filtering Client on an individual workstation. See *Manual Installation of Remote Filtering Client*, page 124 for information.

◆ **Automatic deployment with third-party tool**: Use the Remote Filtering Client Pack and a third-party deployment tool to automatically deploy the Remote Filtering Client to user workstations. See *Installing Remote Filtering Client with a Third-Party Deployment Tool*, page 129 for information.

◆ **Deployment as part of CPM Client Agent** (**Websense Client Policy Manager™ users only**): If you purchased a subscription to the Websense Client Policy Manager™ (CPM), it is not necessary to install the Remote Filtering Client. The Remote Filtering Client application is included as part of the CPM Client Agent, and is deployed automatically when you deploy the CPM Client Agent to user workstations. See your Websense Client Policy Manager documentation for more information.

> **Warning**
>
> Do not install the Remote Filtering Client on:
>
> ◆ Machines running Windows 2000, Service Pack 2 or earlier. The installation will fail. See the *Deployment Guide* for Websense Enterprise and Web Security Suite for information about system requirements.
>
> ◆ Machines where you installed the Remote Filtering Server. A Remote Filtering Client running on the same machine as the Remote Filtering Server will eventually cause remote filtering to fail.

Manual Installation of Remote Filtering Client

To manually install the Remote Filtering Client on a single Windows workstation:

1. Make sure that the Remote Filtering Server with which this client will connect has been correctly installed on a separate machine. See *Remote Filtering Server*, page 115 for Windows installation instructions; see *Remote Filtering Server*, page 149 for Solaris and Linux installation instructions.

2. Install the Remote Filtering Client Pack on the workstation as described in *Remote Filtering Client Pack*, page 122. Or, if you have already installed the Remote Filtering Client Pack on another machine, you can simply copy the `CPMClient.msi` file to a folder on the installation workstation. If you selected the default installation path of `C:\Program Files\Websense`, this file will be located at:

   ```
   C:\Program Files\Websense\bin\
   RemoteFilteringAgentPack\NO_MSI\CPMClient.msi
   ```

3. Double-click the `CPMClient.msi` file.

   The installer for Remote Filtering Client will open.

4. Click **Next** to continue.

Remote Filtering Clients must be able to connect with a Remote Filtering Server from outside your organization's internet gateway or firewall. You are asked to provide connection information for the Remote Filtering Servers that this client will use for web filtering.

Remote Filtering Server Connection Information

The Remote Filtering Client must be configured to connect with a primary Remote Filtering Server.

If optional secondary and tertiary Remote Filtering Servers were installed to provide failover capability for the primary server, the Remote Filtering Client must be configured to connect with these as well. The Remote Filtering Client will attempt to connect with the primary Remote Filtering Server first, then the secondary, then the tertiary, then the primary again, and so on.

5. In the **Primary Remote Filtering Server** section of the screen, enter connection information for the Remote Filtering Server that you want this client to attempt to connect with first:

   ■ Enter the externally visible IP address or fully qualified domain name (FQDN) of the primary Remote Filtering Server machine in the **External IP or Domain Name** field.

   Important

   You must use the same external address in **the same address** *format*—IP address or FQDN—that you entered when you installed this Remote Filtering Server. That is, if you entered an IP address in the **External IP Address or Host Name** field when installing the Remote Filtering Server, you must enter the same IP address in this field. If you entered a machine name in the form of a fully qualified domain name (FQDN), you must enter the same FQDN here.

   ■ In the **Port** field to the right of the **External IP or Domain Name** field, enter the port number for the externally visible port used to communicate with the primary Remote Filtering Server from outside the network firewall. This must be the same port entered in the **External Communication Port** field when this Remote Filtering Server was installed.

   ■ Enter the internal IP address or the fully qualified domain name for the primary Remote Filtering Server machine in the **Internal IP or Hostname** field.

   ■ In the **Port** field to the right of the **Internal IP or Hostname** field, enter the port number for the internal communication port on the primary Remote Filtering Server that can only be accessed from

inside the network firewall. This must be the same port entered in the **Internal Communication Port** field when this Remote Filtering Server was installed.

✓ **Note**

If the Remote Filtering Client is on a notebook computer that is used both inside and outside the network firewall, this port allows the Websense software to determine where the machine is located and filter it appropriately. The machine will be filtered in the same way as an internal client when it is used inside the organization's network firewall, and by the Remote Filtering Service when it is used remotely.

6. If you have installed the optional secondary and tertiary Remote Filtering Servers to provide failover protection for the primary Remote Filtering Server, enter connection information for these servers in the **Secondary Remote Filtering Server** and **Tertiary Remote Filtering Server** sections of the screen.

7. In the **Encryption and Authentication** section, do one of the following:

   ▪ Select **Pass Phrase** and enter the same pass phrase that was entered in the **Pass Phrase** field during installation of the primary Remote Filtering Server. (The secondary and tertiary Remote Filtering Servers must have the same pass phrase as their primary Remote Filtering Server.)

   -OR-

   ▪ Select **Encrypted Key** and enter the encrypted key (shared secret) created from the pass phrase and unpublished Remote Filtering Server keys. The encrypted key can be found in the `WSSEK.dat` file on the Remote Filtering Server machine. If you selected the default installation path, this file will be located at:

   ```
   C:\Program Files\Websense\bin\WSSEK.dat
   ```
   on Windows machines, and
   ```
   /opt/Websense/bin/WSSEK.dat
   ```
   on Solaris and Linux machines.

8. Click **Next** to continue.

9. Click **Install** to begin installation.

When the installer is finished, a message appears advising you that the procedure was successful.

10. Click **Finish** to exit the installer.

11. If a message appears indicating that you must restart the machine, click **Yes** to restart now. Remote filtering will not function properly until the machine is restarted.

If no message appears, restarting the machine is not required.

Installing Remote Filtering Client with a Third-Party Deployment Tool

Before deploying the Remote Filtering Client to user workstations, make sure that the Remote Filtering Server with which these clients will connect has been correctly installed on a separate machine. See *Remote Filtering Server*, page 115 for Windows installation instructions; see *Remote Filtering Server*, page 149 for Solaris and Linux installation instructions.

To obtain the installer for the Remote Filtering Client, install the Remote Filtering Client Pack on a Windows machine (see *Remote Filtering Client Pack*, page 122 for instructions). If you selected the default installation path of C:\Program Files\Websense, the installer is placed in the following location:

```
C:\Program Files\Websense\bin\
RemoteFilteringAgentPack\NO_MSI\CPMClient.msi
```

To deploy the Remote Filtering Client to Windows workstations, use this installer with a third-party deployment tool, such as Microsoft® Systems Management Server (SMS) or Novell® ZENworks®.

Command Line Parameters for Remote Filtering Client Installation

This section provides the command line parameters required to install the Remote Filtering Client using a third-party deployment tool.

Remote Filtering Clients are installed on user workstations or notebook computers that are used outside your organization's internet gateway or firewall. These machines must be able to connect with a Remote Filtering Server that is located inside the internet gateway or firewall.

Each Remote Filtering Client must be configured to connect with a primary Remote Filtering Server. If optional secondary and tertiary Remote Filtering Servers were installed to provide failover capability for the primary server, the Remote Filtering Client must be configured to connect with these as well. The

Remote Filtering Client will attempt to connect with the primary Remote Filtering Server first, then the secondary, then the tertiary, then the primary again, and so on.

Below are the necessary command line parameters for installing the Remote Filtering Client with a third-party deployment tool:

> **Note**
>
> These parameters are *not* case sensitive.

◆ The following parameters must be configured to allow the Remote Filtering Client to communicate with the **primary** Remote Filtering Server:

■ **PRIMARY_WISP_ADDRESS=**<*external IP address or FQDN of primary Remote Filtering Server>*

The externally visible address for the primary Remote Filtering Server machine, as entered in the **External IP Address or Host Name** field when the primary Remote Filtering Server was installed.

> **Important**
>
> This must be the same external address in **the same address** *format*—IP address or FQDN—that was entered when this Remote Filtering Server was installed. That is, if you entered an IP address in the **External IP Address or Host Name** field when installing the Remote Filtering Server, you must enter the same IP address here. If you entered a machine name in the form of a fully qualified domain name (FQDN), you must enter the same FQDN here.

■ **PRIMARY_WISP_PORT=**<*external port number of primary Remote Filtering Server>*

The port number for the externally visible port used to communicate with the primary Remote Filtering Server from outside the network firewall. This must be the same port entered in the **External Communication Port** field when this Remote Filtering Server was installed.

- **`PRIMARY_INTERNAL_WISP_ADDRESS=`**<*internal IP address or FQDN of primary Remote Filtering Server*>

  The internal address, visible from inside the network firewall, for the machine on which the primary Remote Filtering Server is installed.

- **`PRIMARY_INTERNAL_WISP_PORT=`**<*internal port number of primary Remote Filtering Server*>

  The port number for the internal communication port on the primary Remote Filtering Server that can only be accessed from inside the network firewall. This must be the same port entered in the **Internal Communication Port** field when the Remote Filtering Server was installed.

◆ If **secondary** and **tertiary** Remote Filtering Servers have been installed, use the following parameters to configure communication with them:

  - **`SECONDARY_WISP_ADDRESS=`**<*external IP address or FQDN of secondary Remote Filtering Server*>

  - **`SECONDARY_WISP_PORT=`**<*external IP address or FQDN of secondary Remote Filtering Server*>

  - **`SECONDARY_INTERNAL_WISP_ADDRESS=`**<*internal IP address or FQDN of secondary Remote Filtering Server*>

  - **`SECONDARY_INTERNAL_WISP_PORT=`**<*internal IP address or FQDN of secondary Remote Filtering Server*>

  - **`TERTIARY_WISP_ADDRESS=`**<*external IP address or FQDN of tertiary Remote Filtering Server*>

  - **`TERTIARY_WISP_PORT=`**<*external IP address or FQDN of tertiary Remote Filtering Server*>

  - **`TERTIARY_INTERNAL_WISP_ADDRESS=`**<*internal IP address or FQDN of tertiary Remote Filtering Server*>

  - **`TERTIARY_INTERNAL_WISP_PORT=`**<*internal IP address or FQDN of tertiary Remote Filtering Server*>

  These addresses and port numbers must match those entered during installation of the Remote Filtering Servers, as noted above for the primary Remote Filtering Server.

◆ **`PATH=`**<*installation path*>

  Directory where the Remote Filtering Client will be installed on each client workstation. If this parameter is not specified, the default

installation path is `C:\PROGRAM FILES\Websense\WDC`, and the `WDC` directory is hidden by default.

◆ **`PASSPHRASE=`**<*pass phrase for Remote Filtering Server*>

The **Pass Phrase** entered when the primary Remote Filtering Server was installed. Note that all Remote Filtering Servers in the same failover group (primary, secondary, and tertiary) must have the same pass phrase.

◆ **`REBOOT=YES | NO | PROMPT | IF_NEEDED_PROMPT`**

This parameter defines whether the client workstation is automatically restarted after the Remote Filtering Client is installed (or uninstalled). Values for this parameter are:

- **`YES`**: Machines are restarted, and employees are not prompted to restart.

- **`NO`**: Machines are not restarted, and employees are not prompted to restart.

- **`PROMPT`**: Employees are prompted to restart their machines.

- **`IF_NEEDED_PROMPT`**: Employees are prompted to restart their machines only if a restart is required. (Default.)

Important

You must restart the workstation after installing the Remote Filtering Client if:

◆ The workstation's operating system is Windows 2000.

◆ Check Point® VPN-1® is running on the workstation.

You must *always* restart the workstation after uninstalling, upgrading, or repairing the Remote Filtering Client.

◆ **`REINSTALL=ALL`**

This parameter is used only when repairing or upgrading an existing installation of Remote Filtering Client. It indicates the components to remove and reinstall. The value should always be set to `ALL`.

◆ **REINSTALLMODE=veums | voums**

This parameter is used only when repairing or upgrading an existing installation of Remote Filtering Client. It defines either a repair or an upgrade. The possible values are:

- **veums**: for repairs only

- **voums**: for upgrades only

◆ **/qn**

Switch for quiet installation mode. When you use this option, Remote Filtering Client will install without displaying information to the employee at the workstation. If you do not use **/qn**, the installer launches in interactive mode and installation dialog boxes display to the employee during installation. Most organizations choose the quiet mode, as interactive mass deployment has little value.

Installation Syntax

The following is an example of the syntax to install the Remote Filtering Client on employee workstations using a third-party deployment tool. Replace the variables in angle brackets with appropriate values for your network, and type the command on a single line with no returns.

msiexec /i cpmclient.msi PASSPHRASE=<*pass phrase for Remote Filtering Server*> **PRIMARY_WISP_ADDRESS=**<*external IP Address or FQDN of primary Remote Filtering Server*> **PRIMARY_WISP_PORT=**<*external port number of primary Remote Filtering Server*> **PRIMARY_INTERNAL_WISP_ADDRESS=**<*internal IP address or host name of primary Remote Filtering Server*> **PRIMARY_INTERNAL_WISP_PORT=**<*internal port number of primary Remote Filtering Server*> **REBOOT=**<*reboot parameter*> **/qn**

For example, the installation command might look like this:

```
msiexec /i cpmclient.msi PASSPHRASE=2gbatfm
PRIMARY_WISP_ADDRESS=63.16.200.232
PRIMARY_WISP_PORT=80
PRIMARY_INTERNAL_WISP_ADDRESS=10.218.5.60
PRIMARY_INTERNAL_WISP_PORT=9000
REBOOT=IF_NEEDED_PROMPT /qn
```

If you are using secondary or tertiary Remote Filtering Servers, you must enter parameters for those machines as well.

Repair Syntax

The following is an example of the syntax to repair an existing installation of Remote Filtering Client using a third-party deployment tool. This command must be typed on a single line with no returns.

```
msiexec /i cpmclient.msi REINSTALL=ALL
REINSTALLMODE=veums /qn
```

When the installer repairs an installation of the Remote Filtering Client, the current configuration settings are used. If your remote filtering configuration *has not* changed, no additional parameters are necessary. However, if you have changed your configuration, you must include the appropriate parameters and new values in the command.

> ✓ **Note**
>
> For the syntax required to upgrade Remote Filtering Clients to a new version, see *Upgrading Remote Filtering Client with a Third-Party Deployment Tool*, page 53.

Uninstall Command

The following is the actual command that can be used to uninstall the Remote Filtering Client with a third-party deployment tool. This command must be typed on a single line with no returns.

```
msiexec.exe /x - {14D74337-01C2-4F8F-B44B-
67FC613E5B1F} /qn
```

Solaris and Linux Procedures

The steps in this section are common to all separate installations of Websense Enterprise and Web Security Suite components on Solaris or Linux. Start here to download and run the Websense installer, and then refer to the appropriate sections for the component-specific procedures.

To install components separately on a Solaris or Linux machine:

1. Log on to the installation machine as the **root** user.
2. Close all applications and stop any antivirus software.
3. Create a setup directory for the installer files.

   For example: `/root/Websense_setup`

4. Obtain an installer package for either Websense Enterprise or Web Security Suite:

   - **Web download**: To download an installer package, go to www.websense.com, and then navigate to the Downloads page.

     a. Choose your product, the dynamic (online) or full (offline) installer package, the operating system, and the language.

     ✔ **Note**

     The **Dynamic** installer is an **online** installer package that requires web access during installation. It downloads the necessary product files from the website as needed after product selections have been made.

     The **Full** installer is a complete **offline** installer. It is much larger than the online Dynamic installer package, and contains all the files needed to install the Websense Enterprise or Web Security Suite components. Use this package if you experience difficulties with the online installer.

     ---

     b. Save the selected installer package to the setup directory on the installation machine.

5. In the setup directory, enter the following command to unzip the file:

   `gunzip <download file name>`

   For example: `gunzip Websense632Setup_Slr.tar.gz`

6. Expand the file into its components with the following command:

   `tar xvf <unzipped file name>`

   For example: `tar xvf Websense632Setup_Slr.tar`

This places the following files into the setup directory:

File	Description
install.sh	Installation program
Setup	Archive file containing related installation files and documents.
Documentation	Release Notes: An HTML file containing release notes and last minute information about the Websense software. Read this file with any supported browser.

7. Run the installation program from the setup directory with the following command:

   `./install.sh`

   To run the GUI version of the installer, use the following command:

   `./install.sh -g`

   If you are using a non-English based system, the installer will display an error message advising you that the GUI version is not supported.

8. Follow the onscreen instructions through the subscription agreement.

9. (*Web Security Suite only.*) When asked for a product selection, select the Web Security Suite edition you plan to use.

   The installer displays information about the required installation sequence for the components of this product on your operating system.

10. Select **Custom** when asked what type of installation you want.

11. To continue, proceed to the appropriate component section.

Websense Manager

Websense Manager, the administrative interface for your Websense software, can be installed in multiple locations in your network for convenient access. The Websense Manager machine needs network access to the Policy Server machine.

To install Websense Manager on a Solaris or Linux machine.

1. Download and start the installer using the procedure in *Solaris and Linux Procedures*, page 134.

2. Following the **Custom** installation path brings you to a list of components to install. Select **Websense Manager**.

   The installer asks you for the location of your web browser.

3. Provide the full path to the web browser to use when viewing online Help.

   The installer asks you to provide a path to the installation directory in which it can create the `/Manager` subdirectory and install Websense Manager.

4. Enter the path to the installation directory, or accept the default installation directory (`/opt/Websense`). If this directory does not already exist, the installer will create it.

   > **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 installation you have selected with the resources of the installation machine. If the machine has inadequate disk space or memory, separate warnings are displayed.

   - If the installation machine has insufficient disk space, the selected components cannot be installed, and the installer will quit.

   - If the installation machine has less than the recommended amount of memory, the installation can continue. To ensure the best performance of the components you are installing, you should upgrade your machine's memory to the recommended amount.

   A summary list appears, showing the installation path, the installation size, and the component (Websense Manager) you have selected.

5. Select **Next** to begin installing Websense Manager.

6. If you are using the online installer, the Download Manager downloads the appropriate installer files from the Websense website. Installation begins automatically when the necessary files have been downloaded.

   If Network Agent was not installed, a message reminds you that features such as Protocol Management and Bandwidth Optimizer cannot be used unless Network Agent is installed on a machine with direct access to internet traffic. Select **Next** to continue.

7. When a message announcing successful completion of the installation is displayed:

   ■ If you chose a non-English language installer, select **Next** to continue. The Websense Language Pack installer starts. Follow the onscreen instructions.

   ■ If you chose an English language installer:

      • If you are installing in command line mode, select **Finish** to exit the installer.

      • If you are installing in GUI mode, select **Next** to continue. The installer asks if you want to start Websense Manager. Make a choice and select **Finish** to exit the installer.

8. If you stopped your antivirus software, remember to start it again after Websense components have been installed.

> **Note**
>
> To launch Websense Manager on a Solaris or Linux machine, go to the `/Manager` subdirectory in the Websense installation directory (by default, `opt/Websense/Manager`) and enter:
>
> `./start_manager`

Network Agent

You can install Network Agent on a Solaris or Linux machine separate from the Filtering Service. Network Agent must be able to monitor 2-way internet traffic from the internal network. Install Network Agent on a machine that can see the internet requests *from* the internal network as well as the internet response *to* the requesting workstations.

> **Important**
>
> If you install Network Agent on a machine that cannot monitor the targeted traffic, Network Agent features such as Protocol Management, Bandwidth Optimizer, and IM Attachment Manager will not perform as expected.

If this installation is part of a multiple deployment of the Network Agent (for load balancing purposes), you must be sure that the IP address ranges for each instance of the Network Agent do not overlap. This will result in double logging. Deploy the Network Agents so that they can filter the entire network. Partial deployment will result in incomplete filtering by protocol and bandwidth, as well as the loss of log data from network segments not watched by Network Agent.

To define IP address ranges for multiple Network Agents, follow the instructions in the *Administrator's Guide* for Websense Enterprise and Web Security Suite. For detailed information about deploying Network Agent, see the *Deployment Guide* for Websense Enterprise and Web Security Suite.

Do not install Network Agent on a machine running any type of firewall. Network Agent uses a packet capturing utility which may not work properly when installed on a firewall machine.

If you are attempting to install Network Agent on a machine on which the Filtering Service and Policy Server are already installed, see the procedures in *Adding Components*, page 154.

> **Important**
>
> The Websense Filtering Service and Policy Server must be installed and running prior to installing Network Agent, or installed at the same time as Network Agent. The installer asks for the IP addresses and port numbers of these components and will not install Network Agent if the Policy Server and Filtering Service cannot be located.

1. Download and start the installer using the procedure in *Solaris and Linux Procedures*, page 134.

2. Following the **Custom** installation path brings you to a list of components to install. Select **Network Agent**.

   The installer asks you to identify the machine on which the Policy Server is installed.

✓ **Note**

The displayed configuration port (55806) is the default port number used by the installer to install the Policy Server. If you installed the Policy Server using a different port number, enter that port number.

3. Enter the IP address of the Policy Server machine, and the port number if different from the default, and then select **Next**.

   The installer asks you if this machine is running a firewall. Make sure that the installation machine is not being used as a firewall before continuing.

   Important

   Network Agent cannot function properly on a machine running a firewall.

   The only exception is a blade server or appliance that has separate processors or virtual processors to accommodate Network Agent and the firewall software.

4. Select **Yes** or **No** and then select **Next** to continue:

   - Select **Yes** if the installation machine is *not* being used as a firewall. Installation will continue.

   - Select **No** if you are attempting to install Network Agent on a firewall machine, and Setup will exit. Install Network Agent on a machine that is not running a firewall.

   All enabled network interface cards (NICs) on the machine appear in a list.

5. If the machine has multiple NICs, select the one that has visibility into the internet traffic you want Network Agent to filter.

   ✓ **Note**

   After installation, you can run the Traffic Visibility Tool to test whether the selected NIC can see the appropriate user internet traffic. See *Testing Visibility of Internet Traffic to Network Agent*, page 199.

The installer asks you for the IP address and filter port number for the machine on which Filtering Service is installed.

> **Note**
>
> The displayed filter port (15868) is the default port number used by the installer to install Filtering Service. If you installed Filtering Service using a different port number, enter that port number.

6. Enter the IP address of the Filtering Service machine, and the port number if different from the default, and then select **Next** to continue.

   The installer asks if you want to allow Websense, Inc., to gather information about the use of Websense-defined protocols. Information will be used in the development of 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. Select a Network Agent feedback option, and then select **Next** to continue.

   The installer asks you for the location of the installation directory.

8. Enter the path to the installation directory, or accept the default Websense installation directory (`/opt/Websense`). If this directory does not already exist, the installer will create it.

> **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 installation you have selected with the resources of the installation machine. If the machine has inadequate disk space or memory, separate warnings are displayed.

- If the installation machine has insufficient disk space, the selected components cannot be installed, and the installer will quit.

- If the installation machine has less than the recommended amount of memory, the installation can continue. To ensure the best performance of the components you are installing, you should upgrade your machine's memory to the recommended amount.

A summary of all the components that will be installed appears.

9. Select **Next** to begin installation.

   If you are using the online installer, the Download Manager downloads the appropriate installer files from the Websense website. Installation begins automatically when the necessary files have been downloaded.

10. When a message announcing successful completion of the installation is displayed:

    - If you chose a non-English language installer, select **Next** to continue. The Websense Language Pack installer starts. Follow the onscreen instructions.

    - If you chose an English language installer, select **Finish** to exit the installer.

11. If you stopped your antivirus software, remember to start it again after Websense components have been installed.

12. Configure Network Agent for use in your network. See the instructions for initial configuration of Network Agent in *Chapter 5: Initial Setup*, as well as the Network Agent chapter in the *Administrator's Guide* for Websense Enterprise and Web Security Suite.

RADIUS Agent

The Websense RADIUS Agent allows you to integrate your Websense filtering policies with authentication provided by a RADIUS server. The RADIUS Agent enables Websense software to transparently identify users who access your network using a dial-up, Virtual Private Network (VPN), Digital Subscriber Line (DSL), or other remote connection.

To install the RADIUS Agent on a Solaris or Linux machine:

1. Download and start the installer using the procedure in *Solaris and Linux Procedures*, page 134.

2. Following the **Custom** installation path brings you to a list of components to install. Select **RADIUS Agent**.

If the installation machine is multihomed, all enabled network interface cards (NICs) with an IP address are displayed.

3. Select the IP address of the card you want RADIUS Agent to use to communicate.

   The installer asks you to identify the machine on which the Policy Server is installed.

   > ✔ **Note**
   >
   > The displayed configuration port (55806) is the default port number used by the installer to install the Policy Server. If you installed the Policy Server using a different port number, enter that port number.

4. Enter the IP address of the Policy Server machine, and the port number if different from the default, and then select **Next** to continue.

   The installer asks you for the location of the installation directory.

5. Enter the path to the installation directory, or accept the default Websense installation directory (`/opt/Websense`). If this directory does not already exist, the installer will create it.

   > ! **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 installation you have selected with the resources of the installation machine. If the machine has inadequate disk space or memory, separate warnings are displayed.

   - If the installation machine has insufficient disk space, the selected components cannot be installed, and the installer will quit.
   - If the installation machine has less than the recommended amount of memory, the installation can continue. To ensure the best performance of the components you are installing, you should upgrade your machine's memory to the recommended amount.

   A summary of all the components that will be installed appears.

6. Select **Next** to begin installation.

   If you are using the online installer, the Download Manager downloads the appropriate installer files from the Websense website. Installation begins automatically when the necessary files have been downloaded.

   If Network Agent was not installed, a message reminds you that features such as Protocol Management and Bandwidth Optimizer cannot be used unless Network Agent is installed on a machine with direct access to internet traffic. Select **Next** to continue.

7. When a message announcing successful completion of the installation is displayed:

   - If you chose a non-English language installer, select **Next** to continue. The Websense Language Pack installer starts. Follow the onscreen instructions.

   - If you chose an English language installer, select **Finish** to exit the installer.

8. If you stopped your antivirus software, remember to start it again after Websense components have been installed.

9. Configure the RADIUS Agent, and configure your environment for RADIUS Agent. For instructions, see the User Identification chapter in the *Administrator's Guide* for Websense Enterprise and Web Security Suite.

eDirectory Agent

The Websense eDirectory Agent works together with Novell eDirectory to identify users transparently so that Websense software can filter requests according to particular policies assigned to users or groups.

Do not install eDirectory Agent on the same machine as DC Agent or Logon Agent, as this can cause conflicts.

To install the eDirectory Agent on a Solaris or Linux machine:

1. Download and start the installer using the procedure in *Solaris and Linux Procedures*, page 134.

2. Following the **Custom** installation path brings you to a list of components to install. Select **eDirectory Agent**.

The installer asks you to identify the machine on which the Policy Server is installed.

✓ **Note**

The displayed configuration port (55806) is the default port number used by the installer to install the Policy Server. If you installed the Policy Server using a different port number, enter that port number.

---

3. Enter the IP address of the Policy Server machine, and the port number if different from the default, and then select **Next** to continue.

   If the installation machine is multihomed, all enabled network interface cards (NICs) with an IP address are displayed.

4. Select the IP address of the card you want eDirectory Agent to use to communicate, and then select **Next** to continue.

   The installer asks for the Novell eDirectory name and password.

5. Enter the full *distinguished name* and a valid password, and then select **Next** to continue.

   The installer asks you for the location of the installation directory.

6. Enter the path to the installation directory, or accept the default Websense installation directory (`/opt/Websense`). If this directory does not already exist, the installer will create it.

❗ **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 installation you have selected with the resources of the installation machine. If the machine has inadequate disk space or memory, separate warnings are displayed.

- If the installation machine has insufficient disk space, the selected components cannot be installed, and the installer will quit.

- If the installation machine has less than the recommended amount of memory, the installation can continue. To ensure the best performance

of the components you are installing, you should upgrade your machine's memory to the recommended amount.

A summary of all the components that will be installed appears.

7. Select **Next** to begin installation.

    If you are using the online installer, the Download Manager downloads the appropriate installer files from the Websense website. Installation begins automatically when the necessary files have been downloaded.

    If Network Agent was not installed, a message reminds you that features such as Protocol Management and Bandwidth Optimizer cannot be used unless Network Agent is installed on a machine with direct access to internet traffic. Select **Next** to continue.

8. When a message announcing successful completion of the installation is displayed:

    ■   If you chose a non-English language installer, select **Next** to continue. The Websense Language Pack installer starts. Follow the onscreen instructions.

    ■   If you chose an English language installer, select **Finish** to exit the installer.

9. If you stopped your antivirus software, remember to start it again after Websense components have been installed.

10. Configure the eDirectory Agent and Novell eDirectory by following the instructions in the User Identification chapter of the *Administrator's Guide* for Websense Enterprise and Web Security Suite.

Logon Agent

Logon Agent is a Websense transparent identification agent that detects users as they log on to Windows domains in your network via client machines. The Logon Agent receives logon information from LogonApp.exe, a separate client application that runs only on Windows client machines, and must be run by a logon script. For information about setting up this script in your network, see *Creating and Running the Script for Logon Agent*, page 189.

Logon Agent can be run together with DC Agent if some of the users in your network are not being authenticated properly. This might happen if your network uses Windows 98 workstations, which do not permit DC Agent to poll users for their identification when they make an internet request.

Do not install Logon Agent on the same machine as eDirectory Agent, as this can cause conflicts.

To install the Logon Agent on a Solaris or Linux machine:

✔ **Note**

`LogonApp.exe`, the client application that passes user logon information to Logon Agent, runs only on Windows client machines.

1. Download and start the installer using the procedure in *Solaris and Linux Procedures*, page 134.

2. Following the **Custom** installation path brings you to the component selection screen. Select **Logon Agent**.

   The installer asks you to identify the machine on which the Policy Server is installed.

   ✔ **Note**

   The displayed configuration port (55806) is the default port number used by the installer to install the Policy Server. If you installed the Policy Server using a different port number, enter that port number.

3. Enter the IP address of the Policy Server machine, and the port number if different from the default, and then select **Next** to continue.

   If the installation machine is multihomed, all enabled network interface cards (NICs) with an IP address appear in a list.

4. Select the IP address of the card you want Logon Agent to use to communicate.

   The installer asks you for the location of the installation directory.

5. Enter the path to the installation directory, or accept the default Websense installation directory (`/opt/Websense`). If this directory does not already exist, the installer will create it.

> ### 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 installation you have selected with the resources of the installation machine. If the machine has inadequate disk space or memory, separate warnings are displayed.

- If the installation machine has insufficient disk space, the selected components cannot be installed, and the installer will quit.

- If the installation machine has less than the recommended amount of memory, the installation can continue. To ensure the best performance of the components you are installing, you should upgrade your machine's memory to the recommended amount.

A summary of all the components that will be installed appears.

6. Select **Next** to begin installation.

If you are using the online installer, the Download Manager downloads the appropriate installer files from the Websense website. Installation begins automatically when the necessary files have been downloaded.

If Network Agent was not installed, a message reminds you that features such as Protocol Management and Bandwidth Optimizer cannot be used unless Network Agent is installed on a machine with direct access to internet traffic. Select **Next** to continue.

7. When a message announcing successful completion of the installation is displayed:

- If you chose a non-English language installer, select **Next** to continue. The Websense Language Pack installer starts. Follow the onscreen instructions.

- If you chose an English language installer, select **Finish** to exit the installer.

8. If you stopped your antivirus software, remember to start it again after Websense components have been installed.

9. Set up the required logon script by following the instructions is *Creating and Running the Script for Logon Agent*, page 189.

10. Configure Logon Agent to communicate with client workstations and the Filtering Service by following the instructions in the User Identification chapter of the *Administrator's Guide* for Websense Enterprise and Web Security Suite.

Remote Filtering Server

The Remote Filtering Server provides web filtering for user workstations located outside the network firewall. In order to be filtered through the Remote Filtering Server, a remote workstation must be running the Remote Filtering Client. (For Remote Filtering Client installation instructions, see *Remote Filtering Client*, page 123.)

> ✓ **Note**
>
> To enable the Remote Filtering components, you must subscribe to the remote filtering service.

The Remote Filtering Server should be installed on a separate, dedicated machine. This machine must be able to communicate with the Websense Filtering Service and with the remote workstations outside the network firewall. The Remote Filtering Server machine does not have to be joined to a domain.

The Remote Filtering Server should be installed inside your organization's outermost network firewall, but in the DMZ outside the firewall that protects the rest of the corporate network. For more information about deploying the Remote Filtering Server in your network, see the *Remote Filtering* section in the *Deployment Guide* for Websense Enterprise and Web Security Suite.

To provide failover capability for the primary Remote Filtering Server, you can install secondary and tertiary Remote Filtering Servers. Each Remote Filtering Client can be configured to connect with a primary, secondary, and tertiary Remote Filtering Server. If the primary server is unavailable, the

client attempts to connect with the secondary, then the tertiary, then the primary again, and so on.

> **Important**
>
> - Install only one primary Remote Filtering Server for each Filtering Service in your network.
> - Do not install the Remote Filtering Server on the same machine as the Filtering Service or Network Agent.
> - Do not enable DHCP on the Remote Filtering Server machine.

To install the Remote Filtering Server on a Solaris or Linux machine:

1. Download and start the installer using the procedure in *Solaris and Linux Procedures*, page 134.

2. Following the **Custom** installation path brings you to a list of components to install. Select **Remote Filtering Server**.

   If the installation machine is multihomed, all enabled network interface cards (NICs) with an IP address are displayed.

3. Select the IP address of the card you want the Remote Filtering Server to use to communicate with other Websense components inside the network firewall, and then select **Next** to continue.

   Remote Filtering Clients must be able to connect to the Remote Filtering Server, both from inside and from outside the internet gateway or network firewall. The installer asks you to provide connection information for this machine.

4. In the **External IP Address or Host Name** field, enter an IP address or machine name (in the form of a fully qualified domain name) that is visible from *outside* the firewall.

5. In the **External Communication Port** field, enter a port number (from 10 to 65535) that is not in use, and that is accessible from *outside* the network firewall. The default value is 80. (If there is a web server installed on the machine, port 80 may already be in use, so you may need to change the default value.)

> **Important**
>
> The port entered as the **External Communication Port** must be opened on your network firewall to accept connections from Remote Filtering Clients on workstations located outside the firewall. For more information, see *Firewall Configuration for Remote Filtering*, page 206.

6. In the **Internal Communication Port** field, enter a port number (from 1024 to 65535) that is not in use, and that is accessible only from *inside* the network firewall. The default value is 8800.

> **Important**
>
> Be sure that your network firewall is configured to block connections to the **Internal Communication Port** from workstations located outside the firewall. For more information, see *Firewall Configuration for Remote Filtering*, page 206.

The installer asks you to enter a pass phrase of any length for the Remote Filtering Server. This pass phrase will be combined with unpublished keys to create an encrypted authentication key (shared secret) for secure client/server communication.

7. Before selecting a **pass phrase**, consider the following requirements:

- If Websense Client Policy Manager (CPM) is already installed in your network, you must enter the same pass phrase used when installing CPM.

- If you install Websense Client Policy Manager (CPM) in your network in the future, you must use the pass phrase you enter in this screen.

- If you want this installation of the Remote Filtering Server to function as a backup (secondary or tertiary) server for a primary Remote Filtering Server, you must enter the same pass phrase used when installing the primary Remote Filtering Server.

- The pass phrase must include only ASCII characters. Do not use extended ASCII or double-byte characters.

- You must use the pass phrase you enter in this screen when you install the Remote Filtering Clients that will connect with this server. (See *Remote Filtering Server Connection Information*, page 126.)

Warning

Be sure to record your **pass phrase** and keep it in a safe place, as it cannot be retrieved from the Websense system later.

---

8. Enter and confirm your **pass phrase**.

   The installer asks you to provide information about the machine on which the Websense Filtering Service is installed.

9. Enter the actual (internal) IP address of the Filtering Service machine.

   The installer asks if there is a firewall or other network device that performs network address translation between the Filtering Service machine and this Remote Filtering Server machine.

10. Enter **yes** or **no**.

   If you entered **yes**, the installer asks for the translated (external) IP address of the Filtering Service machine, visible to this machine. Enter the translated IP address.

11. Enter the filter port number for the Filtering Service machine, if it was changed from the default of 15868.

Note

The filter port is the default communication port used by the installer to install Filtering Service. If you installed Filtering Service using a different communication port, enter that port number.

---

12. Enter the block page port number for the Filtering Service machine, if it was changed from the default value of 15871.

> **Important**
>
> If there is a firewall between the Filtering Service machine and the Remote Filtering Server machine, be sure to open the filter port (15868) and block page port (15871) on that firewall. Filtering Service must be able to accept connections from the Remote Filtering Server, and serve block pages to remote users. For more information, see *Firewall Configuration for Remote Filtering*, page 206.

The installer asks you for the location of the installation directory.

13. Enter the path to the installation directory, or accept the default Websense installation directory (`/opt/Websense`). If this directory does not already exist, the installer will create it.

> **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 installation you have selected with the resources of the installation machine. If the machine has inadequate disk space or memory, separate warnings are displayed.

- If the installation machine has insufficient disk space, the selected components cannot be installed, and the installer will quit.

- If the installation machine has less than the recommended amount of memory, the installation can continue. To ensure the best performance of the components you are installing, you should upgrade your machine's memory to the recommended amount.

A summary of all the components that will be installed appears.

14. Select **Next** to begin installation.

If you are using the online installer, the Download Manager downloads the appropriate installer files from the Websense website. Installation begins automatically when the necessary files have been downloaded.

Since the Network Agent was not installed on this machine, a message reminds you that features such as Protocol Management and Bandwidth Optimizer cannot be used unless Network Agent is installed on a machine with direct access to internet traffic. Select **Next** to continue.

15. When a message announcing successful completion of the installation is displayed:

    - If you chose a non-English language installer, select **Next** to continue. The Websense Language Pack installer starts. Follow the onscreen instructions.

    - If you chose an English language installer, select **Finish** to exit the installer.

16. If you stopped your antivirus software, remember to start it again after Websense components have been installed.

For more information about how remote filtering works, see the *Filtering Remote Clients* section in the *Administrator's Guide* for Websense Enterprise and Web Security Suite.

Modifying an Installation

If you decide to change the location of a Websense component or modify your Websense installation, run the installer again on the machine you want to modify and select the appropriate option. The installer detects the presence of Websense components and offers you the following installation options:

- Add Websense components.
- Remove Websense components.
- Repair existing Websense components.

Adding Components

After installing Websense Enterprise or Web Security Suite, you may want to add components to change the configuration of Websense software in your network. The following procedures assume that the Filtering Service, Policy Server, User Service, Usage Monitor, and Websense Manager are already installed, and that additional components are going to be added. If you are adding remote components, the installer will ask you for the location of the Policy Server.

Windows

To add Websense components in a Windows environment:

> ✔ **Note**
> Before adding new components, we recommend that you perform a full system backup as a fallback strategy. This backup allows you to restore your current system with minimum downtime, should you decide to do so.

1. Log on to the installation machine with **domain** and **local** administrator privileges.

    If you are adding User Service or DC Agent, this will assure that they have administrator privileges on the domain.

    > ! **Important**
    > User Service and DC Agent must have administrator privileges on the network to retrieve user login information from the domain controller. Without this information, Websense software cannot filter by users and groups. If you cannot install these components with such privileges, you can configure domain administrator privileges for these services after installation. For instructions, see *Configure Domain Administrator Privileges*, page 202.

2. Close all applications and stop any antivirus software.

3. Go to the folder where you extracted the Windows Websense installer files, and double-click Setup.exe to launch the installer.

4. Click **Next** in the welcome screen.

    A dialog box appears asking you what action you want to take with the Websense components the installer has detected on the machine.

5. Select **Add Websense components** and click **Next**.

    The installer displays a product selection screen.

6. If you are running the Websense Enterprise installer, select **Websense Enterprise**. If you are running the Web Security Suite installer, select **Web Security Suite**.

7. Click **Next** to continue.

   The installer displays a list of components not currently installed on the installation machine.
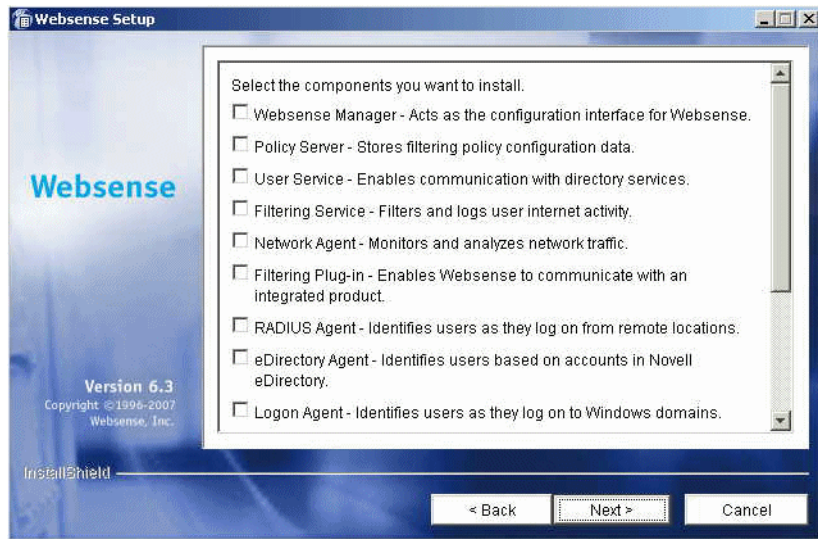
Websense Component Selection

8. Select the components you want to install and click **Next**.

If you are installing the Real-Time Analyzer and are using IIS as your web server, you are prompted to select the name of the website in the IIS Manager under which the installer should create a *virtual directory*. The default value is **Default Web Site**, which is correct in most instances.
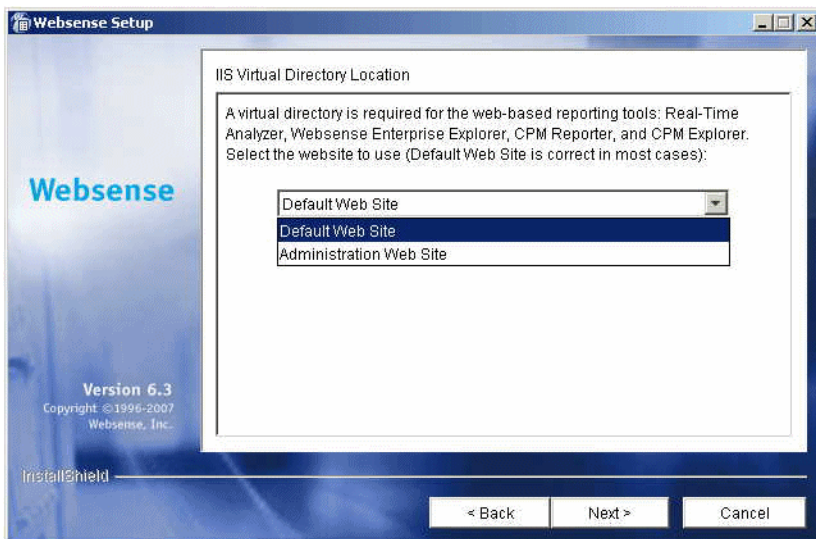
Virtual Directory Selection

9. If you have renamed the default website in the IIS Manager or are using a language version of Windows other than English, select the proper website from the names in the drop-down list, and then click **Next** to continue.

   If you are installing Network Agent, the installer asks you if this machine is running a firewall. Network Agent cannot function properly on a machine that is being used as a firewall. (The only exception is a blade server or appliance that has separate processors or virtual processors to accommodate Websense software and the firewall software.)

10. Select **Yes** or **No** and click **Next** to continue:

    ■ Select **Yes** if the installation machine is *not* being used as a firewall. Installation will continue.

    ■ Select **No** if you are attempting to install Network Agent on a firewall machine, and Setup will exit. Install Network Agent on a machine that is not running a firewall.

> **Important**
>
> The machine on which Network Agent is installed must be able to monitor 2-way employee internet traffic to function correctly. If you install Network Agent on a machine that cannot monitor the targeted traffic, Network Agent features such as Protocol Management, Bandwidth Optimizer, and IM Attachment Manager will not perform as expected.

If you are installing Network Agent, a screen appears asking you to select the network interface card (NIC) that you want Network Agent to use for capturing traffic. All network interface cards enabled in the machine appear in a list.

11. If the machine has multiple NICs, select the one that has visibility into the internet traffic you want Network Agent to filter.

> **Note**
>
> After installation, you can run the Traffic Visibility Tool to test whether the selected NIC can see the appropriate user internet traffic. See *Testing Visibility of Internet Traffic to Network Agent*, page 199.

12. Click **Next** to continue.

    If you are installing Network Agent, a screen appears asking if you want to allow Websense, Inc., to gather information about the use of Websense-defined protocols. Information will be used in the development of 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.

13. Select a Network Agent feedback option and click **Next** to continue.

If you selected DC Agent for installation, you are asked to provide a user name and a password with administrative privileges on the domain. DC Agent needs access to directory information to be able to identify users transparently.
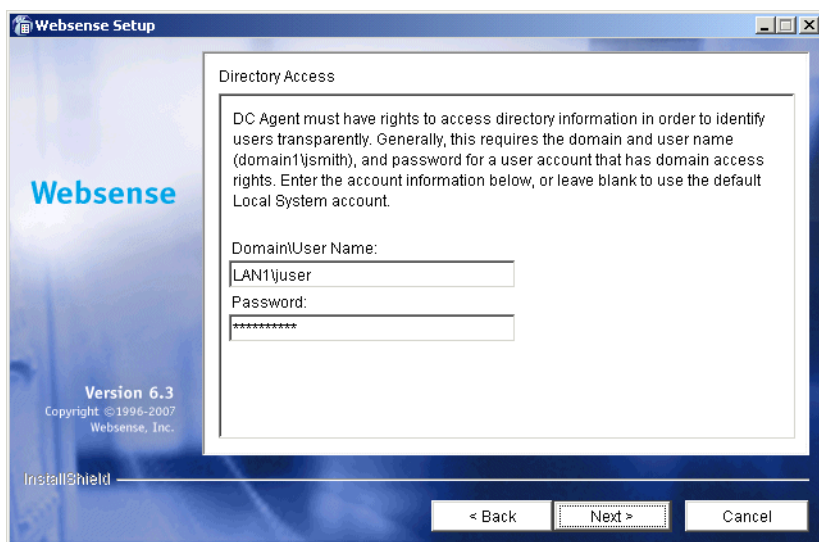
Directory Access for DC Agent

14. Enter the domain and user name, followed by the network password for an account with domain privileges, and click **Next** to continue.

> ✓ **Note**
>
> If you cannot install DC Agent with the appropriate privileges, you can configure domain administrator privileges for it after installation. For instructions, see *Configure Domain Administrator Privileges*, page 202.

The installer compares the system requirements for the installation you have selected with the resources of the installation machine. If the machine has inadequate disk space or memory, separate warnings are displayed.

- If the installation machine has insufficient disk space, the selected components cannot be installed, and the installer will quit.

- If the installation machine has less than the recommended amount of memory, the installation can continue. To ensure the best performance of the components you are installing, you should upgrade your machine's memory to the recommended amount.

A summary screen appears, listing the installation path, the installation size, and the components that will be installed.

15. Click **Next** to begin installation.

If you are using the online installer, the Download Manager progress bars are displayed as the appropriate installer files are downloaded from the Websense website. Installation begins automatically when the necessary files have been downloaded.

If Network Agent was *not* installed, a message reminds you that features such as Protocol Management and Bandwidth Optimizer cannot be used unless Network Agent is installed on a machine with direct access to internet traffic. Click **Next** to continue.

16. When a message announcing successful completion of the installation is displayed:

- If you chose a non-English language installer, the Websense Language Pack installer starts.

   Click **Next** in the welcome screen and follow the onscreen instructions to update Websense components with text in the selected language.

- If you chose an English language installer:

   • If Websense Manager was not installed, click **Finish** to exit the installer.

   • If Websense Manager was installed, click **Next** to continue.

      The installer displays a screen asking if you want to launch Websense Manager. If you do not want to launch Manager, clear the checkbox. Click **Finish** to exit the installer.

> ✔ **Note**
>
> Before you can access Real-Time Analyzer and other Websense Reporting Tools, you must first log on to Websense Manager and configure user permissions. For more information, see the *Administrator's Guide* for Websense Enterprise and Web Security Suite.

17. If you stopped your antivirus software, be sure to start it again.

Solaris or Linux

To add Websense Enterprise or Web Security Suite components in a Solaris or Linux environment:

> ✔ **Note**
>
> Before adding new components, we recommend that you perform a full system backup as a fallback strategy. This will allow you to restore your current system with a minimum of downtime, should you decide to do so.

1. Log on to the installation machine as the **root** user.
2. Close all applications and stop any antivirus software.
3. Run the installation program from the directory where it resides using the following command:

   ```
   ./install.sh
   ```

   To run the GUI version of the installer, use the following command:

   ```
   ./install.sh -g
   ```

   If you are using a non-English based system, the installer will display an error message advising you that the GUI version is not supported.

   The installer detects the currently installed Websense components and asks you what action you want to take.
4. Select **Add Websense components**.

   The installer asks you to select the components that you want to install.

   The installer displays a list of components not currently installed on the installation machine.
5. Select the components you want to install, and then select **Next** to continue.
6. Make the following selections during installation:
   - **Firewall installation warning**: If you are installing Network Agent, the installer displays a warning that Network Agent cannot function properly on a machine running a firewall. (The only exception is a blade server or appliance that has separate processors or virtual processors to accommodate Websense software and the firewall software.)

Select **Yes** or **No** when asked if you want to install Network Agent:

- Select **Yes** if the installation machine is *not* being used as a firewall. Installation will continue.

- Select **No** if you are attempting to install Network Agent on a firewall machine, and Setup will exit. Install Network Agent on a machine that is not running a firewall.

Important

The machine on which Network Agent is installed must be able to monitor 2-way employee internet traffic to function correctly. If you install Network Agent on a machine that cannot monitor the targeted traffic, Network Agent features such as Protocol Management, Bandwidth Optimizer, and IM Attachment Manager will not perform as expected.

- **Network Interface Card (NIC) selection**: If you are installing Network Agent, all enabled network interface cards (NICs) appear in a list. If the machine has multiple NICs, select the one to use for Network Agent. Be sure that this card has visibility into the internet traffic you want Network Agent to filter.

Note

After installation, you can run the Traffic Visibility Tool to test whether the selected NIC can see the appropriate user internet traffic. See *Testing Visibility of Internet Traffic to Network Agent*, page 199.

- **Network Agent Feedback**: If you are installing Network Agent, the installer asks if you want to allow Websense, Inc., to gather information about the use of Websense-defined protocols. Information will be used in the development of protocol filtering. Select a Network Agent feedback option and continue.

Note

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

- **System requirements check**: The installer compares the system requirements for the installation you have selected with the resources of the installation machine. If the machine has inadequate disk space or memory, separate warnings are displayed.

  - If the installation machine has insufficient disk space, the selected components cannot be installed, and the installer will quit.
  - If the installation machine has less than the recommended amount of memory, the installation can continue. To ensure the best performance of the components you are installing, you should upgrade your machine's memory to the recommended amount.

- **Installation summary**: A summary list appears, showing the installation path, the installation size, and the components that will be installed.

7. Select **Next** to begin installing the displayed Websense components.

   If you are using the online installer, the Download Manager downloads the appropriate installer files from the Websense website. Installation begins automatically when the necessary files have been downloaded.

   If Network Agent was not installed, a message reminds you that features such as Protocol Management and Bandwidth Optimizer cannot be used unless Network Agent is installed on a machine with direct access to internet traffic. Select **Next** to continue.

8. When a message announcing successful completion of the installation is displayed:

   - If you chose a non-English language installer, select **Next** to continue. The Websense Language Pack installer starts. Follow the onscreen instructions to update Websense components with text in the selected language.

   - If you chose an English language installer:

     - If you are installing in command line mode, or if you are installing in GUI mode and did not install Websense Manager, select **Finish** to exit the installer.
     - If you are installing in GUI mode and you installed Websense Manager, select **Next** to continue. The installer asks if you want to start Websense Manager. Make a choice and select **Finish** to exit the installer.

9. If you stopped your antivirus software, be sure to start it again.

Removing Components

After installing Websense Enterprise or Web Security Suite or any of their components, you may want to remove components to change the configuration of Websense software in your network.

> **Important**
>
> The Policy Server service must be running to uninstall any Websense components. To remove the Policy Server, you must also remove all the other components installed on the machine.

Windows

To remove installed Websense Enterprise or Web Security Suite components in a Windows environment:

> **Note**
>
> Before removing components, we recommend that you perform a full system backup as a fallback strategy.

1. Log on to the installation machine with **local** administrator privileges.
2. Close all applications and stop any antivirus software.
3. Go to the Windows Add or Remove Programs dialog box:
   - *Windows Server 2003*: Select **Start** > **Control Panel** > **Add or Remove Programs**.
   - *Windows 2000*: Select **Start** > **Settings** > **Control Panel**, and then double-click **Add/Remove Programs**.

4. Select **Websense** from the list of installed applications.
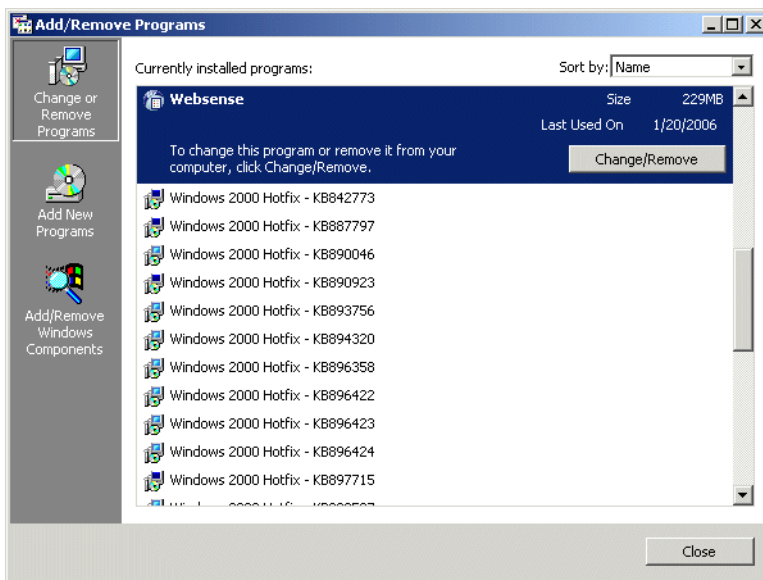
Add/Remove Programs Control Panel, Windows 2000

5. Click **Change/Remove** to launch the Websense uninstaller.

There may be a delay of several seconds while the Websense uninstaller starts.

A list of installed components appears.
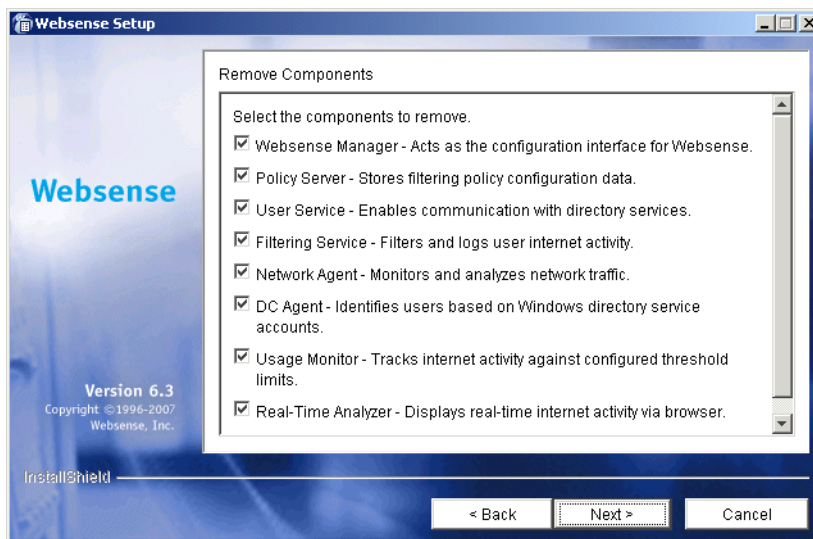
Remove Components

By default, all components are checked for removal.

> ⚠️ **Warning**
>
> Do not uninstall the Policy Server without uninstalling all of the Websense components. Removing the Policy Server will sever communication with the remaining Websense components and will require the reinstallation of those components.

6. To keep a component, remove the check mark from the box next to it. When all of the components you want to uninstall are checked, click **Next** to continue.

> ✓ **Note**
>
> If you are uninstalling Filtering Service, make sure that all associated Network Agents are uninstalled. If you try to uninstall Network Agent *after* its associated Filtering Service has been removed, the installer will be unable to stop Network Agent and will display an error message.

If the Policy Server is not running, a dialog box appears advising you that removing Websense components may require communication with the Policy Server. You may exit the installer to restart the Policy Server, or continue uninstalling the selected components.

> **⚠ Warning**
>
> If the Policy Server is not running, the files for the selected components will be removed, but not the information about the components recorded in the `config.xml` file. This could cause problems if you decide to add these components again at a later date.

A summary list of the components you have selected to remove appears.

7. Click **Next** to begin uninstalling the components.

   If you are uninstalling Network Agent on a remote machine after removing the Policy Server, expect the process to take several minutes. Network Agent will be successfully uninstalled, although no progress notification will be displayed.

   A completion messages advises you when the procedure is finished.

8. Click **Next** to continue.

   A dialog box appears advising you that the machine must be restarted to complete the uninstall process.

9. Select a restart option and click **Finish** to exit the installer.

10. If you stopped your antivirus software, be sure to start it again.

Solaris or Linux

To remove installed components on a Solaris or Linux machine:

> **✓ Note**
>
> Before removing components, we recommend that you perform a full system backup as a fallback strategy.

1. Log on to the installation machine as the **root** user.

2. Close all applications and stop any antivirus software.

3. Run the following program from the Websense installation directory (default is `/opt/Websense`):

   `./uninstall.sh`

   Run the GUI version of the installer with the following command:

   `./uninstall.sh -g`

   If you are using a non-English based system, the installer will display an error message advising you that the GUI version is not supported.

   The installer detects the currently installed Websense components and displays a list of installed components. By default, all components are selected for removal.

   > **Warning**
   >
   > Do not uninstall the Policy Server without uninstalling all of the Websense components. Removing the Policy Server will sever communication with the remaining Websense components and will require the reinstallation of those components.

4. Make sure that only the components you want to remove are selected, and then select **Next** to continue.

   ■ **Policy Server status**: If the Policy Server is not running, a dialog box appears advising you that removing Websense components may require communication with the Policy Server. You may exit the installer to restart the Policy Server, or continue uninstalling the selected components.

   > **Warning**
   >
   > If the Policy Server is not running, the files for the selected components will be removed, but not the information about the components recorded in the `config.xml` file. This could cause problems if you decide to add these components again at a later date.

   ■ **Summary list**: A summary list of the components you have selected to remove appears. Select **Next** to remove these components.

- **Network Agent**: If you are uninstalling Network Agent on a remote machine after removing the Policy Server, expect the process to take several minutes. Network Agent will be successfully uninstalled, although no progress notification will be displayed.

- **Completion**: A completion message advises you when the procedure is finished.

5. Exit the installer.

6. If you stopped your antivirus software, be sure to start it again.

Repairing an Installation

If a component fails to install properly, or is not performing normally, you can run the Websense installer again and *repair* the installation. This procedure does not troubleshoot components, but merely replaces missing files.

> ✔ **Note**
>
> To repair (reinstall) a Policy Server in a distributed environment, see *Repairing the Policy Server*, page 174 for instructions.

Windows

To repair your Websense Enterprise or Web Security Suite installation in a Windows environment:

> ✔ **Note**
>
> Before repairing components, we recommend that you perform a full system backup as a fallback strategy.

1. Log on to the installation machine with **domain** and **local** administrator privileges.

   If you are repairing User Service or DC Agent, this will assure that they have administrator privileges on the domain.

> **Important**
>
> User Service and DC Agent must have administrator
> privileges on the network to retrieve user login information
> from the domain controller. Without this information,
> Websense software cannot filter by users and groups. If
> you cannot install these components with such privileges,
> you can configure domain administrator privileges for
> these services after installation. For instructions, see
> *Configure Domain Administrator Privileges*, page 202.

2. Back up the following files to a safe location:

   - `config.xml`
   - `websense.ini`
   - `eimserver.ini`

3. Close all applications and stop any antivirus software.

> **Warning**
>
> Be sure to close the Windows Event Viewer, or the repair
> may fail.

4. Run the Websense Enterprise or Web Security Suite installer.

5. Click **Next** in the welcome screen.

   The installer detects the current Websense installation and asks if you
   want to add, remove, or repair components.

6. Select **Repair existing Websense components** and click **Next**.

   The installer advises you that it will repair the current installation by
   reinstalling the existing Websense components and asks if you want to
   continue.

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

   A list of currently running Websense services appears. The message
   explains that the installer will stop these services before installation.

8. Click **Next** to begin installation.

The installer compares the system requirements for the installation you have selected with the resources of the installation machine. If the machine has inadequate disk space or memory, separate warnings are displayed.

- If the installation machine has insufficient disk space, the selected components cannot be installed, and the installer will quit.

- If the installation machine has less than the recommended amount of memory, the installation can continue. To ensure the best performance of the components you are installing, you should upgrade your machine's memory to the recommended amount.

A progress message appears while the installer shuts down Websense services.

If you are using the online installer, the Download Manager progress bars are displayed as the appropriate installer files are downloaded from the Websense website. Installation begins automatically when the necessary files have been downloaded.

9. If you are repairing Filtering Service, the installer asks if you want to download the Websense Master Database now or at a later time using Websense Manager. Select a database download option and click **Next**.

> **Warning**
>
> During repair of the Filtering Service, the installer removes the existing Master Database. Websense filtering cannot resume until the new Master Database has been successfully downloaded, decompressed, and loaded. This 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.

If you have chosen to download the Master Database now, a progress bar appears. The database must first be downloaded from the internet, and then decompressed and loaded into local memory. Downloading the database from the internet can take a few minutes or more than 30 minutes, depending on factors such as internet connectivity, bandwidth, time of day, and your location relative to the download server. Decompressing and loading the database can take a few minutes or more than 30 minutes, depending on factors such as available memory, free disk space, and server process utilization.

When the database has finished loading, a message appears advising you of the status of the download. Click **Next** to continue.

10. When a message announcing successful completion of the installation is displayed:

    ■ If you chose a non-English language installer, click **Next** to continue. The Websense Language Pack installer starts. Follow the onscreen instructions to update Websense components with text in the selected language.

    ■ If you chose an English language installer:

        • If Websense Manager was not repaired, no further action is required and you can click **Finish** to exit the installer.

        • If Websense Manager was repaired, click **Next** to continue. The installer displays a screen asking if you want to launch Websense Manager. If you do not want to launch Manager, clear the checkbox. Click **Finish** to exit the installer.

11. If you stopped your antivirus software, be sure to start it again.

Solaris or Linux

To repair Websense Enterprise or Web Security Suite components on a Solaris or Linux machine:

> ✔ **Note**
> Before repairing components, we recommend that you perform a full system backup as a fallback strategy.

1. Log on to the installation machine as the **root** user.

2. Close all applications and stop any antivirus software.

3. Run the installation program from the directory where it resides by entering the following command:

   `./install.sh`

   To run the GUI version of the installer, use the following command:

   `./install.sh -g`

   If you are using a non-English based system, the installer will display an error message advising you that the GUI version is not supported.

The installer detects the currently installed Websense components and asks you what action you want to take.

4.   Select **Repair existing Websense components**, and select **Next** to advance through the procedure.

- **Repair components**: The installer advises you that it will repair the current installation by reinstalling the existing Websense components.

- **Websense services**: A list of currently running Websense services appears. The message explains that the installer will stop these services before continuing with the installation.

- **Web browser**: If you are repairing Websense Manager, the installer prompts you for the location of the browser.

- **System requirements check**: The installer compares the system requirements for the installation you have selected with the resources of the installation machine. If the machine has inadequate disk space or memory, separate warnings are displayed.

  - If the installation machine has insufficient disk space, the selected components cannot be installed, and the installer will quit.

  - If the installation machine has less than the recommended amount of memory, the installation will continue. To ensure the best performance of the components you are installing, you should upgrade your machine's memory to the recommended amount.

- **Services restarted**: The Websense services are restarted after the files are reinstalled.

- **Master Database Download**: If you are repairing Filtering Service, the installer asks if you want to download the Websense Master Database now or at a later time using Websense Manager. Select a database download option and then select **Next** to continue.

> ⚠️ **Warning**
>
> During repair of the Filtering Service, the installer removes the existing Master Database. Websense filtering cannot resume until the new Master Database has been successfully downloaded, decompressed, and loaded. This 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.

If you have chosen to download the Master Database now, the download begins. The database must first be downloaded from the internet, and then decompressed and loaded into local memory. Downloading the database from the internet can take a few minutes or more than 30 minutes, depending on factors such as internet connectivity, bandwidth, time of day, and your location relative to the download server. Decompressing and loading the database can take a few minutes or more than 30 minutes, depending on factors such as available memory, free disk space, and server process utilization.

When the database has finished loading, a message appears advising you of the status of the download. Select **Next** to continue.

5. When a message announcing successful completion of the installation is displayed:

   - If you chose a non-English language installer, select **Next** to continue. The Websense Language Pack installer starts. Follow the onscreen instructions to update Websense components with text in the selected language.

   - If you chose an English language installer:

     • If you are installing in GUI mode, and Websense Manager was repaired, select **Next** to continue. The installer asks if you want to start Websense Manager. Make a choice and select **Finish** to exit the installer.

     • Otherwise, select **Finish** to exit the installer.

6. If you stopped your antivirus software, be sure to start it again.

Repairing the Policy Server

It may become necessary to repair (reinstall) the Policy Server in a distributed environment. Unless this is done correctly, communication with components installed on separate machines will be broken.

To repair the Policy Server and preserve the connection between distributed components:

> **Note**
>
> Before repairing components, we recommend that you perform a full system backup as a fallback strategy.

1. Stop the Policy Server. For instructions, see *Stopping or Starting Websense Services*, page 176.

2. Make a backup copy of the `config.xml` file and put it in a safe location.

> ✔ **Note**
>
> If you cannot make a backup copy of the current configuration file due to a system crash or other hardware problems, you can use the most recent backup copy of the file saved to a shared network drive to restore the system.

3. Restart the Policy Server.

4. Stop the services of the distributed Websense components on the individual machines. For instructions, see *Stopping or Starting Websense Services*, page 176.

5. Close all applications on the Policy Server machine, and stop any antivirus software.

6. Run the Websense installer on the Policy Server machine.

   The installer detects installed Websense components and asks you what action you want to take.

7. Select **Repair existing Websense components** when prompted.

   For specific instructions, see *Repairing an Installation*, page 169.

8. When the installer is finished repairing the system, exit the installer and stop the newly installed Policy Server.

9. Replace the `config.xml` file created by the repair procedure with your backup copy.

10. Restart the Policy Server.

11. If you stopped your antivirus software, be sure to start it again.

12. Restart the services of the Websense components on other machines.

13. Use Websense Manager to reload the Websense Master Database.

Stopping or Starting Websense Services

By default, Websense services are configured to start automatically when the computer is started.

Occasionally you may need to stop or start a Websense service. For example, you must stop the Filtering Service whenever you edit the `websense.ini` file, and after customizing default block messages.

> **Note**
>
> When Filtering Service is started, CPU usage can be 90% or more for several minutes while the Websense Master Database is loaded into local memory.

Manually Stopping Services

Certain Websense components must be stopped and started in a prescribed order. Optional components may be stopped and started in any order.

Optional Components

You can manually start or stop these Websense services in any order.

◆ eDirectory
◆ RADIUS Agent
◆ DC Agent
◆ Real-Time Analyzer
◆ Logon Agent
◆ Usage Monitor
◆ Remote Filtering Server

Principal Components

The following list is the preferred order for stopping the components. Start or stop optional components before stopping the components on this list. Policy Server should always be stopped last.

1. Network Agent
2. Filtering Service

3. User Service

4. Policy Server

When restarting Websense services, reverse the order, starting with the Policy Server first. In Linux and Solaris, a command stops and starts components in the proper order.

Windows

Stop, start, or restart a Websense service by using the **Services** dialog box. Restarting stops the service, then restarts it again immediately from a single command.

To stop or start Websense services on a Windows machine:

1. From the **Control Panel**, select **Administrative Tools > Services**.

2. Scroll down the list of available services and select a Websense service.
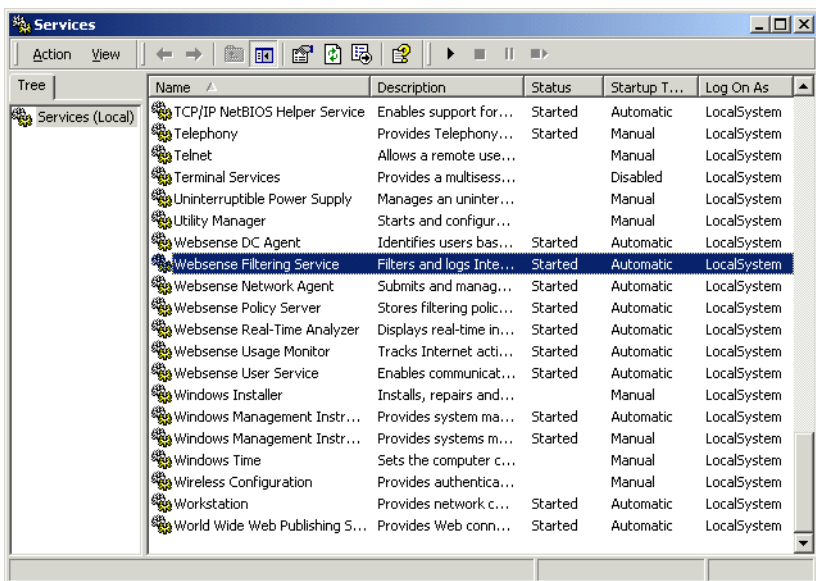
Windows 2000 Services List
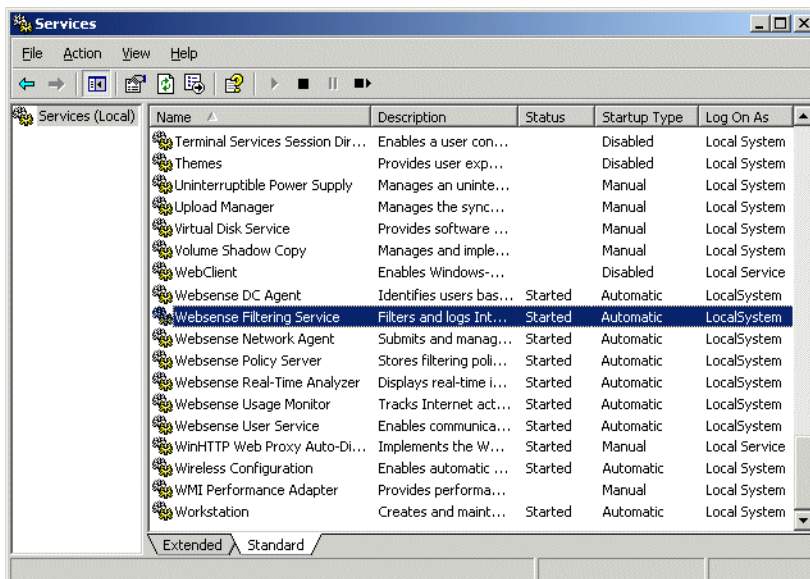
Windows Server 2003 Services List

3. From the **Action** menu, select **Start**, **Stop**, or **Restart** or click one of the control buttons in the toolbar (**Stop** ■ , **Start** ▶ , or **Restart** ■ ▶). **Restart** stops the service, then restarts it again immediately from a single command.

> **Warning**
>
> DO NOT use the taskkill command to stop Websense services. This procedure may corrupt the services.

Solaris and Linux

You can stop, start, or restart Websense services on a machine from a command line on a Solaris or Linux machine. Restarting stops the services, then restarts them again immediately from a single command. If the components are spread across multiple machines, be sure that Policy Server is stopped last and started first. See *Principal Components*, page 176 for the preferred stopping and starting order.

1. Go to the /Websense directory.

2. Use the following commands to stop, start, or restart all Websense services in the correct order:

   - `./WebsenseAdmin stop`
   - `./WebsenseAdmin start`
   - `./WebsenseAdmin restart`

3. View the running status of all Websense services with the following command:

   `./WebsenseAdmin status`

Warning

DO NOT use the `kill -9` command to stop Websense services. This procedure may corrupt the services.

CHAPTER 5 | Initial Setup

This chapter provides initial setup and configuration procedures for preparing your Websense software to communicate with the Squid Web Proxy Cache.

After installing the Websense software and your integration product, perform the following tasks to complete the setup process.

◆ If you did not download the Websense Master Database during installation, use Websense Manager and your Websense subscription key to download the database. See *Subscription Key and Master Database Download*, page 183 for instructions.

◆ If the Filtering Service is installed on a multihomed machine, identify the Filtering Service by its IP address in your network so that Websense block messages can be sent to users. See *Identifying the Filtering Service for the Block Page URL*, page 187 for instructions.

◆ All Windows workstations being filtered must have the Messenger Service enabled to receive protocol block messages. See *Displaying Protocol Block Messages*, page 188 for instructions.

◆ If the Logon Agent was installed, you must create a logon script for your users that will identify them transparently as they log on to a Windows domain. See *Creating and Running the Script for Logon Agent*, page 189 for instructions.

◆ If Network Agent was installed, the IP addresses of all proxy servers through which workstations route their internet requests must be defined. See *Identifying the Proxy Server for Network Agent*, page 196 for instructions.

◆ If Network Agent was installed on a machine with multiple network interface cards (NICs), you can configure Network Agent to use more than one NIC. See *Configuring Network Agent to use Multiple NICs*, page 199.

◆ If Network Agent was installed, use the Traffic Visibility Tool to test whether Network Agent can see the user internet traffic that you want it to monitor. See *Testing Visibility of Internet Traffic to Network Agent*, page 199.

◆ If you were unable to grant User Service or DC Agent administrator privileges during installation, do so now to ensure that they will function correctly. See *Configure Domain Administrator Privileges*, page 202.

◆ To block HTTPS traffic, you must configure Squid appropriately. See *HTTPS Blocking*, page 203 for instructions.

◆ Configure your firewall or internet router appropriately. See *Configuring Firewalls or Routers*, page 204 for instructions.

◆ Configure internet browsers on user workstations. See *User Workstation Configuration*, page 204 for instructions.

◆ If you installed Websense Web Security Suite, activate your subscription to the Websense Web Protection Services™: SiteWatcher™, BrandWatcher™, and ThreatWatcher™. See *Activating the Websense Web Protection Services™*, page 204 for instructions.

◆ If the optional Remote Filtering components were installed, the firewalls in your network must be configured to allow correct filtering of remote users. See *Firewall Configuration for Remote Filtering*, page 206 for instructions.

◆ If you are using the optional Remote Filtering feature, you can configure how internet access requests from remote users are handled when the Remote Filtering Service is unavailable. See *Blocking remote users' internet access when Remote Filtering is unavailable*, page 207 for instructions.

◆ If you are using the optional Remote Filtering feature, you can configure the size of the Remote Filtering Client's log file. See *Configuring the Remote Filtering Client Log*, page 208 for instructions.

For additional Websense configuration information, see the *Administrator's Guide* for Websense Enterprise and Web Security Suite.

Subscription Key and Master Database Download

The Websense Master Database is the basis for filtering, and is updated daily by default. It is downloaded from a remote database server so that your version is the most current.

For the database download to occur, the machine running the Websense Filtering Service must have internet access to the download servers at the following URLs:

◆ download.websense.com

◆ ddsdom.websense.com

◆ ddsint.websense.com

◆ portal.websense.com

◆ my.websense.com

Make sure that these addresses are permitted by all firewalls, proxy servers, routers, or host files that control the URLs that the Filtering Service can access.

If you did not enter a subscription key to download the Master Database during installation, follow the instructions below to enter your key and download the Master Database now.

> ✔ **Note**
> If you have just upgraded your Websense software, your subscription key was retained by the installer and these steps are not necessary.

To download the Master Database:

1. Launch Websense Manager on any machine where it is installed.

   ■ **Windows 2000 Server**: Select **Start > Programs > Websense > Websense Manager**, or double-click the Websense Manager icon on the desktop.

   ■ **Windows Server 2003**: Select **Start > All Programs > Websense > Websense Manager**, or double-click the Websense Manager icon on the desktop.

- **Solaris or Linux**: Go to the /Manager subdirectory in the Websense installation directory (by default, opt/Websense/Manager) and enter:

      ./start_manager

2. For a first-time installation, if Policy Server was not installed with Websense Manager, the **Add Policy Server** dialog box appears the first time you open Websense Manager.

    a. Enter the IP address or machine name of the machine on which you installed the Policy Server, and the configuration port established during installation (default is 55806).

    b. Click **OK**. The Policy Server machine's IP address or machine name appears beside a server icon in the Manager's navigation pane.

3. Double-click the icon of the Policy Server in the navigation pane.

    For a first-time installation, the **Set Websense Password** dialog box appears.

4. Set a password (between 4 and 25 characters) for the Policy Server.

> ✔ **Note**
>
> Retain this password. It must be entered when you connect to this Policy Server from this or any other Websense Manager, and when you log on to the Reporting Tools web interface.

5. Click **OK**.

    - If you have not yet entered your subscription or evaluation key, the **Settings** dialog box appears with the **Database Download** pane displayed.

    - If you entered your key during installation, navigate to the database download settings pane by selecting **Server** > **Settings** > **Database Download**.
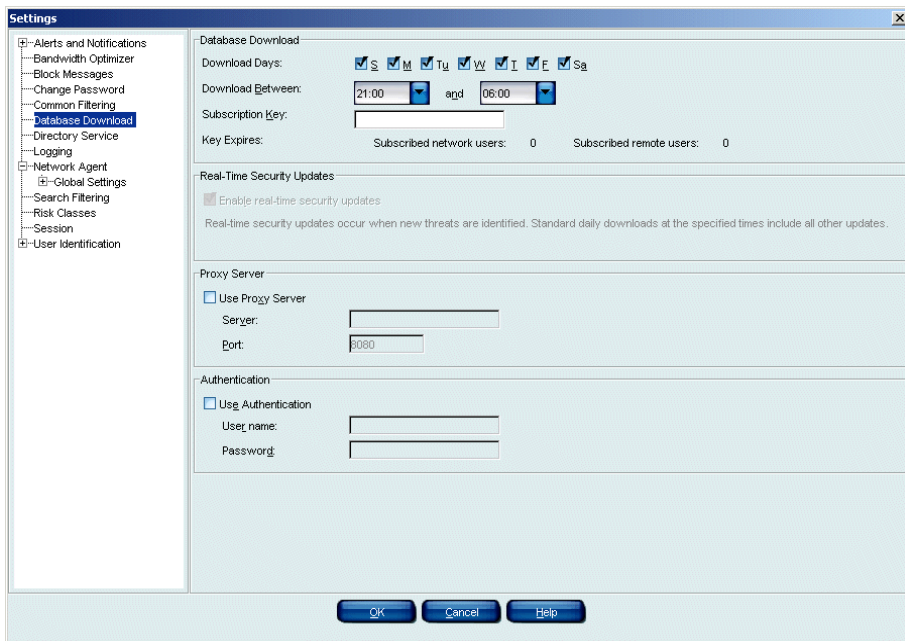
Database Download Settings

6. Enter your alphanumeric key in the **Subscription Key** field.

    The **Subscribed network users** and **Subscribed remote users** fields show a value of **0** until the database is successfully downloaded.

7. If your network requires that browsers use an upstream proxy server to reach the internet, the same proxy settings used by the browser must be used for downloading the Websense Master Database. Establish the proxy settings for the database download as follows:

    a. Check **Use Proxy Server**.

    b. Identify the upstream proxy server or firewall by entering the machine's IP address or machine name in the **Server** field.

        Supported machine name formats are as follows:

        •   **Windows**: 7-bit ASCII and UTF-8 characters. The DNS server must be able to recognize UTF-8 characters and resolve the name into an IP address. Do NOT use a machine name that has extended ASCII or double-byte characters.
        •   **Solaris or Linux**: 7-bit ASCII only.

✓ **Note**
If Websense software is installed on a proxy server machine in your network, *do not* enter that IP address in your proxy settings. Use **localhost** instead.

    c. Enter the **Port** of the upstream proxy server or firewall (default is 8080).

8. If your network requires authentication to an upstream proxy server or firewall to reach the internet and download the Websense Master Database, perform the following procedure:

    a. Check **Use Authentication**.

    b. Be sure to configure the upstream proxy server or firewall to accept clear text or basic authentication (to allow download of the Master Database).

    c. Enter the **User name** required by the upstream proxy server or firewall to download the Master Database.

    d. Enter the **Password** required by the upstream proxy server or firewall.

9. Click **OK** to save your changes.

The Websense Filtering Service automatically contacts the Websense database server and begins downloading the Master Database. The status of the download is displayed in the **Database Download** dialog box. When the download has completed, the **Last Download Result** field displays **Successful**.

10. Click **Close** in the **Database Download** dialog box when the download is complete.

✓ **Note**
After downloading the Master Database or updates to the Master Database, and when the Filtering Service is started, CPU usage can be 90% or more while the database is loaded into local memory.

To download the Websense Master Database manually at any time, choose **Server** > **Database Download** in Websense Manager.

Identifying the Filtering Service for the Block Page URL

If the Filtering Service is installed on a multihomed machine (with two or more network interface cards), you must identify the Filtering Service by its IP address in your network so that Websense block messages can be sent to users.

When Websense software blocks an internet request, the user's browser is redirected by default to a block message page hosted by the Filtering Service. The block page URL typically takes the form:

> **http://**<*WebsenseServerIPAddress*>**:**<*MessagePort*>**/cgi-bin/
> blockpage.cgi?ws-session=**#########

If the Filtering Service machine name, rather than the IP address, is contained in the block page URL, users could see a blank page instead of the block message that tells them why the site is blocked.

Identify the Filtering Service by IP address to ensure that block pages display correctly on users' workstations:

◆ If you have an internal DNS server, associate the machine name of the Filtering Service machine with its correct (typically internal) IP address by entering the IP address as a resource record in your DNS server. See your DNS server documentation for instructions.

◆ If you do not have internal DNS, add an entry to the `eimserver.ini` file by following these instructions:

1. On the Filtering Service machine, go to the `\bin` folder in the Websense installation directory (by default, `Websense\bin`).

2. Make a backup copy of the `eimserver.ini` file and store it in another folder.

3. Open the original `eimserver.ini` file in a text editor.

4. In the `[WebsenseServer]` area, enter the following command on a blank line:

   ```
   BlockMsgServerName=<IP address>
   ```

   where `<IP address>` is the correct (typically internal) IP address of the machine running Filtering Service.

Important

Do not use the loopback address 127.0.0.1.

---

5. Save the file.

6. Stop and then restart the Filtering Service (see *Stopping or Starting Websense Services*, page 176).

Displaying Protocol Block Messages

Websense software will filter protocol requests normally whether or not protocol block messages are configured to display on user workstations.

Protocol block messages cannot be displayed on the following workstation operating systems:

◆ Solaris

◆ Linux

◆ Macintosh

> ✔ **Note**
>
> Windows XP Service Pack 2 only displays protocol block messages under the following conditions:
>
> ◆ The firewall function must be either be disabled or modified not to block the messages.
>
> ◆ The Windows Messenger service must be started.

For users to view protocol block messages in Windows NT, Windows 2000, and Windows Server 2003:

◆ Make sure that the User Service has administrator privileges. For instructions, see *Configure Domain Administrator Privileges*, page 202.

◆ Make sure the Messenger Service is enabled on *each* client workstation that is being filtered. If you have activated Websense protocol management, check the Windows **Services** dialog box to see if the Messenger Service is running. If your company policy requires the Messenger Service to be disabled, you should advise your users that certain protocols will be blocked without notification.

To view protocol block messages on a Windows 98 machine, you must start winpopup.exe, found in the Windows directory of your local drive. You can start this application from a command prompt or configure it to start

automatically by copying it into the Startup folder. For instructions, see your operating system documentation.

Creating and Running the Script for Logon Agent

If you have installed Websense Logon Agent, you must create a logon script for your users that will identify them transparently as they log on to a Windows domain. Identification is accomplished by the Websense `LogonApp.exe` application, which provides a user name and IP address to the Logon Agent each time a Windows client machine connects to an Active Directory or a Windows NTLM directory service.

Prerequisites for Running the Logon Script

Make the following network preparations so that the Websense logon script can execute properly on users' Windows workstations:

◆ Be sure that all workstations can connect to the shared drive on the domain controller where the logon script and `LogonApp.exe` will be placed. To determine if a workstation has access to the domain controller, run the following command from a Windows command prompt:

```
net view /domain:<domain name>
```

◆ NetBIOS for TCP/IP must be enabled. In Windows 98, TCP/IP NetBIOS is enabled by default.

◆ The TCP/IP NetBIOS Helper Service must be running on each client machine that will be identified by Logon Agent. This service runs on Windows 2000, Windows XP, Windows Server 2003, and Windows NT®.

File Location

All relevant files are located in the `Websense\bin` folder on the Logon Agent machine:

◆ `LogonApp.exe`: the Websense executable that communicates user information to the Logon Agent.

◆ `Logon.bat`: batch file containing sample logon and logout scripts.

◆ `LogonApp_ReadMe.txt`: a summary of the procedures for creating and running the Websense logon script and optional logout script.

Deployment Tasks

To deploy `LogonApp.exe` with a logon script, perform the following tasks:

Task 1: Prepare the logon script: Edit the parameters in the sample script file (`Logon.bat`) to suit your needs. This file contains two sample scripts: a logon script and a logout script. Active Directory can use both types of scripts. If you plan to use both types, you will need two separate `.bat` files with different names.

Task 2: Configure the script to run: You can run your logon script from Active Directory or Windows NTLM directory services using group policies. This requires you to move the Websense executable and logon batch file to a shared drive on the domain controller that is visible to all user workstations. If you use Active Directory, you may create and deploy an optional logout batch file on the shared drive.

Preparing the Logon Script

A batch file, called `Logon.bat`, is installed with Logon Agent in the `Websense\bin` folder. This file contains some instructions for using the scripting parameters, and two sample scripts: a logon script that runs `LogonApp.exe`, and a logout script for Active Directory that removes user information from the Websense user map when the user logs out.

Script Parameters

Using the samples provided, construct a script for your users that employs the parameters in the following table. The required portion of the script is:

```
LogonApp.exe http://<server>:<port>
```

This command runs `LogonApp.exe` in *persistent* mode (the default), which sends user information to the Logon Agent at predefined intervals.

> **Note**
>
> You can edit the sample, or create a new batch file containing a single command.

Parameter	Description
<server>	IP address or name of the machine running the Websense Logon Agent. This must match the machine address or name entered when you configured Logon Agent in Websense Manager.
<port>	The port number used by Logon Agent. Enter 15880 if you accepted the default port number when you configured Logon Agent in Websense Manager.
/NOPERSIST	Causes LogonApp.exe to send user information to the Logon Agent at logon only. The user name and IP address are communicated to the server at logon and remain in the Websense user map until the user's data is automatically cleared at a predefined time interval. The default interval is 24 hours. If the NOPERSIST parameter is not present, LogonApp.exe operates in the *persistent* mode. In persistent mode, LogonApp.exe resides in memory on the domain server and updates the Logon Agent with the user names and IP addresses at predefined intervals. The default interval is 15 minutes. For information about configuring Logon Agent via Websense Manager, see the User Identification chapter in the *Administrator's Guide* for Websense Enterprise and Web Security Suite.
/COPY	Copies the LogonApp.exe application to the users' machines, where it is run by the logon script from local memory. This optional parameter can be helpful if you experience any hangs with your logon script. The application is copied into the %USERPROFILE%\Local Settings\Temp folder. COPY can be used only in the *persistent* mode.
/VERBOSE	Debugging parameter that must be used only at the direction of Technical Support.
/LOGOUT	(Used only in an optional logout script) Removes the user's logon information from the Websense user map when the user logs off. If you use Active Directory, you can use this parameter to clear the logon information from the user map before the interval defined in Logon Agent has elapsed. Use this optional parameter in a logout script in a different batch file than the one containing the logon script. See the example scripts below.

Websense User Map and the Persistent Mode

User identification provided at logon by `LogonApp.exe` is stored in the Websense user map. This information is updated periodically if `LogonApp.exe` is run in persistent mode. The update time interval for the persistent mode and the interval at which the user map is automatically cleared of logon information are configured in the **Logon Agent** tab of the **Settings** dialog box in Websense Manager. In Active Directory, if you decide to clear the logon information from the Websense user map before the interval defined in the Manager, you can create an accompanying logout script. You cannot configure a logout script with Windows NTLM.

In the non-persistent mode, information in the user map is created at logon and is not updated. The use of the non-persistent mode creates less traffic between the Websense software and the workstations in your network than does the persistent mode.

For detailed information about configuring Logon Agent in Websense Manager, see the User Identification chapter in the *Administrator's Guide* for Websense Enterprise and Web Security Suite.

Examples

The following are examples of commands for a logon script and the companion logout script that might be run in Active Directory. The two scripts must be run from separate batch files.

◆ **Logon Script:** In this example, the edited `Logon.bat` file contains this single command:

```
LogonApp.exe http://10.2.2.95:15880 /NOPERSIST
```

The sample script above sends user information to the Logon Agent at logon only. The information is not updated during the user's session (`NOPERSIST`). The information is sent to port 15880 on the server machine identified by IP address 10.2.2.95.

With Active Directory you have the option to clear the logon information for each user as soon as the user logs out. (This alternative is not available with Windows NTLM.) To accomplish this, you create a companion logout script in a different batch file.

◆ **Logout Script:** Continuing the example, copy the logon batch file and rename it `Logout.bat`. Then edit the script in `Logout.bat` as shown here:

```
LogonApp.exe http://10.2.2.95:15880 /NOPERSIST /LOGOUT
```

Configuring the Logon Script to Run

You can configure your logon script to run with a group policy on Active Directory or on a Windows NTLM directory service.

✔ **Note**

The following procedures are specific to Microsoft operating systems and are provided here as a courtesy. Websense, Inc., cannot be responsible for changes to these procedures or to the operating systems that employ them. For more information, see the links provided.

Active Directory

If your network uses Windows 98 client machines, go to the Microsoft website for assistance.

To configure a logon script (and optional logout script) using Active Directory:

1. Make sure your environment meets the conditions described in *Prerequisites for Running the Logon Script*, page 189.
2. On the Active Directory machine, go to the Windows **Control Panel** and select **Administrative Tools > Active Directory Users and Computers**.
3. Right-click the domain and select **Properties**.

   The domain **Properties** dialog box appears.
4. Select the **Group Policy** tab.
5. Click **New** and create a policy called **Websense Logon Script**.
6. Double-click your new policy or click **Edit** to edit the policy.

   The **Group Policy Object Editor** dialog box appears.
7. In the tree structure displayed, expand **User Configuration**.
8. Expand the **Windows Settings** structure.

9. Select **Scripts (Logon/Logoff)**.

10. In the right pane, double-click **Logon**.

11. In the **Logon Properties** dialog box displayed, click **Show Files** to open the logon script folder for this policy.

    The folder opens in a Windows Explorer window.

12. Copy two files into this folder: your edited logon batch file (Logon.bat) and the application LogonApp.exe.

13. Close the Explorer window and click **Add** in the **Logon Properties** dialog box.

    The **Add a Script** dialog box appears.

14. Enter the file name of the logon batch file (Logon.bat) in the **Script Name** field or browse for the file.

15. Leave the **Script Parameters** field empty.

16. Click **OK** twice to accept the changes.

17. (Optional.) If you have prepared a logout script, repeat Step 7 through Step 16. Choose **Logoff** at Step 10, and use your logout batch file whenever you are prompted to copy or name the batch file.

18. Close the **Group Policy Object Editor** dialog box.

19. Click **OK** in the domain **Properties** dialog box to apply the script.

20. Repeat this procedure on each domain controller in your network as needed.

✔ **Note**

You can determine if your script is running as intended by configuring your Websense software for manual authentication. If transparent authentication with Logon Agent fails for any reason, users will be prompted for a user name and password. Advise your users to notify you if this occurs. To enable manual authentication, follow the instructions in the User Identification chapter of the *Administrator's Guide* for Websense Enterprise and Web Security Suite.

For additional information about deploying logon scripts to users and groups in Active Directory, please see:

Windows NTLM

To configure the Websense logon script in Windows NTLM:

1. Make sure your environment meets the conditions described in *Prerequisites for Running the Logon Script*, page 189.

2. Copy the `Logon.bat` and `LogonApp.exe` files from the `Websense\bin` folder on the Logon Agent machine to the netlogon share directory on the domain controller machine.

   ```
   C:\WINNT\system32\Repl\Import\Scripts
   ```

   Depending on your configuration, you may need to copy these files to other domain controllers in the network to run the script for all your users.

3. In the **Control Panel** of the domain controller, select **Administrative Tools > User Manager for Domains**.

4. Select the users for whom the script must be run and double-click to edit the user properties.

   The **User Properties** dialog box appears.

5. Click **Profile**.

   The **User Environment Profile** dialog box appears.

6. Enter the path to the logon batch file in the **User Profile Path** field (from Step 2).

7. Enter the name of the logon batch file (`Logon.bat`) in the **Logon Script Name** field.

8. Click **OK**.

9. Repeat this procedure on each domain controller in your network as needed.

> ✔ **Note**
>
> You can determine if your script is running as intended by configuring your Websense software for manual authentication. If transparent authentication with Logon Agent fails for any reason, users will be prompted for a user name and password. Advise your users to notify you if this occurs. To enable manual authentication, follow the instructions in the User Identification chapter in the *Administrator's Guide* for Websense Enterprise and Web Security Suite.

For additional information about creating and deploying logon scripts to users in Windows NTLM, please see:

http://windows.about.com/library/weekly/aa031200a.htm

Identifying the Proxy Server for Network Agent

If you have installed Network Agent, you must provide the IP addresses of all Squid machines through which internet requests from the workstations monitored by Network Agent are routed. Without this address, Network Agent cannot filter or log requests properly.

To define proxy server IP addresses:

1. Open Websense Manager and connect to the Policy Server.
2. Select **Server > Settings**.

   The **Settings** dialog box appears.
3. In the left pane, click the plus sign beside **Network Agent** to expand the tree.
4. Click the plus sign beside **Global Settings**.
5. Select the IP address of the Network Agent you want to configure from the tree structure.
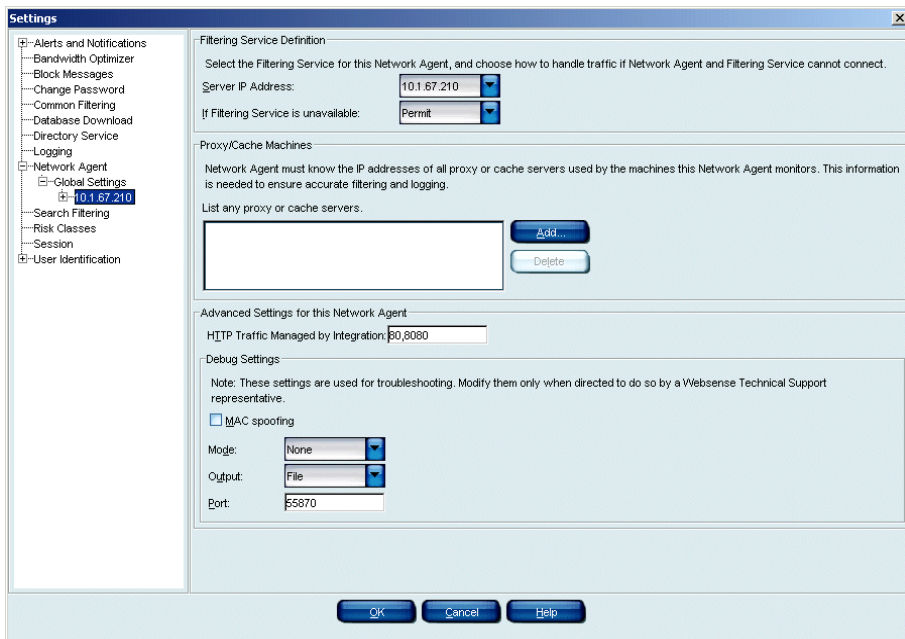
Network Agent Local Settings

6. In the **Proxy/Cache Machines** section of the right panel, click **Add**.

    A dialog box appears allowing you to define an IP address or a range of addresses.
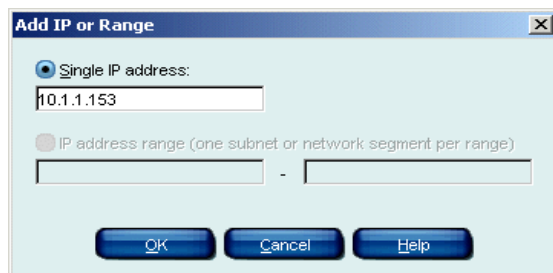
7. Enter an IP address and click **OK** to add the IP address to the list of proxy or cache servers.
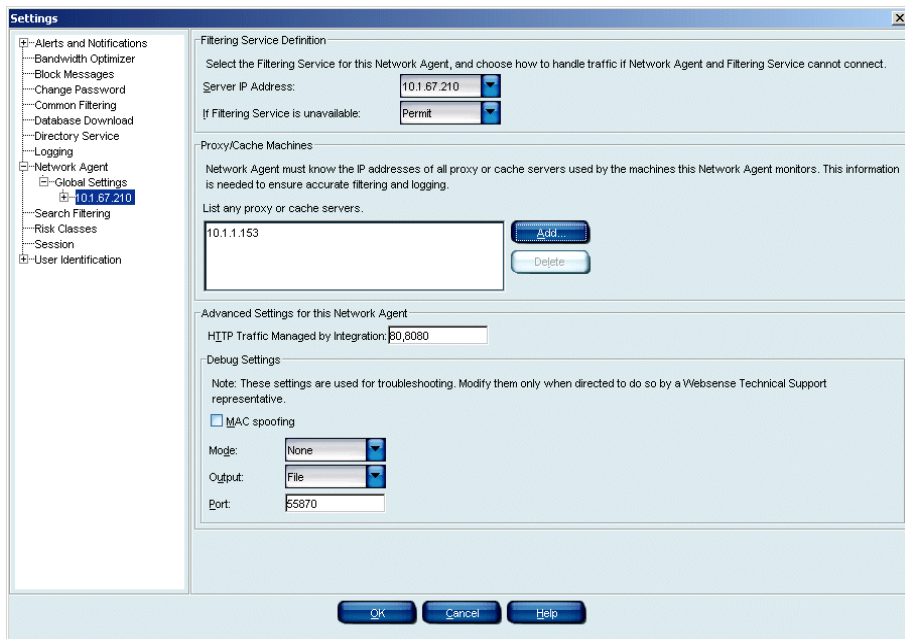
Proxy/Cache Server List

8. Repeat Step 6 and Step 7 for each proxy server in your network.

9. Click **OK** to save your changes.

For additional information about configuring Network Agent, see the Network Agent chapter in the *Administrator's Guide* for Websense Enterprise and Web Security Suite.

Configuring Network Agent to use Multiple NICs

Each Network Agent instance must use at least one designated NIC. However, Network Agent is capable of using multiple NICs. If you installed Network Agent on a machine with multiple NICs, you can configure it to use different NICs for different purposes. For example, you can configure Network Agent to use one NIC for monitoring traffic, and another to send blocking information to Filtering Service.

To configure Network Agent to use additional NICs, follow the instructions in the Network Agent chapter in the *Administrator's Guide* for Websense Enterprise and Web Security Suite.

Testing Visibility of Internet Traffic to Network Agent

If you installed Network Agent and have any doubt about its ability to monitor internet requests from the desired network and to see the replies, you can conduct a traffic visibility test on the Network Agent machine using the Websense Traffic Visibility Tool.

Running the Websense Traffic Visibility Tool

Run the Websense Traffic Visibility Tool on the Network Agent machine to test internet traffic visibility. The NIC that Network Agent is configured to use must be able to monitor 2-way employee internet traffic for Network Agent to function properly.

1. To start the tool:

   - **Windows**: From the **Start** menu, choose **Programs** (or **All Programs**) > **Websense** > **Utilities** > **Traffic Visibility Tool**.

   - **Linux or Solaris**: Run `./TrafficVisibility.sh` from the Websense installation directory (`/opt/Websense`).

     To start a GUI version, run `./TrafficVisibility.sh -g`

The Websense Traffic Visibility Tool appears.
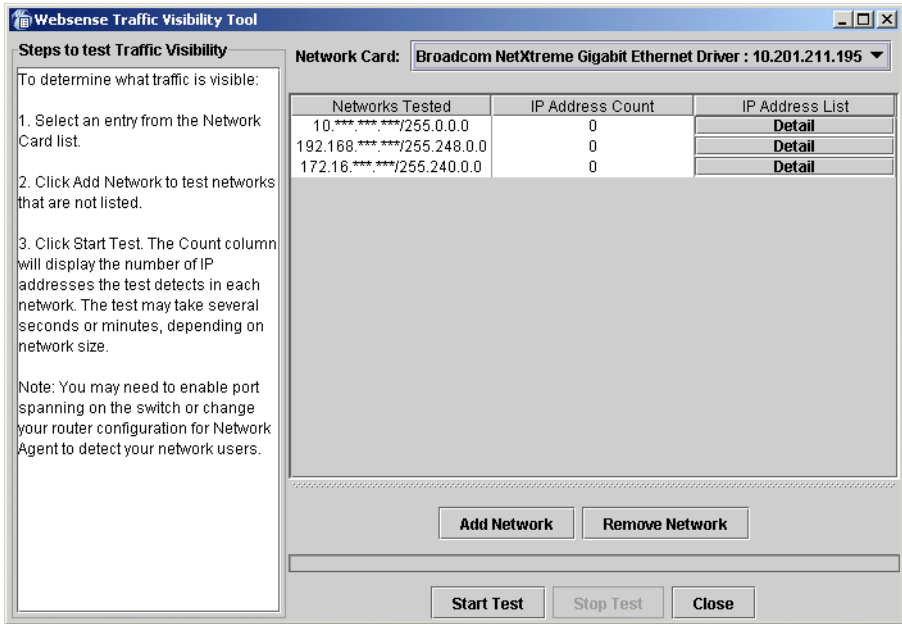
Traffic Visibility Tool

Field	Description
Network Card	Name of the network interface card (NIC) to test. Active cards on the installation machine appear in this list. Cards without an IP address will not appear in this list.
Networks Tested	Displays the netmasks that are being tested. You may use the defaults provided or add your own. These netmasks can reside in different network segments depending upon the IP address ranges to be filtered.
IP Address Count	Number of IP addresses for which traffic is detected during the test of a network.
IP Address List Detail	Lists all the IP addresses in the network from which internet traffic is being detected.

2. From the **Network Card** drop-down list, select the network interface card (NIC) that the Network Agent is configured to use.

A default list of networks (netmasks) to test appears. You may use the defaults provided or add your own. These netmasks can reside in different network segments depending upon the IP address ranges to be filtered.

3. If the network you want to test with the NIC does not appear in the default list, click **Add Network**.

The **Add Network** dialog box appears.

a. Enter a new netmask value in the **Network ID** field.

The subnet mask defaults to 255.0.0.0 and changes appropriately as the netmask is defined.

b. Click **OK** to return to the Websense Traffic Visibility Tool dialog box.

Your new network appears in the list.

4. Select **Remove Network** to delete a network from the list.

5. Click **Start Test** to begin testing all the networks in the list.

The counter in the **IP Address Count** column should begin recording internet traffic immediately from the networks listed. The counter increments each time the NIC detects an individual IP address from the target network in a passing packet. The activity bar at the bottom of the dialog box indicates that a test is in progress.

If the count for a network remains at zero or is very low, the selected NIC cannot see the traffic it is supposed to monitor.

6. If the Network Agent NIC is unable to see the desired traffic, perform one or both of the following tasks:

   ■ If the installation machine has multiple NICs, select a different card to test. If this card can see the desired traffic, configure Network Agent to use this card. For instructions, see the Network Agent chapter in the *Administrator's Guide* for Websense Enterprise and Web Security Suite.

   ■ Resolve network configuration issues to make sure that the NIC can see the desired traffic. This might involve connecting to a different router or configuring for port spanning in a switched environment. See *Chapter 2: Network Configuration* for deployment information. Make the necessary changes and retest the NIC.
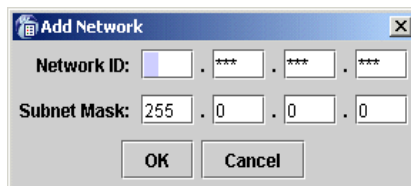
7. Click **Stop Test** when you are finished testing.

8. Click **Close** to exit the Traffic Visibility Tool.

The Network Agent NIC must be able to monitor all targeted internet traffic. If Network Agent cannot see the necessary traffic, you must either reposition the machine in the network, or select another machine on which to install the Network Agent.

Configure Domain Administrator Privileges

User Service and DC Agent must have administrator privileges on the network to retrieve user logon information from the domain controller. If you were not able to grant these privileges during installation, you can do so now.

User Service and DC Agent on Windows

If you were unable to grant User Service or DC Agent domain administrator privileges during installation on a Windows machine, you can edit the properties of these services now so that they can access directory service information. This procedure may vary slightly, depending upon the version of Windows you are using.

1. From the Control Panel on the installation machine, select **Administrative Tools > Services**.

2. In the **Services** dialog box, double-click **Websense User Service**.

3. Select the **Log On** tab in the **Properties** dialog box.

4. Select **This account** and enter a valid domain/user name and password for an account with **domain** administrator privileges in your network.

5. Click **OK**.

6. If DC Agent was installed, repeat the process for the **Websense DC Agent** service.

DC Agent on Linux

If you installed DC Agent on Linux, but were unable to grant it administrator privileges on the domain controller during installation, follow these steps.

1. In Websense Manager, select **Server > Settings**, and then select **Directory Service** in the left-hand pane.

2. Select **Windows NT Directory / Active Directory (Mixed Mode)**.
   (Make this selection even if you are not using Mixed Mode.)

3. Enter domain administrator credentials in the fields on the screen.

4. Click **OK**.

HTTPS Blocking

There are two options for blocking HTTPS traffic with a Squid integration:

◆ Install the Websense Network Agent, the Websense component that
performs protocol filtering, and configure it to block HTTPS traffic.

For information about installing Network Agent on a Windows machine,
see *Network Agent*, page 99. For information about installing Network
Agent on a Linux or Solaris machine, see *Network Agent*, page 138.
Detailed information about configuring Network Agent is provided in the
Network Agent chapter in the *Administrator's Guide* for Websense
Enterprise and Web Security Suite.

◆ If Squid is configured to act as a proxy server, you can configure Squid to
filter all HTTPS traffic.

To configure the Squid Web Proxy Server to filter all HTTPS traffic:

1. Open the wsSquid.ini file in a text editor. This file is located in the
   /etc/wsLib/ directory.

2. Under the **initSection** heading, change the value of the
   UseHTTPSBlockPage parameter to **yes**.

   The default setting for this parameter is **no**, causing Squid to permit
   all HTTPS traffic.

3. Save your changes.

4. Restart the Squid Web Proxy Server.

All requests for HTTPS pages will be filtered, but if a request is blocked,
Squid will send the user a Squid-generated error page. Users will not see a
Websense HTTP block page, because Squid does not have the ability to
take an HTTPS request from the user and return a Websense HTTP block
page.

Configuring Firewalls or Routers

To prevent users from circumventing Websense filtering, your firewall or internet router should be configured to allow outbound HTTP, HTTPS, FTP, and Gopher requests only from the Squid Web Proxy Cache. Contact your router or firewall vendor for information about configuring access lists on the router or firewall.

> **Important**
>
> If internet connectivity of Websense software requires authentication through a proxy server or firewall for HTTP traffic, the proxy or firewall must be configured to accept clear text or basic authentication to enable the Websense Master Database download.

User Workstation Configuration

User workstations must have a web browser that supports proxy-based connections and Java technology. Versions 4.0 or later of Microsoft Internet Explorer® or Netscape Navigator® and most newer browsers support proxy-based connections and Java technology.

Internet browsers on user workstations must be configured to use the Squid Server to handle HTTP, HTTPS, FTP, and Gopher requests. Browsers must point to the same port (default-3128) that the Squid Server uses for each protocol.

See your browser documentation for instructions to configure your browser to send all internet requests to the Squid Web Proxy Cache.

Activating the Websense Web Protection Services™

The Websense® Web Protection Services™—SiteWatcher™, BrandWatcher™, and ThreatWatcher™—protect your organization's websites, brands, and web servers. These services are included if you purchased a Web Security Suite subscription, but they must be activated.

To turn on ThreatWatcher, SiteWatcher, and BrandWatcher:

1. Go to www.my.websense.com, log in, and enter your Web Security Suite subscription key.
2. On your My Websense main page, go to the Websense Security Labs box.
3. Click the links beside each of the services in turn, and follow the onscreen instructions.

The following sections provide a brief description of each of the Web Protection Services. More information is available at www.websense.com.

SiteWatcher™

SiteWatcher alerts you when your organization's websites have been infected with malicious mobile code. SiteWatcher allows you to take immediate action to prevent its spread to customers, prospects, and partners who might visit the website.

BrandWatcher™

BrandWatcher alerts you when your organization's websites or brands have been targeted in phishing or malicious keylogging code attacks. BrandWatcher provides you with internet security intelligence, attack details, and other security-related information so that you can take action, including notifying your customers and minimizing any public relations impact.

ThreatWatcher™

ThreatWatcher provides you with a *hacker's-eye* view of your organization's web server, regularly scanning for known vulnerabilities and potential threats, and reporting on risk levels and recommended actions through a web-based portal. ThreatWatcher helps you prevent malicious attacks on your web servers before they happen.

Firewall Configuration for Remote Filtering

Remote Filtering is an optional Websense service that allows you to filter user workstations located outside your organization's network firewall. If you installed the Remote Filtering components, some firewall configuration is necessary to enable web filtering on remote workstations. Firewalls must be configured to allow the Remote Filtering Server to communicate with the remote workstations and with the Filtering Service.

Enabling communication between Remote Filtering Server and Remote User Workstations

The external network firewall and any additional firewalls located between the Remote Filtering Server machine and the remote workstations should be configured as follows:

◆ Open the Remote Filtering Server's **External Communication Port** on these firewalls to accept connections from Remote Filtering Clients on workstations located outside the network firewall. By default, this is port 80, unless it was changed during installation of the Remote Filtering Server.

◆ Block connections to the Remote Filtering Server's **Internal Communication Port** from workstations located outside the network firewall. By default, this is port 8800, unless it was changed during installation of the Remote Filtering Server.

See the documentation for your firewall product if you need information about how to accomplish these firewall configuration tasks.

Enabling communication between Remote Filtering Server and Filtering Service

If there is a firewall between the Remote Filtering Server machine and the Filtering Service machine, configure it as follows:

◆ Open the Filtering Service's **Filter port** (by default, 15868) on this firewall to accept connections from the Remote Filtering Server.

◆ Open the Filtering Service's **Block Page port** (by default, 15871) on this firewall to allow Filtering Service to serve block pages to remote users.

See the documentation for your firewall product if you need information about how to accomplish these firewall configuration tasks.

Blocking remote users' internet access when Remote Filtering is unavailable

If you are using the optional Websense Remote Filtering feature, you can configure it to block remote users' internet access when they are unable to connect with the Remote Filtering Server. You can also configure the length of time that the Remote Filtering Client on a remote user's machine will attempt to connect with a Remote Filtering Server before failing closed and blocking access to all websites.

This behavior is controlled by the following two parameters in the `securewispproxy.ini` file on the Remote Filtering Server machine:

◆ **FailClose**: The `FailClose` parameter specifies whether a Remote Filtering Client fails open or closed when connectivity with the Remote Filtering Server is lost.

- When set to `false`, the Filtering Client fails open and all HTTP traffic is allowed. The default value is `false`.

- When set to `true`, the Filtering Client fails closed and all HTTP traffic is blocked.

◆ **FailCloseTimeout**: The `FailCloseTimeout` parameter applies only when Remote Filtering clients are set to fail closed (`FailClose=true`). `FailCloseTimeout` specifies the amount of time, in minutes, that the Remote Filtering Client tries to connect with the Remote Filtering Server before failing closed and blocking all HTTP traffic. During this time, all HTTP traffic is permitted. The default value is 15, but can be set to any integer from 0 to 60. A value of 0 disables the timeout. If any other value is entered, the default of 15 minutes is enforced.

To set these parameters so that remote users' internet access is blocked when they are unable to establish a connection with the Remote Filtering Server:

1. On the Remote Filtering Server machine, locate the `securewispproxy.ini` file in the `bin` subdirectory in the Websense installation directory. The default location of this file is:

- Windows: `\Program Files\Websense\bin`

- Linux and Solaris: `/opt/Websense/bin`

2. Open the `securewispproxy.ini` file in a text editor.

3. Change the value of the `FailClose` parameter to `true`.

4. If you leave the `FailCloseTimeout` set to its default value of 15, the Remote Filtering Client tries to connect with the Remote Filtering Server for 15 minutes before failing closed and blocking all HTTP traffic.

   - To change the length of time, in minutes, that the Remote Filtering Client tries to connect, change the value of `FailCloseTimeout` to an integer from 1 to 60.
   - To disable the timeout, change the value of `FailCloseTimeout` to 0. The Remote Filtering Client keeps trying to establish a connection.

5. Save your changes.

6. Restart the Remote Filtering Server.

   For instructions, see *Stopping or Starting Websense Services*, page 176.

The new settings are applied to all Remote Filtering Clients that connect with the Remote Filtering Server.

✔ **Note**

If you are using Websense Client Policy Manager (CPM) in your network, Remote Filtering parameters are configured in the Desktop tab of Websense Manager. If the CPM Server is present, values set for the `FailClose` and `FailCloseTimeout` parameters in the `securewispproxy.ini` file are ignored.

For information about configuring Remote Filtering features when you are using CPM, see your Websense Client Policy Manager documentation.

Configuring the Remote Filtering Client Log

If you are using the optional Websense Remote Filtering feature, each Remote Filtering Client installed on a user workstation maintains a local log file.

The Remote Filtering Client logs each time the Client:

- is activated after the machine leaves the corporate network
- is deactivated after the machine enters the corporate network
- is restarted
- fails open (allows access to all websites when connectivity with Remote Filtering Server is lost)
- fails closed (blocks access to all websites when connectivity with Remote Filtering Server is lost)
- receives a policy update

The maximum size of this local log file can be changed by editing the `LocalLogSize` parameter in the `securewispproxy.ini` file on the Remote Filtering Server machine.

The `LocalLogSize` parameter defines the maximum size, in MB, of the log file. Once the maximum file size is reached, the log file name is time stamped with the current date and time and saved. A maximum of two log files are maintained; the oldest log is deleted when a third log is started. The default value of `LocalLogSize` is 1, but it can be set to any integer from 0 to 10. To disable the log, enter a value of 0.

To change the maximum size of the Remote Filtering Client's local log file:

1. On the Remote Filtering Server machine, locate the `securewispproxy.ini` file in the `bin` subdirectory in the Websense installation directory. The default location of this file is:
   - Windows: `\Program Files\Websense\bin`
   - Linux and Solaris: `/opt/Websense/bin`
2. Open the `securewispproxy.ini` file in a text editor.
3. Change the value of the `LocalLogSize` parameter to any integer from 0 to 10.

   This integer defines the maximum size of the log in MB. A value of 0 disables the log.
4. Save your changes.
5. Restart the Remote Filtering Server. For instructions, see *Stopping or Starting Websense Services*, page 176.

The new maximum log size setting is applied to all Remote Filtering Clients that connect with the Remote Filtering Server.

Note

If you are using Websense Client Policy Manager (CPM) in your network, Remote Filtering parameters are configured in the Desktop tab of Websense Manager. If the CPM Server is present, values set for the `LocalLogSize` parameter in the `securewispproxy.ini` file are ignored.

For information about configuring Remote Filtering features when you are using CPM, see your Websense Client Policy Manager documentation.

CHAPTER 6 | Authentication

Authentication is the process of identifying a user within a network who has an account in a directory service. Depending on the authentication method you choose, Squid may be able to obtain user identification and send it to the Websense Filtering Service along with the internet request. Once the Filtering Service receives this information, it can filter requests based on policies assigned to individual directory objects.

✓ **Note**
In any environment, Websense Enterprise or Web Security Suite can filter based on workstation or network policies. Workstations are identified within the Websense software by their IP addresses, and networks are identified as IP address ranges.

In order to filter internet requests for individual directory objects, the Filtering Service must be able to identify the user making the request. This can be accomplished with one or more of the following methods:

◆ Select an authentication method within Squid so that it sends user information to the Filtering Service.

◆ Enable manual authentication within the Websense software so that if the Filtering Service is not able to identify users transparently, it will prompt users for authentication. For more information about manual authentication, see the *Administrator's Guide* for Websense Enterprise and Web Security Suite.

◆ Select an authentication method that identifies users transparently and sends the information to the Filtering Service along with the internet request.

Client Types

The term *clients* in this environment refers to workstations or applications that run on workstations and rely on a server to perform some operations. Each type of client can be configured so that the Filtering Service is able to obtain user identification and filter internet requests based on user and group policies.

Squid works with two types of clients.

◆ Firewall
◆ Web Proxy

Firewall Clients

If you are behind a firewall you cannot make direct connections to the outside world without the use of a parent cache. Squid doesn't use ICP queries for a request if Squid is behind a firewall or if there is only one parent.

Use the following lists in the squid.conf file to deal with internet requests.

◆ **never_direct**: specifies which requests must be forwarded to your parent cache outside the firewall
◆ **always_direct**: specifies which requests must not be forwarded

Consult your Squid documentation for more information.

Web Proxy Clients

Web Proxy clients send internet requests directly to the Squid server machine after the browser is configured to use the Squid server as the proxy server.

You can assign individual user or group policies by doing one or more of the following:

◆ If the network uses multiple types of browsers, you can enable one or more of the Squid authentication methods, discussed in the next section. Some of these methods may require users to authenticate manually.

◆ Enable the Websense software to prompt users for authentication. This allows the Websense software to obtain the user information it needs if it does not receive it from Squid or DC Agent (see the Manual Authentication section in the *Administrator's Guide* for Websense Enterprise and Web Security Suite).

Authentication Methods

Squid v2.5 offers the following authentication methods:

◆ Anonymous

◆ Basic

◆ Windows NT® Challenge/Response

◆ Digest

See your Squid documentation for information about enabling authentication within Squid.

> **Important**
>
> Before changing authentication methods, please consider the impact the change could make on other proxy server functions.

Anonymous Authentication

When anonymous authentication is enabled within Squid, user identification is not received from the browser that requests a site. Users cannot be filtered based on individual user or group policies unless anonymous authentication is disabled and another method of authentication is enabled. Anonymous authentication does, however, allow internet filtering based on workstation or network policies, if applicable, or by the Global policy.

Basic Authentication

When basic authentication is enabled within Squid, users are prompted to authenticate (log on) each time they open a browser. This allows Squid to obtain user identification, regardless of the browser, and send it to the Filtering Service, which is then able to filter internet requests based on individual user and group policies. Basic authentication can be enabled in combination with Windows NT Challenge/Response or Integrated Windows Authentication, discussed in the next section.

Digest Authentication

Digest Authentication is a secure form of authentication that can be used only in Windows 2000 and Windows Server 2003 domains. Digest Authentication offers the same features as Basic authentication, but has a clear advantage because the user name and password are scrambled when sent from the browser to Squid. This allows the user to authenticate to Squid without the user name and password being intercepted, and permits the Filtering Service to obtain user identification for user and group based policies.

Windows NT Challenge/Response and Integrated Windows Authentication

If Windows NT Challenge/Response is enabled, Squid obtains user identification transparently from Microsoft Internet Explorer browsers and sends it to the Websense software, which is then able to filter internet requests based on individual user and group policies.

> ✔ **Note**
> Windows NT Challenge/Response and Integrated Windows Authentication cannot obtain user identification information transparently from browsers other than Microsoft Internet Explorer.

If your network has a mixture of Microsoft Internet Explorer browsers and other browsers, you can enable both Basic and Windows NT Challenge/Response or Basic and Integrated Windows Authentication. In this case, users with Microsoft Internet Explorer browsers are identified transparently and users with other browsers are prompted to authenticate.

> ✔ **Note**
> To transparently identify all users in a mixed browser environment, you can enable Anonymous authentication within Squid and use the Websense transparent identification feature.

Transparent Identification

The Websense transparent identification feature allows Websense Enterprise or Web Security Suite to filter internet requests from users identified in a directory service without prompting them to authenticate manually. This feature comes into play only if the authentication method enabled within Squid does not send user information to the Websense Filtering Service.

To use the transparent identification feature, a Websense transparent identification agent—DC Agent, eDirectory Agent, Logon Agent, or RADIUS Agent—must be installed and configured. The transparent identification agent obtains user information and sends it to the Filtering Service.

For example, if you are using a Windows-based directory service, you can install the Websense DC Agent on a Windows or Linux machine in the network. Once the Filtering Service is configured to communicate with DC Agent, DC Agent obtains user information from a Windows-based directory service and sends it to the Filtering Service. When the Filtering Service receives the IP address of a machine making an internet request, the Filtering Service matches the address with the corresponding user name provided by DC Agent. This allows the Filtering Service to identify users transparently whenever they open a browser that sends internet requests to Squid. DC Agent can be installed on the same machine as Filtering Service, or on a different machine.

Similarly, if you are using Novell eDirectory Service in your network, you can install eDirectory Agent on a Solaris or Linux machine to obtain user information from the directory service and send it to Filtering Service. eDirectory Agent can be installed on the same machine as Filtering Service, or on a different machine.

For more information about each of the Websense transparent identification agents and where they can be installed, see *Websense Enterprise and Web Security Suite Components*, page 15. For information about installing a transparent identification agent separately, see *Installing Websense Components Separately*, page 91. For information about configuring and using transparent identification agents after installation, and information about Websense manual authentication, see the *Administrator's Guide* for Websense Enterprise and Web Security Suite.

More detailed information about deploying and using Websense transparent identification agents can be found in the white paper titled *Transparent Identification of Users in Websense Enterprise*, available at: www.websense.com/SupportPortal/   .

Stealth Mode

In some cases, it might be desirable to configure the Network Agent to inspect all packets with a network interface card (NIC) that has been configured for *stealth mode*. A NIC in stealth mode has no IP address and cannot be used for communication. The advantages for this type of configuration are security and network performance. Removing the IP address prevents connections to the interface from outside and stops unwanted broadcasts.

Configuring for Stealth Mode

If the Network Agent is configured for a stealth mode NIC, the installation machine must be multihomed. In remote installations of Network Agent, a second, TCP/IP-capable interface must be configured to communicate with the central Websense software for filtering and logging purposes.

Stealth mode NICs display normally during Network Agent installation. You may test a stealth mode NIC for traffic visibility and select it for Network Agent to use to monitor internet traffic. When installing on Windows, stealth mode interfaces do not display as a choice for Websense communications.

> **Important**
>
> In Solaris and Linux, stealth mode NICs appear together with TCP/IP-capable interfaces and must not be selected for communication.

Make sure you know the configuration of all the interfaces in the machine before attempting an installation.

Windows

Stealth mode for the Network Agent interface is supported in Windows.

To configure a NIC for stealth mode:

1. From the Start menu, select **Settings** > **Network and Dial-up Connection**.

   A list of all the interfaces active in the machine is displayed.

2. Select the interface you want to configure.

3. Select **File** > **Properties** or right-click and select **Properties** from the pop-up menu.

   A dialog box displays the connections properties of the interface you have chosen.
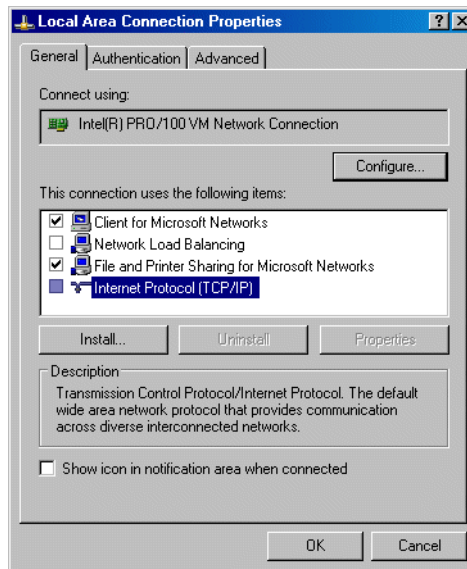
Interface Connections Properties

4. Clear the **Internet Protocol (TCP/IP)** checkbox.

5. Click **OK**.

Solaris or Linux

To configure a NIC for stealth mode in Solaris or Linux, you must disable the Address Resolution Protocol (ARP), which severs the link between the IP address and the MAC address of the interface.

Solaris

◆ To configure a NIC for stealth mode, run the following from a command prompt:

```
ifconfig <interface> plumb -arp up
```

◆ To return the NIC to a normal mode, run the following from a command prompt:

```
ifconfig <interface> plumb arp up
```

Linux

◆ To configure a NIC for stealth mode, run the following from a command prompt:

```
ifconfig <interface> -arp up
```

◆ To return the NIC to a normal mode, run the following from a command prompt:

```
ifconfig <interface> arp up
```

> **Important**
> Network Agent can work with a stealth mode NIC only if the interface retains its old IP address in the Solaris or Linux system configuration file.

APPENDIX B | Troubleshooting

You may encounter a situation while installing Websense Enterprise or Web Security Suite and configuring the Squid Web Proxy that is not addressed in the previous chapters. This appendix provides troubleshooting information for installation and initial configuration issues that have been called in to Websense Technical Support. Please check this chapter for information about the problem you are having before you contact Technical Support. For issues not related to installation or communication between Websense software and your integration product, see the *Administrator's Guide* for Websense Enterprise and Web Security Suite.

If you still need to contact Technical Support, please see *Appendix C: Technical Support* for contact information. The situations addressed in this chapter are as follows:

◆ I made a mistake during installation.

◆ I installed using a non-English language version of the Websense installer, and the Language Pack installer did not automatically start.

◆ I forgot my Websense Policy Server password.

◆ Where can I find download and error messages?

◆ The Master Database does not download.

◆ Policy Server fails to install.

◆ I upgraded my Websense software, and configured users no longer appear under Directory Objects in Websense Manager.

◆ Network Agent fails to start on Linux with stealth mode NIC.

◆ Network Agent is not filtering or logging accurately.

◆ Windows 9x workstations are not being filtered as expected.

◆ I am using Logon Agent and some users are receiving the Websense Global policy.

◆ Websense splash screen is displayed, but installer does not launch on Windows 2000.

◆ Internet requests are not being filtered.

- ◆ Outgoing internet traffic seems slow.
- ◆ Network Agent cannot communicate with Filtering Service after it has been reinstalled.
- ◆ Users filtered via remote filtering are not receiving block pages.
- ◆ Remote filtering is not working.

I made a mistake during installation

Run the installation program again. The installer will detect the current installation and allow you to **Add**, **Remove**, or **Repair** Websense components. The **Repair** option does not troubleshoot the installation, but merely reinstalls the files it detects.

> ✓ **Note**
> On Windows, you may need to restart the machine before running the installer again.

For instructions, see *Modifying an Installation*, page 154.

I installed using a non-English Websense installer, but the Language Pack installer did not start

When you install Websense software using one of the non-English installer packages, the Language Pack installer should start after installation of the selected Websense components is complete.

If the Language Pack installer does not start automatically, you can start it manually as follows:

- ◆ **Windows**: Go to the setup folder where you unpacked the Websense installer, and double-click on SetupLanguagePack.exe.
- ◆ **Solaris or Linux**: Go to the setup directory where you unpacked the Websense installer, and enter the following command:

    ```
    ./installLanguagePack.sh
    ```

    If you are using an English-based UNIX system, you can run the GUI mode of the installer by entering the following command:

    ```
    ./installLanguagePack.sh -g
    ```

Follow the onscreen instructions to complete installation of the Language Pack. Websense components and files on the machine are updated with text in the language you selected.

I forgot my Websense Policy Server password

Contact Websense Technical Support for assistance. You can find contact information in *Appendix C: Technical Support*.

Where can I find download and error messages?

Windows

Check the Windows Application Event log or `Websense.log` (`Websense\bin`) for any listings about the database download as well as other error or status messages. Access the Application Event log by choosing **Start** > **Settings** > **Control Panel** > **Administrative Tools** > **Event Viewer**. Expand the **Event Viewer** tree and click **Application Log**.

Solaris and Linux

The Websense software creates `Websense.log` (located in `Websense/bin`) when there are errors to record. This log file records error messages and messages pertaining to database downloads. `Websense.log` is located on the Policy Server machine only.

The Master Database does not download

There are several reasons why you might have difficulty receiving Websense Master Database downloads.

Subscription Key

Verify that the subscription key is entered correctly and has not expired by going to the **Database Download** screen in Websense Manager (**Server** > **Settings** > **Database Download**).

◆ Compare the key you received via email or in the Websense package to the key in the **Subscription Key** field (the key is not case sensitive) and correct any errors. You must click **OK** to close the **Settings** dialog box before the key takes effect and enables the database download.

◆ Check the date shown in the **Key Expires** field. If this date has passed, contact Websense, Inc., to renew your subscription.

Internet Access

The machine running the Filtering Service must have access to the internet via HTTP, and must be able to receive incoming transmissions.

To verify internet access on the Websense Filtering Service machine:

1. Determine whether the Websense software is accessing the internet through a proxy server by checking the **Database Download** screen of the **Settings** dialog box in Websense Manager.

2. If a proxy server is being used, open a web browser.

3. Configure the browser to access the internet with the same proxy settings as those shown in the **Settings** dialog box.

4. Request one of the following addresses:

    http://download.websense.com

    http://asia.download.websense.com

    http://europe.download.websense.com

   - If you reach the site, the Websense logo appears, along with a message indicating that it will redirect you to the Websense home page. This means that the Filtering Service's proxy settings are correct, and the Filtering Service should have appropriate HTTP access for downloading.

   - If you are not able to reach the download site, and the system requires proxy information, the Filtering Service proxy settings must be corrected.

   - If no proxy information is required, use the **nslookup** command (at the command prompt) with the address of your download site to make sure the Filtering Service machine is able to resolve the download location to an IP address. For example:

     nslookup asia.download.websense.com

     If this does not return an IP address, you must set up the machine running Filtering Service to access a DNS server.

If you need assistance, contact Websense Technical Support (see *Appendix C: Technical Support* for information).

5. If the Websense software must access the internet through an upstream firewall or proxy server that requires authentication, check the following:

   ■ The correct user name and password must be entered in the **Database Download** screen of the **Settings** dialog box. Verify spelling and capitalization.

   ■ The firewall or proxy server must be configured to accept clear text or basic authentication.

Restriction Applications

Some restriction applications, such as virus scanners or size-limiting applications, can interfere with database downloads. Disable the restrictions relating to the Filtering Service machine and the Websense download location.

Policy Server fails to install

If you attempt to install Websense software on a machine with insufficient resources (RAM or processor speed), the Policy Server may fail to install. Certain applications (such as print services) can bind up the resources that the installer needs to install the Policy Server. If the Policy Server fails to install, Setup must quit. If you receive the error message: *Could not install current service: Policy Server*, during installation, take one of the following actions:

◆ Install Websense software on a different machine. See *System Requirements*, page 32 for minimum installation requirements.

◆ Stop all memory-intensive services running on the machine before attempting another Websense installation.

I upgraded the Websense software, and configured users no longer appear under Directory Objects in Websense Manager

If you are using Active Directory as your Directory Service, you may find that user names disappear from the list of directory objects in Websense Manager when you upgrade your Websense software. This change occurs if your user names include characters that are not part of the UTF-8 character set.

To support LDAP 3.0, the Websense installer changes the character set from MBCS to UTF-8 during upgrade, so if your user names include non-UTF-8 characters, those characters will not be properly recognized. To fix this problem, try changing the character set back to MBCS.

1. In Websense Manager, go to **Server** > **Settings** > **Directory Service**.

   A**ctive Directory (Native Mode)** will be selected in the **Directories** pane if you are using Active Directory.

2. Click the **Advanced Settings** button.

3. Click **MBCS** under **Character Set** to change the character set from UTF-8 to MBCS.

Network Agent fails to start with stealth mode NIC

IP address removed from Linux configuration file

Network Agent can work with a stealth mode NIC only if the interface retains its old IP address in the Linux system configuration file. If you have bound Network Agent to a network interface card configured for stealth mode, and then removed the IP address of the NIC from the Linux configuration file (`/etc/sysconfig/network-scripts/ifcfg-<adapter name>`), Network Agent will not start.

An interface without an IP address will not appear in the list of adapters displayed in the installer or in Websense Manager and will be unavailable for use. To reconnect Network Agent to the NIC, restore the IP address in the configuration file.

Stealth mode NIC selected for Websense communications in Solaris and Linux

Network interface cards configured for stealth mode in Solaris and Linux are displayed in the Websense installer as choices for Websense communications. If you have inadvertently selected a stealth mode NIC for communications, Network Agent will not start, and Websense services will not work.

To correct this problem, open the `websense.ini` file in `Websense/bin` and change the IP address to that of a NIC in normal mode. Start the Websense services.

Network Agent is not filtering or logging accurately

If you have configured your Squid machine to act as a proxy for internet traffic, you must define the IP address of the proxy server machine in Websense Manager. Without this address, Network Agent cannot filter or log requests accurately. Network Agent will log the address of the proxy server as

the source IP address of all permitted requests and will not log blocked requests at all. For instructions, see *Identifying the Proxy Server for Network Agent*, page 196.

If user- and group-specific policies are not being applied to protocol requests (i.e., all protocol requests are being filtered by the Global policy), your integration product may not be passing user credentials to Network Agent. You can install a Websense transparent identification agent to authenticate protocol traffic. For information about installing transparent identification agents, see the sections on DC Agent, eDirectory Agent, Logon Agent, and RADIUS Agent in *Installing Websense Components Separately*, page 91. For information about configuring transparent identification agents, see the User Identification chapter in the *Administrator's Guide* for Websense Enterprise and Web Security Suite.

Windows 9x workstations are not being filtered as expected

If you are running DC Agent for user identification, your Windows 9x workstation machine names must not contain any spaces. This situation could prevent DC Agent from receiving a user name when an internet request is made from that workstation. Check the machine names of any Window 9x workstations experiencing filtering problems and remove any spaces you find.

I am using Logon Agent and some users are receiving the Websense Global policy

There may be a number of reasons why users are not being filtered as expected; however, if your network uses Logon Agent to identify users, and if some of those users are receiving the Websense Global policy instead of their usual user or group policies, a network problem may exist.

If the Logon Agent logon script fails to execute properly on a workstation, the Websense software cannot identify the user to apply the proper policy. The Global policy will be applied as a default.

The first step is to determine if the settings for the Windows Group Policy Objects (GPO) are being applied correctly to these workstations. If not, then this is a network connectivity problem and not a Websense configuration issue.

Proceed with the following network checks:

◆ Check the user machine's visibility to the domain controller from which the logon script is being run.

◆ Make sure that NetBIOS is enabled on the machine.

◆ Make sure the user profile is not blocking the execution of the logon script.

Domain Controller Visibility

To determine is the domain controller is visible to the workstation:

◆ Attempt to map a drive on the client workstation to the domain controller's root shared drive. This is the drive from which the logon script is normally run, and on which `LogonApp.exe` resides.

◆ Run the following command from a Windows command prompt on the workstation that is not being identified:

```
net view /domain:<domain name>
```

If either of these tests fails, see your Windows operating system documentation for possible solutions. This is a network connectivity problem and not a Websense issue.

NetBIOS

Make sure that NetBIOS for TCP/IP is enabled and that the TCP/IP NetBIOS Helper service is running on the client machine. If either of these is not running, the Websense logon script will not execute on the user machine.

The TCP/IP NetBIOS Helper service runs on Windows 2000, Windows XP, Windows Server 2003, and Windows NT. In Windows 98, TCP/IP NetBIOS is enabled by default.

If your network uses Active Directory, and if you have Windows 98 client machines, go to the Microsoft website for assistance: www.microsoft.com/windows2000/server/evaluation/news/bulletins/adextension.asp.

User Profile Issues

If the user profile on the local workstation is corrupt, it can prevent the Websense logon script (as well as the Windows GPO settings) from running. To eliminate this as a cause:

1. Log on to the workstation as a local administrator.

2. Delete the following directory that contains the user profile:

   `C:\Documents & Settings\<user name>`

3. Restart the machine.

4. Log on as the normal user.

   The user profile will be created automatically.

5. Check to make sure the user is being filtered as expected.

Websense splash screen is displayed, but installer does not launch on Windows 2000

This problem is a software issue with the installation machine which prevents it from displaying the Java-based Websense installer interface. This problem also prevents Websense Manager from launching on this machine.

There are two possible solutions for this problem.

◆ **Install DirectX on the installation machine**. DirectX is a Windows suite of application programming interfaces (APIs) that developers use to write applications for the Windows operating system. The Java-based Websense installer uses these APIs to display its interface, as does Websense Manager. If DirectX is not present, neither the Websense installer interface nor the Websense Manager interface can be displayed.

◆ **Run the installer in console mode**. You can configure `Setup.exe` to start in a Windows command prompt, which will allow you to install Websense software in the console mode.

To install Websense software in console mode:

1. Open the `launch.ini` file using a text editor.

   This file is located on the same level as `Setup.exe` in the folder where you unzipped your Websense installer.

2. Add the following line to the file:

   `ARGS=-console –is:javaconsole`

3. Save the file and exit.

4. Double-click `Setup.exe` or run the application from the command line.

   The installer starts in the Windows command prompt.

5. Follow the onscreen instructions to install Websense software.

> ✔ **Note**
>
> The installation sequence for the console mode is identical to that of the GUI mode.

6. Install Websense Manager on a Solaris machine or a Windows machine capable of displaying the Java interface.

Internet requests are not being filtered

If you integrated Websense Enterprise or Web Security Suite with the Squid Web Proxy Cache on a machine running the Red Hat Enterprise Linux ES 4 operating system, and Websense filtering is not working, the problem may be the Security-enhanced Linux (SELinux) configuration.

The Red Hat Enterprise Linux ES 4 operating system installs SELinux by default. The SELinux installation is a kernel modification that lessens root user and hierarchical privilege vulnerabilities. The default SELinux installation packaged with Red Hat Enterprise Linux ES release 4 prevents Squid from launching the Websense Squid Plug-in (`WsRedtor`). If `WsRedtor` does not launch, Websense filtering cannot occur.

To determine if this is the problem, check the following on the Red Hat Enterprise Linux ES 4 machine to verify that `WsRedtor` is not launching:

1. `WsRedtor` does not appear in the process command list, although other Websense services do.

2. Error messages associated with `WsRedtor` appear in the Squid `cache.log`, found by default at `/var/log/squid/cache.log`.

3. Error messages associated with `WsRedtor` appear in the Linux system log, found by default at `/var/log/messages`.

If you determine that `WsRedtor` is not launching, there are several ways to resolve the issue:

◆   If you are familiar with configuring permissions for SELinux-enabled Red Hat, you can configure permissions so that `WsRedtor` can launch. See your Red Hat Enterprise Linux ES documentation for instructions. Additional information about SELinux is available at www.nsa.gov/selinux/.

◆ Do not install Websense software on a machine using an SELinux-enabled Red Hat Enterprise Linux operating system and the version of Squid prepackaged with the Red Hat installation. If SELinux is *not* enabled, you can install Websense software on a machine using a Red Hat Enterprise Linux operating system and the prepackaged version of Squid.

◆ Before you install Websense software on a machine using an SELinux-enabled Red Hat Enterprise Linux operating system, you can install Squid directly from the official Squid website at www.squid-cache.org. This "official" Squid installation does not stop `WsRedtor` as does the version packaged with the Red Hat Enterprise Linux ES release 4 operating system.

Outgoing internet traffic seems slow

If outgoing internet traffic is slower than expected, increase the number of redirectors spawned by Squid. In the `squid.conf` file, go to the **redirect_children** tag and increase the number by 10. The current default is 30.

If the performance continues to be slow, consult your Squid Web Proxy Server documentation, and check your network settings.

Network Agent cannot communicate with Filtering Service after it has been reinstalled

When Filtering Service has been uninstalled and reinstalled, Network Agent does not automatically update the internal identifier (UID) for the Filtering Service. After the new installation of Filtering Service is complete, Websense Manager still attempts to query Filtering Service using the old UID, which no longer exists.

To re-establish connection to the Filtering Service:

1. Open Websense Manager.

   An error message is displayed stating **Network Agent *<IP address>* is unable to connect with Filtering Service**.

2. Clear the message and select **Server > Settings**.

   The same error message is displayed.

3. Clear the message again and select **Network Agent** from the **Settings Selections** list.

4. Click **Local Settings**.

5. Select the IP address listed above the NIC for the Network Agent.

6. Click **Edit Selection**.

   The **Filtering Service Connection** dialog box appears.

7. Select the IP address of the Filtering Service machine from the **Server IP Address** drop-down list.

8. Click **Finish**.

9. Click **OK** in the **Local Settings** dialog box.

10. Click **OK** in the **Settings** dialog box to save the changes.

Users filtered by remote filtering do not receive block pages

If users with the Remote Filtering Client on their workstations are being filtered properly, but are not receiving Websense block pages, try the following:

◆ If there is a firewall between the Websense Filtering Service machine and the Remote Filtering Server machine, check that it has been properly configured, as described in *Enabling communication between Remote Filtering Server and Filtering Service*, page 206:

   ■ Make sure the **Block Page port** (by default, 15871) has been opened on the firewall. This allows Filtering Service to send block pages to remote users.

   See the documentation for your firewall product if you need information about how to configure your firewall.

◆ Make sure Remote Filtering Client is not installed on the Remote Filtering Server machine. An instance of Remote Filtering Client running on the Remote Filtering Server machine eventually uses all available connections to the server. When the connections are not available, remote workstations cannot connect to the Remote Filtering Server and are not filtered. Uninstall the Remote Filtering Client from the Remote Filtering Server machine.

Remote filtering is not working

If you installed the remote filtering components, but the user workstations on which you installed the Remote Filtering Client are not being filtered properly, you may have one or more of the following problems:

◆ You do not have the correct subscription key to enable the remote filtering service.

◆ Remote Filtering Server is not running.

◆ Remote Filtering Server and Filtering Service are installed on the same machine.

◆ Firewalls located between Remote Filtering Server and the Filtering Service have not been correctly configured.

◆ The external network firewall and any additional firewalls located between the Remote Filtering Server machine and the remote workstations have not been correctly configured.

◆ Network Agent is filtering responses to remote filtering requests.

◆ Other connection problems.

◆ DHCP is enabled for the Remote Filtering Server machine.

◆ The Remote Filtering Server machine is running Windows Server 2003, but Service Pack 1 is not installed.

◆ Parameters for communication between Remote Filtering Server and Remote Filtering Clients are not properly configured:

■ IP addresses for internal and external communication are not properly configured.

■ Ports for internal and external communication are not properly configured.

◆ Pass phrases entered for Remote Filtering Server and Remote Filtering Clients do not match.

◆ If a load balancer is in use, it is not forwarding packets to the Remote Filtering Server.

Troubleshooting Procedure for remote filtering

Follow these procedures to determine the cause of the problem:

1. Check that your subscription key includes remote filtering.

   The remote filtering service is available as an optional add-on. Check that your Websense subscription key includes the remote filtering service.

2. Check that Remote Filtering Server is running.

   - Windows: Use the Windows Services Control Panel to check that **Websense Remote Filtering Service** is running.

   - Linux and Solaris:

     a. Go to the /opt/Websense directory.

     b. From a command prompt, run ./WebsenseAdmin status

     c. The Remote Filtering Server service should be running. If not, run ./WebsenseAdmin start

3. Make sure Remote Filtering Server is *not* installed on the same machine as Filtering Service.

   Installing these components on the same machine will cause a serious drain on resources on the machine. Filtering will become very slow, and may eventually fail and allow all requests.

4. Check that any firewalls located between Websense Filtering Service and Remote Filtering Server are correctly configured.

   If there are one or more firewalls between the Filtering Service machine and the Remote Filtering Server machine, check that they have been properly configured, as described in *Enabling communication between Remote Filtering Server and Filtering Service*, page 206.

   - Make sure the Filtering Service's **Filter port** (by default, 15868) has been opened on all firewalls between the Filtering Service and Remote Filtering Server. If this port is not open, Filtering Service cannot accept connections from the Remote Filtering Server.

   - Make sure that the **Block Page port** (by default, 15871) has been opened on all firewalls between the Filtering Service and Remote Filtering Server. If this port is not open, Filtering Service cannot send block pages to remote users.

5. Check that the external network firewall and any additional firewalls located between the Remote Filtering Server machine and the remote workstations have been properly configured, as described in *Enabling communication between Remote Filtering Server and Remote User Workstations*, page 206.

   ■ The Remote Filtering Server's **External Communication Port** on these firewalls must be able to accept connections from Remote Filtering Clients on workstations located outside the network firewall. By default, this is port 80, unless it was changed during installation of the Remote Filtering Server.

   ■ Access to the Remote Filtering Server's **Internal Communication Port** must be blocked from workstations located outside the network firewall. By default, this is port 8800, unless it was changed during installation of the Remote Filtering Server.

6. Make sure Network Agent is *not* filtering responses to remote filtering requests.

   Check that Network Agent is *not* monitoring the machine on which Remote Filtering Server is installed:

   a. Open Websense Manager and connect to the Policy Server.

   b. Select **Server > Settings**.

   c. The **Settings** dialog box appears.

   d. In the **Settings** pane, click **Global Settings** under **Network Agent**.

   e. In the **Internal Network Definition** section of the window, check that the IP address for the machine running Remote Filtering Server is *not* included.

      • If the server's IP address is listed individually, select the address from the list and click **Delete**.

      • If the server's IP address is in a range, delete the range and add two ranges around that IP address.

   f. When you are finished, click **OK** at the bottom of the screen to save your changes.

   See the Network Agent chapter in the *Administrator's Guide* for Websense Enterprise and Web Security Suite for more information about configuring Network Agent's global settings.

7. Check that connections are working properly.

   - Check that the remote workstations on which Remote Filtering Client has been installed are able to communicate with the Remote Filtering Server machine. The ping command can be used to verify this connection.

   - Check that the Remote Filtering Server machine is communicating properly with the network. Try to ping the Filtering Service machine and other machines on the local network.

8. Check the RFSErrors.log on the Remote Filtering Server machine.

   a. Open the RFSErrors.log in a text editor. The default location of the RFSErrors.log file is:

      • Windows: \Program Files\Websense\bin

      • Linux and Solaris: /opt/Websense/bin

   b. Check for error 64. This error might indicate that DHCP is enabled for the machine running the Remote Filtering Server.

      • Acquire a static IP address and disable DHCP on this machine.

   c. Check for error 121. This error occurs in a Windows Server 2003 environment, and might indicate that Service Pack 1 is not installed. This service pack is required to run Remote Filtering Server.

      • Download and install the service pack from the Microsoft website.

9. Check that communications are properly configured for the Remote Filtering Server and the Remote Filtering Clients.

   Remote Filtering Clients must be able to connect to the Remote Filtering Server from both inside and outside the internet gateway or network firewall. The correct communication information—IP addresses and port numbers for internal and external communications—must be entered during installation. See *Remote Filtering Server*, page 115 (Windows) or *Remote Filtering Server*, page 149 (Solaris and Linux) for more information.

   a. On the Remote Filtering Server machine, open the securewispproxy.ini file in a text editor. The default location of this file is:

      • Windows: \Program Files\Websense\bin

      • Linux and Solaris: /opt/Websense/bin

b. Under `Proxy Server parameters`, make note of these settings:

- **`ProxyIP`**: Must match the IP address of the network interface card (NIC) on the Remote Filtering Server machine that is used for internal communications.
- **`ProxyPort`**: The port on the Remote Filtering Server machine used for external communications. The default is 80.
- **`ProxyPublicAddress`**: The IP address or host name used for external access to the Remote Filtering Server machine from outside the external network firewall or internet gateway.

c. Under `HeartBeat Server Parameters`, make note of the **`HeartBeatPort`** setting. This is the Internal Communication Port on the Remote Filtering Server machine, used for communication with Remote Filtering Client machines that have been moved inside the external network firewall. The default setting is 8800.

d. Open a command prompt and run an IP configuration command on the Remote Filtering Server machine to get the IP addresses for each network interface card (NIC) in that machine:

- Windows: `ipconfig`
- Linux and Solaris: `ifconfig -a`

e. Check that these IP address values match the Proxy Server parameters found in the `securewispproxy.ini` file.

f. The values need to be checked on the Remote Filtering Client machines. Contact Websense Technical Support for assistance. The technician will need the information gathered in the previous steps to verify that communications are properly configured.

10. Check that the pass phrases match.

The pass phrase for Remote Filtering Server and the Remote Filtering Clients must match. Checking to see if they match requires access to configuration and registry files. Incorrect changes to these files can interfere with machine operation. Contact Websense Technical Support for assistance.

If the pass phrase used for all Remote Filtering Clients does not match the pass phrase configured for the Remote Filtering Server:

a. Reinstall the Remote Filtering Server and enter the proper pass phrase when prompted.

b. Reinstall the Remote Filtering Clients, using the same pass phrase.

If Websense Client Policy Manager (CPM) is installed, or will be installed in the future, note the following:

- If Websense Client Policy Manager (CPM) is already installed in your network, you must enter the same pass phrase used when installing CPM.

- If you install CPM in your network in the future, you must use the same pass phrase you used to install the remote filtering components.

11. Ensure that the load balancer is forwarding packets to the Remote Filtering Server.

    If you are using a load balancer, ensure that it is forwarding packets to the Remote Filtering Server. See your load balancing appliance or software documentation for configuration information.

APPENDIX C | Technical Support

Websense, Inc., is committed to providing excellent service worldwide. Our goal is to provide professional assistance in the use of our software wherever you are located.

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

Websense, Inc., is committed to customer satisfaction. Go to the Websense Technical Support website any time for the latest release information, to access the Knowledge Base or product documentation, or to create a support request.

www.websense.com/SupportPortal/

Telephone assistance is also available. For quick and efficient answers to telephone requests, please be ready with the following:

◆ Websense subscription key

◆ Access to Websense Manager

◆ Access to the machine running Filtering Service, the machine running reporting tools, and the database server (Microsoft SQL Server or MSDE)

◆ Permission to access the Websense Log Database

◆ Familiarity with your network's architecture, or access to a person who has this knowledge

◆ Specifications of the machines running Filtering Service and Websense Manager

◆ A list of other applications running on the Filtering Service machine

Index