v5.5

Installation Guide

for use with
Squid Web Proxy Cache

Websense Enterprise Installation Guide

Published April 4, 2005
Printed in the United States of America

NP33-0003SQD

Trademarks

WinPcap

Contents

CHAPTER 1

Introduction

Thank you for choosing Websense Enterprise, the leading Employee Internet Management system that integrates with the Squid Web Proxy Cache. Using Websense in conjunction with Squid Web Proxy Cache provides you with a highly effective Internet filtering service.

Websense gives network administrators in business, education, government, and other enterprises the ability to monitor and control network traffic to Internet sites. In the business setting, Websense Enterprise is an invaluable tool for minimizing employee downtime due to Internet surfing that is not work related. In addition, Websense helps control the misuse of network resources and the threat of potential legal action due to inappropriate access.

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

The following is a list of Websense Enterprise components:

- **Filtering Service:** interacts with the Squid Web Proxy Cache to provide Internet filtering.
- **Policy Server:** stores all Websense Enterprise configuration information and communicates this data to other Websense services.
- **User Service:** allows you to apply filtering policies based on users, groups, domains and organizational units.
- **Websense Enterprise Manager:** administrative interface that communicates with the Policy Server to configure and manage the Filtering Service.
- **Network Agent:** detects HTTP network activity and instructs the Filtering Service to log this information. You must install the Network Agent and configure it properly to use the Bandwidth Optimizer, Protocol Management, IM Attachments, and enhanced reporting (bytes transferred and duration) features. Network Agent is also used as the filtering component for a stand-alone (non-integrated) system.

- **DC Agent:** an optional component that transparently identifies users who authenticate through a Windows directory service. DC Agent enables Websense to filter Internet requests according to particular policies assigned to 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 application (`LogonApp.exe`) to transparently identify users as they log on to a Windows domain. Logon Agent receives its user information from an application called `LogonApp.exe` that 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. RTA graphically displays bandwidth information and shows requests by category or protocol.
- **Event Publisher:** an optional component that creates SNMP *traps* from the log messages that are generated by the Websense Filtering Service. These traps are then forwarded, or *published*, to an application that manages SNMP and used as needed.
- **Master Database:** contains a collection of millions of Internet sites, representing more than 800 million pages, 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 Reporter:** a separate program available free of charge with Websense Enterprise. 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. Refer to the Websense Reporter documentation for installation and configuration procedures.
- **Websense Explorer:** a web-based application which provides a view into the Log Database. Explorer displays summary information, as well as specific detail about users' Internet activity. Refer to the *Websense Enterprise Explorer Administrator's Guide* for installation and configuration procedures.

How Websense Works

Websense Enterprise is the engine by which content filtering is enforced. With its flexible, policy-based filtering approach, Websense 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 Websense Enterprise to find out whether the requested site should be blocked or not. To make this determination, Websense 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, Websense Enterprise 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, Websense Enterprise notifies the Squid Web Proxy that the site is not blocked, and the site is returned to the user.

Websense Enterprise filters network applications that use TCP-based protocols and measures bandwidth usage of UDP-based messages as well. If an initial Internet request is made with TCP, and the request is blocked by Websense Enterprise, all subsequent UDP traffic will also be blocked. UDP protocols such as RTSP and RTP are monitored and logged by Websense Enterprise.

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, refer to your Websense Enterprise *Administrator's Guide*.

With the Protocol Management feature, Websense Enterprise can 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.

If you have purchased Bandwidth Optimizer and have installed the Network Agent, Websense Enterprise 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.

Deployment Tasks

The following sequence is recommended for installing Websense Enterprise and configuring it to filter Internet traffic 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 what Websense components to install and where to put them is your first task. Consult *Chapter 2: Network Configuration* for sample deployment options and system requirements for typical installations in a small network. If you are deploying Websense Enterprise in a network containing more than 500 users, refer to the *Websense Deployment Guide*.
2. **Install Websense:** Once you have decided how to deploy Websense on your network, you must install the selected components and perform initial setup tasks. Refer to *Chapter 4: Installation* for the installation procedures for each operating system.

Documentation Feedback

Websense, Inc. welcomes comments and suggestions regarding the product documentation. Please send feedback to **DocFeedback@websense.com**. If possible, include your organization's name in your message.

CHAPTER 2

Network Configuration

Websense Enterprise components can be installed in a number of possible configurations, depending upon the nature of your network and your filtering requirements. The information in this chapter will help you determine both your hardware needs and the relationship of Websense components to one another.

Websense Enterprise Components

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

- **Filtering Service:** typically installed on the same machine as the Policy Server and may be installed on the same machine as the Websense Enterprise 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. The 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, refer to the Websense Enterprise *Deployment Guide*.
- **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 Enterprise Manager:** may be installed on the same machine as the Websense Filtering Service. The Websense Enterprise Manager may be installed on multiple machines in the network to enable remote configuration of the Filtering Service. The Websense Enterprise Manager may be used on a different operating system from the Filtering Service. The Websense Enterprise Manager installs on Windows and Solaris.

- **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 Filtering Service and is typically installed on the same machine; however, you may install User Service on a different operating system than the Filtering Service. If the Filtering Service 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 the Filtering Service) for each supported language on machines configured for that language.

- **Network Agent:** Network Agent installs on Windows, Solaris, and Linux. When planning the deployment of the Network Agent consider the following:
  - The 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 the Network Agent. For the best performance, install the Network Agent on a dedicated machine, connected to an unmanaged, unswitched hub that is located between an external router and your network. See *Switched Environments*, page 22 if you are installing Network Agent in a network that employs switches.
  - For small to medium sized organizations, the Network Agent can be installed on the same server machine as the other Websense Enterprise components, assuming that the server meets the minimum system requirements. For larger organizations, you may want to put the 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 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 the Network Agent. For instructions on defining IP address ranges for multiple Network Agents, refer to the Websense Enterprise *Administrator's Guide*.
- Avoid deploying the 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 Policy Server on 10.x.x.x through a variety of switches and routers, communication may be slowed enough to prevent the Network Agent from blocking an Internet request in time.
- *Do not* install the Network Agent on a machine running any type of firewall. The Network Agent uses a packet capturing utility which may not work properly when installed on a firewall machine.

- **Real-Time Analyzer (RTA):** can be installed on a separate machine. The Real-Time Analyzer installs on Windows only.

IMPORTANT

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

To use the RTA Web-based interface, you must have one of the following Web servers installed in your network:

- Apache Web Server version 2.x and later
- Microsoft IIS v5.0 or v6.0

NOTE

If you do not have one of the supported Web servers on your system, the Websense Enterprise installer will offer you the option of installing the Apache Web Server.

- **DC Agent:** installed in networks using a Windows directory service (NTLM-based or Active Directory). DC Agent can be installed on any Windows server in the network, either on the same machine as other Websense components, or on a different machine. DC Agent installs on Windows only.
  - For small to medium networks, it is recommended 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 the 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. Websense Enterprise does not support communication with Windows and Novell directory services simultaneously.
  - 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 detailed deployment information, refer to the white paper titled *Transparent Identification of Users in Websense Enterprise* found on the Websense Web site at: http://www.websense.com/support/documentation.
- **RADIUS Agent:** can be installed on the same machine as Websense Enterprise 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. You can install RADIUS Agent and eDirectory Agent on the same machine or on separate machines in

your network. For configuration information, refer to the *User Identification* chapter in the Websense Enterprise *Administrator's Guide*. The RADIUS Agent installs on Windows, Solaris, and Linux from a **Custom** installation only.

- **eDirectory Agent:** can be installed on the same machine as Websense Enterprise 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. For configuration information, refer to the *User Identification* chapter in the Websense Enterprise *Administrator's Guide*. The eDirectory Agent installs on Windows, Solaris, and Linux. To avoid a port conflict, do not attempt to install the eDirectory Agent together with the DC Agent.
- **Logon Agent:** can be installed on the same machine as Websense Enterprise or installed on a separate machine in your network. Logon Agent may be installed together with DC Agent to improve user authentication in your network. The Logon Agent installs on Windows, Linux, and Solaris. The logon script that runs `LogonApp.exe` runs on Windows only. Refer to *Creating and Running the Script for Logon Agent*, page 135 for instructions.
- **Websense Enterprise Reporter components:** installed on a separate machine from the Filtering Service except when evaluating Websense Enterprise. The Log Server receives and saves information on Internet requests filtered by Websense Enterprise. Reporter then uses this information to create reports. See the Websense Reporter documentation for installation and administrative information.

NOTE

To generate reports properly, you must use the same version of Websense Enterprise and Websense Enterprise Reporter.

Websense Deployment

Websense Enterprise components can be installed on a dedicated server machine as emphasized in this guide or widely distributed across a network on various operating systems. In many cases, Websense Enterprise can be installed on the same machine as your integration product, if the machine has adequate resources. Wherever you decide to deploy Websense Enterprise, make sure that the installation machine can handle the expected traffic load.

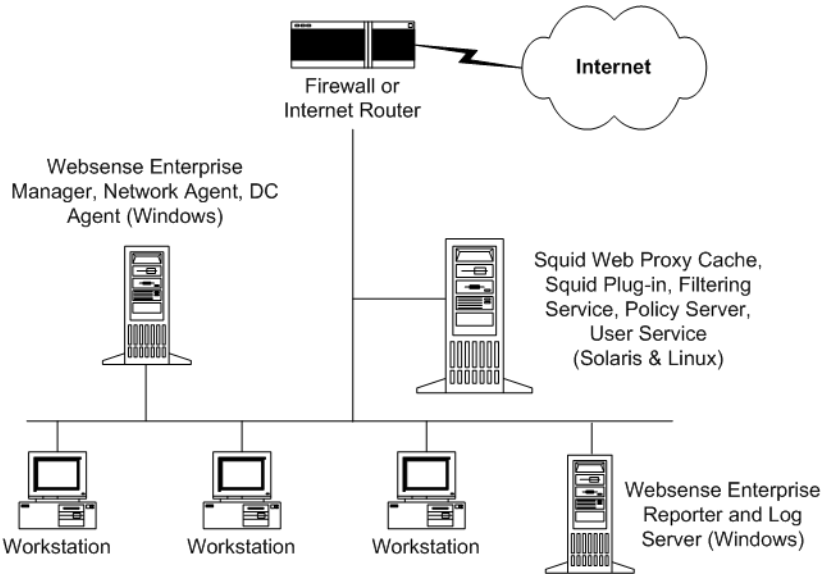
The following network diagrams represent common configurations that are intended for smaller networks and are maximized for efficiency. The network architecture in this guide may not be suitable for your network, particularly if your network contains 500 or more users. For larger, distributed networks, refer to the *Websense Enterprise Deployment Guide* for detailed deployment recommendations. Otherwise, refer to the *Websense Enterprise Components* and *System Requirements* sections of this manual for installation guidelines when planning your deployment.

In environments with a large number of workstations, installing multiple instances of Filtering Service for load balancing purposes may be appropriate. Some load balancing configurations, however, permit the same user to be filtered by different Filtering Services, depending on the current load. For instructions on how to configure Websense for multiple Filtering Service installations, refer to the Websense Enterprise *Administrator's Guide.*

Do not install Websense Enterprise and Websense Enterprise Reporter together on the same machine or on a machine running a firewall. Filtering and logging functions are CPU intensive and could cause serious operating system errors. Install Websense Enterprise and Websense Enterprise Reporter on separate machines inside the network, where they will not have to compete for resources. The exception to this is when Websense Enterprise is being evaluated on a small network or segment of a larger network.

Single Squid Web Proxy Configuration

The following diagram shows the entire Websense Enterprise suite, Squid Plug-in, and Squid Web Proxy running on the same machine.

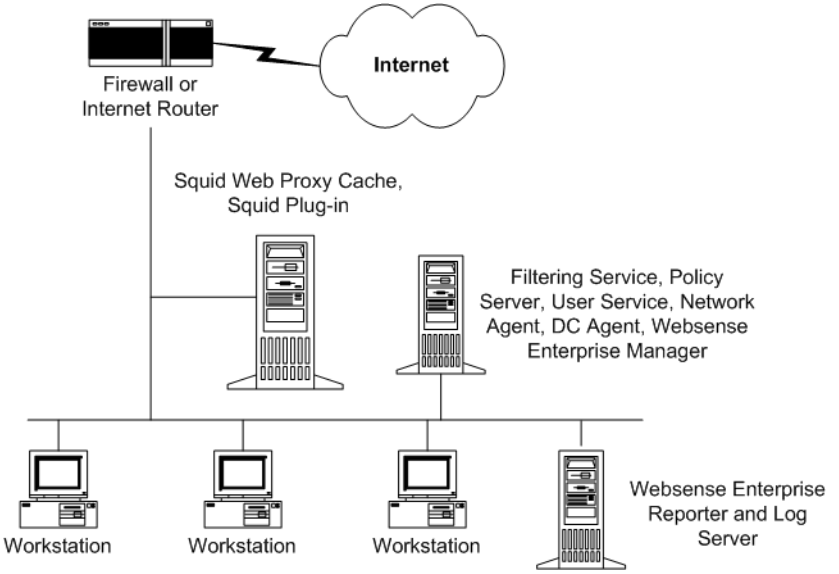


Filtering Service Installed on the Same Machine as the Squid Web Proxy

In this configuration, the main Websense Enterprise components are installed with the Squid Web Proxy on a Solaris or Linux machine. The remaining Websense Enterprise components, including the Network Agent, are installed on a Windows machine that can directly monitor all employee Internet traffic.

An alternate setup places the Websense Enterprise components and Websense Enterprise Manager together on a 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.

The following diagram shows this alternate setup.



Filtering Service Installed Separately from the Squid Web Proxy Cache

This configuration eases the load on the Squid Web Proxy machine by placing all the Websense Enterprise components on a separate Windows machine. The Websense Filtering Service and Squid Web Proxy machine must be able to communicate over the network in this setup. Websense Enterprise Manager can also be installed on multiple machines for added flexibility.

The Log Server, which is installed with Websense Reporter on a separate machine from Websense, receives and saves information on Internet requests filtered by Websense. See your Websense Reporter documentation for more information.

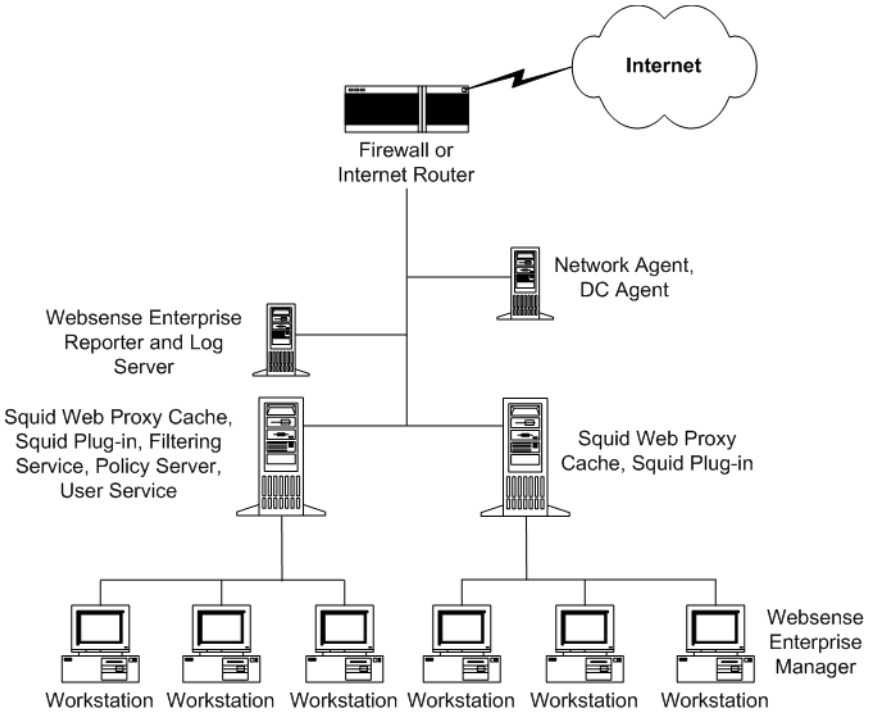
NOTE

Websense Enterprise v5.5 sends log information that can only be read by Websense Reporter v5.5. Therefore, you must install or upgrade to Reporter v5.5 in order to generate reports.

Array Configuration

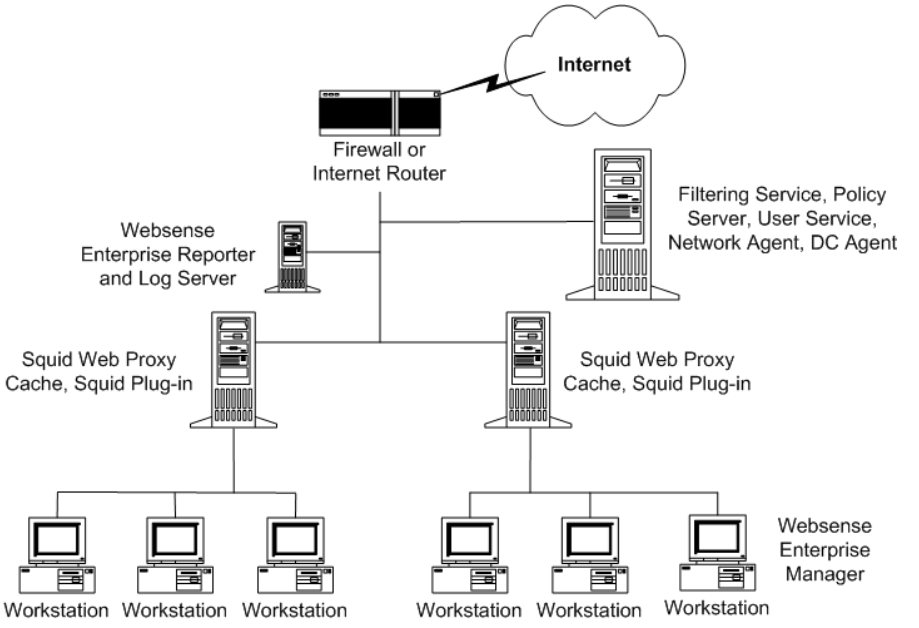
Websense Enterprise is compatible with most array configurations, including Cache Array Routing Protocol (CARP) arrays. If the Squid Web Proxy machines in the array can run Websense Enterprise without a loss of performance, installing all the Websense Enterprise components on one of the array machines is recommended. In this configuration, the two applications will not have to communicate over the network.

The following diagram shows Websense Enterprise components running on a Squid Web Proxy machine, with the Websense Enterprise Manager installed on a workstation machine.



Array Configuration—First Option

If there is a potential loss of performance by installing the Websense Enterprise components on the Squid Web Proxy machine, you can install Websense Enterprise on a separate machine outside the array, and then install the Squid Plug-in on each member of the array. When Websense 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.

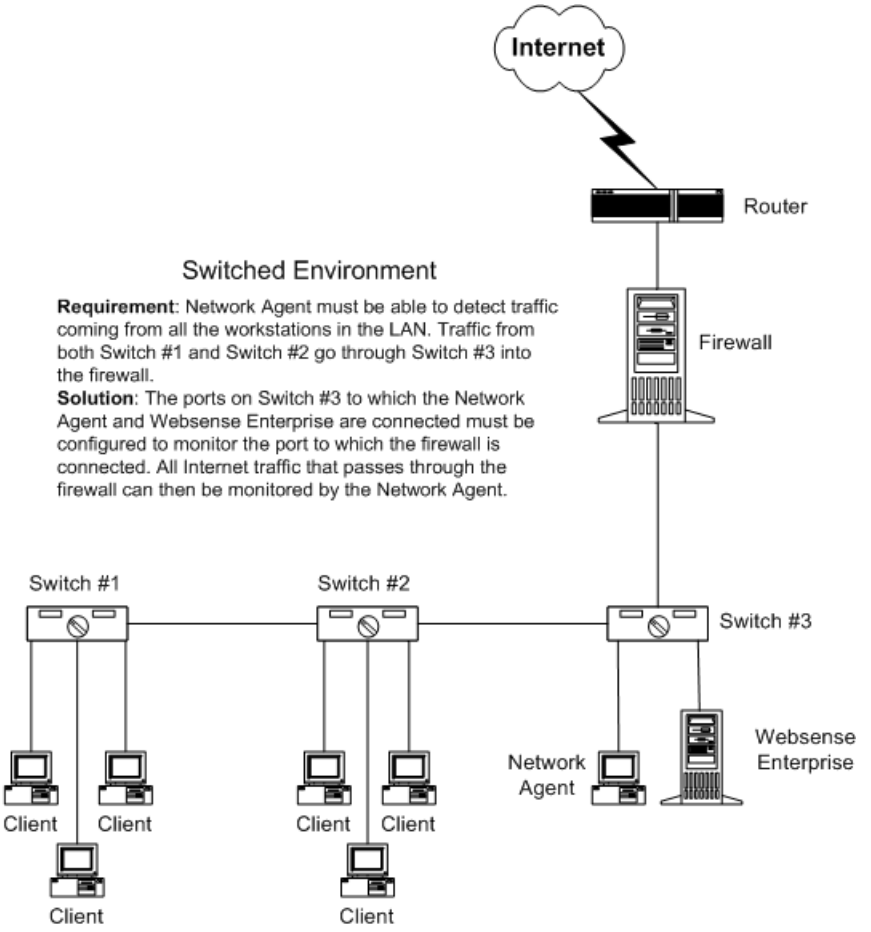
Switched Environments

In a switched environment, configure a switch to use *mirroring* or 2-way port spanning, so that the Network Agent can detect Internet requests from all the workstations.

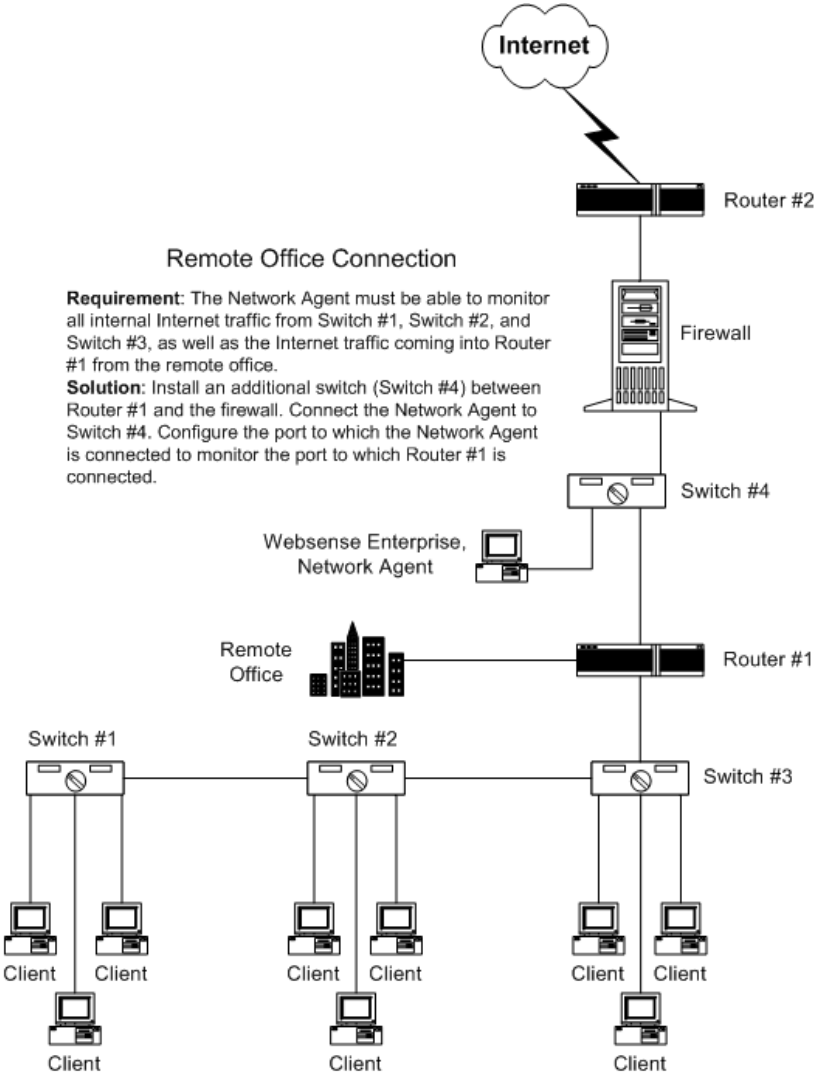
NOTE

Contact your switch vendor to determine if your switch is capable of mirroring or port spanning and to learn how to implement the correct configuration.

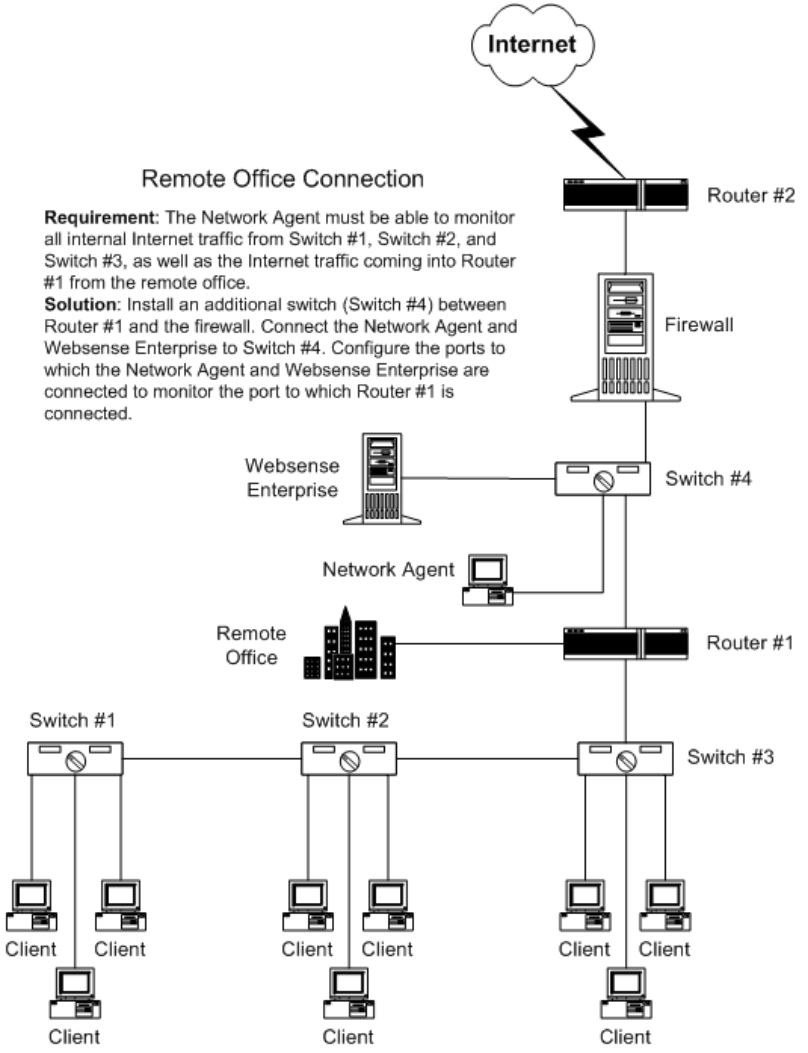
The following network diagrams represent the logical relationship of network elements in a switched environment and are not intended to reflect the actual deployment of Websense Enterprise with Squid Web Proxy Cache.



Basic Deployment in a Switched Environment



Switched Environment with a Remote Office Connection

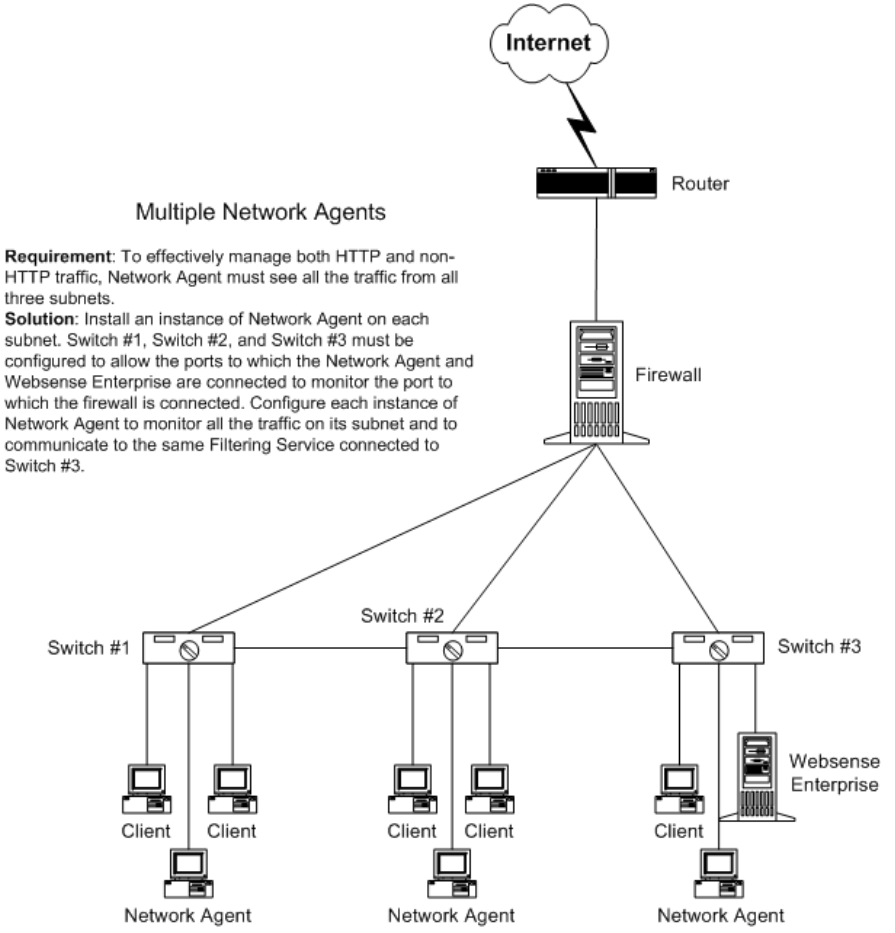


Switched Environment with a Remote Office Connection

On a large network, you may need to install multiple Network Agents and assign them to monitor various IP address ranges in your network. If you install multiple Network Agents, consider the following:

- Do not assign overlapping IP address ranges. If the IP ranges overlap, network bandwidth measurements will not be accurate, and bandwidth-based filtering will not be applied correctly.

- 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 the Network Agent.



Multiple Network Agents in a Switched Environment

NAT and Network Agent Deployment

The use of Network Address Translation (NAT) on internal routers can prevent the Network Agent from identifying the source IP addresses of client machines making Internet requests. If you are deploying the Network Agent to monitor traffic from multiple subnets *after* it passes through such a router, you must disable NAT, or the Network Agent will see the IP address of the router's external interface as the source of the request. An alternative would be to install the Network Agent on a machine located *between* the NAT router and the clients to be monitored.

Directory Services

If your environment includes a directory service, you may also assign different policies to individual users or groups with accounts in that directory service. Websense can communicate with the following directory services:

- Windows NTLM-based directories
- Windows Active Directory
- Sun Java System Directory Server v4.2 and v5.2
- Novell Directory Services/eDirectory v8.51, v8.6, and v8.7 installed on a Windows or NetWare operating system

For information about configuring directory service access, see your Websense Enterprise *Administrator's Guide*.

NOTE

Websense Enterprise can communicate with your directory service whether it runs on the same operating system as Websense or on a different system.

Filtering can be based on individual user, group, and domain/organizational unit policies, providing that Websense 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 Websense Enterprise *Administrator's Guide*.

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 Service or Novell directory service:
  1. Enable the appropriate directory service within Websense.
  2. Enable Websense to identify users transparently with Novell by installing and configuring the Websense eDirectory Agent.
  3. Enable Websense manual authentication so that Websense can identify users.
- If you are using a Windows NTLM-based directory or Active Directory:
  1. Configure the Windows directory service within Websense.
  2. Enable Websense to identify users transparently by installing and configuring the Websense DC Agent or the eDirectory Agent.
  3. Enable manual authentication within Websense so that if Websense is unable to identify users transparently, it will prompt users to manually authenticate. For information about Websense manual authentication, see the Websense Enterprise *Administrator's Guide.*

Websense Enterprise can transparently identify users in a Windows domain if the Websense DC Agent is installed on a Windows 2000 or 2003 Server in the network. In networks using a Novell directory service you can transparently identify users by installing the Websense eDirectory Agent. The Websense transparent identification feature allows Websense to filter Internet requests from users identified in a Window or Novell directory service without prompting them to authenticate manually.

Once the Websense Filtering Service is configured to communicate with the transparent identification agent (DC Agent or the eDirectory Agent), the agent obtains user information from the directory service and sends the information 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 the transparent identification agent. This allows Websense to transparently identify users whenever they open a browser that sends an Internet request to. For information about transparent identification and the Websense DC Agent or the eDirectory Agent, please see the Websense Enterprise *Administrator's Guide*.

System Requirements

The following recommended system requirements are for a typical Websense Enterprise installation in a small network, in which all components are installed on the same machine. Separate requirements are provided for the Websense Enterprise Manager only, which is often installed on an administrator's machine for convenience. All components, with the exception of the Squid Plug-in, can run on the same Windows machine or can be distributed on separate Windows, Solaris, or Linux machines. Websense Enterprise components can be installed on machines with the same or different operating systems. For system requirements and deployment recommendations not covered in this guide, refer to the *Websense Enterprise Deployment Guide*.

Such factors as network size, network configuration, and Internet traffic volume can affect the ability of Websense Enterprise to filter Internet requests. If you plan to install Websense Enterprise on a machine that has high CPU demands, make sure that the machine has sufficient resources to accommodate all the software loaded on it. The recommended system requirements listed here may not provide enough speed or memory for Websense Enterprise to function correctly on a busy network if it is forced to compete for resources.

External Resources

Websense Enterprise relies on certain external resources to function properly in your network. Make sure that the following network elements can adequately support the filtering efforts of Websense Enterprise.

- **TCP/IP**: Websense Enterprise supports TCP/IP-based networks only. If your network uses both TCP/IP and non-TCP protocols, only those users on the TCP/IP portion of your network will be filtered by Websense Enterprise.
- **DNS server**: If IP addresses are not sent to the Websense Filtering Service together with a URL request, a DNS server can be used to resolve the URL into an IP address. Websense Enterprise or your integration product (where applicable) require efficient DNS performance. Make sure your DNS servers are fast enough to support Websense Enterprise filtering without becoming overloaded.
- **Directory services**: The Websense Filtering Service can be configured with policies based on user and group names. The Filtering Service

queries the directory service to identify users and their associated groups as specified in a policy. Although these users and group relationships are cached by Websense, directory service machines must have the resources to rebuild the cache rapidly when the Websense Filtering Service requests user information.

- **Network efficiency**: Connectivity to resources such as DNS and directory services is critical to the Websense Filtering Service. Network latency must be minimized if the Filtering Service is to perform efficiently. Excessive delays under high load circumstances can affect the performance of the Filtering Service and may cause lapses in filtering. Make sure your network is configured for efficient communication between Websense Enterprise and its external resources.

Supported Squid Version

Websense Enterprise v5.5 supports Squid v2.5. or higher.

Typical Solaris Installation

In the typical Solaris installation, Filtering Service, Policy Server, User Service, and Websense Enterprise Manager are installed on the same machine. The minimum system requirements for this type of installation are as follows:

- UltraSPARC IIIi
- 1 GB of RAM
- Solaris 8 and 9
- 1 GB of free disk space

NOTE

You can reduce the disk space needed by deleting the original installation files.

Typical Linux Installation

In the typical Linux installation, Filtering Service, Policy Server, User Service, and Network Agent are installed on the same machine. You must install Websense Manager on a Windows or Solaris machine.

The minimum system requirements for this type of installation are as follows:

- Pentium 4, or greater
- 512 MB RAM (or more)

- Operating systems:
  - Red Hat Linux version 9.0
  - Red Hat Enterprise Linux AS (Advanced Server) v3.0
  - Red Hat Enterprise Linux ES (Enterprise Server) v3.0
  - Red Hat Enterprise WS (Workstation) v3.0
- 2 GB of free disk space

NOTE

You can reduce the disk space used by deleting the original installation files.

Solaris Patches

Make sure you install the proper patch cluster on your Solaris 8 operating system before attempting to run the Websense Enterprise installer. If you are unsure about which patches are required, run the Websense Enterprise installer and check the patch level of the installation machine when prompted. If the patch comparison utility displays an error in the patches you have installed on your machine, consult the following Sun Web site for a list of current patches for your version of Solaris. No patches are required for Solaris 9.

http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/J2SE

Websense Enterprise Manager

Requirements are listed separately for Windows and Solaris installations. A Websense Enterprise Manager installed on a Windows or Solaris machine can configure a Policy Server installed on a Windows, Solaris, or Linux machine.

NOTE

Websense Manager is not supported on Linux.

Windows

- Pentium 4
- 256 MB RAM (or more)
- Supported operating systems:
  - Windows 2003 Server
  - Windows 2000 Server or Professional (Service Pack 3 and higher)

- Windows NT 4.0 Workstation or Server, Service Pack 6a
- Windows XP Professional
- Windows Millennium Edition
- Windows 98 (with updated Microsoft Virtual Machine)

- Internet Explorer or Netscape with Java support enabled (required to view online Help)
- Color depth set to 8 bit (256 colors) or greater
- 130 MB of free disk space

Solaris

The Websense Enterprise Manager will not run on a non-GUI Solaris system. To run the Manager, you *must* have Common Desktop Environment (CDE), Java Virtual Machine (JVM) and a browser.

- UltraSPARC IIIi
- 256 MB RAM (or more)
- One of the following Sun Operating Environments with all current patches applied. Refer to *Solaris Patches*, page 31 for a link to the Sun Web site for patch information.
  - Solaris 9 (no patches required)
  - Solaris 8
- Netscape with Java support enabled (required to view online Help)
- Color depth set to 8 bit (256 colors) or greater
- 130 MB of disk space

User Workstations

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

Browsers must be set for proxy-based connections.

Macintosh Support

Websense Enterprise supports the filtering of Macintosh client machines that meet the following requirements:

- Mac OS X v10.3 and later
- Microsoft Internet Explorer v5.x or later
- Apple Safari 1.2 and later

Mac clients will generate valid log files for a Windows-based MSDE or SQL Server database.

> **NOTE**
> Websense Enterprise components cannot be installed on any Macintosh operating system.

Novell Clients

Websense eDirectory Agent requires one of the following Novell Client versions:

- Novell Client v4.81 for Windows NT/2000
- Novell Client v4.81 for Windows NT/2000 updates 5MAY2003
- Novell Client v4.83 for Windows NT/2000/XP (Recommended)
- Novell Client v4.83 SP3 for Windows NT/2000/XP 30JAN2004
- Novell Client v4.9 for Windows NT/2000/XP (Recommended)
- Novell Client v4.90 SP2 for Windows NT/2000/XP 29JUN2004

CHAPTER 3 | Upgrading Websense Enterprise

Before upgrading Websense Enterprise, make sure your equipment meets or exceeds the system requirements listed in the previous chapter. If you are upgrading from a previous version of Websense Enterprise, follow the procedures in *Upgrading on Solaris or Linux*, page 37.

The Websense Enterprise installer will upgrade all the Websense Enterprise components detected on the installation machine. The installer automatically assigns the same port numbers to the v5.5 Filtering Service that the existing v5.x EIM Server/Filtering Service uses.

You can download the Websense Enterprise Master Database during the upgrade or continue without downloading the database. The download can be performed any time after the upgrade by using the Websense Manager.

Transferring Configuration Data Without Upgrading

The recommended path for upgrading Websense Enterprise 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 Websense Enterprise 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. 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 by copying the `config.xml` file into a v5.5 system. Configuration files from earlier versions are not compatible with v5.5.

For detailed instructions on converting to v5.5 without upgrading, refer to the white paper entitled *Transferring Configuration Settings to a v5.5 System Without Upgrading* located at:

http://www.websense.com/support/documentation/

Before You Upgrade

- **Backing up files:** Before upgrading to a new version of Websense Enterprise, we recommend 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 Enterprise configuration file and the initialization files. To back up these files, stop the EIM Server/Filtering Service 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:** If you are currently running a non-English language version of Websense Enterprise, upgrading your system will convert it to English. To convert your system back to the previous non-English language version, you must install the v5.5 Language Pack, released separately from Websense Enterprise. Installation instructions are provided with the Language Pack product.
- **Upgrading distributed components:** To upgrade your system, you must run the Websense Enterprise installer on each machine on which a Websense component is installed. The installer detects all Websense Enterprise components, including the Squid Plug-in, and upgrades them accordingly.
- **Upgrading the Squid Plug-in:** To upgrade the plug-in, run the Websense Enterprise 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 Filtering Service *before* upgrading the plug-in.
- **Reporting:** To properly generate reports, you must use the same version of Websense Enterprise and Websense Reporter.
- **Websense services:** Websense services must be running when the upgrade process begins. Setup will stop and start these services as necessary during the upgrade. If these services have been running uninterrupted for several months, however, Setup 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.

- **Matching locales:** When upgrading an EIM Server/Filtering Service that is installed on a different machine from Websense Enterprise Manager, you must upgrade the EIM Server/Filtering Service in the same locale environment (language and character set) as the v5.x Websense Enterprise Manager. When upgrading on Solaris or Linux, log on to the EIM Server/Filtering Service machine with the locale appropriate to the Websense Enterprise Manager. Once the upgrade is complete, the Websense services can be restarted with any locale setting.
- **Network interface cards (NIC):** The NIC that you use for Network Agent must be in *promiscuous* mode.Contact the manufacturer of your card to see if it supports promiscuous mode.

Upgrading on Solaris or Linux

Remember to stop and restart the Websense services before attempting an upgrade if the services have been running uninterrupted for several months. The installer may time out if it is unable to stop the services promptly.

To upgrade from Websense Enterprise v5.x to v5.5:

1. Back up the following files before proceeding:
   - `websense.ini`
   - `eimserver.ini`
   - `config.xml`

NOTE

Before upgrading to a new version of Websense Enterprise, we recommend 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. Log on to the installation machine as the **root** user.
3. Create a setup directory.

   For example: `/root/Websense_Setup`

4. Download the appropriate file from http://www.my.websense.com/download and copy it to the setup directory.
   - **Solaris**: `Websense552Setup_Slr.tar.gz`
   - **Linux**: `Websense552Setup_Lnx.tar.gz`
5. Enter the following command to unzip the installer file:

   ```
   gunzip <download file name>
   ```

   For example: `gunzip Websense552Setup_Slr.tar.gz`
6. Expand the file into its components with the following command:

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

   For example: `Websense552Setup_Lnx.tar`

   This places the following files into the installation 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 Websense. Read this file with any supported browser.

7. Run the installation program from the setup directory in which it resides 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.

   The upgrade sequence is as follows:

   - **Solaris patch cluster:** If you are installing on Solaris, the installer offers to check your system for the current patch cluster.
     a. If you are unsure of the status of your patches, select **Yes** to begin the scan.

b. If Setup advises you that the proper patches are not installed, quit the installer and install the appropriate patch cluster.

WARNING

You may continue without the proper patches, but the installation could fail.

c. Continue the installation when you are sure the patches are correct for your system.

- **Upgrade option:** The installer detects the earlier version of Websense Enterprise and gives you the choice of upgrading the existing installation or exiting the installer. Be sure to close any Websense Managers connected to this Policy Server before continuing. Select **Upgrade** and press **Enter**.

IMPORTANT

You must upgrade any other Websense Enterprise modules that may have a dependency on the system you are upgrading. This will prevent conflicts caused by incompatible versions.

- **Websense services:** A list of currently running Websense services from the earlier version is displayed. A message explains that the installer must stop these services before the upgrade can proceed.
- **Communication interface:** If the installation machine contains multiple network interface cards (NIC), the installer asks which IP address Websense Enterprise should use for communication.
- **Browser location on Solaris:** If the Websense Enterprise Manager is being upgraded on Solaris, you must provide the installer with the location of Netscape.
- **Protocol block messages:** Setup advises you that you must install the Samba client (v2.2.8a and higher) to display block messages on Windows workstations blocked by Protocol Management. You may continue installing Websense and download the Samba client later. To download the Samba client, go to the Sun freeware Web site at:

  http://www.sunfreeware.com

> **NOTE**
> The Samba client is not required for protocol blocking to occur. This software controls the display of protocol blocking messages only.

- **System requirements:** 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 for optimal performance, 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 minimum.
- **Installation summary:** A summary list is displayed, showing the installation path, installation size, and the components to be upgraded.

8. Press **Enter** to begin the upgrade.

   The Download Manager progress bars are displayed as the installer downloads the upgrade files from Websense. When the download process is complete, the installer stops the Websense services and begins the upgrade.

   An installation progress bar is displayed while the installer upgrades your system and restarts the Websense services.

   The installer displays a screen announcing the success of the installation.

9. Exit the installer.
   - If you have not upgraded the Websense Manager, you are ready to select **Finish** and exit the installer.
   - If you are upgrading the Websense Manager (Solaris only), the installer asks if you want to open the Manager. By default, the Manager is selected. Select **Finish** when you are ready to exit the installer.

Upgrading Distributed Components on Windows

Run the Websense Enterprise installer on each machine on which a Websense Enterprise component is installed.

> **IMPORTANT**
> Make sure to back up the `websense.ini` file before proceeding. A full system backup is recommended.

To upgrade your v5.x Windows components to v5.5:

1. Log on to the installation machine with **domain** and **local** administrator privileges.
2. If you are installing 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 Enterprise cannot filter by users and groups. If you cannot install these components with such privileges, you may configure administrator privileges for these services after installation by using the Services Properties dialog box.

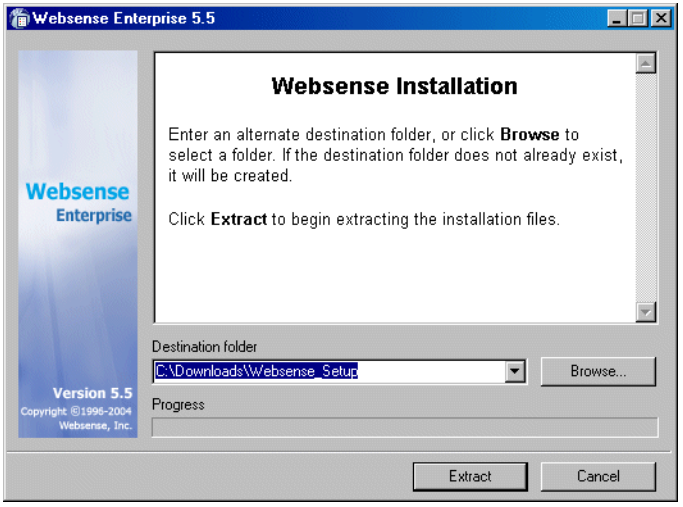
3. Run one of the following Websense Enterprise installers:
   - **Web download**: Download one of the following packages from http://www.my.websense.com/download to a folder on the installation machine and double-click to extract the installer files.
     - **Online installer**: The online installer package (`Setup552.exe`) contains only the installer files. The necessary product files are downloaded from the Web site as needed after product selections have been made.
     - **Offline installer**: The offline installer (`Websense552Setup.exe`) is much larger than the online package and contains all the files needed to upgrade Websense

Enterprise components. Use this package only if you experience difficulties upgrading Websense with the online installer.

- **Product CD**: Run `WebsenseStart.exe` from the Websense Enterprise v5.5 product CD to launch the installer start screen. Select a Websense product installation to extract the installer files.

  The file will run automatically if *autorun* is enabled. The product CD contains all the files needed to upgrade Websense Enterprise components.

A screen displays instructions for extracting the setup program.



Installer Download Extraction Screen

a. 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.

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

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.

If Websense Enterprise 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.

c. Double-click on the file and follow the steps for the online installer.

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

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

5. Select **Upgrade** and click **Next**.

NOTE

Make sure you upgrade any other Websense modules that may have a dependency on the system you are about to upgrade. This will prevent conflicts caused by incompatible versions.

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

6. Click **Next** to continue the upgrade.

   If you are upgrading on a machine with multiple network interface cards (NIC), a screen displays a list of currently active NICs.

7. Select a NIC to use for Websense Enterprise communications and 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 for optimal performance, warnings are displayed in separate screens. Installation will continue, but you should upgrade your machine for the best performance.

   - 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 will continue. To ensure the best performance of the components you are installing, you should upgrade your machine's memory to the recommended minimum.

8. If you have received a RAM warning click **Next** to continue with the installation.

   A summary screen is displayed, listing the installation path, installation size, and the components that will be installed.

9. Click **Next** to download the necessary files.

   The Download Manager progress bars are displayed as Setup downloads the necessary files from Websense. When the download process is complete, Setup stops the Websense services and begins the upgrade.

   An installation progress bar is displayed while the installer upgrades your system and restarts the Websense services.

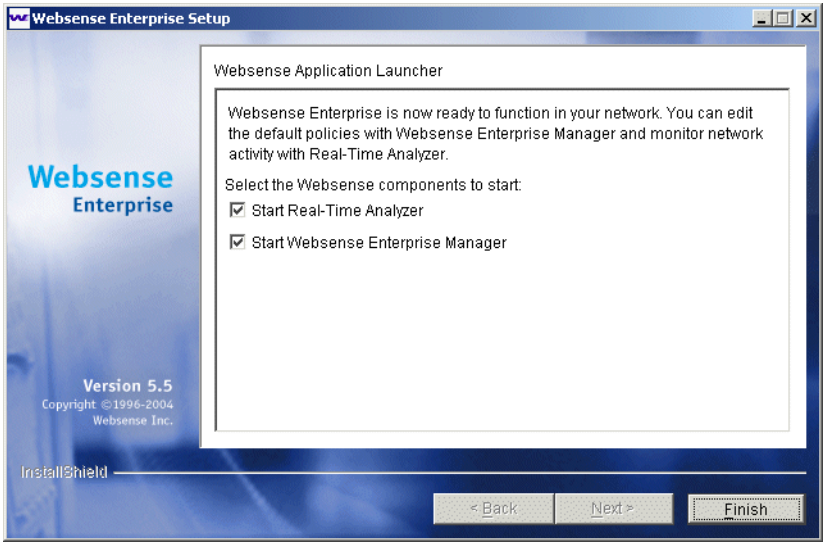
   - If the Network Agent was not upgraded, a message reminds you that Protocol Management and Bandwidth Optimizer cannot be used unless Network Agent is installed on a machine with direct access to Internet traffic. Click **Next** to continue.
   - The Websense Enterprise upgrade converts all non-English language systems to English. When a non-English language system is upgraded, the installer displays a message advising you that the Websense Enterprise Language Pack is available for converting your upgraded system to any of the supported non-English languages. The Language Pack is free and can be downloaded from http://www.my.websense.com/download.

   The final screen is displayed, announcing the success of the upgrade.

10. Click **Next** to continue.

    - If you have upgraded DC Agent, a dialog box displays advising you that the machine must be restarted to complete the installation. Select a restart option and click **Finish** to exit the installer.
    - If DC Agent was not upgraded, but you have upgraded Real-Time Analyzer and/or Websense Manager, the installer displays a screen asking if you want to launch either of those applications. By default, both are selected. Clear the checkbox of the component you do not want to launch and click **Finish**.

- If neither DC Agent, Real-Time Analyzer, nor Websense Manager were upgraded, no further action is required and you can click **Finish** to exit the installer.



Application Launcher

11. Clear the checkbox of any component you do not want to start and click **Finish** to exit the installer.
12. Click **Next** to exit the installer.

NOTE

To properly generate reports, you must use the same version of Websense Enterprise and Websense Reporter.

Converting a Stand-Alone System to an Integrated System

You can convert your Stand-Alone system to a system using Squid without losing any configuration settings. The conversion process preserves such settings as port numbers and IP addresses. Upgrades are available for the following Stand-Alone Websense Enterprise systems:

- Linux: v5.1 and v5.2
- Solaris: v5.2

> **NOTE**
> Microsoft Windows Stand-Alone systems *cannot* be converted to a system integrated with Squid. No upgrade path exists that will preserve the configuration settings.

All Components on the Same Machine

To convert Stand-Alone systems to integrated systems with all Websense components installed on the same machine, perform the following tasks:

Task 1: Perform an upgrade of the Websense Enterprise v5.x Stand-Alone system to the v5.5 Stand-Alone Edition. This will preserve your configuration data and use the settings from your original system. Follow the procedures in *Upgrading to the Stand-Alone Edition*, page 47.

Task 2: Run the Websense Enterprise installer again to convert the v5.5 Stand-Alone system to an integrated system using Squid. Follow the procedures in *Converting to an Integrated System*, page 51.

Task 3: Perform the tasks in *Chapter 5: Initial Setup*.

Distributed Components

If you want to convert your Stand-Alone system to use Squid and distribute some Websense Enterprise components to other machines, perform the following tasks:

Task 1: Perform an upgrade of the Websense Enterprise v5.x Stand-Alone system to the Websense v5.5 Stand-Alone Edition. This will preserve your configuration data and use the settings from your original system. Follow the procedures in *Upgrading to the Stand-Alone Edition*, page 47.

Task 2: Run the Websense Enterprise installer again and remove those components that you want to distribute in your network.

Task 3: Run the Websense Enterprise installer a third time to convert the v5.5 Stand-Alone system to an integrated system using Squid. Follow the procedures in *Converting to an Integrated System*, page 51.

Task 4: Run the Websense Enterprise 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 can be found in *Installing Websense Enterprise Components Separately*, page 69 for the following components:

- Websense Enterprise Manager
- DC Agent
- Network Agent
- RADIUS Agent
- eDirectory Agent
- Authentication Server

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

Upgrading to the Stand-Alone Edition

Your first task is to upgrade your v5.x Stand-Alone system to the v5.5 Stand-Alone Edition.

IMPORTANT

Websense services must be running when the upgrade process begins. Setup will stop and start these services as necessary during the upgrade. If these services have run uninterrupted for several months, however, Setup 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. For instructions on stopping and starting Websense services, refer to *Stopping or Starting Websense Services*, page 124.

The Websense installer can upgrade the following Stand-Alone versions of Websense Enterprise:

- **Solaris**: v5.2
- **Linux**: v5.1, v5.2

1. Back up the following files before proceeding:
   - `websense.ini`
   - `eimserver.ini`
   - `config.xml`

NOTE

Before upgrading to a new version of Websense Enterprise, we recommend 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. Log on to the installation machine as the **root** user.
3. Create a setup directory.

   For example: `/root/Websense_setup`
4. Download the appropriate file from http://www.my.websense.com/download to the setup directory or copy the file from the Websense Enterprise CD to the installation machine.
   - **Solaris**: `Websense552Setup_Slr.tar.gz`
   - **Linux**: `Websense552Setup_Lnx.tar.gz`
5. Enter the following command to unzip the installer file:

   `gunzip <download file name>`

   For example: `gunzip Websense552Setup_Slr.tar.gz`
6. Expand the file into its components with the following command:

   `tar xvf <unzipped file name>`

   For example: `tar xvf Websense552Setup_Lnx.tar`

This places the following files into the installation 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 Websense. Read this file with any supported browser.

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

   ```
   ./install.sh
   ```

   The installer detects the earlier version of the EIM Server/Filtering Service and gives you the choice of upgrading the existing installation or exiting Setup. Be sure to close any Websense Managers connected to this Policy Server before continuing.

8. Select **Upgrade** and press **Enter**.

   The upgrade sequence is as follows:

   - **Websense services:** A list of currently running Websense services from the earlier version is displayed. A message explains that the installer must stop these services before the upgrade can proceed.
   - **Protocol block messages:** Setup advises you that you must install the Samba client (v2.2.8a and higher) to display block messages on Windows workstations blocked by Protocol Management. You may continue installing Websense and download the Samba client later. To download the Samba client, go to the Sun freeware Web site at:

     http://www.sunfreeware.com

NOTE

The Samba client is not required for protocol blocking to occur. This software controls the display of protocol blocking messages only.

   - **Browser location on Solaris**: If the Websense Enterprise Manager is being upgraded on Solaris, you must provide the installer with the location of Netscape.

- **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 for optimal performance, 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 minimum.
- **Installation summary:** A summary list is displayed, showing the installation path, installation size, and the components to be upgraded.

9. Press **Enter** to begin the upgrade.
   - The Download Manager indicates the progress of the file download from Websense. After the files are downloaded, the installer stops all Websense services.
   - An installation progress bar is displayed and the Websense services are restarted.
   - The Websense Enterprise upgrade converts all non-English language systems to English. When a non-English language system is upgraded, the installer displays a message advising you that the Websense Enterprise Language Pack is available for converting your upgraded system to any of the supported non-English languages. The Language Pack is free and can be downloaded from http://www.websense.com.
   - Setup asks if you want to download the Websense Master Database now or at a later time using the Websense Enterprise Manager.
10. Select a download option and press **Enter**.

NOTE

Because of its size, the database can take up to 20 minutes to download.

When the database download is complete, a message is displayed advising you that the upgrade of Websense Enterprise has been successful.

A message is displayed, announcing the success of the upgrade.

11. Exit the installer.
    - If you have not upgraded the Websense Manager, you are ready to select **Finish** and exit the installer.
    - If you are upgrading the Websense Manager (Solaris GUI mode only), the installer asks if you want to open the Manager. By default, the Manager is selected. Select **Finish** when you are ready to exit the installer.

Converting to an Integrated System

Once you have upgraded your v5.x Stand-Alone system to the v5.5 Stand-Alone Edition, you are ready to convert that system to one that integrates with Squid.

IMPORTANT

If you are planning to deploy Websense Enterprise components on separate machines, run the main installer now to remove components from the Websense machine before performing the upgrade.

To convert a Solaris or Linux Stand-Alone Edition to a system integrated with Squid:

1. Back up the following files before proceeding:
    - `websense.ini`
    - `eimserver.ini`
    - `config.xml`
2. Log on to the installation machine as the **root** user.
3. Create a setup directory for the installer files.

    For example: `/root/Websense_setup`
4. Download the Websense Enterprise installer appropriate for your operating system from http://www.my.websense.com/download to the setup directory or copy it from the Websense Enterprise CD.
    - **Solaris:** `Websense552Setup_Slr.tar.gz`
    - **Linux:** `Websense552Setup_Lnx.tar.gz`

5. Enter the following command to unzip the file:

   ```
   gunzip <download file name>
   ```

   For example: `gunzip Websense552Setup_Slr.tar.gz`

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

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

   For example: `tar xvf Websense552Setup_Lnx.tar`

   This places the following files into the installation 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 Websense. 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.

   The upgrade sequence is as follows:

   - **Solaris patch cluster:** If you are installing on Solaris, setup offers to check your system for the current patch cluster.
     a. If you are unsure of the status of your patches, select **Yes** to begin the scan.
     b. If Setup advises you that the proper patches are not installed, quit the installer and install the appropriate patch cluster.

WARNING

You may continue without the proper patches, but the installation could fail.

c. Continue the installation when you are sure the patches are correct for your system.

- **Modifying an installation:** The installer detects the presence of the Websense Enterprise Stand-Alone Edition and gives you the choice of modifying the installation or converting it to an integrated system. Select **Integrate with a firewall, proxy server, or network appliance** and press **Enter** to continue.
- **Websense Filtering Service:** A message explains that the installer must stop the Filtering Service before the installation can proceed.
- **Integration selection:** Select **Squid Web Proxy Cache** from the list of supported integration types.
- **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 for optimal performance, 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 minimum.
- **Installation summary:** A summary list is displayed, showing the installation path, installation size, and the components to be updated (in this case, the Filtering Service).

8. Press **Enter** to begin the installation.

   The Download Manager copies the appropriate installer files from Websense and begins the conversion.

   The installer displays a screen announcing the success of the installation.

9. Exit the installer.

   A message is displayed advising you that the machine must be restarted to complete the installation.

10. Select a restart option and click **Enter** to exit the installer.

Changing Network Addresses of Installed Components

Websense Enterprise 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 Enterprise 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, refer to the Websense Enterprise *Administrator's Guide*.

CHAPTER 4

Installation

This chapter contains instructions for a new installation of all the Websense components and the initial setup procedures for preparing Websense Enterprise to communicate with the Squid Web Proxy Cache.

Before Installing

Please read the following information before installing Websense Enterprise.

- **Non-English language versions:** Websense Enterprise v5.5 installs in English only. Language Packs for converting systems to non-English language versions are released separately from Websense Enterprise. Installation instructions are provided with the Language Pack product.
- **Reporting:** To properly generate reports, you must use the same version of Websense Enterprise and Websense Enterprise Reporter.
- **Deployment:** Websense Enterprise for the Squid Web Proxy Cache is supported on Solaris and Linux operating systems only. You can install the main Websense Enterprise components (Filtering Service, Policy Server, and User Service) on the Squid machine or together on a separate machine. The Websense Enterprise Manager can be installed with the main Websense Enterprise components on Solaris or separately on Windows. Network Agent can be installed on Windows and Linux. DC Agent is supported on Windows only.

  You can install the Filtering Service, Policy Server, User Service, and Websense Enterprise Manager on machines with different operating systems. For example, you can install Websense Enterprise Manager on a Windows machine and use it to configure a Policy Server running on a Linux machine.
- **LDAP directory:** If your directory service information resides in an LDAP directory, Websense uses LDAP-related information such as the LDAP server IP Address and port, base domain, LDAP cache, etc. from the `records.config` file.

- **Network Interface Cards (NIC):** The NIC that you use for Network Agent must be in *promiscuous* mode. (Contact the manufacturer of your card to see if it supports promiscuous mode.) Network Agent is capable of supporting multiple NICs. For instructions on configuring Network Agent to work with additional NICs, refer to the Websense Enterprise *Administrator's Guide*.
- **Web server:** To install Real-Time Analyzer (RTA) you must have either Microsoft IIS or Apache Web Server installed. If neither supported Web server is detected, the installer gives you the option to install the Apache Web Server or continue the installation without installing RTA.
- **Internet access:** For the database download to occur during installation, the Websense Enterprise machine 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 Websense Enterprise machine can access.
- **Enabling Java Interfaces:** If you are installing any Websense Enterprise 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, refer to the procedure in the troubleshooting topic *Websense Enterprise splash screen is displayed, but installer does not launch on Windows 2000*, page 174.

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

Installing Websense Enterprise

You can install the supported Websense Enterprise components on the Squid Web Proxy machine or on a separate machine. If you are installing Websense Enterprise and Squid together, you also must install the Squid Plug-in. This allows Websense to communicate with the Squid Web Proxy.

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 machine that will communicate with Websense. For instruction on installing the Squid Plug-in, refer to *Installing the Plug-in on the Squid Web Proxy Machine*, page 66.

Follow these installation procedures for each Solaris or Linux machine on which you want to install Websense Enterprise.

You may install the following Websense Enterprise components together on the same machine:

- Filtering Service
- Policy Server
- User Service
- Websense Enterprise Manager (Solaris only)
- Network Agent
- eDirectory Agent
- Logon Agent

You can install the Websense Enterprise Manager after you finish installing the main Websense Enterprise components. The Websense Manager is not supported on Linux, and must be installed on either a Windows machine or a Solaris machine. See *Installing Websense Enterprise Components Separately*, page 69 for instructions on installing individual Websense components.

To install all the Websense Enterprise components on a Solaris or Linux machine:

1. Log on to the installation machine as the **root** user.
2. Create a setup directory.

   For example: `/root/Websense_setup`
3. Download the installer file for your operating system from http://www.websense.com/downloads, or copy it from the Websense Enterprise CD and save it to the setup directory.

- **Solaris:** `Websense552Setup_Slr.tar.gz`
- **Linux:** `Websense552Setup_Lnx.tar.gz`

4. Enter the following command to unzip the file:

   `gunzip <download file name>`

   For example: `gunzip Websense552Setup_Slr.tar.gz`

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

   `tar xvf <unzipped file name>`

   For example: `tar xvf Websense552Setup_Lnx.tar`

   This places the following files into the installation 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 Websense. Read this file with any supported browser.

6. 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.

   The installer sequence is as follows:

   - **Solaris patch cluster:** If you are installing on Solaris, setup offers to check your system for the current patch cluster.

     a. If you are unsure of the status of your patches, select **Yes** to begin the scan.

b. If Setup advises you that the proper patches are not installed, quit the installer and install the appropriate patch cluster.

WARNING

You may continue without the proper patches, but the installation could fail.

c. Continue the installation when you are sure the patches are correct for your system.

- **Installation type:** Select either **Typical** or **Custom** to install all the components.
  - **Typical:** installs Websense Filtering Service, Policy Server, and User Service together on the same machine. The installer gives you the option of installing Network Agent, eDirectory Agent, and the Logon Agent. The Websense Manager is installed automatically on Solaris.
  - **Custom:** allows you to install individual Websense Enterprise components. You can use this option to install additional instances on separate machines.
- **Communication interface:** If the installation machine is multihomed, all enabled network interface cards (NIC) with an IP address appear in a list. Select the card you want Websense Enterprise to use to communicate.

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.

- **Setup type:** Select **Integrated.**
- **Integration product:** Select **Squid Web Proxy Cache**.
- **Configuration type:** If you are installing Websense Enterprise on the Squid Web Proxy machine, select **Install plug-in and other selected Websense Enterprise components**. If you are installing Websense Enterprise on a separate machine, select **Install selected Websense Enterprise components without plug-in**.

- **Configuration file:** If you are installing Websense Enterprise 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 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 and to the Filtering Service. If either of the default ports is in use, you will be required to select an alternate port. The range of valid port numbers is from 1024 to 65535.

NOTE

Remember the port numbers if you change them from the defaults. You will need them when you install the Websense Enterprise Reporter.

- **Subscription key:** Setup can download and install the Websense Master Database during installation.
  - **I have a Websense subscription key:** If you have a valid subscription key, select this option and enter your key when prompted. Setup will download the Websense Master Database during installation.
  - **I need a 30-day evaluation key:** If you select this option, you are directed to fill out a form on http://www.websense.com/keyrequest. An evaluation key will be sent to you by email. You can enter your key as soon as you receive it, and Setup will download the Master Database.
  - **I do not wish to use a key at this time:** Select this option if you want to download the Master Database after installation via the Websense Manager. Refer to *Subscription Key and Database Download*, page 129 for instructions.

- **Network Agent:** Install Network Agent or test the visibility of Internet traffic from this screen.

IMPORTANT

The machine on which the Network Agent is installed must be able to monitor 2-way employee Internet traffic for Network Agent to function properly. If you install the Network Agent on a machine that cannot monitor targeted Internet traffic, Dynamic Protocol Management, Bandwidth Optimizer, and IM Attachments will not perform as expected.

You are given the following three options:

- **Test Traffic Visibility:** launches the utility that tests the Internet visibility of the active network interface cards (NIC) in the installation machine.
- **Install Network Agent:** installs the Network Agent without conducting the traffic visibility test. Use this option if you know that the installation machine has the necessary Internet traffic visibility.
- **Do not install Network Agent:** allows you to continue the Websense Enterprise installation without installing the Network Agent.

To check the visibility of Internet traffic from the installation machine:

a. Select **Test Traffic Visibility**.

b. Select the network interface card (NIC) that you want to use for the Network Agent and continue to the next panel. Active cards on the installation machine appear in this list, including NICs without IP addresses (stealth mode).

   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.

c. If the network you want to test with the NIC does not appear in the default list, select **Add Network**.

   – 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.

– Select **Redisplay** to return to the options list.

Your new network appears in the list.

d. Select **Remove a Network** to delete a network from the list.

e. Select **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 panel 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 needs to monitor.

f. If the Network Agent 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.

– 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. You may continue with the installation without installing Network Agent and reconfigure your network later, or make the necessary changes and retest immediately.

g. Select **Exit Tool** when you are ready to continue installation.

h. Select **Install Network Agent** if you are sure that your NIC is able to monitor all targeted Internet traffic.

Select **Do not install Network Agent** if the visibility test fails or if you have decided to wait to install Network Agent. 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.

- **Network interface card (NIC) selection:** If the installation machine has multiple network interface cards, all enabled cards appear in a list. Select the NIC that you tested successfully for network visibility. Cards configured for stealth mode will appear on this list.

- **Initial filtering options:** Websense Enterprise can be configured to filter Internet traffic immediately after installation, based on a predefined policy, or to monitor Internet traffic only. Select **Yes** to filter traffic initially, or **No** if you want to evaluate your network before applying any type of filtering. You must install a Websense Enterprise reporting tool to report on network activity.
- **Transparent user identification:** Select one of the following:
  - **Identify users via Novell eDirectory authentication**: Select this option to install and configure Websense eDirectory to authenticate users transparently through Novell Directory Server.
  - **Identify users as they log on to domains:** Select this option to install the Logon Agent to authenticate Windows users transparently when they log onto 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. Refer to *Creating and Running the Script for Logon Agent*, page 135 for instructions.
  - **Do not install an Agent**: This option configures Websense Enterprise to authenticate users through **Squid Web Proxy Cache**.

NOTE

You can configure manual authentication in the Websense Enterprise Manager after installation and initial setup.

Protocol block messages: Setup advises you that you must install the Samba client (v2.2.8a and higher) to display block messages on Windows workstations blocked by Protocol Management. You may continue installing Websense and download the Samba client later. To download the Samba client, go to the Sun freeware Web site at:

http://www.sunfreeware.com

NOTE

The Samba client is not required for protocol blocking to occur. This software controls the display of protocol blocking messages only.

- **Web browser:** For Solaris installations, you must provide the full path to the Web browser you want to use when viewing online help. This information is requested only when you choose a **Typical** installation or are installing Websense Enterprise Manager separately.
- **Directory path:** This is the path to the installation directory where Websense will create the `/opt/Websense` directory. If this directory does not already exist, the installer will create it automatically.

IMPORTANT

The full installation path must use ASCII characters *only*.

- **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 for optimal performance, 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 minimum.
- **Installation summary:** A summary list appears, showing the installation path, installation size, and the components you have selected. Press **Enter** to begin the installation.
- **Installation:** The Download Manager copies the appropriate installer files from Websense and begins the installation. The installer creates the `/opt/Websense` directory, and the `/opt/Websense/Manager` directory if you installed Websense Enterprise Manager (Solaris only). It also sets up the necessary files, including `/etc/rc3.d/S11WebsenseAdmin`, which enables Filtering Service to start automatically each time the system starts.
  - If the Network Agent was not installed, a message reminds you that Protocol Management and Bandwidth Optimizer cannot be used unless Network Agent is installed on a machine with direct access to Internet traffic. Click **OK** to continue.
- **Restart Squid**: If you have installed Websense Enterprise on the Squid machine, the installer prompts you restart Squid.

If you provided a valid subscription key when prompted, setup asks if you want to download the Websense Master Database now or at a later time using the Websense Enterprise Manager.

7. Select a download option and press Enter.

> **NOTE**
>
> Because of its size, the database can take up to 20 minutes to decompress and download.

When the database download is complete, a message appears advising you that the upgrade of Websense Enterprise has been successful.

The installer displays a screen announcing the success of the installation.

8. Exit the installer.
   - If you have not installed the Websense Manager, you are ready to select **Finish** and exit the installer.
   - If you are installing the Websense Manager (Solaris GUI mode only), the installer asks if you want to open the Manager. By default, the Manager is selected. Select **Finish** when you are ready to exit the installer.
9. If you did not install the Websense Enterprise Manager on this machine, you must install it on a separate Windows or Solaris machine in your network. Follow the instructions under *Installing Websense Enterprise Components Separately*, page 69.

> **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 Enterprise components and offers you options for modifying your installation. For instructions, refer to *Modifying an Installation*, page 102.

Installing the Plug-in on the Squid Web Proxy Machine

If you installed Websense Enterprise 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 Websense and Squid can communicate. You must install the Squid Plug-in after installing the Websense Filtering Service.

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. Create a setup directory.

   For example: `/root/Websense_setup`
4. Download the installer file from http://www.websense.com/downloads, or copy it from the Websense Enterprise CD and save it to the setup directory.
   - **Solaris**: `Websense552Setup_Slr.tar.gz`
   - **Linux**: `Websense552Setup_Lnx.tar.gz`
5. Enter the following command to unzip the installer file:

   `gunzip <download file name>`

   For example: `gunzip Websense552Setup_Slr.tar.gz`
6. Expand the file into its components with the following command:

   `tar xvf <unzipped file name>`

   For example: `tar xvf Websense552Setup_Lnx.tar`

   This places the following files into the installation 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 Websense. 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.

   The installation sequence is as follows:

   - **Solaris patch cluster**: If you are installing on Solaris, Setup offers to check your system for the current patch cluster.
     a. If you are unsure of the status of your patches, select **Yes** to begin the scan.
     b. If Setup advises you that the proper patches are not installed, quit the installer and install the appropriate patch cluster.

WARNING

You may continue without the proper patches, but the installation could fail.

     c. Continue the installation when you are sure the patches are correct for your 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.

IMPORTANT

The default for the configuration port (55806) is the 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 in this dialog box.

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

- **Installation directory:** path to the installation directory where Websense will create the `/opt/Websense` directory. If this directory does not already exist, the installer will create it automatically. If you want to install the Squid Plug-in into a different directory, type in the new path.

IMPORTANT

The full installation path must use ASCII characters *only*.

- **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 for optimal performance, 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 minimum.
- **Installation summary:** A summary list appears, showing the installation path, installation size, and the component you have selected.

8. Press **Enter** to begin the installation.

   The Download Manager copies the appropriate installer files from Websense and begins the installation. The installer creates the `/opt/Websense` directory and installs the Squid Plug-in in that location.

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

9. Exit the installer when the installer displays the successful installation message.
10. Restart the Squid Web Proxy Cache.

Installing Websense Enterprise Components Separately

All Websense Enterprise components can be installed separately using the **Custom** feature of the Websense installer. Your environment may require you to install the Websense Manager and some of the optional components apart from the Websense Filtering Service. You can install these components alone or together on remote machines in your network. This section describes the procedures for installing the following Websense components on separate machines in your network:

- **Websense Manager**: Websense Manager can be installed on Windows and Solaris operating systems and can connect to a Policy Server on the same operating system or on a different operating system. Websense Manager is not supported on Linux.
- **DC Agent**: DC Agent runs on Windows only and is installed in networks using 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.
- **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.
- **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.
- **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, Linux, and Solaris. Logon Agent receives user information at logon from an application called `LogonApp.exe`, which must be run by a logon script. For instructions on creating and running this logon script, refer to *Creating and Running the Script for Logon Agent*, page 135.

NOTE

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

If you want to install Websense Enterprise core components in a distributed environment, refer to the Websense *Deployment Guide* for instructions.

Windows Procedures

The steps in this section are common to all separate installations of Websense Enterprise 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

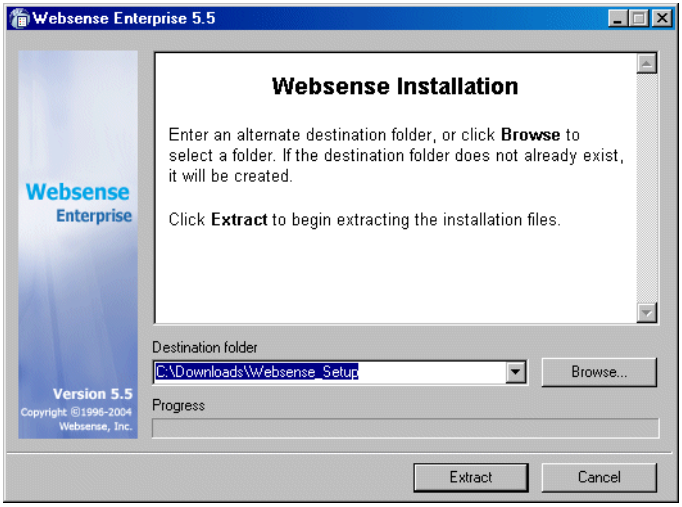
If you are installing DC Agent, log on with **domain** administrator privileges. DC Agent must have administrator privileges on the network to retrieve user login information from the domain controller. Without this information, Websense Enterprise cannot filter by users and groups. If you cannot install these components with such privileges, you may configure administrator privileges for these services after installation in the Properties dialog box for Windows services.

2. Run one of the following Websense Enterprise installers:
   - **Web download**: Download one of the following packages from http://www.websense.com/downloads to a folder on the installation machine and double-click to extract the installer files.
     - **Online installer**: The online installer package (`Setup552.exe`) contains only the installer files. The necessary product files are downloaded from the Web site as needed after product selections have been made.
     - **Offline installer**: The offline installer (`Websense552Setup.exe`) is much larger than the online package and contains all the files needed to install Websense Enterprise components. Use this package only if you experience difficulties installing Websense with the online installer.

- **Product CD**: Run `WebsenseStart.exe` from the Websense Enterprise v5.5 product CD (`\WebsenseStart`) to launch the installer start screen. Select a Websense product installation to extract the installer files.

  The file will run automatically if *autorun* is enabled. The product CD contains all the files needed to upgrade Websense Enterprise components.

A screen displays instructions for extracting the setup program.



Installer Download Extraction Screen

a. 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.

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

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.

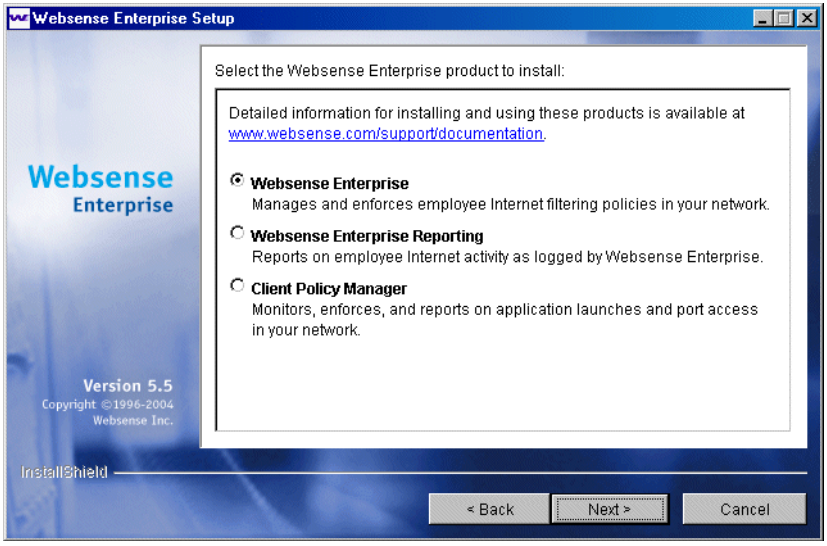
If Websense Enterprise installation files already exist in that location, you may choose to overwrite the existing files.

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.

3. Click **Next** on the welcome screen and follow the on-screen instructions through the subscription agreement.

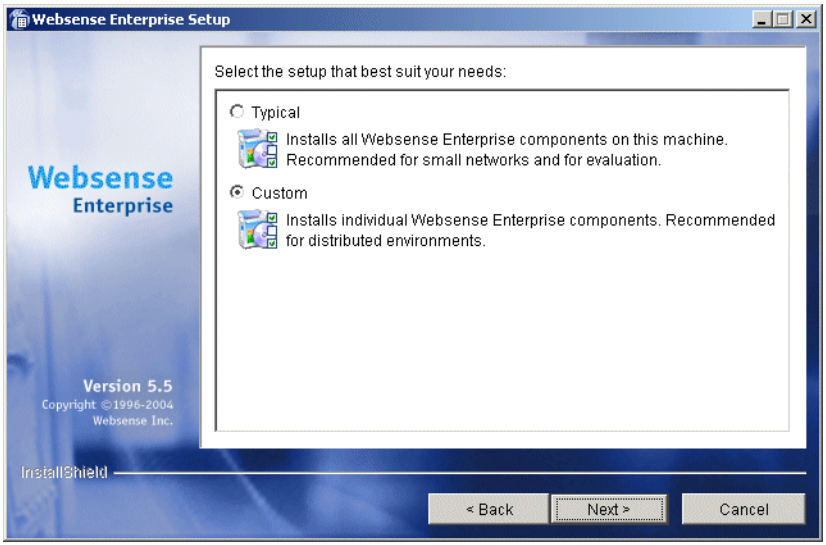
   You are asked to select a Websense product to install.



Websense Product Selection Screen

4. Select **Websense Enterprise** and click **Next**.

   You are offered a choice of two setup types.



Setup Type Dialog Box

5. Select **Custom** and click **Next**.
6. To continue, proceed to the appropriate component section below.

Websense Enterprise Manager

When you install Websense Enterprise on Linux, you must install the Websense Manager on a separate Windows or Solaris machine in your network. Use the following procedure to install the Websense Manager on a Windows machine.

1. Download and start the Windows installer using the procedure in *Windows Procedures*, page 70.
2. Select **Websense Enterprise Manager** from the list of components to install and click **Next**.

   A dialog box appears, asking you to select an installation directory for the Websense Enterprise 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 minimum.

A summary list appears, showing the installation path, installation size, and the components you have selected.

4. Click **Next** to start the installation.
   - The Download Manager progress bars are displayed as Setup downloads the appropriate installer files from Websense. Installation begins automatically when the necessary files have been downloaded.
   - If the Network Agent was not installed, a message reminds you that Protocol Management and Bandwidth Optimizer cannot be used unless Network Agent is installed on a machine with direct access to Internet traffic. Click **OK** to continue.
   - When the installation is finished, a message appears advising you that the procedure was successful.
5. Click **Next** to continue.

   The installer displays a screen asking if you want to launch the Websense Manager. By default, the Manager is selected for launch.
6. Make a selection, and click **Finish**.

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.

If this 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 the Network Agent. For instructions on defining IP address ranges for multiple Network Agents, refer to the Websense Enterprise *Administrator's Guide*.

If you are attempting to install the Network Agent on a machine on which the Filtering Service and Policy Server are already installed, refer to the procedures in *Adding Components*, page 102.

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

To install the Network Agent on a Windows system:

1. Download and start the Windows installer using the procedure in *Windows Procedures*, page 70.
2. Select **Network Agent** from the list of components to install and click Next.

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

   > **IMPORTANT**
   > 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 in this dialog box.

3. Enter the IP address of the Policy Server machine and click **Next**.

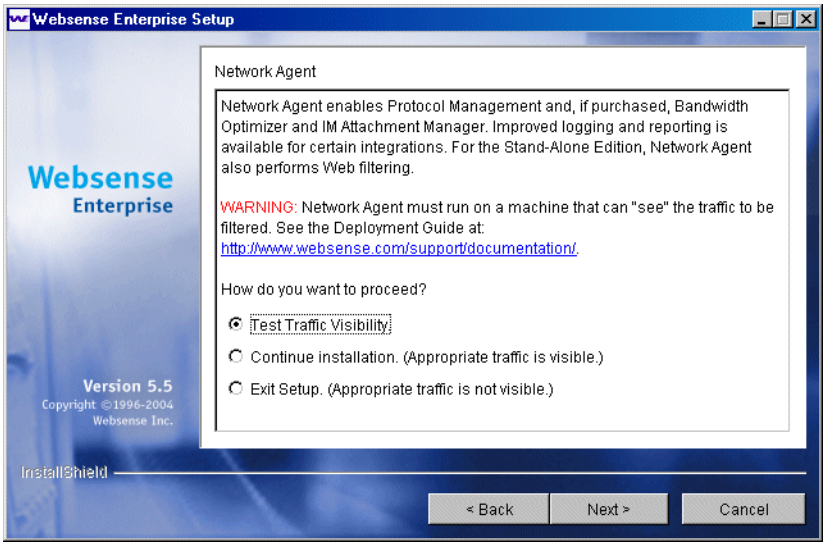
   If the installation machine is multihomed, all enabled network interface cards (NIC) with an IP address appear in a list.
4. Select the card you want Websense Enterprise to use to communicate and click **Next**.

   The installer displays the Network Agent installation screen and offers you the option of testing your machine's visibility to Internet traffic. The

machine on which the Network Agent is installed must be able to monitor 2-way employee Internet traffic for Network Agent to function properly.

IMPORTANT

If you install the Network Agent on a machine that cannot monitor targeted Internet traffic, some features, such as Dynamic Protocol Management and Bandwidth Optimizer, will not perform as expected.



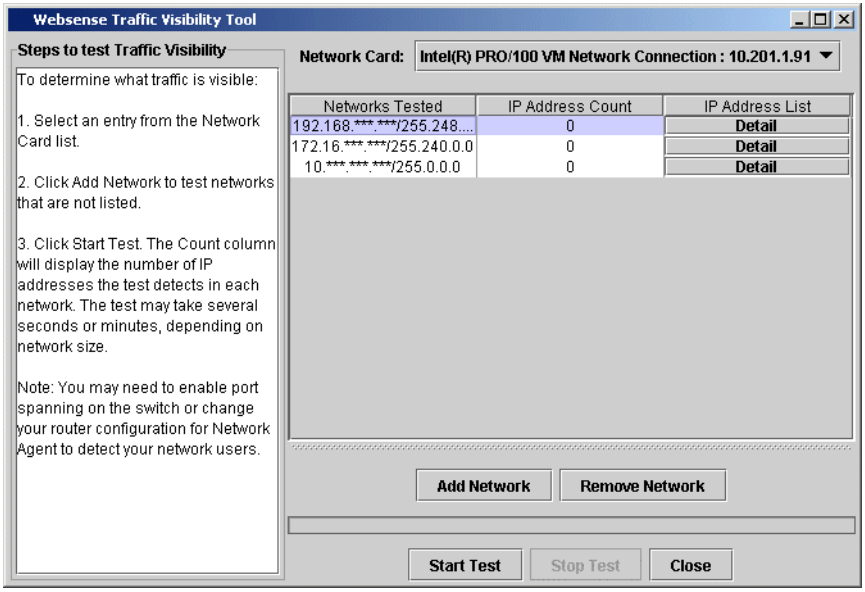
Network Agent Installation Screen

You are given the following three options:

- **Test Traffic Visibility**: This selection launches the utility that tests the Internet visibility of the active network interface cards (NIC) in the installation machine.
- **Continue installation**: If you know that the installation machine has the necessary Internet traffic visibility, you may select this option and continue the installation without conducting the visibility test.
- **Exit Setup**: If you determine that the installation machine cannot see the appropriate Internet traffic, select this option to exit Setup. Select another machine for installation, reposition the current machine in the network, or replace the NIC. Remember that the NIC must have an IP address for Network Agent to function.

5. Click **Test Traffic Visibility** to check the visibility of Internet traffic from the installation machine.

   The **Traffic Visibility Test** tool appears.



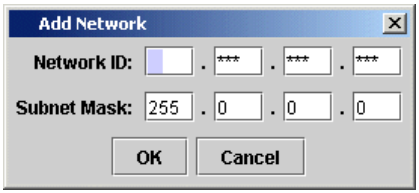
Traffic Visibility Test Tool

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.
Detail	Lists all the IP addresses in the network from which Internet traffic is being detected.

a. From the **Network Card** drop-down list, select the network interface card (NIC) that you want to use for the Network Agent.

b. 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.



c. 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.

d. Click **OK** to return to the **Traffic Visibility Test** dialog box.

Your new Network appears in the list.

e. 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.

f. If the Network Agent 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.
- 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.

g. Click **Stop Test** when you are ready to continue installation.

h. Click **Close** to exit the traffic visibility test screen.

6. Continue with the installation or exit Setup.

- Select **Continue installation** if you are sure that your NIC is able to monitor all targeted Internet traffic. This will install the Network Agent.

- Select **Exit Setup** if the visibility test fails. You must either reposition the machine in the network, select another machine on which to install the Network Agent, or install a different NIC.

7. Click **Next** to continue.

   The installer asks you if the Network Agent is being installed on a machine that is acting as a firewall. Network Agent cannot function properly on a machine running a firewall.

8. Select **Yes** or **No,** and then click **Next** to continue.

   - Select **Yes** if you are attempting to install Network Agent on a firewall machine, and Setup will close. Continue the Network Agent installation on a machine that is not running a firewall.
   - Select **No** if the installation machine is not being used as a firewall. Installation will continue.

   If the installation machine has multiple network interface cards (NIC), a screen appears asking you to select the network interface card (NIC) that you want to use for capturing traffic. All network interface cards enabled in the machine appear in a list.

9. If presented with a list, select the desired card and click **Next** to continue.

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

IMPORTANT

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

10. Enter the IP address and port number of the Filtering Service machine and click **Next**.

    Setup asks you to select an installation folder for the Websense Enterprise components.

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

A summary list appears, showing the installation path, installation size, and the components you have selected.

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

    The Download Manager progress bars are displayed as Setup downloads the appropriate installer files from Websense. Installation begins automatically when the necessary files have been downloaded.

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

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

DC Agent

DC Agent installs on Windows only and is used in networks that authenticate users with a Windows directory service (NTLM-based or Active Directory). If you installed Websense Enterprise on a Windows machine, you were prompted to install the Websense DC Agent. If you did not install it together with the Filtering Service at that time, or if you need to authenticate through a Windows-based directory service, you can install DC Agent 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, refer to *Websense Enterprise Components*, page 13.

To install DC Agent on a Windows system:

1. Download and start the Windows installer using the procedure in *Windows Procedures*, page 70.

2. Select **DC Agent** from the list of components to install and click **Next**.

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

3. Select the card you want Websense Enterprise to use to communicate and click **Next**.

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

> **IMPORTANT**
>
> 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 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. If you attempt to install DC Agent without providing access to directory information, DC Agent will be unable to identify users transparently.

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

   Setup asks you to select an installation folder for the Websense Enterprise components.

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

A summary list appears, showing the installation path, installation size, and the components you have selected.

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

   The Download Manager progress bars are displayed as Setup downloads the appropriate installer files from Websense. Installation begins automatically when the necessary files have been downloaded.

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

   A message appears advising you that the procedure was successful.

8. Click **Next** to continue.

   A dialog box appears advising you that the machine must be restarted to complete the installation.

9. Select a restart option and click **Finish** to exit the installer.

10. Configure User Service to communicate with DC Agent by following the instructions for identifying users in the Websense Enterprise *Administrator's Guide*.

Real-Time Analyzer (RTA)

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

To install RTA:

1. Download and start the Windows installer using the procedure in *Windows Procedures*, page 70.

2. Select **Real-Time Analyzer** from the list of components to install and click **Next**.

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

3. Select the card you want Websense Enterprise to use to communicate and click **Next**.

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

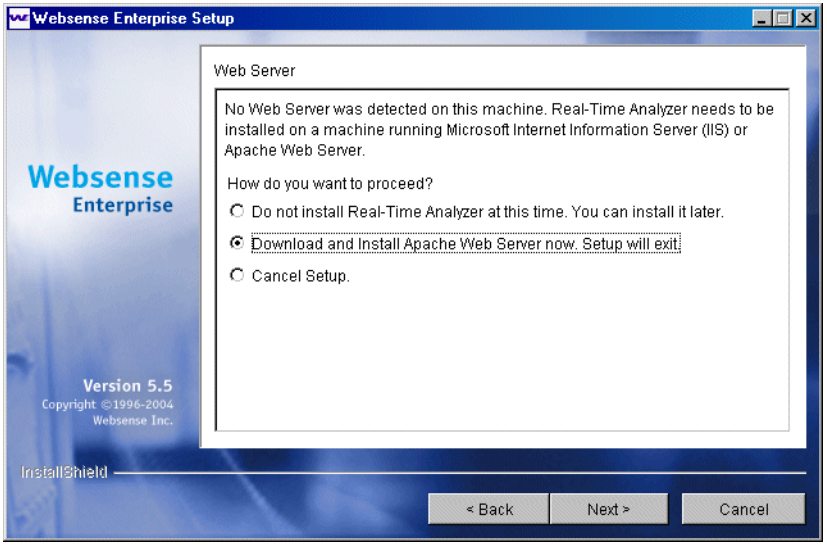
IMPORTANT

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 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 Web 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 Web Server or continue the installation without installing RTA.



RTA Web Server Dialog Box

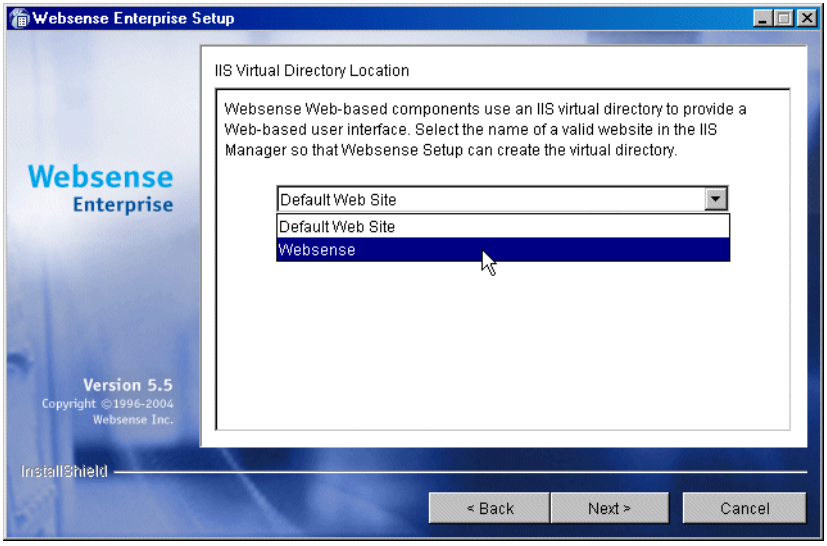
If you select the Apache Web Server installation option, the Websense installer starts the Apache installer and exits without installing any Websense Enterprise components. You must restart your computer after installing the Apache Web Server and run the Websense Enterprise installer again to install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

NOTE

Apache Web Server documentation is installed in HTML format in the `docs/manual/` directory. The latest version can be found 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 for the name of the Web site 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.



Default Web Site Selection

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

   Setup asks you to select an installation folder for the Websense Enterprise components.

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

   A summary list appears, showing the installation path, installation size, and the components you have selected.

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

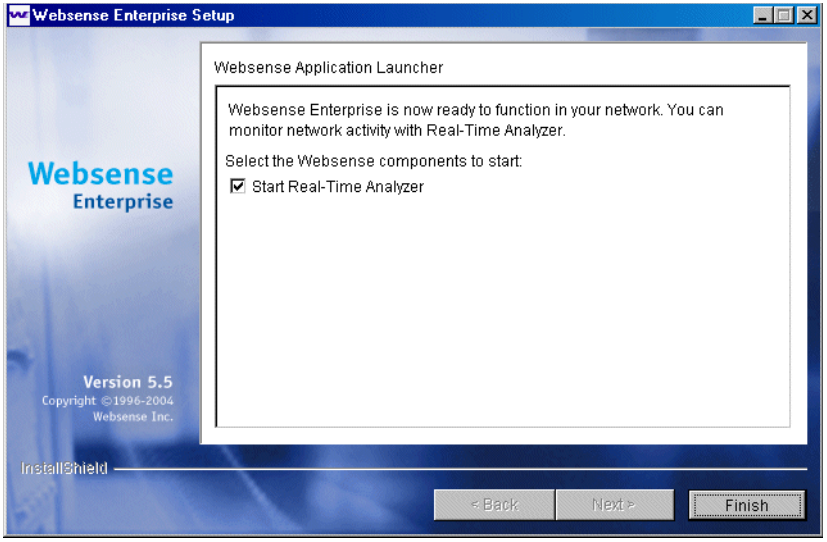
   The Download Manager progress bars are displayed as Setup downloads the appropriate installer files from Websense. Installation begins automatically when the necessary files have been downloaded.

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

   A message appears advising you that the procedure was successful.

9. Click **Next** to continue.

   The application launcher screen appears asking if you want to start the Real-Time Analyzer. The checkbox is checked by default.



Application Launcher

10. Make your selection and click **Finish** to exit the installer.

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 Enterprise to identify users transparently 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 system:

1. Download and start the Windows installer using the procedure in *Windows Procedures*, page 70.
2. Select **RADIUS Agent** from the list of components to install and click **Next**.

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

> **IMPORTANT**
>
> 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 in this dialog box.

3. Enter the IP address of the Policy Server machine and click **Next**.

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

4. Select the card you want Websense Enterprise to use to communicate and click **Next**.

   Setup asks you to select an installation folder for the Websense Enterprise components.

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

   A summary list appears, showing the installation path, installation size, and the components you have selected.

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

   The Download Manager progress bars are displayed as Setup downloads the appropriate installer files from Websense. Installation begins automatically when the necessary files have been downloaded.

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

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

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

8. Configure the RADIUS Agent in the Websense Enterprise Manager by selecting **Server > Settings > User Identification > RADIUS Agent**.

eDirectory Agent

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

To install the eDirectory Agent on a Windows system:

1. Download and start the Windows installer using the procedure in *Windows Procedures*, page 70.
2. Select **eDirectory Agent** from the list of components to install and click **Next**.

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

   IMPORTANT

   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 in this dialog box.

3. Enter the IP address of the Policy Server machine and click **Next**.

   If the installation machine is multihomed, all enabled network interface cards (NIC) with an IP address appear in a list.
4. Select the card you want Websense Enterprise to use to communicate and click **Next**.

   Setup asks for the Novell eDirectory name and password.
5. Enter the full *distinguished name* and a valid password, and then click **Next** to continue.

   Setup asks you to select an installation folder for the Websense Enterprise components.
6. Accept the default path (`C:\Program Files\Websense`), or click **Browse** to locate another installation folder and 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 minimum.

A summary list appears, showing the installation path, installation size, and the components you have selected.

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

   The Download Manager progress bars are displayed as Setup downloads the appropriate installer files from Websense. Installation begins automatically when the necessary files have been downloaded.

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

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

8. Click **Finish** to exit the installer.
9. Configure the eDirectory Agent in the Websense Enterprise Manager by selecting **Server > Settings > User Identification > eDirectory Agent**.

Logon Agent

The Websense Logon Agent identifies users as they log on to a Windows domain. The Logon Agent receives logon information from `LogonApp.exe`, a separate application that must be run by a logon script. For information on setting up this script, refer to *Creating and Running the Script for Logon Agent*, page 135.

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.

To install the Logon Agent on a Windows system:

1. Download and start the Windows installer using the procedure in *Windows Procedures*, page 70.

2. Select **Logon Agent** from the list of components to install and click **Next**.

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

   IMPORTANT

   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 in this dialog box.

3. Enter the IP address of the Policy Server machine and click **Next**.

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

4. Select the card you want Websense Enterprise to use to communicate and click **Next**.

   Setup asks you to select an installation folder for the Websense Enterprise components.

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

   A summary list appears, showing the installation path, installation size, and the components you have selected.

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

   The Download Manager progress bars are displayed as Setup downloads the appropriate installer files from Websense. Installation begins automatically when the necessary files have been downloaded.

7. Click **OK** to continue.

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

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

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

Solaris and Linux Procedures

The steps in this section are common to all separate installations of Websense Enterprise 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 Solaris or Linux:

1. Log on to the installation machine as the **root** user.
2. Create a setup directory for the installer files.

   For example: `/root/Websense_setup`

3. Download the installer file from http://www.websense.com/downloads, or copy it from the Websense Enterprise CD and save it to the setup directory.
   - **Solaris**: `Websense552Setup_Slr.tar.gz`
   - **Linux**: `Websense552Setup_Lnx.tar.gz`
4. Enter the following command to unzip the installer file:

   ```
   gunzip <download file name>
   ```

   For example: `gunzip Websense552Setup_Slr.tar.gz`

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

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

   For example:

   ```
   tar xvf Websense552Setup_Lnx.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 Websense. Read this file with any supported browser.

6. 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.

7. If you are installing on Solaris, make sure your patches are current.

   Setup offers to check your system for the current patch cluster.

   a. If you are unsure of the status of your patches, select **Yes** to begin the scan.

   b. If Setup advises you that the proper patches are not installed, quit the installer and install the appropriate patch cluster.

   WARNING

   You may continue without the proper patches, but the installation could fail.

   c. Continue the installation when you are sure the patches are correct for your system.

8. Select **Custom** when asked what type of installation you want.

9. To continue, proceed to the appropriate component section.

Websense Enterprise Manager

When you install Websense Enterprise on Linux, you must install the Websense Manager on a separate Windows or Solaris machine in your network. Use the following procedure to install the Websense Manager on a Solaris machine.

1. Download and start the Solaris installer using the procedure in *Solaris and Linux Procedures*, page 91.
2. Select **Websense Enterprise Manager** from the list of components to install and press **Enter**.

   Setup 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 where Websense Enterprise will create the Websense directory
4. Provide a path to the installation directory or accept the default (`/opt/Websense/`).

   If this directory does not already exist, the installer creates it automatically.

   IMPORTANT
   The full installation path must use only ASCII 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 minimum.

   A summary list appears, showing the installation path, installation size, and the component (Websense Manager) you have selected.
5. Press **Enter** to begin installing the Websense Manager.

   The Download Manager copies the appropriate installer files from Websense and begins the installation.

If the Network Agent was not installed, a message reminds you that Protocol Management and Bandwidth Optimizer cannot be used unless Network Agent is installed on a machine with direct access to Internet traffic.

The installer displays a screen announcing the success of the installation.

6. Press **Enter** to continue.

   If you are installing in GUI mode, the installer displays a screen asking if you want to launch the Websense Manager. By default, the Manager is selected for launch.

7. Make a selection, and select **Finish** to exit the installer.
8. Refer to *Chapter 5: Initial Setup* to prepare your Websense Enterprise system to begin filtering.

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.

If this 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 the Network Agent. For instructions on defining IP address ranges for multiple Network Agents, refer to the Websense Enterprise *Administrator's Guide*.

If you are attempting to install the Network Agent on a machine on which the Filtering Service and Policy Server are already installed, refer to the procedures in *Adding Components*, page 102.

> **IMPORTANT**
> The Websense Filtering Service and the Policy Server must be installed and running prior to installing the Network Agent. The installer asks for the IP addresses and port numbers of these components and will not install the 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 91.
2. Select **Network Agent** from the list of components to install and press **Enter**.

   If the installation machine is multihomed, all enabled network interface cards (NIC) with an IP address are displayed.
3. Select the card you want Websense Enterprise to use to communicate and press **Enter**.

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

> **IMPORTANT**
> 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 in this dialog box.

4. Enter the IP address of the Policy Server machine and press **Enter**.

   The installer gives you the opportunity to test your machine's visibility to Internet traffic with the Traffic Visibility Test tool. The machine on which

the Network Agent is installed must be able to monitor 2-way employee Internet traffic for Network Agent to function properly.

> **IMPORTANT**
> If you install the Network Agent on a machine that cannot monitor targeted Internet traffic, Dynamic Protocol Management and Bandwidth Optimizer, will not perform as expected.

You are given the following three options:

- **Test Traffic Visibility**: This selection launches the utility that tests the Internet visibility of the active network interface cards (NIC) in the installation machine.
- **Continue installation**: If you know that the installation machine has the necessary Internet traffic visibility, you may select this option and continue the installation without testing the visibility of the interfaces.
- **Exit Setup**: If you determine that the installation machine cannot see the appropriate Internet traffic, select this option to exit Setup. Select another machine for installation, reposition the current machine in the network, or replace the NIC. Remember that the NIC must have an IP address for Network Agent to function.

5. Select **Test Traffic Visibility** to check the visibility of Internet traffic from the installation machine.
    a. Select the network interface card (NIC) that you want to use for the Network Agent and continue to the next panel. Active cards on the installation machine appear in this list, including NICs without IP addresses (stealth mode).

       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.

    b. If the network you want to test with the NIC does not appear in the default list, select **Add Network**.

       – 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.

– Select **Redisplay** to return to the options list.

Your new network appears in the list.

c. Select **Remove a Network** to delete a network from the list.

d. Select **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 panel 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 needs to monitor.

e. If the Network Agent 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.

– 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. You may continue with the installation without installing Network Agent and reconfigure your network later, or make the necessary changes and retest immediately.

f. Select **Exit Tool** when you are ready to continue installation.

g. Select **Continue installation** if you are sure that your NIC is able to monitor all targeted Internet traffic.

h. Select **Exit Setup** if the appropriate traffic is not visible. 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.

Setup asks if Network Agent is being installed on a machine that is being used as a firewall.

6. 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.

- Select **No** if the installation machine is not being used as a firewall. Installation will continue.
- Select **Yes** if you are attempting to install Network Agent on a firewall machine, and Setup will exit. Continue the Network Agent installation on a machine that is not running a firewall.

If the installation machine has multiple network interface cards (NIC), all enabled cards are displayed in a list.

7. Select the NIC that you tested successfully for network visibility.

   Setup asks you for the IP address and filter port number for the machine on which the Filtering Service is installed.

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

8. Enter the IP address of the Websense Filtering Service.

   Setup displays the path it will create to the Websense installation directory. For example, `/opt/Websense`.

9. Accept this default or create another directory.

> **IMPORTANT**
>
> The full installation path must use only ASCII 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 for optimal performance, 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 minimum.

A summary of all the components that will be installed appears.

10. Press **Enter** to accept this installation configuration and to begin installing Websense Enterprise.

    The Download Manager copies the appropriate installer files from Websense and begins the installation.

11. Exit the installer when the success message appears.

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 Enterprise to identify users transparently 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 Solaris or Linux:

1. Download and start the installer using the procedure in *Solaris and Linux Procedures*, page 91.
2. Select **RADIUS Agent** from the list of components to install and press **Enter**.

   If the installation machine is multihomed, all enabled network interface cards (NIC) with an IP address are displayed.
3. Select the card you want Websense Enterprise to use to communicate and press **Enter**.

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

IMPORTANT

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 in this dialog box.

4. Enter the IP address of the Policy Server machine and press **Enter**.

   Setup displays the path it will create to the Websense installation directory. For example, `/opt/Websense`.

5. Accept this default or create another directory.

   IMPORTANT
   The full installation path must use only ASCII 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 for optimal performance, 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 minimum.

   A summary of all the components that will be installed appears.

6. Press **Enter** to begin installation.

   The Download Manager copies the appropriate installer files from Websense and begins the installation.

   If the Network Agent was not installed, a message reminds you that Protocol Management and Bandwidth Optimizer cannot be used unless Network Agent is installed on a machine with direct access to Internet traffic.

7. Exit the installer when the success message appears.
8. Configure the RADIUS Agent in the Websense Enterprise Manager by selecting **Server > Settings > User Identification > RADIUS Agent**.

eDirectory Agent

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

To install the eDirectory Agent on Solaris or Linux:

1. Download and start the installer using the procedure in *Solaris and Linux Procedures*, page 91.

2. Select **eDirectory Agent** from the list of components to install and press **Enter**.

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

   IMPORTANT

   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 in this dialog box.

3. Enter the IP address of the Policy Server machine and press **Enter**.

   If the installation machine is multihomed, all enabled network interface cards (NIC) with an IP address are displayed.

4. Select the card you want Websense Enterprise to use to communicate and press **Enter**.

   Setup asks for the Novell eDirectory name and password.

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

   Setup displays the path it will create to the Websense installation directory. For example, `/opt/Websense`.

6. Accept this default or create another directory.

   IMPORTANT

   The full installation path must use only ASCII 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 for optimal performance, 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 minimum.

A summary of all the components that will be installed appears.

7. Press **Enter** to begin installation.

   The Download Manager copies the appropriate installer files from Websense and begins the installation.

   If the Network Agent was not installed, a message reminds you that Protocol Management and Bandwidth Optimizer cannot be used unless Network Agent is installed on a machine with direct access to Internet traffic.

8. Exit the installer when the success message appears.
9. Configure the eDirectory Agent in the Websense Enterprise Manager by selecting **Server > Settings > User Identification > eDirectory Agent**.

Modifying an Installation

If you decide to change the location of a Websense Enterprise component or modify your Websense Enterprise installation, run the full 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 Enterprise components
- Remove Websense Enterprise components
- Repair existing Websense Enterprise components

Adding Components

After installing Websense Enterprise, you may want to add components to change the configuration of Websense in your network. The following procedures assumes that the Filtering Service, Policy Server, Websense Enterprise Manager (Solaris and Windows only), and User Service are already installed, and that the remaining components, supported on your operating system, 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 components in a Windows environment:

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

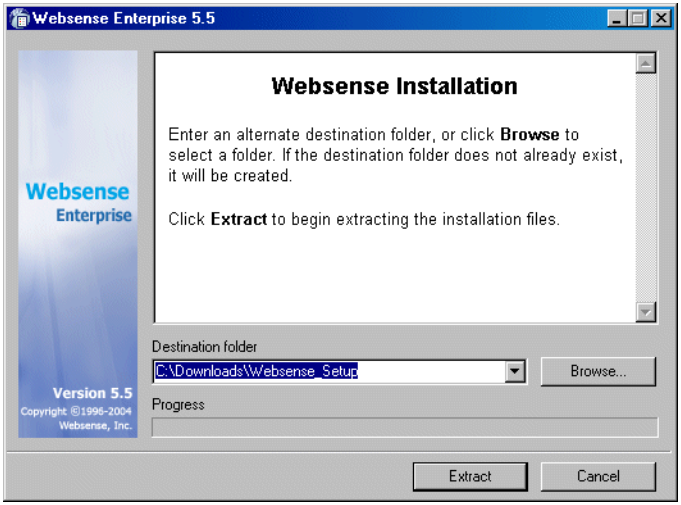
IMPORTANT

If you are installing DC Agent, log on with **domain** administrator privileges. DC Agent must have administrator privileges on the network to retrieve user login information from the domain controller. Without this information, Websense Enterprise cannot filter by users and groups. If you cannot install these components with such privileges, you may configure administrator privileges for these services after installation in the Properties dialog box for Windows services.

2. Run one of the following Websense Enterprise installers:
   - **Web download**: Download one of the following packages from http://www.websense.com/downloads to a folder on the installation machine and double-click to extract the installer files.
     - **Online installer**: The online installer package (`Setup552.exe`) contains only the installer files. The necessary product files are downloaded from the Web site as needed after product selections have been made.
     - **Offline installer**: The offline installer (`Websense552Setup.exe`) is much larger than the online package and contains all the files needed to install Websense Enterprise components. Use this package only if you experience difficulties installing Websense with the online installer.
   - **Product CD**: Run `WebsenseStart.exe` from the Websense Enterprise v5.5 product CD (`\WebsenseStart`) to launch the installer start screen. Select a Websense product installation to extract the installer files.

     The file will run automatically if *autorun* is enabled. The product CD contains all the files needed to upgrade Websense Enterprise components.

   A screen displays instructions for extracting the setup program.



Installer Download Extraction Screen

a. 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.

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

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.

If Websense Enterprise 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.

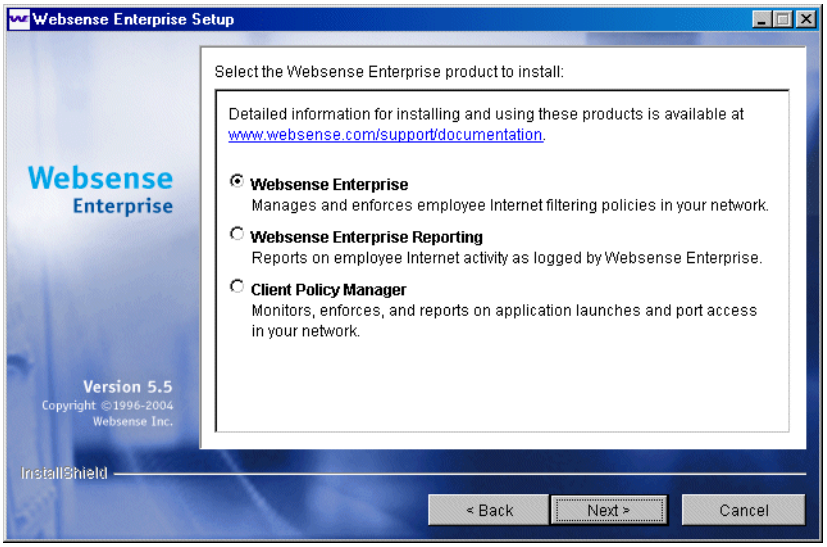
`Setup.exe` runs automatically after the files are decompressed.

3. Click **Next** on 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.

4. Select **Add Websense Enterprise components** and click **Next**.

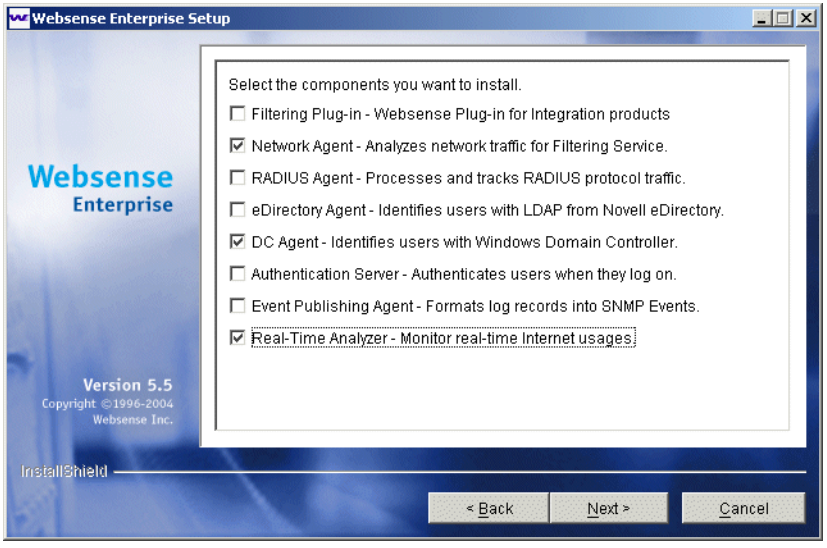
Setup displays a product selection screen.



Websense Product Selection Screen

5. Select **Websense Enterprise** and click **Next** to continue.

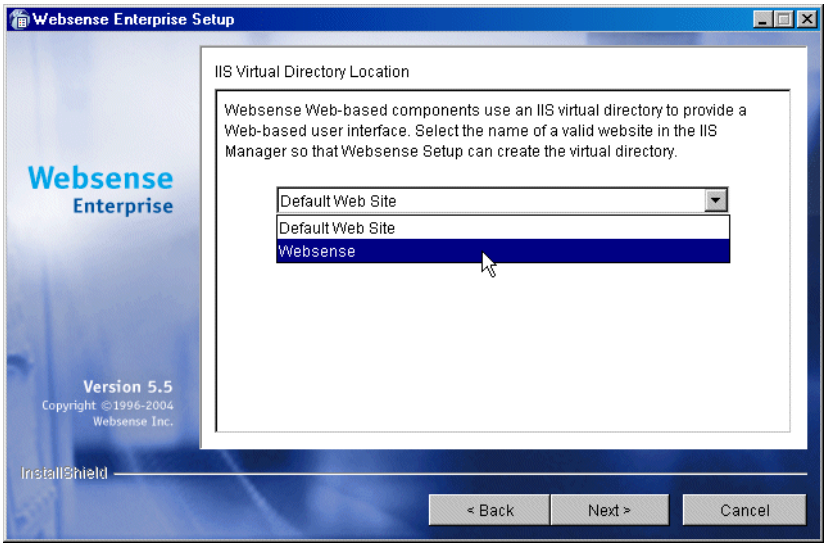
   The installer displays a list of components not currently installed on the installation machine.



Component Selection Screen

6. 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 for the name of the Web site 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.

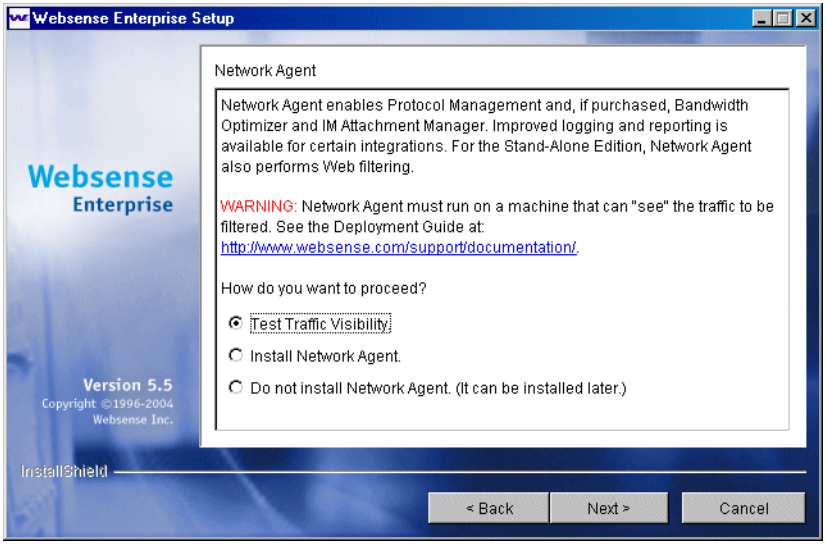


Default Web Site Selection

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

   If you are installing Network Agent, the installer displays a screen describing the features enabled by the Network Agent and offers you the option of testing your machine's visibility to Internet traffic. The machine on which the Network Agent is installed must be able to monitor 2-way employee Internet traffic for Network Agent to function properly.

> **IMPORTANT**
>
> If you install the Network Agent on a machine that cannot monitor targeted Internet traffic, some features, such as Dynamic Protocol Management and Bandwidth Optimizer, will not perform as expected.



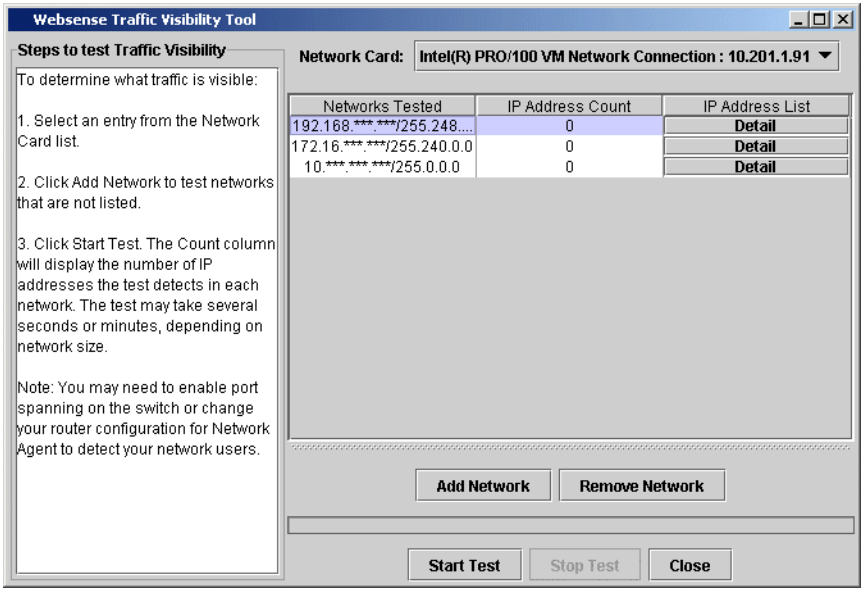
Network Agent Visibility Test Screen

You are given the following three options:

- **Test Traffic Visibility:** This selection launches the utility that tests the Internet visibility of the active network interface cards (NIC) in the installation machine.
- **Install Network Agent:** installs the Network Agent without conducting the traffic visibility test. Use this option if you know that the installation machine has the necessary Internet traffic visibility.
- **Do not install Network Agent:** allows you to continue the Websense Enterprise installation without installing the Network Agent.

8. Click **Test Traffic Visibility** to check the visibility of Internet traffic from the installation machine.

   The **Traffic Visibility Test** utility appears.



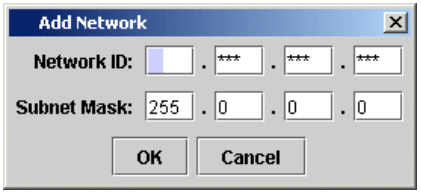
Traffic Visibility Test Tool

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.
Detail	Lists all the IP addresses in the network from which Internet traffic is being detected.

a. From the **Network Card** drop-down list, select the network interface card (NIC) that you want to use for the Network Agent.

b. 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.



c. 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.

d. Click **OK** to return to the **Traffic Visibility Test** dialog box.

   Your new Network appears in the list.

e. 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.

f. If the Network Agent 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.
   - 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. You may continue with the installation without installing Network Agent and reconfigure your network later, or make the necessary changes and retest immediately.

g. Click **Stop Test** when you are ready to continue installation.

h. Click **Close** to exit the traffic visibility test screen.

9. Continue with the installation.

   - Select **Install Network Agent** if you are sure that your NIC is able to monitor all targeted Internet traffic. This will install the Network Agent.
   - Select **Do not install Network Agent** to continue the Websense Enterprise installation without installing the Network Agent.

10. Click **Install Network Agent** to continue.

    The installer asks you if the Network Agent is being installed on a machine that is acting as a firewall. Network Agent cannot function properly on a machine running a firewall.

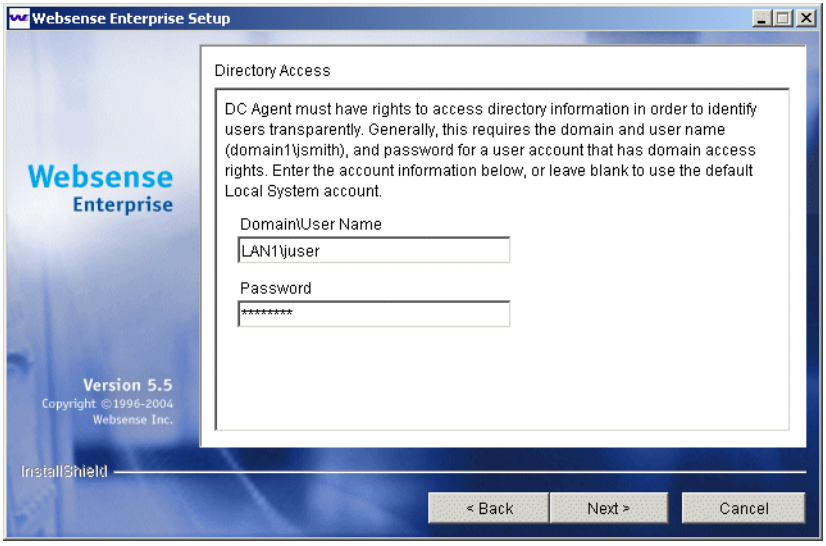
11. Select **Yes** or **No** and click Next to continue.

    - Select **No** if the installation machine is not being used as a firewall. Installation will continue.
    - Select **Yes** if you are attempting to install Network Agent on a firewall machine, and setup will exit. Continue the Network Agent installation on a machine that is not running a firewall.

    If the installation machine has multiple network interface cards (NIC), Setup asks you to select the NIC that you want to use for capturing traffic. All network interface cards enabled in the machine appear in a list.

12. Select the desired card and click **Next** to continue.

    - If you are installing DC Agent, the installer asks you to provide a user name and a password with administrative privileges on the domain. If you attempt to install DC Agent without providing access to directory information, you will be unable to identify users transparently.



Directory Access for DC Agent

13. Enter your domain and user name, followed by your network password, and 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 for optimal performance, 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 minimum.

A summary screen appears, listing the installation path, the installation size, and the components that will be installed.

14. Click **Next** to begin installation.

    The Download Manager progress bars are displayed as Setup downloads the appropriate installer files from Websense. Installation begins automatically when the necessary files have been downloaded.

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

    A message appears advising you that the installation was successful.

15. Click **Next** to continue.

    - If you have installed DC Agent, a dialog box appears advising you that the machine must be restarted to complete the installation. Select a restart option and click **Finish** to exit the installer.
    - If DC Agent was not installed, but you have installed Real-Time Analyzer and/or Websense Manager, the installer displays a screen asking if you want to launch either of those applications. By default, both are selected. Clear the checkbox of the component you do not want to launch and click **Finish**.
    - If neither DC Agent, Real-Time Analyzer, nor Websense Manager were installed, no further action is required and you can click **Finish** to exit the installer.

Solaris or Linux

To add components in a Solaris or Linux environment:

1. Log on to the installation machine as the **root** user.
2. Run the installation program for your operating system from the directory where it resides using the following command:

   ```
   ./install.sh
   ```

   Run the GUI version of the installer with 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.

   If you are installing on Solaris, Setup offers to check your system for the current patch cluster.
3. Determine if your patches are up to date:
   a. If you are unsure of the status of your patches, select **Yes** to begin the scan.
   b. If Setup advises you that the proper patches are not installed, quit the installer and install the appropriate patch cluster.

   WARNING

   You may continue without the proper patches, but the installation could fail.

   c. Continue the installation when you are sure the patches are correct for your system.

   The installer detects the currently installed Websense Enterprise components and asks you what action you want to take.
4. Select **Add Websense Enterprise components**.

   The installer displays a list of components not currently installed on the installation machine.
5. Select the components you want to install.

   If you have selected Network Agent to install, you are given the opportunity to test your machine's visibility to Internet traffic. The

machine on which the Network Agent is installed must be able to monitor 2-way employee Internet traffic for Network Agent to function properly.

> **IMPORTANT**
> If you install the Network Agent on a machine that cannot monitor targeted Internet traffic, Dynamic Protocol Management and Bandwidth Optimizer, will not perform as expected.

You are given the following three options:

- **Test Traffic Visibility**: This selection launches the utility that tests the Internet visibility of the active network interface cards (NIC) in the installation machine.
- **Install Network Agent**: This option installs Network Agent without conducting the traffic visibility test. Use this option if you know that the installation machine has the necessary Internet traffic visibility.
- **Do not install Network Agent**: Continue the Websense Enterprise installation without installing the Network Agent.

6. Select **Test Traffic Visibility** to check the visibility of Internet traffic from the installation machine.
   a. Select the network interface card (NIC) that you want to use for the Network Agent and continue to the next panel. Active cards on the installation machine appear in this list, including NICs without IP addresses (stealth mode).

      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.
   b. If the network you want to test with the NIC does not appear in the default list, select **Add Network**.
      - 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.
      - Select **Redisplay** to return to the options list.

        Your new network appears in the list.
   c. Select **Remove a Network** to delete a network from the list.

d. Select **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 panel 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 needs to monitor.

e. If the Network Agent 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.
   - 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. You may continue with the installation without installing Network Agent and reconfigure your network later, or make the necessary changes and retest immediately.

f. Select **Exit Tool** when you are ready to continue installation.

g. Select **Continue installation** if you are sure that your NIC is able to monitor all targeted Internet traffic.

h. Select **Exit Setup** if the appropriate traffic is not visible. 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.

7. Select a Network Agent installation option and press Enter to continue with the Websense Enterprise installation.

   - **Firewall installation warning:** Network Agent cannot function properly on a machine running a firewall. Select **Yes** or **No** when asked if Network Agent is being installed on a machine that is being used as a firewall.
     - Select **No** if the installation machine is not being used as a firewall. Installation will continue.
     - Select **Yes** if you are attempting to install Network Agent on a firewall machine, and setup will exit. Continue the Network Agent installation on a machine that is not running a firewall.

- **Network interface card (NIC) selection:** If the installation machine has multiple network interface cards, Setup displays a list of all enabled cards. Select the NIC that you tested successfully for network visibility. Cards without an IP address will not appear in this list.
- **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 for optimal performance, 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 minimum.
- **Installation directory:** Setup displays the path to the directory where the existing Websense components are installed. The default is `/opt/Websense`. Accept this default or create another directory.

IMPORTANT

The full installation path must use only ASCII characters.

8. Press **Enter** to accept this installation configuration and to begin installing Websense Enterprise.

   The Download Manager copies the appropriate installer files from Websense and begins the installation.

   A summary of all the components that will be installed appears.
9. Exit the installer when the success message appears.

Removing Components

After installing Websense Enterprise or any of its components, you may want to remove installed components to change the configuration of Websense Enterprise in your network.

IMPORTANT

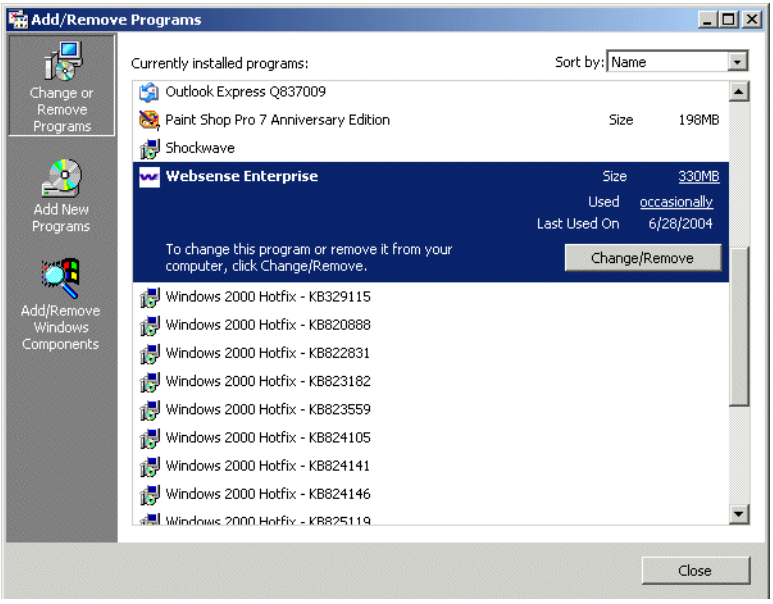
The Policy Server service must be running to uninstall any Websense Enterprise components. To remove the Policy Server, you must also remove all the other components installed on the machine.

Windows

If you have run the Websense installer recently and have not restarted the machine, you must do so before attempting to remove any components.

To remove installed Websense Enterprise components in a Windows environment:

1. Log on to the installation machine with **local** administrator privileges.
2. Close all open applications.
3. Select **Start > Settings > Control Panel**.
4. Double-click **Add/Remove Programs**.
5. Select Websense Enterprise from the list of installed applications.

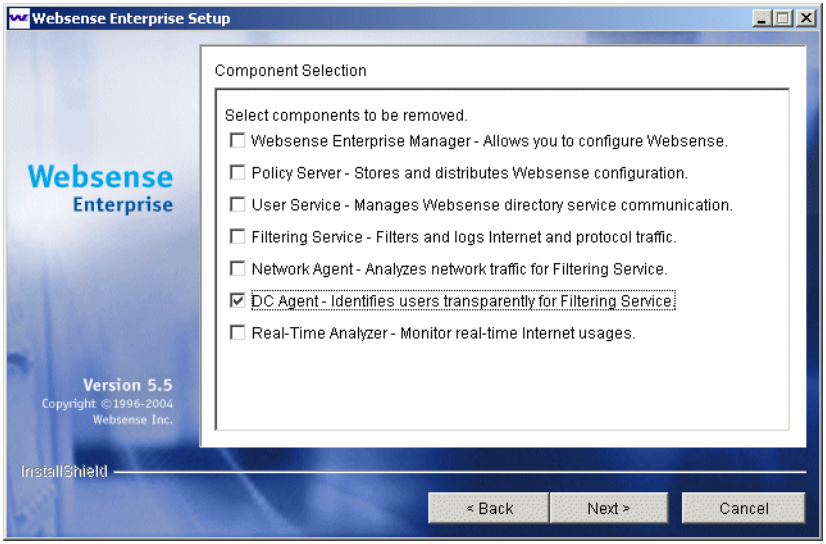


Add/Remove Programs Control Panel from Windows 2000

6. Click **Change/Remove**.

   The Websense Enterprise uninstaller is launched.

   After the welcome screen, a list of installed components appears. By default, all selections are checked.



Component Removal Screen

7. Clear the check boxes of the components you do *not* want to remove, and click **Next**.

   If the Policy Server is not running, a dialog box appears advising you that removing Websense Enterprise components may require communication with the Policy Server. You may exit the installer to restart the Policy Server or continue uninstalling the selected components.

> **IMPORTANT**
> 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.

8. 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.

9. Click **Next** to exit the installer.

Solaris or Linux

To remove components on a Solaris or Linux machine:

1. Log on to the installation machine as the **root** user.
2. Run the following program from the Websense Enterprise directory (`/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 Enterprise components and displays a list of installed components.
3. Select the components you want to remove.

   By default, all selections are checked. Make sure that only the components you want to remove are checked.
4. Press **Enter** to remove the selected components.
   - **Policy Server status:** If the Policy Server is not running, a dialog box appears advising you that removing Websense Enterprise components may require communication with the Policy Server. You may exit the installer to restart the Policy Server or continue uninstalling the selected components.

     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.

WARNING

Do not uninstall the Policy Server without uninstalling all the Websense components. Removing the Policy Server will sever communication with the remaining Websense components and will require the reinstallation of those components.

- **Summary list:** A summary list of the components you have selected to remove appears.
- **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 messages advises you when the procedure is finished.

5. Exit the installer.

Repairing an Installation

If a component fails to install properly, or is not performing normally, you can run the installer again and *repair* the installation. This procedure does not troubleshoot components, but merely replaces missing files.

Windows

To repair your Websense installation in a Windows environment:

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

   If you are repairing 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 Enterprise cannot filter by users and groups. If you cannot install these components with such privileges, you may configure administrator privileges for these services after installation in the Properties dialog box for Windows services.

2. Back up the following files to a safe location:
   - `config.xml`
   - `websense.ini`
   - `eimserver.ini`

3. Run `Setup.exe` from the Websense Enterprise installer.
4. Click **Next** on the welcome screen.

   The installer detects the Websense Enterprise installation and asks you if you want to Add, Remove, or Repair components.
5. Select **Repair existing Websense Enterprise components** and follow the on-screen instructions.

   Setup advises you that it will repair the current installation by reinstalling the existing Websense Enterprise components and asks if you want to continue.
6. 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.
7. Click **Next** to begin downloading the necessary installation files.

   A progress message appears while the installer shuts down Websense services.

   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 for optimal performance, warnings are displayed in separate screens.

   - 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 minimum.
8. Click **Next** to continue.

   The Download Manager progress bars are displayed as Setup downloads the appropriate installer files from Websense. Installation begins automatically when the necessary files have been downloaded.

   A message appears, advising you that the installation has been successful.
9. Click **Next** to continue.

   - If you have repaired DC Agent, a dialog box appears advising you that the machine must be restarted to complete the installation. Select a restart option and click **Finish** to exit the installer.

- If DC Agent was not repaired, but you have repaired Real-Time Analyzer and/or Websense Manager, the installer displays a screen asking if you want to launch either of those applications. By default, both are selected. Clear the checkbox of the component you do not want to launch and click **Finish**.
- If neither DC Agent, Real-Time Analyzer, nor Websense Manager were repaired, no further action is required and you can click **Finish** to exit the installer.

Solaris or Linux

To repair components on a Solaris or Linux system:

1. Log on to the installation machine as the **root** user.
2. Run the installation program from the directory where it resides:

   ```
   ./install.sh
   ```

   Run the GUI version of the installer with 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.

   If you are installing on Solaris, Setup offers to check your system for the current patch cluster.
3. Determine if your patches are up to date:
   a. If you are unsure of the status of your patches, select **Yes** to begin the scan.
   b. If Setup advises you that the proper patches are not installed, quit the installer and install the appropriate patch cluster.

   WARNING

   You may continue without the proper patches, but the installation could fail.

   c. Continue the installation when you are sure the patches are correct for your system.

   The installer detects the currently installed Websense Enterprise components and asks you what action you want to take.

4. Select **Repair Websense Enterprise components** and press **Enter** to advance through the procedure.
   - **Repair feature:** The installer advises you that it will repair the current installation by reinstalling the existing Websense Enterprise 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.
   - **Browser location:** If you are repairing the Websense Enterprise Manager on Solaris, Setup prompts you for the location of the browser.
   - **System requirements:** 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 for optimal performance, 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 minimum.
   - **Services restarted:** The Websense services are restarted after the files are reinstalled.

   A completion messages advises you when the procedure is finished.
5. Exit the installer.
   - If you have not repaired the Websense Manager, you are ready to select **Finish** and exit the installer.
   - If you have repaired the Websense Manager (Solaris GUI mode only), the installer asks if you want to open the Manager. By default, the Manager is selected. Select **Finish** when you are ready to exit the installer.

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:

1. Stop the Policy Server. Refer to *Stopping or Starting Websense Services*, page 124 for instructions.
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 Enterprise components on the individual machines.
5. Run the Websense Enterprise installer on the Policy Server machine.

   The installer detects Websense Enterprise and asks you what action you want to take with the installed components.
6. Select **Repair existing Websense Enterprise components** when prompted.

   For specific instructions, refer to *Repairing an Installation*, page 119.
7. When the installer is finished repairing the system, stop the newly installed Policy Server.
8. Replace the `config.xml` file created by the repair procedure with your backup copy.
9. Restart the Policy Server.
10. Restart the services of the remote Websense Enterprise components.
11. Reload the Websense Master Database, which was removed during the repair process.

Stopping or Starting Websense Services

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 the 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 Enterprise 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
- Event Publisher
- Logon Agent

Principal Components

You must stop the following components in the order indicated. Always start or stop optional components before stopping any of the components on this list.

1. Network Agent
2. Filtering Service
3. User Service
4. Policy Service

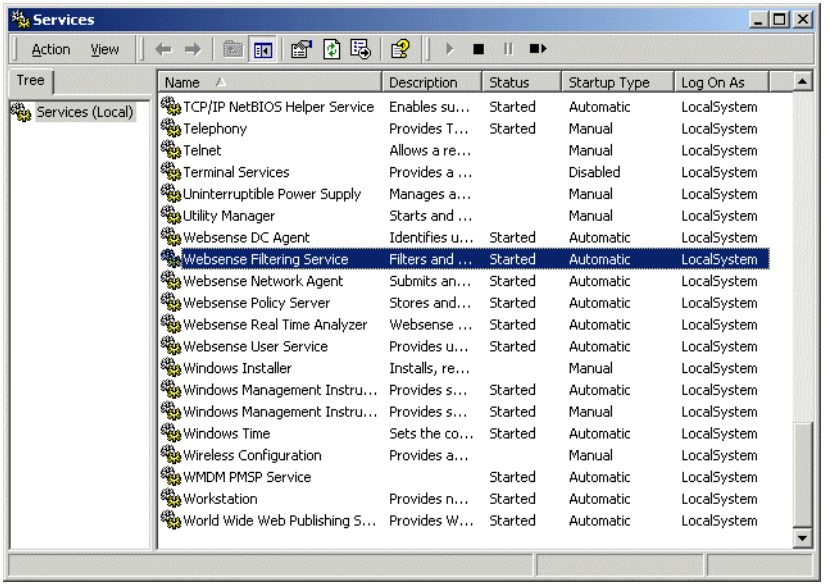
When restarting Websense services, reverse the order, starting with the Policy Server first.

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 2000 or 2003 machine:

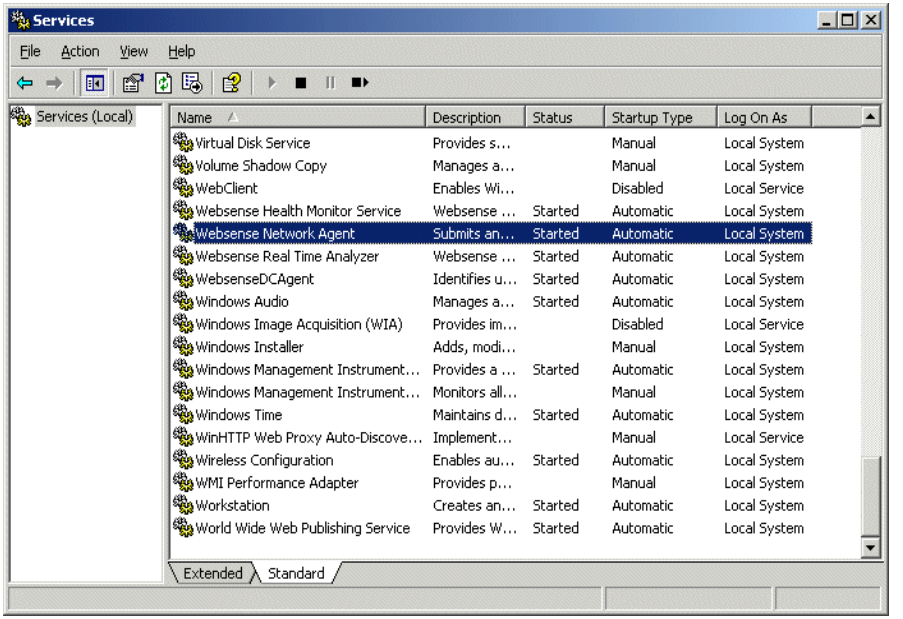
1. From the Control Panel, select **Administrative Tools > Services**.
2. Scroll down the list of available services and select a Websense service.



Windows 2000 Services List

NOTE

By default, Websense services are configured to start automatically when the computer is started.



Windows 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** ■ ▶). Restarting stops the service, then restarts it again immediately from a single command.

Solaris and Linux

You can stop, start, or restart Websense services from a command line on a Solaris or Linux machine. Restarting stops the services, then restarts it again immediately from a single command.

1. Go to the `/Websense` directory.
2. Stop, start, or restart Websense services with one of the following commands:
   - `./WebsenseAdmin stop`
   - `./WebsenseAdmin start`
   - `./WebsenseAdmin restart`

3. View the running status of the Websense services with the following command:

```
./WebsenseAdmin status
```

IMPORTANT

DO NOT use the kill command to stop Websense services. This procedure may corrupt the services.

CHAPTER 5

Initial Setup

After installing Websense Enterprise, you must perform the following tasks to complete the setup process.

- If you have not downloaded the Websense Master Database during installation, you must use your Websense subscription key to download the database from the Websense Manager. See *Subscription Key and Database Download*, page 129 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 133 for instructions.
- All workstations being filtered must have the Messenger Service enabled to receive protocol block messages. See *Displaying Protocol Block Messages*, page 134 for instructions.
- If the 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 the Network Agent*, page 141 for instructions.
- If you want to block https traffic, configure Squid appropriately. See *HTTPS Blocking*, page 144 for instructions.
- Configure your firewall or Internet router appropriately. See *Configuring Firewalls or Routers*, page 145 for instructions.

Subscription Key and 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 Websense Enterprise machine 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 Websense Enterprise server 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 Websense Enterprise, your subscription key was retained by the installer and these steps are not necessary.

To download the Master Database:

1. Open Websense Enterprise Manager on any machine where it is installed.

   Windows: Select **Start > Programs > Websense Enterprise > Websense Enterprise Manager**.

   Solaris: Go to the `Websense/Manager` directory and enter:

   ```
   ./start_manager
   ```

2. For a first time installation, the Add Policy Server dialog box appears.
   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 server's IP address or machine name appears 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.

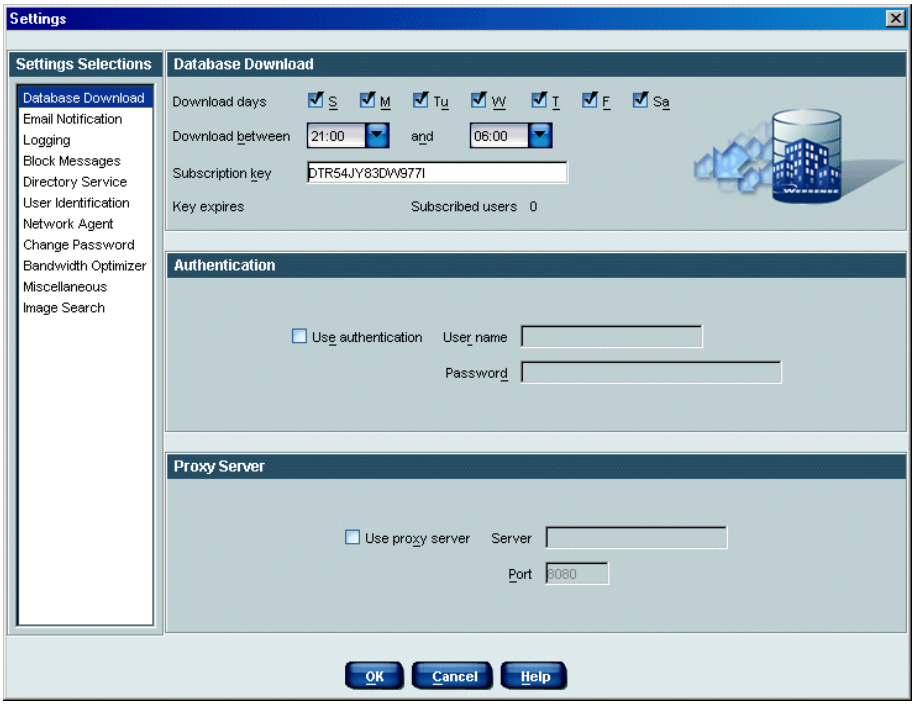
4. Set a password (between 4 and 25 characters) for the Policy Server.

> **NOTE**
> Retain this password. It must be entered when you connect to this Policy Server from this or any other Websense Enterprise Manager, or after the Policy Server is stopped and restarted.

5. Click **OK**.

   The **Settings** dialog box appears.

> **NOTE**
> If you have entered a subscription key previously, you must select **Server > Settings** to display the Settings dialog box.



Settings Dialog Box

6. Enter your alphanumeric key in the **Subscription key** field.

NOTE

The value in the **Subscribed users** field shows 0 until the database is successfully downloaded.

7. If your network requires authentication to an upstream firewall or proxy server 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 (for Websense to download 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.
8. 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 Enterprise Database. Establish the proxy settings for the database download as follows:
   a. Check **Use proxy server**.
   b. Identify the upstream proxy server or firewall in the **Server** field.

      You may identify the machine by IP address or machine name. 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 and Linux:** 7-bit ASCII only.

NOTE

If Websense Enterprise 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).

9. Click **OK**. Websense automatically contacts the Websense database server and begins downloading the Master Database.

> **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.

10. Click **Done** in the **Saving Data** dialog box.

    The first time the key is entered, the following Web site appears:

    http://www.my.websense.com

    My.Websense provides access to technical assistance customized for your particular version of Websense Enterprise, your operating system, and your integration product.

Identifying the Filtering Service for the Block Page URL

When Websense blocks an Internet request, the browser is redirected by default to a block message page hosted by the Filtering Service. The format of the block page URL typically takes the form:

http://<WebsenseServerIPAddress>:<MessagePort>/cgi-bin/blockpage.cgi?ws-session=#########

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 Enterprise block messages can be sent to users. If the Filtering Service machine name, rather than the IP address, is contained in the block page URL, the users could see a blank page instead of the block message.

Use one of the following methods to identify the Filtering Service by IP address:

- 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. Go to the `Websense\bin` folder on the local drive.
  2. Open the `eimserver.ini` file in a text editor.
  3. 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. *Do not* use the loopback address 127.0.0.1.
  4. Save the file.
  5. Stop and then restart the Filtering Service (see *Stopping or Starting Websense Services*, page 124).

Displaying Protocol Block Messages

Websense Enterprise 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

IMPORTANT

Windows XP Service Pack 2 will only display protocol block messages under the following conditions:

- The firewall function must be disabled.
- The Windows Messenger service must be started.

For users to view protocol block messages in Windows NT, Windows 2000, and Windows 2003:

- Make sure that the User Service has administrator privileges. Refer to your operating system documentation for instructions on changing privileges for Windows Services.

- Make sure the Messenger Service is enabled on *each* client workstation that is being filtered. If you have activated protocol management in Websense Enterprise v5.5, 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 on how to do this, refer to your operating system documentation.

Creating and Running the Script for Logon Agent

If you have installed Websense Enterprise 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 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 user workstations:

- Be sure that all workstations can connect to the shared drive on the domain controller where the 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 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
- `Logon.bat`: batch file containing a sample logon scripts
- `LogonApp_ReadMe.txt`: a summary of the procedures for creating and running the Websense logon 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. If you plan to use both types of scripts, 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.

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 will run `LogonApp.exe`; and a logout script that will remove 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>:15880
```

This command will run `LogonApp.exe` in *persistent* mode (the default), which will send 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 Enterprise Logon Agent.
Port number	The port number used by Logon Agent defaults to 15880 but may be edited if a different port is in use.
/COPY	Copies the `LogonApp.exe` application to the users' machines, where it is run by the logon script from local memory. By default, the application is copied into the `%USERPROFILE%\Local Settings\Temp` folder. `Copy` can be used only in the *persistent* mode.
/NOPERSIST	Sends information to the Logon Agent only at logon. No updates are sent during the user's session. If this parameter is not present, `LogonApp.exe` will operate in the *persistent* mode. In this mode, `LogonApp.exe` will reside in memory where it will update the Logon Agent at predefined intervals (defaults to 15 minutes). PERSIST is the default behavior for the logon script. Refer to the Websense Enterprise *Administrator's Guide* for details on configuring the Logon Agent via the Websense Manager.
/VERBOSE	Debugging parameter that must be used only at the direction of Technical Support.
/LOGOUT	Removes the logon information from the Websense user map when the user logs off. Use of this parameter requires a second script.

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 cleared of logon

information are configured in the **Logon Agent** tab of the **Settings** dialog box in the Websense Enterprise 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 Websense and the workstations in your network than does the persistent mode.

For detailed information on configuring Logon Agent in the Websense Enterprise Manager, refer to the Websense Enterprise *Administrator's Guide*.

Examples

The following are examples of commands for a logon script and the accompanying logout script that might be run in Active Directory. The logout script must be run from a separate batch file.

- **Logon script**: The following script sends user information to the Logon Agent at logon only. User information is not updated during the user's session.

  ```
  LogonApp.exe http://10.2.2.95:15880 /NOPERSIST
  ```

- **Logout script**: The accompanying logout script would be written as:

  ```
  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 cannot be responsible for changes to these procedures or to the operating systems that employ them. For more information, refer to the links provided.

Active Directory

If your network uses Windows 98 client machines, refer to: http://www.microsoft.com/windows2000/server/evaluation/news/bulletins/adextension.asp for assistance.

To configure a logon script using Active Directory:

1. Make sure your environment meets the conditions described in *Prerequisites for Running the Logon Script*, page 135.
2. From the **Start** menu on the Active Directory machine, select **Settings > Control Panel > 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 the logon script you edited (`logon.bat`) and `LogonApp.exe` into this folder.
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 script (`logon.bat`) in the **Script Name** field or browse for the file.

    Leave the **Script Parameters** field empty.
15. Click **OK** twice to accept the changes.

16. Close the **Group Policy Object Editor** dialog box.
17. Click **OK** in the domain **Properties** dialog box to apply the script.
18. 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 Websense Enterprise 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. For instructions on enabling manual authentication, refer to the Websense Enterprise *Administrator's Guide*.

For additional information about deploying logon and logout scripts to users and groups in Active Directory, please refer to:

http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/Default.asp?url=/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/sag_assign_LScripts_user_AD.asp

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 135.
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 upon 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 script in the **User Profile Path** field (from Step 2).
7. Enter the name of the logon script (`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 Websense Enterprise 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. For instructions on enabling manual authentication, refer to the Websense Enterprise *Administrator's Guide*.

For additional information about creating and deploying logon scripts to users in Windows NTLM, please refer to:

http://windows.about.com/library/weekly/aa031200a.htm

Identifying the Proxy Server for the 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, the Network Agent cannot filter or log requests properly.

To define proxy server IP addresses:

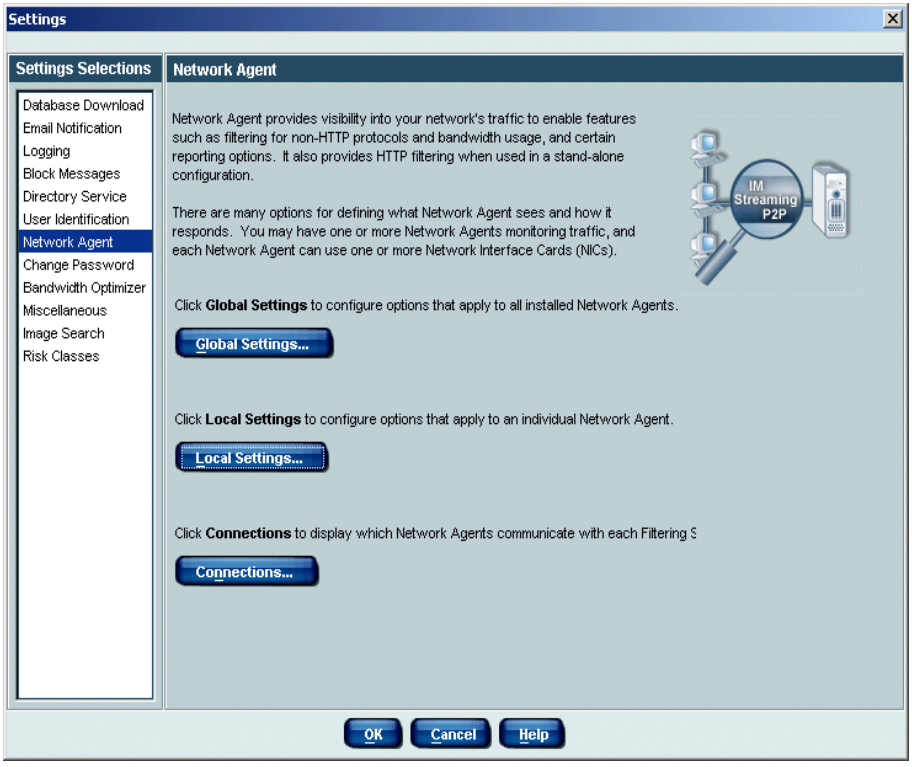
1. Open the Websense Enterprise Manager and connect to the Policy Server.

2. Select **Server > Settings**.

   The Settings dialog box appears.

3. Select **Network Agent** from the **Settings Selections** pane.

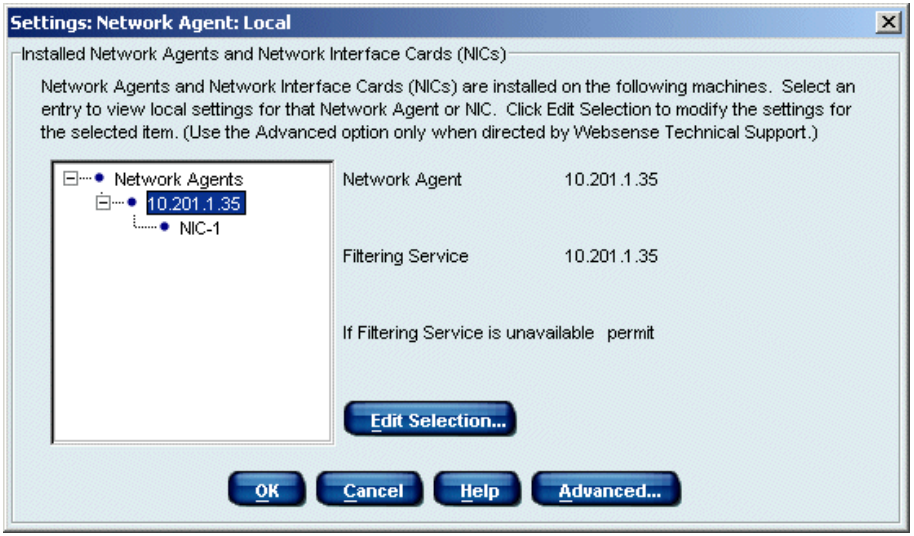
   The **Network Agent** settings dialog box appears.



Network Agent Selection Screen

4. Click **Local Settings**.

   The local Network Agent settings dialog box appears, showing the IP address and interface of the Network Agent.



Network Agent Local Settings

5. Select the IP address of the Network Agent from the tree structure and click **Edit Selection**.

   A Filtering Service connection dialog box appears.

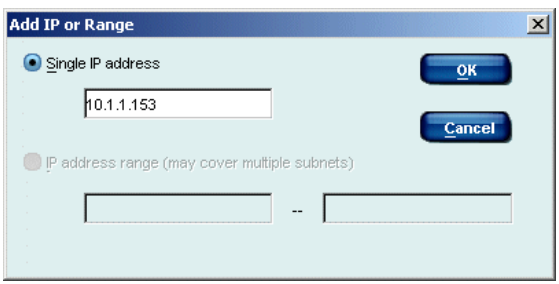
6. Click **Next**.

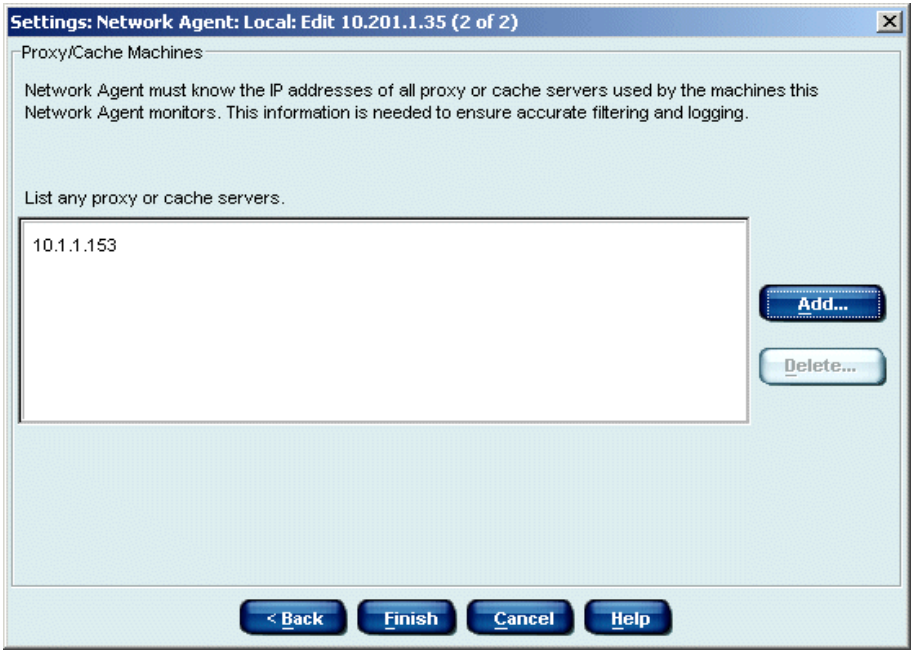
   A blank proxy/cache server list appears.

7. Click **Add**.

   A dialog box appears allowing you to define an IP address or a range of addresses.

8. Enter an IP address and click **OK** to add the IP address to the list of proxy or cache servers.





Proxy/Cache Server List

9. Repeat Step 7 and Step 8 for each proxy server in your network.
10. Click **Finish**.

HTTPS Blocking

There are two options for blocking https traffic with a Squid integration:

- Squid will block https traffic when it is set to transparent mode. For information refer to *Transparent Identification*, page 151.
- If Squid is configured to act as a proxy server, the Squid error page can be used as the block page.

  To configure Squid to present an https block page:

  1. Open the `wsSquid.ini` file in any text editor (located in /etc/wsLib/ in Solaris and Linux).
  2. Set the value of the **UseHTTPSBlockPage** parameter to **yes**.

     The default setting for this parameter is **no**, causing Squid to ignore all https traffic.

3. Save your changes.
4. Restart Squid.

Configuring Firewalls or Routers

To prevent users from circumventing Websense Enterprise 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 on configuring access lists on the router or firewall.

IMPORTANT

If Internet connectivity of the Websense Enterprise Manager 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.

Workstation Configuration

Workstations must have a Web browser that supports proxy-based connections and Java. Among others, versions 4.0 or later of Microsoft Internet Explorer or Netscape Navigator support proxy-based connections and Java technology.

Internet browsers on workstations must be configured to use Squid Server to handle HTTP, HTTPS, FTP, and Gopher requests. Browsers must point to the same port (default-3128) that Squid Server uses for each protocol.

Refer to your browser documentation for instructions on how to configure your browser to send all Internet requests to the Squid Web Proxy Cache.

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 Websense 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 can filter based on workstation or network policies. Workstations are identified within Websense 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 Websense Enterprise so that if the Filtering Service is not able to identify users transparently, it will prompt users for authentication. See your Websense Enterprise *Administrator's Guide* for more information on manual authentication.
- 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.

If you want to assign individual user or group policies, do 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 Websense Enterprise to prompt users for authentication. This allows Websense to obtain the user information it needs if it does not receive it from Squid or DC Agent (see Manual Authentication in the Websense Enterprise *Administrator's Guide*).

Authentication Methods

Squid v2.5 offers the following authentication methods:

- Anonymous
- Basic
- Windows NT Challenge/Response
- Digest

See your Squid documentation for instructions on 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 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 Websense Enterprise, 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

If you want all users in a mixed browser environment to be identified transparently, you can enable Anonymous authentication within Squid and use the Websense transparent identification feature.

Transparent Identification

The Websense transparent identification feature allows the Filtering Service to filter Internet requests from users identified in a Windows directory without prompting them to authenticate manually. This feature comes into play if the authentication method enabled within Squid does not send user information to the Filtering Service.

To take advantage of the transparent identification feature, the Websense DC Agent must be installed on a Windows server machine in the network. The DC Agent can be installed together with the Filtering Service on the same machine, or on a different Windows server machine using a separate installation program.

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.

For information about installing the Websense DC Agent separately, see *DC Agent*, page 80. For information about Websense Enterprise manual authentication, refer to the Websense Enterprise *Administrator's Guide*.

CHAPTER 7

Event Publisher

The Websense Event Publisher creates SNMP *traps* from the log messages that are generated by the Websense Filtering Service. An SNMP trap captures a predefined Websense event. These traps are then forwarded, or *published*, to an application that manages SNMP and used as needed.

Installing Event Publisher

Typically, the Event Publisher is installed on the same machine as Websense Enterprise (Filtering Service, Policy Server, User Service). You can install the Event Publisher together with the other Websense components by performing a Custom installation, or you can add Event Publisher later, after installing and configuring Websense Enterprise.

To install the Event Publisher on the Websense Enterprise machine:

1. Log on to the installation machine with **local** administrator privileges.
2. Close all open applications.
3. Run the main Websense Enterprise installation program (`Setup.exe`).

   After the welcome screen, a dialog box displays asking you what action you want to take with the Websense components the installer has detected on the machine.
4. Select **Add Websense Enterprise components** and click **Next**.

   The installer displays a list of components not currently installed on the installation machine.
5. Select **Event Publishing Agent**.
6. Click **Next**.

   The installer compares the system requirements for the installation you have selected with the resources of the installation machine. If the machine has inadequate memory for optimal performance, warnings are displayed. The installation will continue, but you should upgrade your machine for the best performance.

A summary screen is displayed, listing the component that will be installed, the installation path, and the total size of the installation.

7. Click **Next** to begin installation.

   A progress bar is displayed.

   A message is displayed advising you that the installation was successful.

8. Click **Finish** to exit Setup.

If you decide to deploy the Event Publisher on a separate machine in your network, be sure Websense Enterprise is installed and running before beginning. You must provide the location (IP address and port number) of the Policy Server to install the Event Publisher. Run the main Websense Enterprise v5.5 installer and select a **Custom** installation when prompted. Then select **Event Publishing Agent** from the list of available components.

Integrating Event Publisher with IBM Tivoli

To use the Websense SNMP Event Publisher with IBM® Tivoli® you must have the following properly installed and running:

- Tivoli Enterprise Console (TEC) or Tivoli RiskManager
- Tivoli Framework on the Websense machine with Gateway and Endpoint installed on the Websense machine
- Websense Enterprise v5.5

Two versions of the integration kit are provided, one for use with RiskManager (an optional add-on product layered over the base Tivoli Enterprise Console) and the other for use with the base Tivoli Enterprise Console. In addition, a third component is provided allowing the TEC and RiskManager systems to receive SNMP traps from Websense Event Publisher.

The following configuration files comprise the Websense SNMP Event Publisher integration kit:

File Name	Description
websense_riskmgr.baroc websense_tec.baroc	The BAROC file classifies events from within a rule set to the Event Server. Event classes are agreements between the SNMP adapter and the Event Server about what information the adapter sends to the Event Server.

File Name	Description
websense_riskmgr.cds websense_tec.cds	The Tivoli Enterprise Console (TEC) uses the class (.cds) file to map individual events to event classes and to define event attributes before forwarding the event to the Event Server. Tivoli RiskManager provides .cds files for those adapters that use the SNMP adapter (adapter for ISS RealSecure).
websense.oid	The *object identifier* file maps object identifiers used by SNMP to names.

Tivoli Enterprise Console (TEC)

The following files comprise the TEC portion of the Websense Event Publisher Tivoli integration kit:

- websense_tec.baroc
- websense_tec.cds
- websense.oid

To integrate the Websense Event Publisher with the TEC:

1. Import the BAROC file.

   The BAROC file is installed once (per management region on the system where the TEC Event Server resides.

   a. Load the Tivoli environment variables (in the `setup_env.cmd` file) into your current environment.

   b. Copy the BAROC file into the RiskMgr class directory using the following path:

      `IBM/RISKMRG/etc/baroc`

   c. Open the file `C:/IBM/RISKMGR/etc/riskmgr_baroc.lst` and add an entry for `websense_riskmgr.baroc` at the end of the file.

      The operating system must be either **w32-ix86** (Windows 32) or one of the supported UNIX variants.

   d. Update the class list.

      Refer to your IBM Tivoli documentation for instructions.

   e. Open the file `<TIVOLI>/bin/<OS>/RISKMRG/corr/riskmgr_baroc.lst` and add an entry for `websense_riskmgr.baroc` at the end of the file.

f. Save the file.

g. Update the RiskManager database with the following command:

```
rmcorr_cfg -update
```

To execute this command:

- You must be at a bash shell prompt. In Windows, the bash shell is located in `<TIVOLI>/bin<OS>/tools`.
- Your current directory must be `<TIVOLI>/bin<OS>/RISKMGR/corr`.
- The environment variables defined in `setup_env.cmd` must be present in the current shell environment.

NOTE

The following error messages are normal and do not indicate a problem:

"Failed to delete websense_riskmgr.baroc from rulebase"

"ERROR::ECO:0001;0273 No matching rulesets found"

h. Verify the successful installation of the Websense classes with the following command:

`wlscurrb` [Outputs the name of the currently used RULEBASE]

```
wlsrbclass <RULEBASE> | grep Websense
```

To execute this command:

- You must be at a bash shell prompt. In Windows, the bash shell is located in <*TIVOLI*>/bin<*OS*>/tools.
- The environment variables defined in `setup_env.cmd` must be present in the current shell environment.

These commands will produce output similar to the following:

```
bash$ wlscurrb
The currently used rulel base was loaded
from the rule base named 'RM38RB'.

bash$ wlsrbclass RM38RB | grep Websense
WebsenseBaseEvent
WebsenseL0Event
WebsenseL1AddedEvent
WebsenseL1RemovedEvent
WebsenseL1ChangedEvent
```

2. Using a text editor, copy the contents of the `websense.oid` file and the `websense_riskmgr.cds` file and append them to the end of each of the following files:
   - `\Program Files\Tivoli\lcf\bin\w32-ix86\TME\TEC\adapters\etc\tecad_snmp.oid`
   - `\tecsnmp\etc\tecad_snmp.cds`
3. Distribute the files to the TECSNMP Adapter machine.

   The files must be distributed to the following path:

   `\$TECSNMP\etc`
4. Copy the `websense_riskmgr.baroc` file to the `/$TECSNMP/etc` folder and rename the file `tec_snmp.baroc`.
5. Install the FORMAT file.

   The FORMAT file (`.cds`) must be installed on every machine where Websense Event Publisher is installed and reporting Websense events.

   a. Stop the Tivoli adapter.

      From the Windows Services dialog box, stop the TECWinadapter service.

      If the adapter has not been installed on this system, install the adapter by following the Tivoli installation instructions. These instructions will also have you specify the location of the centralized TEC Event Server (*ServerLocation* and *ServerPort* in the adapter configuration file), which is the server on which the BAROC file was installed above.

b. Copy the FORMAT file into the appropriate locale directory.

   For most installations the locale will be `C:\`, so the full path would be the following:

   ```
   C:\$TECADHOME\etc\<LOCALE>
   ```

c. Change directory to the locale directory.

   ```
   cd $TECADHOME\etc\<LOCALE>
   ```

d. Generate a new FORMAT file.

   Some installations may already be reporting events into Tivoli via the Windows NT Event Log. These sites will already have an existing FORMAT file to which the Websense Event Publisher-specific information needs to be added.

   Append the `websense_riskmgr.cds` file to the existing `.cds` files in the following paths:

   - `\Program Files\Tivoli\Icf\bin\w32-ix86\TME\TEC\adapters\etc`
   - `\$TECSNMP\etc\tecad`

e. Regenerate the class (.cds) file.

   ```
   ..\..\bin\win_gencds\tecad_snmp.cds
   ```

NOTE

Make sure you run this command in the following directory: `cd $TECADHOME\etc\<LOCALE>.`

   It is normal to see some warning messages.

f. Update the RiskManager Event Server and the TECSNMP Adapter configuration files.

g. Make any changes necessary to the RiskManager configuration file.

   For example, if the adapter is running on a Windows machine with Websense Enterprise, it may be necessary to adjust the parameters to aggregate and correlate the SNMP traps that the Tivoli SNMP adapter monitors.

   Websense Event Publisher monitored by a Tivoli RiskManager Adapter could generate a large number of events that represent a set a very similar activity. To minimize event traffic with minimal loss of

information, both the TEC SNMP adapter and the Tivoli Risk Manager Agent can summarize similar events.

h. Restart the adapter by starting the **TECWinadapter** service in the Windows services dialog box.

Tivoli Risk Manager

The following files comprise the Risk Management portion of the Websense Event Publisher Tivoli Integration Kit:

- `websense_riskmgr.baroc`
- `websense_riskmgr.cds`
- `websense.oid`

To integrate the Websense Event Publisher with RiskManager:

1. Import the BAROC file.

   The BAROC file is installed once (per management region) on the system where the TEC Event Server resides.

   a. Load the Tivoli environment variables (in the `setup_env.cmd` file) into your current environment.

   b. Copy the BAROC file into the RiskMgr class directory using the following path:

      ```
      IBM/RISKMRG/etc/baroc
      ```

      The operating system must be either **w32-ix86** (Windows 32) or one of the supported UNIX variants.

   c. Update the class list.

      Refer to your IBM Tivoli documentation for instructions.

   d. Open the file `<TIVOLI>/bin/<OS>/RISKMRG/corr/riskmgr_baroc.lst` and add an entry for `websense_riskmgr.baroc` at the end of the file.

   e. Save the file.

   f. Update the RiskManager database with the following command:

      ```
      rmcorr_cfg -update
      ```

      To execute this command:

      - You must be at a bash shell prompt. In Windows, the bash shell is located in `<TIVOLI>/bin<OS>/tools`.

- Your current directory must be <TIVOLI>/bin<OS>/RISKMGR/corr.
- The environment variables defined in setup_env.cmd must be present in the current shell environment.

NOTE

The following error messages are normal and do not indicate a problem:

"Failed to delete websense_riskmgr.baroc from rulebase"

"ERROR::ECO:0001;0273 No matching rulesets found"

g. Verify the successful installation of the Websense classes with the following command:

wlscurrb [Outputs the name of the currently used RULEBASE]

wlsrbclass <RULEBASE> | grep Websense

To execute this command:

- You must be at a bash shell prompt. In Windows, the bash shell is located in <TIVOLI>/bin<OS>/tools.
- The environment variables defined in setup_env.cmd must be present in the current shell environment.

These commands will produce output similar to the following:

```
bash$ wlscurrb
The currently used rulel base was loaded
from the rule base named 'RM38RB'.

bash$ wlsrbclass RM38RB | grep Websense
WebsenseBaseEvent
WebsenseL0Event
WebsenseL1AddedEvent
WebsenseL1RemovedEvent
WebsenseL1ChangedEvent
```

2. Using a text editor, copy the contents of the `websense.oid` file and the `websense_riskmgr.cds` file and append them to the end of each of the following files:
   - `\Program Files\Tivoli\lcf\bin\w32-ix86\TME\TEC\adapters\etc\tecad_snmp.oid`
   - `\tecsnmp\etc\tecad_snmp.cds`
3. Distribute the files to the TECSNMP Adapter machine.

   The files must be distributed to the following path:

   ```
   \$TECSNMP\etc
   ```
4. Copy the `websense_riskmgr.baroc` file to the `/$TECSNMP/etc` folder and rename the file `tec_snmp.baroc`.
5. Install the FORMAT file.

   The FORMAT file (`.cds`) must be installed on every system where Websense Event Publisher is installed and reporting Websense events.

   a. Stop the Tivoli adapter.

      From the Windows services dialog box stop the TECWinadapter service.

      If the adapter has not been installed on this system, install the adapter by following the Tivoli installation instructions. These instructions will also have you specify the location of the centralized TEC Event server (*ServerLocation* and *ServerPort* in the adapter configuration file), which is the server on which the BAROC file was installed above.

   b. Copy the FORMAT file into the appropriate locale directory.

      For most installations the locale will be `C:\`, so the full path would be the following:

      ```
      C:\$TECADHOME\etc\<LOCALE>
      ```

   c. Change directory to the locale directory.

      ```
      cd $TECADHOME\etc\<LOCALE>
      ```

   d. Generate a new FORMAT file.

      Some installations may already be reporting events into Tivoli via the Windows NT Event Log. These sites will already have an existing FORMAT file to which the Websense Event Publisher specific information needs to be added.

Append the `websense_riskmgr.cds` file to the existing `.cds` files in the following paths:

- `\Program Files\Tivoli\Icf\bin\w32-ix86\TME\TEC\adapters\etc`
- `\$TECSNMP\etc\tecad`

e. Regenerate the class (.cds) file.

```
..\..\bin\win_gencds\tecad_snmp.cds
```

NOTE

Make sure you run this command in the following directory: `cd $TECADHOME\etc\<LOCALE>`.

It is normal to see some warning messages.

f. Update RiskManager Event Server and the TECSNMP Adapter configuration files.

g. Make any changes necessary to the Risk Manager configuration file.

For example, if the adapter is running on a Windows host with Websense, it may be necessary to adjust the parameters to aggregate and correlate the SNMP traps that the Tivoli SNMP adapter monitors.

Websense Event Publisher monitored by a Tivoli RiskManager Adapter could generate a large number of events that represent a set a very similar activity. To minimize event traffic with minimal loss of information, both the TEC SNMP adapter and the Tivoli Risk Manager Agent can summarize similar events.

h. Restart the adapter by starting the **TECWinadapter** service in the Windows services control panel.

APPENDIX A

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 Websense Enterprise 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 Enterprise 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 for Windows 2000 and 2003.

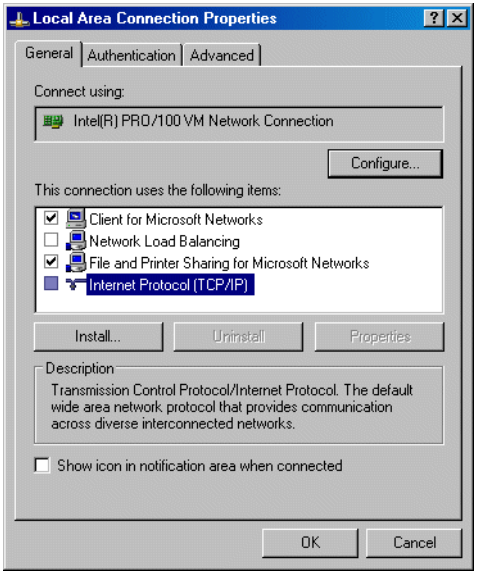
To configure a NIC for stealth mode:

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

The 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 and configuring the Squid Web Proxy that is not addressed in the previous chapters. This appendix troubleshoots installation and integration 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 Enterprise and your integration, refer to your Websense Enterprise *Administrator's Guide*.

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 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.
- 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.
- Some users are receiving the Websense Global policy.
- Websense Enterprise splash screen is displayed, but installer does not launch on Windows 2000.
- Outgoing Internet traffic seems slow.
- Network Agent cannot communicate with Filtering Service after it has been reinstalled.

I made a mistake during installation

Run the installation program again. Setup will detect the current installation and allow you to **Add**, **Remove**, or **Repair** Websense Enterprise 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 Setup again.

Refer to *Modifying an Installation*, page 102 for instructions.

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 2000 and 2003

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

Websense 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 Master Database downloads.

Subscription Key

Verify that the subscription key is entered correctly and has not expired. Open the **Settings** dialog box, and go to the **Database Download** screen.

- Compare the key you received via email or in the Websense Enterprise 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 Websense Enterprise is accessing the Internet through a proxy server by checking the **Database Download** screen of the **Settings** dialog box in Websense Enterprise Manager.
2. If a proxy server is being used, open a Web browser (either Internet Explorer or Netscape).
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 Websense Enterprise to access a DNS server.

If you need assistance, contact Websense Technical Support (see *Appendix C: Technical Support* for information).

5. If Websense 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 Enterprise 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 Setup 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 Enterprise on a different machine. See *System Requirements*, page 29 for minimum installation requirements.
- Stop all memory-intensive services running on the machine before attempting another Websense Enterprise installation.

Network Agent fails to start with stealth mode NIC

IP address removed from Linux configuration file

The 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 the 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>`), the 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 Enterprise 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 Linux and Solaris

Network interface cards configured for stealth mode in Linux and Solaris are displayed in the Websense Enterprise installer as choices for Websense communication. If you have inadvertently selected a stealth mode NIC for communications, the Network Agent will not start, and Websense Enterprise 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 the Websense Enterprise Manager. Without this address, the 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. Refer to *Identifying the Proxy Server for the Network Agent*, page 141 for instructions.

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.

Some users are receiving the Websense Global policy

A number of reasons exist as to 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, Websense cannot identify the user to apply the proper policy. Websense will then apply the Global policy 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 Enterprise 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, refer to your Windows operating system documentation for possible solutions. This is a network connectivity problem and not a Websense Enterprise 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 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, refer to the following Web site for assistance: http://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 Enterprise splash screen is displayed, but installer does not launch on Windows 2000

This is a software issue with the installation machine which prevents it from displaying the Java-based Websense installer interface. This problem also prevents the Websense Enterprise 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 the 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 Enterprise in the console mode.

To install Websense Enterprise in console mode:

1. Open the **launch.ini** file using any text editor.

   This file is located on the same level as **Setup.exe** in the folder where you unzipped your Websense Enterprise 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 on-screen instructions to install Websense Enterprise.

   NOTE

   The installation sequence for the console mode is identical to that of the GUI mode.
6. Install the Websense Manager on a Solaris machine or a Windows machine capable of displaying the Java interface.

Outgoing Internet traffic seems slow

If the performance of 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 Guide and check your network settings.

Network Agent cannot communicate with Filtering Service after it has been reinstalled

When the Filtering Service has been uninstalled and reinstalled, the Network Agent does not automatically update the internal identifier (UID) for the Filtering Service. After the new installation of the Filtering Service is complete, the Websense Enterprise Manager still attempts to query the Filtering Service using the old UID, which no longer exists.

To re-establish connection to the Filtering Service:

1. Open the Websense Enterprise 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 displays.
7. Select the IP address of the Filtering Service machine from the **Server IP Address** drop-down menu.
8. Click **Finish**.
9. Click **OK** in the Local Settings dialog box.
10. Click **OK** in the Settings dialog box to save the changes.

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.

Websense Technical Services Support Center

Technical information about Websense Enterprise is available 24 hours a day from:

http://www.websense.com/support

You will find here the latest release information, Frequently Asked Questions (FAQ), a Knowledge Base, product documentation, and other information.

Fee-based Support

The Websense 24x7 support contract is available for purchase. For a list of services, please visit our Web site at:

http://www.websense.com/support/24x7support.cfm

For additional information, please contact our Sales Department at **800.723.1166** or **858.320.8000**, or send an email to **sales@websense.com**.

Support Options

Websense Technical Support can be requested 24 hours a day.

Web Portal

You can submit support tickets through the Web Portal 24 hours a day. The response time during business hours is approximately 4 hours. Response to after-hours requests will occur the next business day. Support tickets can be submitted at: http://www.websense.com/support/form.

Email Questions

You may email your questions to us at the addresses listed below. Make sure you include your subscription key. This option is available 24 hours a day, 7 days a week. We will respond during business hours Monday through Friday.

- **support@websense.com**—San Diego, California, USA
- **japansupport@websense.com**—Japan (Asia)

> **NOTE**
> For technical support in the UK, submit support tickets through the Web Portal address. See *Web Portal*, page 177.

Email support can take 24 hours or more for a response. If you need a quicker turnaround, submit your issues through the Web Portal.

Telephone Assistance

Before you call a Websense Technical Support representative, please be ready with the following:

- Websense subscription key.
- Access to Websense Enterprise Manager.
- Access to the machine running the Filtering Service, the Websense Reporter server, and the database (MSDE or SQL) server.
- Permission to access the Websense log database.
- Familiarity with your network's architecture, or access to a person who has this familiarity.
- Specifications of the machines running the Filtering Service and Websense Enterprise Manager.
- A list of other applications running on the Filtering Service machine.

For severe problems, additional information may be needed.

Telephone assistance is available during normal business hours Monday through Friday at the following numbers:

- San Diego, California, USA: **858.458.2940**
- London, England: **+44 (0) 1932 796244**

Improving Documentation

Websense, Inc. understands the value of high quality, accurate documentation. If you have any suggestions for improving the documentation, contact us at **DocFeedback@websense.com**. We appreciate your input.

Index

E

F

G

H

I

L

M

N

P

Q

R

S

T

U